DAGSTUHL
REPORTS

Volume 2, Issue 10, October 2012

ISSN 2192-5283

Published online and open access by
Schloss Dagstuhl – Leibniz-Zentrum für Informatik GmbH, Dagstuhl Publishing, Saarbrücken/Wadern, Germany.
Online available at http://www.dagstuhl.de/dagrep

Publication date
February, 2013

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at `http://dnb.d-nb.de`.

Digital Object Identifier: 10.4230/DagRep.2.10.i

Aims and Scope
The periodical *Dagstuhl Reports* documents the program and the results of Dagstuhl Seminars and Dagstuhl Perspectives Workshops.
In principal, for each Dagstuhl Seminar or Dagstuhl Perspectives Workshop a report is published that contains the following:

- an executive summary of the seminar program and the fundamental results,
- an overview of the talks given during the seminar (summarized as talk abstracts), and
- summaries from working groups (if applicable).

This basic framework can be extended by suitable contributions that are related to the program of the seminar, e.g. summaries from panel discussions or open problem sessions.

Contact
Schloss Dagstuhl – Leibniz-Zentrum für Informatik
Dagstuhl Reports, Editorial Office
Oktavie-Allee, 66687 Wadern, Germany
reports@dagstuhl.de

www.dagstuhl.de/dagrep

Report from Dagstuhl Seminar 12401

Web Application Security

Edited by

Lieven Desmet[1], Martin Johns[2], Benjamin Livshits[3], and Andrei Sabelfeld[4]

1 **KU Leuven, BE,** Lieven.Desmet@cs.kuleuven.be
2 **SAP Research CEC – Karlsruhe, DE,** mj@martinjohns.com
3 **Microsoft Research – Redmond, US,** livshits@microsoft.com
4 **Chalmers UT – Göteborg, SE,** andrei@chalmers.se

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 12401 "Web Application Security". The seminar brought 44 web security researchers together, coming from companies and research institutions across Europe and the US.

The seminar had a well-filled program, with 3 keynotes, 28 research talks, and 15 5-minute talks. As web application security is a broad research domain, a diverse set of recent research results was presented during the talks, covering the web security vulnerability landscape, information-flow control, JavaScript formalization, JavaScript confinement, and infrastructure and server hardening. In addition to the plenary program, the seminar also featured three parallel break-out sessions on Cross-Site Scripting (XSS), JavaScript and Information-flow control.

Seminar 30. September – 05. October, 2012 – www.dagstuhl.de/12401
1998 ACM Subject Classification H.3.5 On-line Information Services – Web-based services, K.6.5 Security and Protection, D.4.6 Security and Protection
Keywords and phrases Web application security, JavaScript, Secure interaction, Information flow, Secure composition, Application security, Web 2.0
Digital Object Identifier 10.4230/DagRep.2.10.1

1 Executive Summary

Lieven Desmet
Martin Johns
Benjamin Livshits
Andrei Sabelfeld

The Dagstuhl seminar on *Web Application Security* aimed to bring researchers together in the field of web security, both from academia and industry. The seminar is a follow-up of the Dagstuhl Seminar 09141 on Web Application Security in 2009 [10, 9].

Research context

Since its birth in 1990, the web has evolved from a simple, stateless delivery mechanism for static hypertext documents to a fully-fledged run-time environment for distributed multi-party applications. Recently, the web technologies have gradually shifted from a central server technology towards a rich/stateful client paradigm and lively interaction models. The wave of popular peer-to-peer web applications and web mashup applications confirm this emerging trend. But the shift from the server-centered paradigm poses a significant

challenge of securing web applications in the presence of multiple stakeholders, including security-ignorant end-users. This motivates the need for solid *web application security*.

The seminar aimed to address the open question of how to protect against the pervasive threats to web applications. Some of the key objectives put forward are (i) over-viewing the state of the art to consolidate and structure it, (ii) identifying key challenges, and (iii) brainstorming on new ideas and approaches towards resolving these challenges.

The inception of this Dagstuhl seminar was strongly inspired by the following emerging trends and challenges in the web security landscape:

Fine-grained access control. Fine-grained access control policies define how the application authenticates and authorizes end users, from which application contexts the application can be consulted, and which interaction sequences maintain the application's integrity (i.e. control-flow integrity). Our objective was to address a range of questions from formal foundation of authentication policies and protocols to the practicalities of authentication such as secure session management.

Information-flow control. Information-flow control specifies how sensitive data, possibly originating from multiple content providers in multiple trust domains, can be used in data aggregations, and client-side and server-side processing as is typically done in mashups. Challenges here include reconciling information-flow policies from several involved parties, with possibly conflicting goals. Moreover, tracking end-to-end information flow in web applications remains an open question. Our objective was to establish an enhanced understanding of how to make information-flow control policies and mechanisms practical in a web setting.

Secure composition. Secure composition policies specify how active third-party components, for instance written in JavaScript, can be securely integrated into applications via client-side and server-side mashups. By nature, web mashups heavily depend on interaction and communication across different origins, but contradictory, mashup security relies on separation techniques for protecting both code and data. As a result, traditional HTML techniques (mainly based on the same-origin policies) fail to address both the interaction and separation needs. We wanted to explore principled approaches to achieve the delicate balance between interaction and separation in security composition.

Cross-domain interaction. One of the original and still unresolved problems of the web is the inherent incompatibility between the cross-domain nature of the hyperlink and the same-origin security policy of its active content. In the recent past the situation has become even more complex with the introduction of client-side primitives for cross-domain interaction, such as CORS. Our objective was to assess the impact of current developments and identify promising directions for solutions.

Recent advances in JavaScript and HTML5. There are several technological advances in the latest versions of JavaScript (such as strict mode, frozen objects, proxies and SES), that might contribute to the security of web applications. In addition, the research community did make important steps forward in understanding and improving the language by formalizing its semantics. At the same time, web specification (including HTML5 and CSP) are adding tons of new features as well as security measures as part of the browsing environment. Our objective was to have an enhanced understanding of the latest trends and research advances in JavaScript and HTML5 with respect to security.

Seminar program

The seminar attracted 44 participants, coming from companies and research institutions across Europe and the US. The group represented a nice mix of participants of academia and industry (including researchers of Siemens, SAP, Trend Micro, and Microsoft as well as two banks) and a good balance between junior and senior researchers.

The seminar had a well-filled program, with 3 keynotes, 28 research talks, 3 break-out sessions and 15 5-minute talks. The organizers aimed at keeping enough time during the breaks and in the evening for informal discussion. In addition, the participants went on a hike to the lake on Wednesday afternoon, as part of the social program.

Keynotes

The first three days, the floor was opened by keynotes to set the scene and inspire the discussions. The organizers invited the following three keynote speakers and the keynote abstracts can be found in section 3.

- Martin Johns (SAP Research – Karlsruhe, DE) – *Web Application Security: Are we there yet?*
- Shriram Krishnamurthi (Brown University – Providence, US) – *Browser Extension Analysis and Other JavaScript Adventures*
- John C. Mitchell (Stanford University, US) – *Science of Web Security and third-party tracking*

Martin Johns opened the Dagstuhl seminar on Monday by assessing the current state-of-practice in web security, 3 years after the previous Dagstuhl Seminar on Web application security. He sketched the evolving web landscape, and surveyed to what extend the results achieved so far suffice, and what is still missing. In particular, Martin gave a heads-up on client-side complexity and server-driven security, as being developed in the EU-FP7 project WebSand[1].

Shriram Krishnamurthi discusses techniques based on typing to verify web applications, and demonstrated how these techniques can also be used to verify browser extensions. Such a verification can for instance assure that no unsafe functions are called within an extension, while operating in *private browsing mode*. As part of the underlying toolkit, Shriram presented core semantics of JavaScript in λ_{JS} (lambdaJS), and showed how a JavaScript program can be desugared in λ_{JS} [30].

John C. Mitchell focused on the *science of security and principles*, and demonstrated this by means of relevant web security examples. He emphasized the importance of defining system models, adversary models as well as desired properties of system, and argued that is seems feasible to verify web security properties. An interesting research question to be answered by such a *scientific* approach would be "Does CSP prevent XSS?", and John challenged the audience to tackle this challenge. In addition, he discussed the importance of experimental studies and gave some highlights on recent research results on web tracking.

Research talks

The organizers invited all the participants to take the floor during the seminar, and encouraged the presenters to step away from typical conference presentations, but rather strive for

[1] EU-FP7 STREP WebSand, https://www.websand.eu/

interaction with the audience and engage discussions.

Web security is a broad research domain, and the seminar was able to attract web security researchers with various backgrounds. As a result, a diverse set of recent research results was presented during the seminar, and these can be grouped in 5 topical clusters:

1. Web security vulnerability landscape
2. Information-flow control
3. JavaScript formalization
4. JavaScript confinement
5. Infrastructure and server hardening

For each of the clusters, the list of talks is enumerated in this section. For more detailed information about each of the talks, we refer to the talk abstracts in section 4.

Cluster 1: Web security vulnerability landscape

This first cluster of talks discussed the evolving landscape of web vulnerabilities and presented some novel attack vectors. In addition, some of the talks gave some more insights in setting up large-scale security assessments.

- John Wilander gave us some fruitful insights in the banking domain by highlighting the security pains of an online bank.
- Boris Hemkemeier discussed the state-of-practice in authentication and authorization techniques used in online banks.
- Fabio Massacci illustrated with data from anti-virus vendors the mismatch between vulnerabilities studied by security researchers, and vulnerabilities exploited by bad guys in the wild.
- Nick Nikiforakis gave us insights on the risk of third-party scripts in web applications, based on a large-scale evaluation of remote script inclusions [52].
- Steven Van Acker gave us a view behind the scene in setting up large-scale web security experiments on the basis of the FlashOver research [65].
- Mario Heiderich discussed a novel set of scriptless injection attacks via Cascading Style Sheets (CSS), HTML, SVG and font files [34].

Cluster 2: Information-flow control

Secondly, a set of novel enforcement mechanisms have been presented for information-flow control for JavaScript, as well as quantitative information-flow policies.

- Frank Piessens presented FlowFox, a fully functional web browser that implements the Secure Multi-Execution (SME) technique on top of Firefox [21].
- Cormac Flanagan discussed the the Facets mechanism to simultaneously and efficiently simulate multiple executions for different security levels [3].
- Nataliia Bielova discussed an information-flow analysis technique to quantify leakage by browser fingerprinting.
- Daniel Hedin presented a dynamic type system that guarantees information-flow security for a core subset of JavaScript [33].
- Arnar Birgisson showed how to overcome the permissiveness limit for dynamic information-flow analysis by a novel use of testing [8].
- Michael Hicks introduced knowledge-based security for collaborative web applications [47].
- Martin Ochoa presented a quantification approach for cache side channels [41].

- Sebastian Schinzel discussed timing-based [59] and storage-based [27] side channel attacks for the web.

Cluster 3: JavaScript formalization

Thirdly, the research community did progress quite substantially in formalizing the semantics of JavaScript, in verifying JavaScript code, and using JavaScript as an assembly language.

- Shriram Krishnamurthi discussed how to verify browser extensions written in JavaScript.
- Ravi Chugh presented dependent types for a large subset of JavaScript [17].
- Nikhil Swamy presented recent work on $F*$, to generate JavaScript from cleaner semantics [26].
- Joe Gibbs Politz presented semantics for Getters, Setters and Eval in JavaScript [53].
- Arjun Guha presented a core calculus for scripting languages with support of Setters to avoid run-time errors.

Cluster 4: JavaScript confinement

Fourthly, several techniques have been presented to confine the execution of JavaScript code, and to detect attacks at run-time.

- Akhawe Devdatta presented a privilege separation approach for HTML5 applications, and applied the technique to browser extensions [2].
- Thorsten Holz and Mario Heiderich introduced IceShield, a JavaScript based tool that enables dynamic code analysis on websites, and JSAgents, a client-side framework to detect and mitigate live attacks against web pages and browsers, based on anomaly detection on the DOM.
- Lieven Desmet presented the JSand approach to sandbox third-party JavaScript within the existing browser infrastructure [1].
- Michael Franz proposed compiler-driven diversity to run diversified programs in parallel to detect attacks at run-time.

Cluster 5: Infrastructure and server hardening

Finally, a set of infrastructure and server hardening techniques has been proposed to increase the end-to-end security of the web applications.

- Cédric Fournet presented recent work towards the formal certification of the TLS protocol [6].
- Juraj Somorovsky presented a practical attack on XML Encryption, which allows to decrypt a ciphertext by sending related ciphertexts to a Web Service and evaluating the server response [38, 37].
- John Wilander did put forward some initial ideas to achieve a stateless anti-CSRF mechanism, while ensuring the same level of security.
- Bastian Braun presented server-side techniques to achieve Control-Flow Integrity in web applications [12].
- Sergio Maffeis formalized several configurations of the OAuth 2.0 protocol and verified these with ProVerif [4].

Break-out sessions

To complement the keynotes and the research talks, the organizers opted to have three parallel break-out sessions as part of the seminar program. The break-out sessions enabled participants to discuss selected topics in web security research in an informal setting and in smaller teams. The three topics of the break-out sessions were:

- Cross-Site Scripting (XSS)
- JavaScript
- Information-Flow

The main purpose of the break-out sessions was to informally discuss the most important state-of-the-art and research challenges. As part of the break-out sessions, the teams identified and enlisted in a bottom-up way the most relevant state-of-the-art work, as well as the set of main challenges and research directions for the specific web security research area The break-out sessions consisted of three slots of 70 minutes on Monday, Tuesday and Thursday. Participants joined the break-out sessions of their choice on Monday and Tuesday, and were encouraged to take part of two different sessions. The session on Thursday was used to report back the results of the three break-out sessions to the full group by means of a small presentation. The reports of the tree break-out sessions are summarized in section 5.

5-minute talks

Finally, to encourage participants to pitch new research ideas, or highlight some relevant results, we also had two sessions specifically targeted at **5-minute talks**. The list of speakers and their topics looks as follows:

- Thomas Jensen: Certified analysis of JavaScript
- Daniele Filaretti: JsCert
- Andrei Sabelfeld: GlassTube
- Devdatta Akhawe: Dusting The Web
- Michael Hicks: Build it, break it
- Sebastian Schinzel: Remote fingerprinting of programming libraries
- Joe Gibbs Politz: Finding bugs with type systems
- Céedric Fournet: ZQL: cryptographic compiler for data privacy
- Nikhil Swamy: TypeScript
- Boris Hemkemeier: Why to get rid of the SSL CA
- Valentin Dallmeier: WebMate – Exploring web 2.0 applications
- Mario Heiderich: JsAgents
- Joachim Posegga: Multi-party application platform
- Jorge Cuellar: Location privacy
- Egon Börger: Model web application frameworks

Conclusion

The Dagstuhl seminar on Web Application Security was a timely follow-up of the previous Dagstuhl seminar on this topic in 2009. The research domain has been maturing over the last five years, and new challenges have emerged such as the client-side complexity, the need of information-flow control enforcement, and hardening of JavaScript code.

The seminar brought 44 web security researchers together, coming from companies and research institutions across Europe and the US. The seminar had a well-filled program, with 3 keynotes, 28 research talks, and 15 5-minute talks. As web application security is a broad research domain, a diverse set of recent research results was presented during the talks, covering the web security vulnerability landscape, information-flow control, JavaScript formalization, JavaScript confinement, and infrastructure and server hardening.

In addition to the plenary program, the seminar also featured three parallel break-out sessions on Cross-Site Scripting (XSS), JavaScript and Information-flow control. The main goal of the break-out sessions was to informally discuss the most important state-of-the-art work, as well as to identify the main challenges and research directions for future research, as documented in this report.

Finally, the organizers of the Dagstuhl seminar have set up a *Special Issue on Web Application Security* as part of the *Journal of Computer Security*, specifically devoted to a selection of promising results presented at the seminar. Four participants have been invited to submit an extended paper of their talk to the special issue, and the manuscripts are currently under review.

2 Table of Contents

3 Keynote talks

3.1 Web Application Security: Are we there yet?

Martin Johns (SAP Research – Karlsruhe, DE)

More than twenty years after the invention of the Web, twelve years after the first public report of the XSS vulnerability class, approximately 7 years since the academic world become interested in the topic, and 3 years after the previous Dagstuhl Seminar on Web application security, this talk tries to assess the current state of Web security:

- How has the landscape of real-life Web application changed in the recent past?
- How does this affect our previously achieved security results?
- Are we addressing the whole picture?
- How far have we come and what is still missing?

In the context of the talk recent advances and challenges in the field of server-driven Web security will be shown and the problem of ever growing client-side complexity will be discussed.

3.2 Browser Extension Analysis and Other JavaScript Adventures

Shriram Krishnamurthi (Brown University – Providence, US)

Modern web browsers implement a *private browsing* mode that is intended to leave behind no traces of a user's browsing activity on their computer. This feature is in direct tension with support for *extensions*, which let users add third-party functionality into their browser. I will discuss the dimensions of this problem, present our approach to verifying extensions, and sketch our findings on several real, third-party extensions. I will then generalize this work to talk about other related problems, the toolkit we deploy to tackle them, and open issues for the community to consider.

3.3 Science of Web Security and third-party tracking

John C. Mitchell (Stanford University, US)

This talk focuses on the science of security and principles and examples relevant to web security. We have developed a scientific framework for security that is based on system models, adversary, and desired properties. In this approach, a system is secure if, for all actions of system users and system adversaries, the desired properties hold in spite of attack. Using this perspective, we propose a model of the web, three adversary models, and identify a set of security properties relevant to web security. This model supports automated analysis, which we have used to find and repair vulnerabilities in various mechanisms. With this

background, the second half of the talk presents an experimental web security study and some analysis of web privacy and third-party tracking. In the experimental study, we studied the result of approximately 20 web development teams and correlate security of their sites with features such as the programming language used, developed familiarity with security concepts, and whether the developers are freelancers or part of a startup team. Our web privacy study is based on a web measurement tool, called FourthParty, that uses an instrumented browser to capture events that occur with a site is visited and stores them in a SQL database. With this tool, we have identified sites and companies that violate their stated privacy policies or intentionally subvert privacy mechanisms.

4 Overview of Talks

4.1 Quantifying the Leakage of Browser Fingerprints by Quantitative Information Flow Analysis

Nataliia Bielova (INRIA – Rennes, FR)

Joint work of Bielova, Nataliia; Jensen, Thomas; Besson, Frederic

Web tracking technologies allow the websites to create profiles about its users, but at the same time the users' privacy is breached. Tracking technologies can be separated into stateful and stateless. The first type stores the unique identifier in the user browser, and the second one creates an identifier on the fly. From the legal side, EU ePrivacy directive restricts the usage of stateful technologies, but stateless technologies are left outside of the scope of this law. We address the problem of stateless tracking called fingerprinting. It is based on the properties of the web browser and the OS (a fingerprint) and uses this information to distinguish between the different users visiting the site. We propose a definition of quantified interference that tells how much information about a browser fingerprint a tracker can learn by observing the public outputs of the program. We then present ongoing work on two quantitative information flow analyses: purely dynamic and hybrid. Both techniques safely over-approximate the amount of the information leakage that an attacker could learn from the browser fingerprint. The hybrid analysis is more precise than the dynamic one. Compared to purely static, quantitative information flow analysis, our analyses can give a more precise number for a leaked information because we use the concrete values of the user's browser fingerprint instead of calculating the information entropy for all possible fingerprints.

4.2 Boosting the Permissiveness of Dynamic Information-Flow Tracking by Testing

Arnar Birgisson (Chalmers UT – Göteborg, SE)

Joint work of Birgisson, Arnar; Hedin, Daniel; Sabelfeld, Andrei
Main reference A. Birgisson, D. Hedin, A. Sabelfeld, "Boosting the Permissiveness of Dynamic Information-Flow Tracking by Testing," in Proc. of the European Symp. on Research in Computer Security (ESORICS 2012), Pisa, Italy, LNCS, Vol. 7459, Springer, 2012.
URL http://dx.doi.org/10.1007/978-3-642-33167-1_4

Tracking information flow in dynamic languages remains an open challenge. It might seem natural to address the challenge by runtime monitoring. However, there are well-known fundamental limits of dynamic flow-sensitive tracking of information flow, where paths *not* taken in a given execution contribute to information leaks. This paper shows how to overcome the permissiveness limit for dynamic analysis by a novel use of testing. We start with a program supervised by an information-flow monitor. The security of the execution is guaranteed by the monitor. Testing boosts the permissiveness of the monitor by discovering paths where the monitor raises security exceptions. Upon discovering a security error, the program is modified by injecting an annotation that prevents the same security exception on the next run of the program. The elegance of the approach is that it is sound no matter how much coverage is provided by the testing. Further, we show that when the mechanism has

discovered the necessary annotations, then we have an accuracy guarantee: the results of monitoring a program are at least as accurate as flow-sensitive static analysis. We illustrate our approach for a simple imperative language with records and exceptions. Our experiments with the QuickCheck tool indicate that random testing accurately discovers annotations for a collection of scenarios with rich information flows.

4.3 Control-Flow Integrity in Web Applications

Bastian Braun (Universität Passau, DE)

Joint work of Braun, Bastian; Gemein, Patrick; Reiser, Hans P.; Posegga, Joachim
Main reference B. Braun, P. Gemein, H.P. Reiser, J. Posegga, "Control-Flow Integrity in Web Applications," in Proc. of the Int'l Symp.on Engineering Secure Software and Systems (ESSoS 2013).

Modern web applications frequently implement complex control flows, which require the users to perform actions in a given order. Users interact with a web application by sending HTTP requests with parameters and in response receive web pages with hyperlinks that indicate the expected next actions. If a web application takes for granted that the user sends only those expected requests and parameters, malicious users can exploit this assumption by crafting unintended requests.

We analyze recent attacks on web applications with respect to user-defined requests and identify their root cause in the missing explicit control-flow definition and enforcement. Based on this result, we provide our approach, a control-flow monitor that is applicable to legacy as well as newly developed web applications. It expects a control-flow definition as input and provides guarantees to the web application concerning the sequence of incoming requests and carried parameters. It protects the web application against race condition exploits, a special case of control-flow integrity violation. Moreover, the control-flow monitor supports modern browser features like multi-tabbing and back button usage.

4.4 Dependent Types for JavaScript

Ravi Chugh (University of California – San Diego, US)

Joint work of Chugh, Ravi; Herman, David; Jhala, Ranjit
Main reference R. Chugh, D. Herman, R. Jhala, "Dependent types for JavaScript," in Proc. of the ACM Int'l Conf. on Object oriented Programming Systems Languages and Applications (OOPSLA '12), pp. 587–606. ACM, USA, 2012
URL http://dx.doi.org/10.1145/2384616.2384659

Static reason for JavaScript is hard. We describe recent progress towards building a statically typed dialect called Dependent JavaScript (DJS) that reasons about the mutable, prototype-based objects and arrays found in idiomatic JavaScript, and we show how to track security policies using DJS.

4.5 Contribute your Location Privacy Solution

Jorge Cuéllar (Siemens – München, DE)

After nine years of discussion, draft-ietf-geopriv-policy-27 is finally in RFC-EDITOR state. The result is that only quite trivial solutions have been standardized. But, on the other hand, a mechanisms has been created for adding algorithms, together with a context description of when they apply and a list of informal security properties (requirements) it has or implements. Suppose a user wants to share his location with a group of people, but not to be too precise about his location. The document defines an authorization policy language for controlling access to location information. This language can used by end-users in order to share their location with different friends, or other people, with chosen levels of uncertainty (say, "within 5km"). This may be seen as a declassification problem: What are good declassification functions (for different purposes)? There is no solution to all requirements, in all contexts. One solution could work well for moving in densely populated areas and provide good privacy properties (which ones?).

If you have a partial solution, submit your algorithms: we need them.

4.6 JSand: Server-driven Sandboxing of Third-party JavaScript

Lieven Desmet (KU Leuven, BE)

Joint work of Agten, Pieter; Van Acker, Steven; Brondsema, Yoran; Phung, Phu H.; Desmet, Lieven; Piessens, Frank
Main reference P. Agten, S. Van Acker, Y. Brondsema, P.H. Phung, L. Desmet, F. Piessens, "JSand: Complete client-side sandboxing of third-party JavaScript without browser modifications," Annual Computer Security Applications Conference (ACSAC 2012), Orlando, Florida, USA, 3–7 December 2012.
URL http://dx.doi.org/10.1145/2420950.2420952

The inclusion of third-party scripts in web pages is a common practice, but such script inclusions carry risks, as the included scripts operate with the privileges of the including website.

In this talk, I briefly present JSand, a server-driven but client-side JavaScript sandboxing framework. JSand requires no browser modifications: the sandboxing framework is implemented in JavaScript and is delivered to the browser by the websites that use it. Enforcement is done entirely at the client side.

Furthermore, I discuss some of the challenges and open problems to enforce security policies purely at the client side.

4.7 Privilege Separation for HTML5 Applications

Akhawe Devdatta (University of California – Berkeley, US)

Joint work of Devdatta, Akhawe; Saxena, Prateek; Song, Dawn
Main reference D. Akhawe, P. Saxena, D. Song, "Privilege separation in HTML5 applications," in Proc. of the 21st USENIX Security Symposium (Security'12). USENIX Association, Berkeley, CA, USA, 16 pp., 2012.
URL https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final168.pdf

The standard approach for privilege separation in web applications is to execute application components in different web origins. This limits the practicality of privilege separation since each web origin has financial and administrative cost. In this paper, we propose a new design for achieving effective privilege separation in HTML5 applications that shows how applications can cheaply create arbitrary number of components. Our approach utilizes standardized abstractions already implemented in modern browsers. We do not advocate any changes to the underlying browser or require learning new high-level languages, which contrasts prior approaches. We empirically show that we can retrofit our design to real-world HTML5 applications (browser extensions and rich client-side applications) and achieve reduction of 6x to 10000x in TCB for our case studies. Our mechanism requires less than 13 lines of application-specific code changes and considerably improves auditability.

4.8 Towards Certified Verification for Web Programming

Daniele Filaretti (Imperial College London, GB)

A brief overview of the projects I've been working on during the first year of my PhD at Imperial College London.

4.9 Multiple Facets for Dynamic Information Flow

Cormac Flanagan (University of California – Santa Cruz, US)

Joint work of Austin, Tom; Flanagan, Cormac
Main reference T.H. Austin, C. Flanagan, "Multiple facets for dynamic information flow," in Proc. of the 39th annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL'12). pp. 165-178, ACM, USA, 2012.
URL http://dx.doi.org/10.1145/2103621.2103677

JavaScript has become a central technology of the web, but it is also the source of many security problems, including cross-site scripting attacks and malicious advertising code. Central to these problems is the fact that code from untrusted sources runs with full privileges. We implement information flow controls in Firefox to help prevent violations of data confidentiality and integrity. Most previous information flow techniques have primarily re- lied on either static type systems, which are a poor fit for JavaScript, or on dynamic analyses that sometimes get stuck due to problematic implicit flows, even in situations where the target web application correctly satisfies the desired security policy. We introduce faceted

values, a new mechanism for providing information flow security in a dynamic manner that overcomes these limitations. Taking inspiration from secure multi-execution, we use faceted values to simultaneously and efficiently simulate multiple executions for different security levels, thus providing non-interference with minimal overhead, and without the reliance on the stuck executions of prior dynamic approaches.

4.10 Software Immunity via Large-Scale Diversification

Michael Franz (Univ. California – Irvine, US)

We have been investigating compiler-generated software diversity as a defense mechanism against software attacks. Imagine an "App Store" containing a diversification engine (a *multicompiler*) that automatically generates a unique version of every program for every user. All the different versions of the same program behave in exactly the same way from the perspective of the end-user, but they implement their functionality in subtly different ways. As a result, any specific attack will succeed only on a small fraction of targets. An attacker would require a large number of different attacks and would have no way of knowing a priori which specific attack will succeed on which specific target. Equally importantly, this approach makes it much more difficult for an attacker to generate attack vectors by way of reverse engineering of security patches. We have built such a multicompiler which is now available as a prototype. We can diversify large software distributions such as the Chromium web browser or a complete Linux distribution. In this talk, I present some preliminary benchmarks and also address some practical issues such as the problem of reporting errors when every binary is unique, and updating of diversified software.

4.11 First Class Field Names

Arjun Guha (Cornell University – Ithaca, US)

Joint work of Politz, Joe Gibbs; Guha, Arjun; Krishnamurthi, Shriram
Main reference J. Gibbs Politz, A. Guha, S. Krishnamurthi, "Semantics and Types for Objects with First-Class Member Names."
URL http://www.cs.brown.edu/~sk/Publications/Papers/Published/pgk-sem-type-fc-member-name/

Objects in many programming languages are indexed by first-class strings, not just first-order names. We defineλ_{ob}^{S} "LambdaSOB", an object calculus for such languages. We then develop a type system for LambdaSOB that is built around string pattern types, which describe (possibly infinite) collections of members. We define subtyping over such types, extend them to handle inheritance, and discuss the relationship between the two. We enrich the type system to recognize tests for whether members are present, and briefly discuss exposed inheritance chains. The resulting language permits the ascription of meaningful types to programs that exploit first-class member names for object-relational mapping, sandboxing, dictionaries, ... We prove that well-typed programs never signal member-not-found errors, even when they use reflection and first-class member names. We briefly discuss the implementation of these types in a prototype type-checker for JavaScript

4.12 JSFlow/SnowFox – Implementation of a Dynamic Information Flow Monitor for JavaScript

Daniel Hedin (Chalmers UT – Göteborg, SE)

Joint work of Hedin, Daniel; Sabelfeld, Andrei; Birgisson, Arnar; Bello, Luciano
Main reference D. Hedin, A. Sabelfeld, "Information-Flow Security for a Core of JavaScript," in Proc. of the IEEE Computer Security Foundations Symposium, Harvard University, Cambridge MA, June 25–27, IEEE CCS Press, 2012.
URL http://www.cse.chalmers.se/~andrei/jsflow-csf12.pdf

Web applications and services are rapidly growing more sophisticated and feature rich. This is achieved by including script libraries from different sources; even a standard news paper includes tens of scripts, ranging from libraries for user statistics like Google Analytics, to libraries for ad-provision like DoubleClick, utility like jQuery, or functionality like Tynt. Due to inadequacies in script inclusion, scripts are typically included under full trust. This means that the scripts are able to access any information on the page, including any information the user types into various forms. This raises a number of security concerns. In particular how can we guarantee that the included scripts do no harvest the page for sensitive information? In "Information-Flow Security for a Core of JavaScript" we have previously suggested how to solve this problem using dynamic information flow tracking for a core of JavaScript. In this talk we present JSFlow, an implementation of an information flow monitor for full JavaScript based on non-strict part of Ecma-262 v5. We present an overview of the implementation and show how the monitor is able to stop insecure information flow in actual web pages by viewing them in Firefox using Snowfox, a Firefox extension that replaces the JavaScript engine of Firefox with JSFlow.

4.13 Scriptless Attacks: Stealing the Pie Without Touching the Sill

Mario Heiderich (Ruhr-Universität Bochum, DE)

Joint work of Heiderich, Mario; Niemietz, Marcus; Schuster, Felix; Holz, Thorsten; Schwenk, Jörg
Main reference M. Heiderich, M. Niemietz, F. Schuster, T. Holz, J. Schwenk, "Scriptless attacks: stealing the pie without touching the sill," in Proc. of the 2012 ACM Conf. on Computer and Communications Security (CCS '12), pp. 760-771, ACM, New York, NY, USA, 2012.
URL http://dx.doi.org/10.1145/2382196.2382276

Due to their high practical impact, Cross-Site Scripting (XSS) attacks have attracted a lot of attention from the security community members. In the same way, a plethora of more or less effective defense techniques have been proposed, addressing the causes and effects of XSS vulnerabilities. As a result, an adversary often can no longer inject or even execute arbitrary scripting code in several real-life scenarios.

In this talk, we examine the attack surface that remains after XSS and similar scripting attacks are supposedly mitigated by preventing an attacker from executing JavaScript code. We address the question of whether an attacker really needs JavaScript or similar functionality to perform attacks aiming for information theft. The surprising result is that an attacker can also abuse Cascading Style Sheets (CSS) in combination with other Web techniques like plain HTML, inactive SVG images or font files. Through several case studies, we introduce the so called scriptless attacks and demonstrate that an adversary might not need to execute code to preserve his ability to extract sensitive information from well protected websites. More

precisely, we show that an attacker can use seemingly benign features to build side channel attacks that measure and exfiltrate almost arbitrary data displayed on a given website.

We conclude this talk with a discussion of potential mitigation techniques against this class of attacks. In addition, we have implemented a browser patch that enables a website to make a vital determination as to being loaded in a detached view or pop-up window. This approach proves useful for prevention of certain types of attacks we here discuss.

4.14 JSAgents

Mario Heiderich (Ruhr-Universität Bochum, DE)

Joint work of Heiderich, Mario; Holz, Thorsten;

This presentation provides an overview on the current status of the JSAgents Project, carried out by the department NDS of the Ruhr-University Bochum. Among a small introductory section, outlines of the used technologies a demonstration is being presented, showing off the XSS mitigation capabilities of the chosen approach.

4.15 Toward decentralized collaborative webapps via knowledge-based security

Michael Hicks (University of Maryland – College Park, US)

Joint work of Hicks, Michael; Mardziel,Piotr; Magill, Stephen; Srivatsa, Mudhakar
Main reference P. Mardziel, S. Magill, M. Hicks, S. Srivatsa, "Dynamic Enforcement of Knowledge-Based Security Policies," in Proc. of 24th IEEE Computer Security Foundations Symposium (CSF), pp. 114 -128, 2011.
URL http://dx.doi.org/10.1109/CSF.2011.15

Cloud- and server-based services own your data. Facebook stores your personal information, likes, contacts, and posts. Other cloud-based services, like Google Drive, similarly store your data. You trust them to do the right thing, but privacy policies are often not in your interests, and are subject to sudden change. On the other hand, it is undeniable that cloud-based services facilitate collaboration because they are extremely easy to use.

We are interested in supporting services with the same ease of use, but with stronger technical guarantees of privacy. One line of work is to maintain your data on a separate, trusted storage server, which controls accesses by outside services, like Facebook. The idea is to maintain a personal information archive under your control. Outside parties can send queries to this archive, to request particular bits of information. Thus an important question is how to decide whether to answer a particular query. To do so, one must determine whether the answer (in combination with answers to previous queries) might reveal too much information, thus defeating the goal of storing data separately in the first place. In my talk, I will present our work on using Bayesian reasoning to assess how much a querier can learn from a particular query, and how to use that information as the foundation of a security policy.

4.16 IceShield: Detection and Mitigation of Malicious Websites with a Frozen DOM

Thorsten Holz (Ruhr-Universität Bochum, DE)

Joint work of Heiderich, Mario; Frosch, Tilman; Holz, Thorsten
Main reference M. Heiderich, T. Frosch, T. Holz, "Iceshield: Detection and mitigation of malicious websites with a frozen dom," in Recent Advances in Intrusion Detection, pp. 281–300. Springer Berlin/Heidelberg, 2011.
URL http://dx.doi.org/10.1007/978-3-642-23644-0_15

In this talk, we provide an overview of a recent project called IceShield and briefly introduce JSAgents, a follow-up project we started a few months ago. Due to its flexibility and dynamic character, JavaScript has become an important tool for attackers. The widespread scripting language often helps them to perform a broad variety of malicious activities, for example to initiate drive-by download exploits or to execute clickjacking attacks. Current defense mechanisms as well as reactive analysis and forensic approaches are often slow or complicated to set up and conduct since an attacker can use many different ways to obfuscate the code or make it hard to obtain a copy of the code in the first place.

In this talk, we introduce a novel approach to analyze this class of attacks by demonstrating how dynamic analysis of websites can be accomplished directly in the browser. We present IceShield, a JavaScript based tool that enables in-line dynamic code analysis as well as de-obfuscation, and a set of heuristics to detect attempts of attacking either a website or the user accessing its contents. Special care needs to be taken to implement the instrumentation in a robust and tamper resistant way since an attacker should not be able to bypass our detection process. We show how features of ECMA Script 5 can be used to freeze object properties, so they cannot be modified during runtime. We implemented a prototype version of IceShield and demonstrate that it detects malicious websites with a small overhead even on devices with limited computing power such as smartphones. Furthermore, IceShield can mitigate detected attacks by changing suspicious elements, so they do not cause harm anymore, thus actually protecting users from such attacks.

4.17 Discovering Concrete Attacks on Website Authorization by Formal Analysis

Sergio Maffeis (Imperial College London, GB)

Joint work of Chetan, Bansal; Bhargavan, Karthikeyan; Maffeis, Sergio
Main reference C. Bansal, K. Bhargavan, S. Maffeis, "Discovering concrete attacks on website authorization by formal analysis," in Proc. of 25th IEEE Computer Security Foundations Symposium (CSF), pp. 247–262. IEEE, 2012.
URL http://dx.doi.org/10.1109/CSF.2012.27

Social sign-on and social sharing are becoming an ever more popular feature of web applications. This success is largely due to the APIs and support offered by prominent social networks, such as Facebook, Twitter, and Google, on the basis of new open standards such as the OAuth 2.0 authorization protocol. A formal analysis of these protocols must account for malicious websites and common web application vulnerabilities, such as cross-site request forgery and open redirectors. We model several configurations of the OAuth 2.0 protocol

in the applied pi-calculus and verify them using ProVerif. Our models rely on WebSpi, a new library for modeling web applications and web-based attackers that is designed to help discover concrete website attacks. Our approach is validated by finding dozens of previously unknown vulnerabilities in popular websites such as Yahoo and WordPress, when they connect to social networks such as Twitter and Facebook.

4.18 My software has a vulnerability should i worry?

Fabio Massacci (University of Trento – Povo, IT)

Joint work of Massacci, Fabio; Allodi, Luca

In this talk I show that the work of 90% of security researchers (including many people of the audience) to find vulnerabilities or protect against them is utterly useless. The bad guys are exploiting in the wild only a tiny tiny fraction of them.

4.19 You Are What You Include: Large-scale Evaluation of Remote JavaScript Inclusions

Nick Nikiforakis (KU Leuven, BE)

Joint work of Nikiforakis, Nick; Invernizzi, Luca; Kapravelos, Alexandros; Van Acker, Steven; Joosen, Wouter; Kruegel, Christopher; Piessens, Frank; Vigna, Giovanni
Main reference N. Nikiforakis, L. Invernizzi, A. Kapravelos, S. Van Acker, W. Joosen, C. Kruegel, F. Piessens, G. Vigna, "You are what you include: large-scale evaluation of remote javascript inclusions," in Proc. of the 2012 ACM Conference on Computer and Communications Security (CCS'12), pp. 736–747, 2012.
URL http://dx.doi.org/10.1145/2382196.2382274

An important and widely used feature of JavaScript, is the ability to combine multiple libraries from local and remote sources into the same page, under the same namespace. While this enables the creation of more advanced web applications, it also allows for a malicious JavaScript provider to steal data from other scripts and from the page itself. Today, when developers include remote JavaScript libraries, they trust that the remote providers will not abuse the power bestowed upon them.

In this presentation, we report on a large-scale crawl of more than three million pages of the top 10,000 Alexa sites, and identify the trust relationships of these sites with their library providers. We show the evolution of JavaScript inclusions over time and develop a set of metrics in order to assess the maintenance-quality of each JavaScript provider, showing that in some cases, top Internet sites trust remote providers that could be successfully compromised by determined attackers and subsequently serve malicious JavaScript. In this process, we identify four, previously unknown, types of vulnerabilities that attackers could use to attack popular web sites. Lastly, we review some proposed ways of protecting a web application from malicious remote scripts and show that some of them may not be as effective as previously thought.

4.20 Automatic Quantification of CPU Cache Side-channels

Martin Ochoa (Siemens – München, DE)

Joint work of Köpf, Boris; Mauborgne, Laurent; Ochoa, Martin
Main reference B. Köpf, L. Mauborgne, M. Ochoa, "Automatic quantification of cache side-channels," in Proc. of the 24th Int'l Conf. on Computer Aided Verification (CAV'12), pp. 564–580, Springer-Verlag, 2012.
URL http://dx.doi.org/10.1007/978-3-642-31424-7_40

The latency gap between caches and main memory has been successfully exploited for recovering sensitive input to programs, such as cryptographic keys from implementations of AES and RSA in SSL. So far, there are no practical general-purpose countermeasures against this threat. In this talk we describe a novel method for automatically deriving upper bounds on the amount of information about the input that an adversary can extract from a program by observing the CPU's cache behavior. At the heart of our approach is a novel technique for efficient counting of concretizations of abstract cache states that enables us to connect state-of-the-art techniques for static cache analysis and quantitative information-flow. We implement our counting procedure on top of the AbsInt TimingExplorer, one of the most advanced engines for static cache analysis. We use our tool to perform a case study where we derive upper bounds on the cache leakage of a 128-bit AES executable on an ARM processor with a realistic cache configuration. We also analyze this implementation with a commonly suggested (but until now heuristic) countermeasure applied, obtaining a formal account of the corresponding increase in security.

4.21 FlowFox: an experiment on bringing information flow control to the browser

Frank Piessens (KU Leuven, BE)

Joint work of De Groef, Willem; Devriese, Dominique; Nikiforakis, Nick; Piessens, Frank
Main reference W. De Groef, D. Devriese, N. Nikiforakis, F. Piessens, "FlowFox: a web browser with flexible and precise information flow control," in Proc. of the 2012 ACM Conference on Computer and Communications Security (CCS '12), pp. 748–759, ACM, 2012.
URL http://dx.doi.org/10.1145/2382196.2382275

FlowFox is a fully functional web browser that implements information flow control for scripts using secure multi-execution. I will briefly sketch FlowFox's architecture, and briefly report on our experiences with the browser. The main focus of the talk will be on some of the issues that remain unsolved. In particular, I will discuss how the way in which FlowFox specifies and enforces policies may break some of the theoretical properties of secure multi-execution. I will also propose a number of approaches to deal with these issues and hope to get feedback from the audience on which of these approaches makes most sense.

4.22 A Tested Semantics for Getters, Setters, and Eval in JavaScript

Joe Gibbs Politz (Brown University – Providence, US)

Joint work of Politz, Joe Gibbs; Carroll, Matthew J; Lerner, Benjamin S; Pombrio, Justin; Krishnamurthi, Shriram
Main reference J. Gibbs Politz, M.J. Carroll, B.S. Lerner, J. Pombrio, S. Krishnamurthi, "A tested semantics for getters, setters, and eval in JavaScript," in Proc. of the 8th Symp. on Dynamic languages (DLS '12), pp. 1–16, ACM, 2012.
URL http://dx.doi.org/10.1145/2384577.2384579

We present S5, a semantics for the strict mode of the ECMAScript5.1 (JavaScript) programming language. S5 shrinks the large source language into a manageable core through an implemented transformation. The resulting specification has been tested against real-world conformance suites for the language. This paper focuses on two aspects of S5: accessors (getters and setters) and eval. Since these features are complex and subtle in JavaScript, they warrant special study. Variations on both features are found in several other programming languages, so their study is likely to have broad applicability.

4.23 Progressive Types

Joe Gibbs Politz (Brown University – Providence, US)

Joint work of Politz, Joe Gibbs; Quay-de la Vallee, Hannah; Krishnamurthi, Shriram
Main reference J. Gibbs Politz, H. Quay-de la Vallee, S. Krishnamurthi, "Progressive types," in Proc. of the ACM Int'l Symp. on New ideas, new paradigms, and reflections on programming and software (Onward! '12), pp. 55-66, ACM, 2012.
URL http://dx.doi.org/10.1145/2384592.2384599

As modern type systems grow ever-richer, it can become increasingly onerous for programmers to satisfy them. However, some programs may not require the full power of the type system, while others may wish to obtain these rich guarantees incrementally. In particular, programmers may be willing to exploit the safety checks of the underlying run-time system as a substitute for some static guarantees. Progressive types give programmers this freedom, thus creating a gentler and more flexible environment for using powerful type checkers. In this paper we discuss the idea, motivate it with concrete, real-world scenarios, then show the development of a simple progressive type system and present its(progressive) soundness theorem.

4.24 GlassTube: A Lightweight Approach to Web Application Integrity

Andrei Sabelfeld (Chalmers UT – Göteborg, SE)

Joint work of Hallgren, Per; Mauritzson, Daniel; Sabelfeld, Andrei

The HTTP and HTTPS protocols are the main corner stones of the modern web. From a security point of view, they offer an all-or-nothing choice to web applications: either no security guarantees with HTTP or both confidentiality and integrity with HTTPS. However,

in many scenarios confidentiality is not necessary and even undesired, while integrity is essential to prevent attackers from compromising the data stream. We propose GlassTube, a lightweight approach to web application integrity. GlassTube guarantees integrity at application level, without resorting to the heavyweight HTTPS protocol. GlassTube provides a general method for integrity in web applications and smartphone apps. GlassTube is easily deployed in the form of a library on the server side, and offers flexible deployment options on the client side: from dynamic code distribution, which requires no modification of the browser, to browser plugin and smartphone app, which allow smooth key predistribution. The results of a case study with a web-based chat indicate a boost in the performance compared to HTTPS, achieved with no optimization efforts.

4.25 Side channel attacks on the web

Sebastian Schinzel (Universität Erlangen-Nürnberg, DE)

Joint work of Schinzel, Sebastian; Freiling, Felix
Main reference F. Freiling, S. Schinzel, "Detecting hidden storage side channel vulnerabilities in networked applications," Future Challenges in Security and Privacy for Academia and Industry (2011), pp. 41–55.
URL http://dx.doi.org/10.1007/978-3-642-21424-0_4

Side channels are vulnerabilities that can be attacked by observing the behavior of applications and by inferring sensitive information just from this behavior. Storage side channels are a new type of side channels which leak information through redundancies in protocols such as HTTP or languages such as HTML. We implement a detection method and test it by applying it to real- world web applications and we find that several widely used web applications are prone this type of attack.

Because side channel vulnerabilities appear in such a large spectrum of contexts, there does not seem to be a generic way to prevent all side channel attacks once and for all. A practical approach is to research for new side channels and to specifically tailor mitigations for new side channel attacks. We present a new method to mitigate timing side channels in web applications. The method works by padding the response time using a deterministic and unpredictable delay (DUD). We show that DUD offers security guarantees that can be freely traded with performance reduction. By applying this method to vulnerable web applications, we show that the method offers an effective and performance efficient way to mitigate timing side channels.

4.26 How To Break XML Encryption

Juraj Somorovsky (Ruhr-Universität Bochum, DE)

Joint work of Jager, Tibor; Somorovsky, Juraj
Main reference T. Jager, J. Somorovsky, "How to break XML encryption," in Proc. of the 18th ACM Conf. on Computer and Communications Security (CCS '11), pp. 413–422, ACM, 2011.
URL http://dx.doi.org/10.1145/2046707.2046756

XML Encryption was standardized by W3C in 2002, and is implemented in XML frameworks of major commercial and open-source organizations like Apache, redhat, IBM, and Microsoft.

It is employed in a large number of major web-based applications, ranging from business communications, e-commerce, and financial services over healthcare applications to governmental and military infrastructures. Our work describes several adaptive chosen-ciphertext attacks against PKCS#1 v1.5 and AES-CBC in XML Encryption. In case of PKCS#1 v1.5, the attacker could recover the secret key used for symmetric encryption by issuing a few millions of messages. In case of AES-CBC, the attacker needs to issue about 14 requests to recover one message byte directly. In a sense, our work applies the attacks of Bleichenbacher (Crypto 1998) and Vaudenay (Eurocrypt 2002) on XML Encryption by exploiting various XML specific side-channels. It shows how complicated it could be to mitigate these attacks and thus motivates for usage of secure cryptographic primitives.

This work is of a particular importance as similar side-channels could arise by implementing different specifications such as JSON Web Encryption or Web Cryptographic API.

4.27 Verifying JavaScript programs with the Dijkstra State Monad

Nikhil Swamy (Microsoft – Redmond, US)

Joint work of Swamy, Nikhil; Weinberger, Joel; Schlesinger, Cole; Chen, Juan; Livshits, Benjamin

Several special-purpose systems have been proposed to analyze programs in JavaScript and other dynamically typed languages. However, none of these prior systems support automated, modular verification for both higher-order and stateful features.

This paper proposes a new refinement of the state monad, the Dijkstra state monad, as a way of structuring specifications for higher-order, stateful programs. Relying on a type inference algorithm for the Dijkstra monad, we obtain higher-order verification conditions (VCs) for programs that use a dynamically typed higher-order store. Via a novel encoding, we show that these higher-order VCs can be discharged by an off-the-shelf automated SMT solver. We put the Dijkstra monad to use by building a tool chain to verify JavaScript programs. Our tool chain begins by translating JavaScript programs to F*, a dependently typed dialect of ML. Within F*, we define a library for dynamic typing idioms based on the Dijkstra monad. We then infer and solve precise verification conditions for translated JavaScript clients of this library. We report on our experience using this tool chain to verify a collection of web browser extensions for the absence of JavaScript runtime errors. Despite some limitations of our work (e.g., we do not model asynchrony), we conclude that the Dijkstra monadic approach is a promising and powerful way to structure the verification of JavaScript programs within a general purpose dependently typed programming language.

4.28 Fully Abstract Compilation to JavaScript

Nikhil Swamy (Microsoft – Redmond, US)

Joint work of Fournet, Cedric; Swamy, Nikhil; Chen, Juan; Dagand, Pierre-Evariste; Strub, Pierre-Yves; Livshits, Benjamin

Many tools allow programmers to develop applications in high-level languages and deploy them in web browsers via compilation to JavaScript. While practical and widely used, these

compilers are ad hoc. No guarantee is provided on their correctness for whole programs, nor their security for programs executed within arbitrary JavaScript contexts.

In this paper, we present a compiler with such positive guarantees. We compile an ML-like language with higher-order functions and references down to JavaScript, while preserving all source program properties. We evaluate our compiler on sample programs, including a series of secure libraries. We illustrate the dangers of JavaScript contexts with a series of attacks against naive scripts. We then give a semantics to JavaScript by translation to F*, a variant of ML with richer types. Based on lambdaJS, this semantics reflects the main elements of the EcmaScript 5 standard, as well as our experimental findings on dangerous features in JavaScript implementations (implicit coercions, getters and setters, and special arguments, caller, and callee properties). We present our compilation scheme, expressed as a type-preserving translation between fragments of F*: each source type is mapped to 'dyn', the type of Javascript values, refined with a logical specification of its compiled representation. For whole programs, we show that the translation is a forward simulation. For programs executed in untrusted Javascript contexts, we wrap our translation with defensive filters to import and export values while preserving the translation invariant. Relying on type-based invariants and a new notion of applicative bisimilarity, we show full abstraction: two programs are equivalent in all source contexts if and only if their wrapped translations are equivalent in all Javascript contexts. Thus, programmers can produce JavaScript and still rely on static scopes and types for reasoning about their programs.

4.29 behind FlashOver: Automated Discovery of Cross-site Scripting Vulnerabilities in Rich Internet Applications

Steven Van Acker (KU Leuven, BE)

Joint work of Van Acker, Steven; Nikiforakis, Nick; Desmet, Lieven; Joosen, Wouter; Piessens, Frank
Main reference S. Van Acker, N. Nikiforakis, L. Desmet, W. Joosen, F. Piessens, "FlashOver: Automated discovery of cross-site scripting vulnerabilities in rich internet applications," AsiaCCS, Seoul, 2-4 May 2012.

FlashOver is a system to automatically scan Rich Internet Applications for XSS vulnerabilities by using a combination of static and dynamic code analysis that reports no false positives. It was used in a large-scale experiment to analyze Flash applications found on the top 1,000 Internet sites, exposing XSS vulnerabilities that could compromise 64 of those sites, of which six are in the top 50. In this talk, we will focus on some open-ended questions that surfaced while we were performing our FlashOver experiment.

4.30 The Security Pains of an Online Bank

John Wilander (Hägersten, SE)

Online banking is often used as a primary example of why we need web application security. This talk presents the security challenges from the inside. Session stickiness, session termination, complexity of deploying new countermeasures, and handing of a large legacy web application.

4.31 Stateless CSRF Protection

John Wilander (Hägersten, SE)

CSRF protections most often involve server-side state which makes it hard to convince developers to use them, especially for RESTful services. The so called double submit CSRF protection can be made stateless but then becomes susceptible to subdomain XSS bypass. The current suggestion for stateless anti- CSRF is a triple submit with only a subdomain XSS cookie overflow as known attack vector. This talk will explain the issue and open up for discussion.

5 Break-out sessions

5.1 Break-out session: Cross-Site Scripting (XSS)

This break-out session focused on the problem of Cross-Site Scripting (XSS). In particular, the participants of this break-out session enlisted mitigation techniques used in practice, compiled a survey of recent research activities and open problems in this domain, and did put forward a first step towards a candidate definition of Cross-Site Scripting.

Cross-Site Scripting is a broad category of HTML/JavaScript injection vulnerabilities, typically categorized in three types. The first type of XSS vulnerabilities (XSS-0) is called DOM-based XSS, and operates purely on the client-side. The second (XSS-1) and third type (XSS-2) inject HTML/JavaScript via the server-side, either in a reflected or persistent manner.

The **most common mitigation strategies** for XSS rely on identifying injection attacks and rendering them harmless in the browser environment. For instance, most modern browsers are equipped with XSS filters [5, 54, 46], and support the Content Security Policy (CSP) [61]. Alternatively, untrusted page fragments and scripts can be sandboxed [35], or can be sanitized by browser libraries such as the *toStaticHTML* method in Internet Explorer [13].

Apart from browser mechanisms, other strategies to detect and protect against XSS are the use of automatic sanitization libraries such as HTML Purifier [67], subject the web application to pentesting and static analysis (e.g. [60, 25]), and the use of confined environments such as the Secure ECMAScript library [50] and JavaScript sandboxing approaches [62, 48, 64, 1, 36].

Recent research on XSS includes the automatic context-sensitive sanitization of web content [56, 58, 31], the automated analysis of widgets and applications [57, 29] and novel XSS attacks beyond the classical pattern of HTML and JavaScript injection [34].

In [56], Samuel *et al* propose a type-qualifier mechanism that can be applied onto existing web templating frameworks to achieve context-sensitive sanitization. ScriptGuard [58] focuses on the incorrect use of sanitization libraries (such as context-mismatched sanitization and inconsistent multiple sanitizations) and is capable of detecting and repairing incorrect placement of sanitizers.

In [57], Saxena *et al* propose the tool Kudzu, based on symbolic execution of JavaScript, to discover in a automated way client-side injection vulnerabilities. Gatekeeper [29] allows site administrators to express and enforce security and reliability policies for JavaScript programs, and was successfully applied to automatically analyze JavaScript widgets, with very few false positives and no false negatives.

Finally, Heiderich *et al* demonstrated that a new set of XSS attacks are feasible that do not rely JavaScript, but operate solely on HTML, Cascading Style Sheets (CSS), SVG images and font files [34].

The participants of this break-out session also tried to formulate an accurate and acceptable **definition of Cross-Site Scripting (XSS)**. There was a lot of discussion between the participants, and the candidate definition of XSS stranded on "An XSS attack occurs when a script from an untrusted source is executed in rendering a page" without reaching unanimity. Some of the comments/critics that were mentioned during the break-out session, as well as during the presentation afterwards for the full group, include:

- XSS can be both a client-side and server-side problem. The phrasing "rendering a page" sounds more like client-side only?
- If the unintended or unwanted execution of JavaScript happens via a trusted third party, can it still be called XSS?

- The interpreter is tricked into executing code. Stems from the mix of data and code.
- Unauthorized execution of JavaScript, escalation of privilege.
- XSS used to be about scripting between frames/pages and mostly type 1 (reflected). Has XSS become an umbrella?
- Violate the control flow integrity of the JavaScript program (assuming there is one).
- A script may arise from a dynamic process influenced by more than one source. Therefore the "source of a script" is not always well-defined.
- The untrusted source reflects the trust policy of the site. In principle, this may only exist in the mind of the designer. Or perhaps more accurately, the designer may not know the policy. The attack is relative to the policy.
- Is the source well-defined? Is it better to use principle than source? Maybe. Maybe not.

To conclude, the participants drafted a set of **open research questions related to XSS**, to inspire and guide junior researchers in this research domain.

- Precise definition of XSS
- Does CSP prevent XSS? Does CSP work, in an precise sense?
- Are the CSP policies expressive enough to prevent XSS?
- Is it feasible to apply CSP to new sites? What about securing legacy sites?
- How effective is the state of the art for securing new sites and legacy sites? Can we get XSS prevention to a situation similar to SQL injection?
- Is there an approach towards preventing XSS that is compatible with the complexity of modern web advertisements?

We would like to thank John Wilander for taking notes during this break-out session, and presenting the break-out results to the full group.

5.2 Break-out session: JavaScript

This break-out session focused on the JavaScript language. In particular, the participants of this break-out session enlisted recent achievements in the JavaScript language research, discussed the semantic notion of properties and policies, compiled a survey of recent enforcement techniques, and did put forward a first step towards future directions.

First, the participants gave an overview of the **recent achievements** in the domain of understanding and securing the JavaScript language.

With respect to **formalizing the language semantics**, several lines of work can be identified. Maffeis *et al.* have defined an operational semantic [44] for Javascript and a program logic [28]. Alternatively, a small-step operational semantics for a core set of the language has been proposed [30], as well as a desugaring process that turns JavaScript programs into the core language.

The participants of the break-out stated that the hard, remaining bits of work are in formalizing the error model of JavaScript, the thread model (i.e. the asynchronicity), and the DOM/API.

Also quite some work has been invested in defining **safe subsets of JavaScript**, such as FaceBook JS (FBJS) [63] and AdSafe [20]. Also important here is to mention *strict mode*, introduced in the latest specifications of JavaScript. This mode allows an opt-in to a restricted variant of JavaScript, which eliminates some of the typical JavaScript pitfalls.

The participants of the break-out stated that the hard, remaining bits of work are in stating safety properties, as well as ensuring and using them.

Another emerging trend is the use of **JavaScript as an assembly language**. A well-know example of this is the Google Web Toolkit (GWT), in which the compiler transforms the client-side program (written in Java) into JavaScript. Similarly, the multi-tier language Swift [15] uses JIF as source language, and applies GWT to transform the client-side code to JavaScript. Other practical examples of using JavaScript as an assembly language include CoffeeScript, Dart and TypeScript.

The participants of the break-out stated that the hard, remaining bits of work are to securely isolate compiled JS from *raw* potentially untrusted JavaScript, as well as the safe interaction and cohabitation of JavaScript from multiple sources (Mashic [43], JSand [1]).

An interesting discussion during this break-out session was the **semantic difference between security properties and security policies**. As a conclusion of the discussion, we agreed that properties describe what you want for your system, namely the end-to-end characteristics. An example security property could for instance be the separation of duties. Policies, in contrast, describe how to ensure the security properties.

In the context of security policies become more and more complex to express, an opportunity was raised to converge towards policy templates.

The participants compiled a survey of the various **enforcement techniques** to secure JavaScript. There is a broad domain, and during the discussion the enforcement techniques were categorized in three categories:

Static enforcement techniques In the domain of static enforcement, a first set of techniques (such as AdJail [62], Treehouse [36] and JSand [1]) realizes the enforcement by construction. A second set of techniques uses verification: symbolic execution, static verification [29], types or separation logic [28].

Dynamic enforcement techniques (within the language) The dynamic enforcement typically happens with wrappers. Interesting to mention here is the work on CAJA [49] en AdSafe [20].

Dynamic enforcement techniques (below the language) Enforcement is also possible in the underlying infrastructure, and can happen via proxies or in the browser.

This break-out session ended with summing up some interesting thoughts and possible directions for future research.

- We noticed a transition of JavaScript towards the desktop (Windows 8/Metro), and towards the server (Node.js)
- JavaScript security is hard: Everything is dynamic . . . Everything is mutable . . . Everything leaks . . . Everything . . .
- We have made quite some progress with JavaScript, it is time to rise above JavaScript
- You can break the web if you give something in return...
- We need to identify good programming guidelines

We would like to thank Ranjit Jhala for taking notes during this break-out session, and presenting the break-out results to the full group.

5.3 Break-out session: Information-Flow

This break-out session focused on information-flow control. In particular, the participants of this break-out session highlighted the importance of information-flow control in modern web application scenarios, and compiled a survey of recent research activities and open problems in this domain.

Information-flow control started in the mid seventies with research on multi-level security operating systems [23], and experienced a revival of interest in the nineties with the rise of mobile code. Recently, the research domain has become fully active thanks to emerging challenges in the web application context, in which code from multiple stakeholders coexists in web mashups [22] or via the integration of third-party JavaScript code [52].

Access control is often used to enforce safety properties in software systems, by controlling access to sensitive resources or APIs at run-time. Examples in the web context are the declarative access control in JEE containers, programmatic access control as part of the application itself, and access control mechanisms in the browser environment such as the Same-Origin Policy [55]. More recently, capability-based security achieves access control guarantees without the need of run-time checks. In the mashup context for instance, JavaScript components can be sandboxed in language subsets such as CAJA [49] and AdSafe [20].

Access control is often easy to implement, and a number of sandboxing techniques are available for JavaScript [50, 62, 48, 64, 1, 36]. However, sometimes it is also **necessary to track what happens to the information once it is accessed**. Some of the interesting web scenario's discussed in this context during this DagStuhl seminar include Google Analytics, Google Maps, a loan calculator, and Tynt.

In order to achieve confidentiality of the data, beyond the point of access, information-flow control does not rely on a a single *secure state* or *secure trace* of the program, but needs to take into account all possible traces and their relation (e.g. to detect implicit flows in the application).

Recent research on information-flow control includes dynamic information-flow enforcement and hybrid analysis techniques for both the client-side as the server-side, and novel security policies.

In recent information-flow control research for JavaScript, there has been a significant thrust on **dynamic information-flow enforcement** [21, 3, 33]. For example, FlowFox [21] is a fully functional web browser that implements the Secure Multi-Execution (SME) [24] technique for information-flow control on top of Firefox. Similarly, the Facets mechanism [3], inspired by SME, uses *facet values* to simultaneously and efficiently simulate multiple executions for different security levels. Finally, JsFlow [33] applies a dynamic type system to a core of JavaScript to prohibit information leaks from the program's secret sources to the program's public sinks. A more complete survey of these techniques can be found in [7].

Several researchers have proposed **static and hybrid analysis** techniques to achieve a more efficient information-flow enforcement. In [18], a framework for staging information-flow properties has been proposed to compute a minimal set of syntactic residual checks that are performed on the remaining code when it is dynamically loaded. Similarly, Hammer *et al.* track information flow dynamically but rely on intra-procedural static analysis to capture implicit flows [40].

Several **empirical studies** have been conducted to detect violations against information-flow policies [66, 39]. In [66], tainting techniques are used to track the flow of sensitive information inside the browser in order to stop Cross-Site Scripting attacks. Moreover, Jang *et al.* surveyed the prevalence of privacy violating flows on the Alexa top 50.000 websites to detect four privacy-violating flows: cookie stealing, location hijacking, history sniffing, and behavior tracking [39].

On the **server-side**, it is important to mention the work of the researchers at Cornell [16, 15, 42]. Swift is a multi-tier approach to build web applications that are secure by construction [15]. The source code, written in Jif, is automatically partitioned by the compiler into JavaScript code running in the browser, and Java code running on the server,

and code placement is constrained by information flow policies that strongly enforce the confidentiality and integrity of server-side information. Alternatively, SELinks [19] is a programming language focused on building secure multi-tier web applications, capable of controlling access to labeled data. Moreover, Off-the-Record Messaging provides a server-side enforcement for cryptographic security to achieve confidential communication with plausible deniability [11].

Finally, there were several directions identified in state-of-the-art policies for information-flow control. First, a set of quantitative security policies takes into account the termination and progress channel, as well as side channels [32]. Secondly, more expressive sets of information-flow control policies take into account mutual distrust and a decentralized authority [51, 45]. In such a setting, policies should allow to share information with distrusted script, while still controlling how the script propagates the shared information. Other research in this domain focuses on defining and evaluating lattices for modern web applications and mashups, and the use of relational reasoning in information-flow control.

To conclude, the participants drafted a set of **promising future directions** in information-flow control research:

- Hybrid access control and information-flow control mechanisms
- Extend facets to integrity
- Increase usability of information-flow control mechanisms
- For systems: distributed information-flow control and tainting
- For databases: the provenance of data
- For crypto: achieve robustness, secure multi-party, zero knowledge, secure information retrieval
- For privacy: differential privacy

We would like to thank Andrei Sabelfeld for taking notes during this break-out session, and presenting the break-out results to the full group.

References

1 Pieter Agten, Steven Van Acker, Yoran Brondsema, Phu H. Phung, Lieven Desmet, and Frank Piessens. Jsand: complete client-side sandboxing of third-party javascript without browser modifications. In *Proceedings of the 28th Annual Computer Security Applications Conference*, ACSAC '12, pages 1–10, New York, NY, USA, 2012. ACM.

2 Devdatta Akhawe, Prateek Saxena, and Dawn Song. Privilege separation in html5 applications. pages 23–23, 2012.

3 Thomas H. Austin and Cormac Flanagan. Multiple facets for dynamic information flow. pages 165–178, 2012.

4 Chetan Bansal, Karthikeyan Bhargavan, and Sergio Maffeis. Discovering concrete attacks on website authorization by formal analysis. In Chong [14], pages 247–262.

5 Daniel Bates, Adam Barth, and Collin Jackson. Regular expressions considered harmful in client-side xss filters. In *Proceedings of the 19th international conference on World wide web*, WWW '10, pages 91–100, New York, NY, USA, 2010. ACM.

6 Karthikeyan Bhargavan, Cédric Fournet, Ricardo Corin, and Eugen Zalinescu. Verified cryptographic implementations for tls. *ACM Trans. Inf. Syst. Secur.*, 15(1):3, 2012.

7 Nataliia Bielova. Survey on javascript security policies and their enforcement mechanisms in a web browser. 2012. Under submission.

8 Arnar Birgisson, Daniel Hedin, and Andrei Sabelfeld. Boosting the permissiveness of dynamic information-flow tracking by testing. In Sara Foresti, Moti Yung, and Fabio Martinelli, editors, *Computer Security ESORICS 2012*, volume 7459 of *Lecture Notes in Computer Science*, pages 55–72. Springer Berlin Heidelberg, 2012.

9 Dan Boneh, Ulfar Erlingsson, Martin Johns, and Benjamin Livshits. 09141 abstracts collection – web application security. In Dan Boneh, Ulfar Erlingsson, Martin Johns, and Benjamin Livshits, editors, *Web Application Security*, number 09141 in Dagstuhl Seminar Proceedings, Dagstuhl, Germany, 2010. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, Germany.

10 Dan Boneh, Ulfar Erlingsson, Martin Johns, and Benjamin Livshits. 09141 executive summary – web application security. In Dan Boneh, Ulfar Erlingsson, Martin Johns, and Benjamin Livshits, editors, *Web Application Security*, number 09141 in Dagstuhl Seminar Proceedings, Dagstuhl, Germany, 2010. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, Germany.

11 Nikita Borisov, Ian Goldberg, and Eric Brewer. Off-the-record communication, or, why not to use pgp. In *Proceedings of the 2004 ACM workshop on Privacy in the electronic society*, WPES '04, pages 77–84, New York, NY, USA, 2004. ACM.

12 Bastian Braun, Patrick Gemein, Hans P. Reiser, and Joachim Posegga. Control-flow integrity in web applications. In *International Symposium on Engineering Secure Software and Systems (ESSoS 2013)*, February 2013. [to appear].

13 Internet Explorer Developer Center. Making HTML safer: details for toStaticHTML (Windows Store apps using JavaScript and HTML). http://msdn.microsoft.com/en-us/library/ie/hh465388.aspx, 2012.

14 Stephen Chong, editor. *25th IEEE Computer Security Foundations Symposium, CSF 2012, Cambridge, MA, USA, June 25-27, 2012*. IEEE, 2012.

15 Stephen Chong, Jed Liu, Andrew C. Myers, Xin Qi, K. Vikram, Lantian Zheng, and Xin Zheng. Secure web applications via automatic partitioning. In *Proceedings of twenty-first ACM SIGOPS symposium on Operating systems principles*, SOSP '07, pages 31–44, New York, NY, USA, 2007. ACM.

16 Stephen Chong, K. Vikram, and Andrew C. Myers. Sif: enforcing confidentiality and integrity in web applications. In *Proceedings of 16th USENIX Security Symposium on*

USENIX Security Symposium, SS'07, pages 1:1–1:16, Berkeley, CA, USA, 2007. USENIX Association.

17 Ravi Chugh, David Herman, and Ranjit Jhala. Dependent types for javascript. In *Proceedings of the ACM international conference on Object oriented programming systems languages and applications*, OOPSLA '12, pages 587–606, New York, NY, USA, 2012. ACM.

18 Ravi Chugh, Jeffrey A. Meister, Ranjit Jhala, and Sorin Lerner. Staged information flow for javascript. In *Proceedings of the 2009 ACM SIGPLAN conference on Programming language design and implementation*, PLDI '09, pages 50–62, New York, NY, USA, 2009. ACM.

19 Brian J. Corcoran, Nikhil Swamy, and Michael Hicks. Cross-tier, label-based security enforcement for web applications. In *Proceedings of the 2009 ACM SIGMOD International Conference on Management of data*, SIGMOD '09, pages 269–282, New York, NY, USA, 2009. ACM.

20 Douglas Crockford. ADsafe – making JavaScript safe for advertising. http://adsafe.org/.

21 Willem De Groef, Dominique Devriese, Nick Nikiforakis, and Frank Piessens. Flowfox: a web browser with flexible and precise information flow control. In *Proceedings of the 2012 ACM conference on Computer and communications security*, CCS '12, pages 748–759, New York, NY, USA, 2012. ACM.

22 Philippe De Ryck, Maarten Decat, Lieven Desmet, Frank Piessens, and Wouter Joosen. Security of web mashups: a survey. In *Proceedings of the 15th Nordic conference on Information Security Technology for Applications*, NordSec'10, pages 223–238, Berlin, Heidelberg, 2012. Springer-Verlag.

23 Dorothy E. Denning. A lattice model of secure information flow. *Commun. ACM*, 19(5):236–243, May 1976.

24 Dominique Devriese and Frank Piessens. Noninterference through secure multi-execution. In *Proceedings of the 2010 IEEE Symposium on Security and Privacy*, SP '10, pages 109–124, Washington, DC, USA, 2010. IEEE Computer Society.

25 Veracode Fergal Glynn. Static Code Analysis. http://www.veracode.com/security/static-code-analysis, 2012.

26 Cedric Fournet, Nikhil Swamy, Juan Chen, Pierre-Evariste Dagand, Pierre-Yves Strub, and Benjamin Livshits. Fully abstract compilation to javascript. In *Proceedings of the Sympolisium on Principles of Programming Languages (POPL)*, January 2013.

27 Felix Freiling and Sebastian Schinzel. Detecting hidden storage side channel vulnerabilities in networked applications. In Jan Camenisch, Simone Fischer-Hübner, Yuko Murayama, Armand Portmann, and Carlos Rieder, editors, *Future Challenges in Security and Privacy for Academia and Industry*, volume 354 of *IFIP Advances in Information and Communication Technology*, pages 41–55. Springer Berlin Heidelberg, 2011.

28 Philippa Anne Gardner, Sergio Maffeis, and Gareth David Smith. Towards a program logic for javascript. In *Proceedings of the 39th annual ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, POPL '12, pages 31–44, New York, NY, USA, 2012. ACM.

29 Salvatore Guarnieri and Benjamin Livshits. Gatekeeper: Mostly static enforcement of security and reliability policies for javascript code. In *Proceedings of the Usenix Security Symposium*, August 2009.

30 Arjun Guha, Claudiu Saftoiu, and Shriram Krishnamurthi. The essence of javascript. In *Proceedings of the 24th European conference on Object-oriented programming*, ECOOP'10, pages 126–150. Springer-Verlag, Berlin, Heidelberg, 2010.

31 Google Web Toolkit (GWT). AutoEscape implementation for GWT. http://code.google.com/p/google-web-toolkit/source/browse/tools/lib/streamhtmlparser/streamhtmlparser-jsilver-r10/streamhtmlparser-jsilver-r10-1.5.jar, 2010.

32 D. Hedin and A. Sabelfeld. A perspective on information-flow control. *Proc. of the 2011 Marktoberdorf Summer School*, 2011.

33 Daniel Hedin and Andrei Sabelfeld. Information-flow security for a core of javascript. In Chong [14], pages 3–18.

34 Mario Heiderich, Marcus Niemietz, Felix Schuster, Thorsten Holz, and Jörg Schwenk. Scriptless attacks: stealing the pie without touching the sill. In *Proceedings of the 2012 ACM conference on Computer and communications security*, CCS '12, pages 760–771, New York, NY, USA, 2012. ACM.

35 I. Hickson and D. Hyatt. HTML 5 Working Draft - The sandbox Attribute. http://www.w3.org/TR/html5/the-iframe-element.html#attr-iframe-sandbox, June 2010.

36 Lon Ingram and Michael Walfish. TreeHouse: JavaScript sandboxes to help web developers help themselves. In *USENIX ATC*, 2012.

37 Tibor Jager, Sebastian Schinzel, and Juraj Somorovsky. Bleichenbacher's attack strikes again: Breaking pkcs#1 v1.5 in xml encryption. In Sara Foresti, Moti Yung, and Fabio Martinelli, editors, *Computer Security ESORICS 2012*, volume 7459 of *Lecture Notes in Computer Science*, pages 752–769. Springer Berlin Heidelberg, 2012.

38 Tibor Jager and Juraj Somorovsky. How to break xml encryption. In *Proceedings of the 18th ACM conference on Computer and communications security*, CCS '11, pages 413–422, New York, NY, USA, 2011. ACM.

39 Dongseok Jang, Ranjit Jhala, Sorin Lerner, and Hovav Shacham. An empirical study of privacy-violating information flows in javascript web applications. In *Proceedings of the 17th ACM conference on Computer and communications security*, CCS '10, pages 270–283, New York, NY, USA, 2010. ACM.

40 Seth Just, Alan Cleary, Brandon Shirley, and Christian Hammer. Information flow analysis for javascript. In *Proceedings of the 1st ACM SIGPLAN international workshop on Programming language and systems technologies for internet clients*, PLASTIC '11, pages 9–18, New York, NY, USA, 2011. ACM.

41 Boris K¨opf, Laurent Mauborgne, and Martín Ochoa. Automatic quantification of cache side-channels. In *Computer Aided Verification*, volume 7358 of *Lecture Notes in Computer Science*, pages 564–580. Springer Berlin Heidelberg, 2012.

42 Jed Liu, Michael D. George, K. Vikram, Xin Qi, Lucas Waye, and Andrew C. Myers. Fabric: a platform for secure distributed computation and storage. In *Proceedings of the ACM SIGOPS 22nd symposium on Operating systems principles*, SOSP '09, pages 321–334, New York, NY, USA, 2009. ACM.

43 Zhengqin Luo and Tamara Rezk. Mashic compiler: Mashup sandboxing based on inter-frame communication. In Chong [14], pages 157–170.

44 Sergio Maffeis, John C. Mitchell, and Ankur Taly. An operational semantics for javascript. In *Proceedings of the 6th Asian Symposium on Programming Languages and Systems*, APLAS '08, pages 307–325. Springer-Verlag, Berlin, Heidelberg, 2008.

45 Jonas Magazinius, Aslan Askarov, and Andrei Sabelfeld. Decentralized delimited release. In *Proceedings of the 9th Asian conference on Programming Languages and Systems*, APLAS'11, pages 220–237, Berlin, Heidelberg, 2011. Springer-Verlag.

46 Giorgio Maone. NoScript - JavaScript/Java/Flash blocker for a safer Firefox experience! http://noscript.net/, 2012.

47 Piotr Mardziel, Stephen Magill, Michael Hicks, and Mudhakar Srivatsa. Dynamic enforcement of knowledge-based security policies. *2012 IEEE 25th Computer Security Foundations Symposium*, 0:114–128, 2011.

48 Leo Meyerovich and Benjamin Livshits. ConScript: Specifying and enforcing fine-grained security policies for Javascript in the browser. In *Proc. of SP'10*, 2010.

49 M. S. Miller, M. Samuel, B. Laurie, I. Awad, and M. Stay. Caja: Safe active content in sanitized javascript. http://google-caja.googlecode.com/files/caja-spec-2008-01-15.pdf, January 2008.

50 Mark Samuel Miller. Secure EcmaScript 5. http://code.google.com/p/es-lab/wiki/SecureEcmaScript.

51 Andrew C. Myers and Barbara Liskov. A decentralized model for information flow control. In *Proceedings of the sixteenth ACM symposium on Operating systems principles*, SOSP '97, pages 129–142, New York, NY, USA, 1997. ACM.

52 Nick Nikiforakis, Luca Invernizzi, Alexandros Kapravelos, Steven Van Acker, Wouter Joosen, Christopher Kruegel, Frank Piessens, and Giovanni Vigna. You are what you include: large-scale evaluation of remote javascript inclusions. In *Proceedings of the 2012 ACM conference on Computer and communications security*, CCS '12, pages 736–747, New York, NY, USA, 2012. ACM.

53 Joe Gibbs Politz, Matthew J. Carroll, Benjamin S. Lerner, Justin Pombrio, and Shriram Krishnamurthi. A tested semantics for getters, setters, and eval in javascript. In *Proceedings of the 8th symposium on Dynamic languages*, DLS '12, pages 1–16, New York, NY, USA, 2012. ACM.

54 David Ross. IE 8 XSS Filter Architecture / Implementation. http://blogs.technet.com/b/srd/archive/2008/08/19/ie-8-xss-filter-architecture-implementation.aspx, 2008.

55 J. Ruderman. Same origin policy for javascript, 2009.

56 Mike Samuel, Prateek Saxena, and Dawn Song. Context-sensitive auto-sanitization in web templating languages using type qualifiers. In *Proceedings of the 18th ACM conference on Computer and communications security*, CCS '11, pages 587–600, New York, NY, USA, 2011. ACM.

57 Prateek Saxena, Devdatta Akhawe, Steve Hanna, Feng Mao, Stephen McCamant, and Dawn Song. A symbolic execution framework for javascript. In *Proceedings of the 2010 IEEE Symposium on Security and Privacy*, SP '10, pages 513–528, Washington, DC, USA, 2010. IEEE Computer Society.

58 Prateek Saxena, David Molnar, and Benjamin Livshits. Scriptgard: automatic context-sensitive sanitization for large-scale legacy web applications. In *Proceedings of the 18th ACM conference on Computer and communications security*, CCS '11, pages 601–614, New York, NY, USA, 2011. ACM.

59 S. Schinzel. An efficient mitigation method for timing side channels on the web. In *2nd International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE)*, 2011.

60 HP Enterprise Security. HP Fortify Static Code Analyzer (SCA). http://www.hpenterprisesecurity.com/products/hp-fortify-software-security-center/hp-fortify-static-code-analyzer, 2012.

61 Brandon Sterne and Adam Barth. Content security policy. http://www.w3.org/TR/CSP/, November 2011.

62 Mike Ter Louw, Karthik Thotta Ganesh, and V.N. Venkatakrishnan. AdJail: Practical Enforcement of Confidentiality and Integrity Policies on Web Advertisements. In *19th USENIX Security Symposium*, August 2010.

63 The FaceBook Team. FBJS. http://wiki.developers.facebook.com/index.php/FBJS.

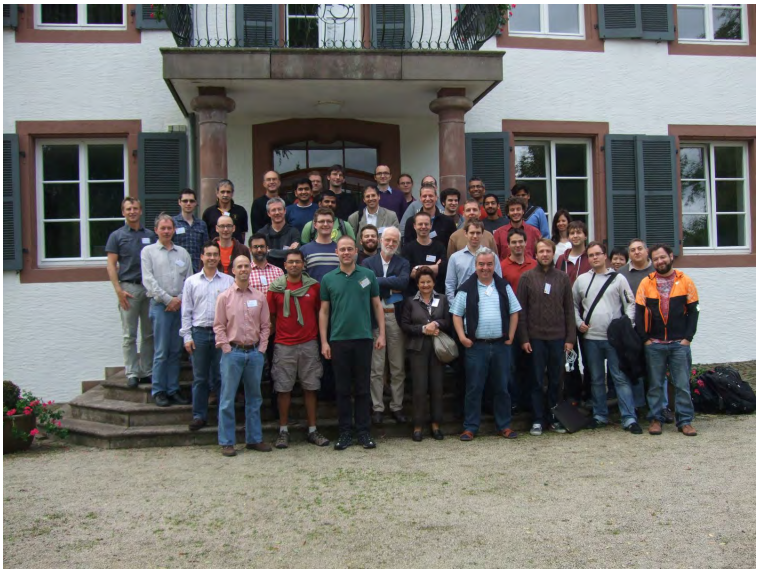
64 Steven Van Acker, Philippe De Ryck, Lieven Desmet, Frank Piessens, and Wouter Joosen. WebJail: least-privilege integration of third-party components in web mashups. ACSAC '11, pages 307–316, New York, NY, USA, 2011. ACM.

65 Steven Van Acker, Nick Nikiforakis, Lieven Desmet, Wouter Joosen, and Frank Piessens. FlashOver: Automated discovery of cross-site scripting vulnerabilities in rich internet applications. In *AsiaCCS, Seoul, 2-4 May 2012*, May 2012.

66 Philipp Vogt, Florian Nentwich, Nenad Jovanovic, Engin Kirda, Christopher Krügel, and Giovanni Vigna. Cross site scripting prevention with dynamic data tainting and static analysis. In *NDSS*. The Internet Society, 2007.
67 Edward Z. Yang. HTML Purifier. http://htmlpurifier.org/, 2012.

Participants

- Marco Balduzzi
TREND MICRO Italy S.r.l. – Sesto San Giovanni, IT
- Nataliia Bielova
INRIA – Rennes, FR
- Arnar Birgisson
Chalmers UT – Göteborg, SE
- Egon Börger
University of Pisa, IT
- Bastian Braun
Universität Passau, DE
- Juan Chen
Microsoft Res. – Redmond, US
- Ravi Chugh
University of California – San Diego, US
- Jorge Cuellar
Siemens – München, DE
- Valentin Dallmeier
Universität des Saarlandes, DE
- Philippe De Ryck
KU Leuven, BE
- Lieven Desmet
KU Leuven, BE
- Akhawe Devdatta
University of California – Berkeley, US
- Daniele Filaretti
Imperial College London, GB
- Cormac Flanagan
University of California – Santa Cruz, US
- Cédric Fournet
Microsoft Research UK – Cambridge, GB
- Michael Franz
Univ. California – Irvine, US
- Dieter Gollmann
TU Hamburg–Harburg, DE
- Arjun Guha
Cornell University – Ithaca, US
- Daniel Hedin
Chalmers UT – Göteborg, SE
- Mario Heiderich
Ruhr–Universität Bochum, DE
- Boris Hemkemeier
Commerzbank AG – Frankfurt, DE
- Michael Hicks
University of Maryland – College Park, US
- Thorsten Holz
Ruhr–Universität Bochum, DE
- Thomas Jensen
INRIA – Rennes, FR
- Ranjit Jhala
University of California – San Diego, US
- Martin Johns
SAP Research – Karlsruhe, DE
- Shriram Krishnamurthi
Brown Univ. – Providence, US
- Benjamin Livshits
Microsoft – Redmond, US
- Sergio Maffeis
Imperial College London, GB
- Fabio Massacci
University of Trento – Povo, IT
- John C. Mitchell
Stanford University, US
- Nick Nikiforakis
KU Leuven, BE
- Martin Ochoa
Siemens – München, DE
- Frank Piessens
KU Leuven, BE
- Joe Gibbs Politz
Brown Univ. – Providence, US
- Joachim Posegga
Universität Passau, DE
- Tamara Rezk
INRIA Sophia Antipolis, FR
- Eric Rothstein
Universität Passau, DE
- Andrei Sabelfeld
Chalmers UT – Göteborg, SE
- Sebastian Schinzel
Univ. Erlangen–Nürnberg, DE
- Juraj Somorovsky
Ruhr–Universität Bochum, DE
- Nikhil Swamy
Microsoft – Redmond, US
- Steven Van Acker
KU Leuven, BE
- John Wilander
Hägersten, SE



Report from Dagstuhl Seminar 12411

Coalgebraic Logics

Edited by

Ernst-Erich Doberkat[1] and Alexander Kurz[2]

1 TU Dortmund, DE, ernst-erich.doberkat@udo.edu
2 University of Leicester, GB, kurz@mcs.le.ac.uk

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 12411 "Coalgebraic Logics". The seminar deals with recent developments in the area of coalgebraic logic, a branch of logics which combines modal logics with coalgebraic semantics. Modal logic finds its uses when reasoning about behavioural and temporal properties of computation and communication, coalgebras have evolved into a general theory of systems. Consequently, it is natural to combine both areas for a mathematical description of system specification. Coalgebraic logics are closely related to the broader categories semantics/formal methods and verification/logic.

Seminar 08.–12. October, 2012 – www.dagstuhl.de/12411
1998 ACM Subject Classification F.4 Mathematical Logic and Formal Languages, F.3.2 Semantics of Programming Languages, G.3 Probability and Statistics
Keywords and phrases Modal Logic, Coalgebra, Category Theory, Stochastic Logic, Categorical Semantics
Digital Object Identifier 10.4230/DagRep.2.10.38
Edited in cooperation with Ingo Battenfeld

1 Executive Summary

Alexander Kurz (University of Leicester, GB)
Ernst-Erich Doberkat (TU Dortmund, DE)

Background

Modal Logic is a field with roots in philosophical logic and mathematics. As applied to Computer Science it has become central in order to reason about the behavioural and temporal properties of computing and communicating systems, as well as to model properties of agents such as knowledge, obligations, and permissions. Two of the reasons for the success of Modal Logic are the following. First, many modal logics are—despite their remarkable expressive power—decidable and, therefore, amenable to automated reasoning and verification. Second, Kripke's relational semantics of modal logic turned out to be amazingly flexible, both in terms of providing techniques to prove properties of modal logics and in terms of allowing the different applications of Modal Logic to Artificial Intelligence, Software Agents, etc.

Coalgebra is a more recent area. Following on from Aczel's seminal work on non-well founded set theory , coalgebra has been developed into a general theory of systems. The basic idea is that coalgebras are given with respect to a parameter F. Technically, the parameter F is a *functor* on a *category* $\mathcal{C}$.

Coalgebraic Logics, *Dagstuhl Reports*, Vol. 2, Issue 10, pp. 38–59
Editors: Ernst-Erich Doberkat, and Alexander Kurz
Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Different choices of F yield, for example, the Kripke frames and models of modal logic, the labelled transition systems of process algebra, the deterministic automata of formal language theory, or the Markov chains used in statistics. Rutten showed that, in analogy with Universal Algebra, a theory of systems, called Universal Coalgebra, can be built uniformly in the parameter F, simultaneously covering the above and other examples. Crucial notions such as behavioural equivalence (observational equivalence, bisimilarity), final semantics and coinduction find their natural place here.

Coalgebraic Logic combines Coalgebra and Modal Logic to study *logics of systems* uniformly in the parameter F. Given the plethora of different transition systems and their ad hoc logics, such a uniform theory is clearly desirable. *Uniformity* means that results on, for example, completeness, expressivity, finite model property and complexity of satisfiability can be established at once for all functors (possibly satisfying some, usually mild, conditions). Additionally, there is also a concern for *modularity*: Typically, a parameter F is composed of basic features (such as input, output, non-determinism, probability). Modularity then means that the syntax/proof systems/algorithms for the logic of F are obtained compositionally from the syntax/proof systems/algorithms for the logics of the basic features.

What has been achieved: The power of uniformity and modularity Following on from Moss' seminal paper, Coalgebraic Logic is now growing into a successful area. Conferences in this area now treat topics such as completeness, expressivity, compositionality, complexity, rule formats for process calculi, containing several hitherto unknown results on these classic topics.

The uniformity achieved in the above cited work is based on varying the type F for a given base category $\mathcal{C}$, usually the category of sets. But it is also of interest to vary $\mathcal{C}$.

Here probabilistic approaches deserve to be mentioned. In a number of papers Markov transition systems could be shown to interpret modal logics under different assumptions on the probabilistic structure. It was shown that general measurable spaces provide too general a structure, but that analytic spaces with Borel transition laws offer just the right blend of generality and measure theoretic accessibility. In this context, it was shown that logical equivalence, bisimilarity, and behavioral equivalence are equivalent concepts . Recent work shows that this can be extended to distributional aspects as well: instead of comparing states proper, one has a look at distributions over the states of a Kripke model. This approach was recently generalized from general modal logics to coalgebraic logics ; these logics are interpreted through coalgebras in which the subprobability functor and the functor suggested by the phenomenon to be modelled form various syntactic alliances. This generalization brings stochastic coalgebraic logic into the mainstream of coalgebraic logics: the problems considered are similar, and one sees a convergence of methods.

Nevertheless it is to be mentioned that the probabilistic approach brings its own idiosyncratic touch due to measure theoretic problems. This entails among others that one sometimes has to work in a very specific topological context, for otherwise solutions are not available. On the other hand, leaving a topological context and working in general measurable spaces poses the question of the limits to the coalgebraic approach: What can be achieved in general measurable spaces, or in measurable spaces in which some of the properties are available (like Blackwell spaces, which are countably generated without being topological)?

Quantitative aspects are also considered when it comes to approximate Markov transition processes defined on uncountably infinite state spaces through finite processes . This is a classical problem that arises mostly in practical applications of Markov transition systems; it has to be investigated from a logical vantage point as well.

Structuring the Seminar

When we planned the seminar, we envisaged six broad topics. One of the outcomes of this seminar, as compared to the one of 2009, is that the different subcommunities in coalgebraic logic moved closer together, exchanging ideas, techniques, problems and also researchers. Consequently, it seems difficult, if not impossible, to divide up all the talks consistently among the distinct research topics. We will nevertheless try to describe some trends.

Probabilistic Transition Systems

The focus of Markov transition systems shifted from the consideration of specific problems (like interpreting a particular class of logics) to structural problems which are treated with the instruments provided by coalgebras. The talk presented Panangaden concentrated on the duality of Markov transition systems and various function spaces, most of them well known in functional analysis. The Radom-Nikodym Theorem provides a very sophisticated tool for switching between these representations. Doberkat's talk dealt with stochastic effectivity functions as an extension of Markov transition systems for the interpretation of more complicated logics like, e.g., Parikh's game logic. Urbat showed that both the Hausdorff and the Kantorovic functor, which are widely used to model probabilistic nondeterminism are finitary, improving some well known results; at the same time, this results raises some interesting topological questions.

Quite apart from structural problems, another approach has been presented by Srivastava; he gave a tutorial talk on deduction systems for probabilistic logics, based on the work by Goldblatt and by Zhou. The set theoretic problems which originate with bisimilarity were taken up by Terraf, who extended a well-known result from descriptive set theory on the structure of equivalence relations to bisimulations, hereby indicating some of the caveats one has to observe in classical set theory.

Coalgebras and automata theory

Whereas the final coalgebra describes all infinite behaviours, the theory of formal languages suggests that the regular or rational sets of behaviours should be of special interest. This is indeed the case and the talks of Milius, Myers, Sokolova and Winter presented some of the latest developments. More generally, this direction of generalising results from automata theory also saw talks of Hansen/Silva and of Venema.

Process algebra and operational semantics

Bonsangue presented a coalgebraic account of the 'bisimulation-up-to' proof technique and Staton had new results on finite power set functors. Another direction is concerned with applying coalgebraic techniques to other process equivalences than bisimulation. In particular, Hasuo and Cirstea studied trace equivalence, whereas Levy's tutorial on relation liftings was concerned with various notions of simulation.

Coalgebraic logic beyond sets

After the successes of set-based coalgebra, quite some effort goes now into extending results to more general settings. Jacobs presented a novel framework uniformly covering the classical, probabilistic and quantum case. Pavlovic introduced his ideas about a monoidal computer to bridge the gap between high-level specification and low-level computational models such as Turing machines. Talks by Bilkova, Dostal, and Velebil explored now to harness enriched

category theory whereas Moshier is extending coalgebraic logics from the discrete to the setting of compact Hausdorff topological spaces, a topic that also surfaced in Hofmann's contribution. Petrisan studied final coalgebra in nominal sets.

Extensions of coalgebraic logics

Litak led a discussion session about the directions of generalising coalgebraic modal logic to formalisms with explicit quantifiers. Palmigiano reported latest results on extensions with fixpoint operators and Venema discussed some of the challenges and open problems in this area. Sano showed how to extend coalgebraic logic by an actuality operator and whereas Schröder explored the border of decidability for coalgebraic hybrid logic.

Applications

One of the outcomes of the seminar was the excitement generated by the wide range of applications which are now coming into the scope of coalgebraic techniques. Examples include Abramsky's results on infinite economic non-cooperative games, Trancon y Widemann's contributions to a reformulation of the foundations of ecology, and Kozen's ideas of making coalgebraic techniques available to the working programmer and to the working mathematician.

2 Table of Contents

3 Overview of Talks

3.1 Moss' coalgebraic logic in preorders and beyond

Marta Bilkova (Charles University – Prague, CZ)

Joint work of Bilkova, Marta; Velebil, Jiri

In this talk we built on results obtained in , namely existence of functorial relation lifting for functors preserving exact squares in the category of preorders, generalised in to the enriched case of V-categories, where V is a commutative quantale. For the preorder case we present Moss' coalgebraic language based on the logic of distributive lattices equiped with cover modalities nabla and delta, its semantics, and a sound axiomatics (it is a work in progress and completeness yet remains to be shown). As expected, axiomatics consists of certain distributive laws which are straightforward analogues of those known from the Set case, see . Formally, the laws look the same as in the Set case, yet the techniques used have to be more subtle and they reveal the hidden symmetries. Moreover, the proofs apply also to the case of the V-categories. For the case of V-categories we propose the propositional part of the logic to consist of connectives based on (weighted) limits and colimits. In the case of preorders they collapse to meets and joins.

Work of the first author has been supported by grant no. P202/11/P304 of the Czech Grant Agency. Work of the second author has been supported by grant no. P202/11/1632 of the Czech Grant Agency.

References

1 M. Bilkova, A. Kurz, D. Petrisan and J. Velebil, Relation Liftings on Preorders, in proccedings CALCO 2011, LNCS 6859 (2011), pp. 115-129.
2 M. Bilkova, A. Kurz, D. Petrisan and J. Velebil, Relation lifting, with an application to the many-valued cover modality, submitted to LMCS, 2012.
3 C. Kupke, A. Kurz, Y. Venema, Completeness for the coalgebraic cover modality. LMCS 8 (3:14) 2012.

3.2 Coalgebraic Bisimulation-up-to

Marcello M. Bonsangue (Leiden University, NL)

Joint work of Rot, Jurriaan; Bonsangue, Marcello; Rutten, Jan
Main reference J. Rot, M. Bonsangue, J. Rutten, "Coalgebraic bisimulation-up-to," in Proc. of SOFSEM, 2013. To appear.
URL http://www.liacs.nl/~jrot/sofsem.pdf

In this talk I will present a systematic study of bisimulation-up-to techniques for coalgebras. These techniques enhance the bisimulation proof method for a large class of state based systems, including labelled transition systems but also stream systems and weighted automata. Our approach allows for compositional reasoning about the soundness of enhancements. Applications include the soundness of bisimulation up to bisimilarity, up to equivalence and up to congruence. All in all, this gives a powerful and modular framework for simplifed coinductive proofs of equivalence.

3.3 Coalgebraic logic over concrete categories

Liang-Ting Chen (University of Birmingham, GB)

Joint work of Chen, Liang-Ting; Jung, Achim

Coalgebraic logic for **Sets** coalgebras given by predicate lifting has been applied to different areas in computer science, e.g. modal logic, automata theory, and program verification. However, there are currently few studies beyond **Sets**. Exceptions are, for example, coalgebraic logic over the category of posets for positive modal logic (by Kapulkin, Balan, Kurz, Velebil) and coalgebra logic over the category of measurable spaces for stochastic coalgebraic logic. There are more general approaches based on dual adjunctions, but it is not clear how to describe modalities explicitly.

In this talk, we relate few different notions. A dual adjunction over concrete categories with a mild condition provides generalised predicates as morphisms to the dualising object, so we can give straightforward definitions and prove the adequacy of coalgebraic logic easily. Objects which contain predicate liftings are identified, and we derive a logic of all predicate liftings as a corollary from algebraic theory. As for expressivity, we argue that propositional geometric logic might be an interesting local logic to use for coalgebraic logic.

3.4 Interaction and observation: dialgebras in program semantics

Vincenzo Ciancia (CNR – Pisa, IT)

Main reference V. Ciancia, "Interaction and observation: categorical semantics of reactive systems trough dialgebras," arXiv:1209.5903v1 [cs.LO].
URL http://arxiv.org/abs/1209.5903v1

Interactive systems are collections of entities that may interact with each other, and produce a resulting entity and an observable effect. Their semantics is typically described by so-called reaction rules.

In this work, we try to address the question "what are reaction rules" in a categorical way. As an answer we propose dialgebras, generalising both algebras and coalgebras.

The focus is on providing a semantic model, alternative to coalgebras, where interaction is built-in, instead of relying on a (possibly difficult) understanding of the side effects of a component in isolation.

Dialgebras are arrows of the form FX -> GX for suitable endofunctors F and G. The functor G gives rise to observable effects, just like in coalgebras. The functor F takes into account interaction between different elements, like in algebras. Behavioural equivalence is defined as kernel equivalence. Due to the interplay of F and G, such equivalence gives non-trivial semantics to reaction rules, when letting G be some variant of the power set functor and F be a product.

Dialgebras lack a final object for useful cases of F and G. This requires a change of point of view, and the adoption of quotient categories as grounds for reasoning. As a consequence, comparing different categories of dialgebras becomes a "local" task which is better carried out in sub-categories of quotients of some given interesting objects. Minimization and simplification of dialgebras are similarly affected.

We will discuss and motivate these aspects, and look at some examples.

3.5 On Logics for Maximal Traces

Corina Cirstea (University of Southampton, GB)

The coalgebraic theory of finite traces is well understood , and some preliminary results exist on logics that characterise finite trace equivalence .

Initial steps towards a coalgebraic account of maximal, possibly infinite traces have also been made . Here we revisit the definition of maximal traces in loc. cit. by taking the view that only finite (but arbitrarily long) prefixes of infinite traces are observable, and use a dual adjunction approach similar to that of to derive logics that characterise maximal traces.

References

1 C. Cîrstea. Maximal traces and path-based coalgebraic temporal logics. *Theor. Comput. Sci.*, 412(38), 2011.
2 I. Hasuo, B. Jacobs, and A. Sokolova. Generic trace semantics via coinduction. *Logical Methods in Computer Science*, 3:1–36, 2007.
3 C. Kissig and A. Kurz. Generic trace logics. arXiv:1103.3239, 2011.

3.6 Stochastic Game Frames

Ernst-Erich Doberkat (TU Dortmund, DE)

Parikh's Game Logic is interpreted through game frames, i.e., collections of stochastic effectivity functions. Stochastic game frames are introduced and compared to Kripke models. Goldblatt's Theorem on deduction systems helps to clarify the relationship between both. We show how to construct from such a game frame an interpretation of Game Logic. Some analogies to Kozen's proposal for interpreting PDL are drawn, they are helpful for compensating the lack of suitable algebraic structures in the space of stochastic effectivity functions.

This is work in progress.

3.7 Many-valued relation liftings and coalgebraic logics

Matej Dostal (Czech Technical University, CZ)

Joint work of Dostal, Matej; Bilkova, Marta; Velebil, Jiri
Main reference M. Dostal, "Many-valued coalgebraic logic," Diploma thesis, to be published 2013.

The coalgebraic approach to modal logic enables us to talk about logics for various kinds of Kripke-like structures. We concern ourselves with the coalgebraic logic based on the cover modality. It seems natural to wonder how far we can get when trying to generalise this approach to a many-valued setting. We present a notion of many-valued relation liftings for finitary functors as a tool for talking about many-valued coalgebraic logics and present some examples of logics that arise this way.

This work has been supported by grant no. SGS12/060/OHK3/1T/13 of SGS CVUT.

3.8 Functor- and Logic Patterns

H. Peter Gumm (Universität Marburg, DE)

Preservation properties of a Set-Endofunctor F have been recognized as essential for the structure of the category SetF of F-coalgebras. Over 30 years ago, V.Trnková in Prague has studied similar problems in the general context of categories with a factorization system (E;M). We recollect some relevant fragment of her findings, and we add some new results and open questions concerning functors weakly preserving kernel pairs.

Finitary functors can be described by sets of finitary patterns. Sets of 0-1 patterns determine logical modalities and pattern rules correspond to frame axioms in coalgebraic modal logic. We shall present examples of such correspondences.

3.9 Coalgebraic Trace Semantics for Higher-Order Computation, Especially The Quantum One

Ichiro Hasuo (University of Tokyo, JP)

Joint work of Hasuo, Ichiro; Hoshino, Naohiko
Main reference I. Hasuo, N. Hoshino, "Semantics of Higher-Order Quantum Computation via Geometry of Interaction," LICS 2011: 237–246.
URL http://dx.doi.org/10.1109/LICS.2011.26

Unlike the standard setting of the category of sets and functions where coinduction captures bisimilarity, coinduction in Kleisli categories (for certain monads with cpo-enriched structures) captures (finitary) trace semantics. Underlying this observation is the coincidence of an initial algebra and a final coalgebra, a phenomenon typical of cpo-enriched settings.

In [Jacobs, CMCS'10] it is observed that this coalgebraic "trace" semantics (a usage in concurrency theory) is closely related to "trace" in traced monoidal categories—in fact, most known "particle-style" examples of traced monoidal categories arise from coalgebraic trace semantics, i.e. coinduction in Kleisli categories. Traced monoidal categories, in turn, have been used as a categorical foundation for Girard's geometry of interaction (a denotational semantics "doctrine" that is close to game semantics), by Abramsky, Haghverdi and P. Scott. Therefore, here we are seeing an exciting opportunity of combining theory of coalgebra and that of denotational semantics for functional programming. I'll exhibit one example of a quantum lambda calculus.

The talk will be based on the joint work with Naohiko Hoshino (RIMS, Kyoto Univ.), presented at LICS 2011.

3.10 Variations on a theme of Vietoris

Dirk Hofmann (University of Aveiro, PT)

The motivation for this talk stems from several duality results extending the classical Priestley and Stone dualities to categories of algebras with operators (see , for instance), all of these make essential use of the Vietoris construction . Here we find it worthwhile to note that the upper Vietoris space is part of a lax idempotent monad on the category Top of topological spaces which can be restricted to the full subcategory of locally compact spaces and the (non-full) subcategory of stably compact spaces and spectral maps, as well as to compact Hausdorff spaces. In this talk we shall

- follow an idea of Halmos and consider larger categories "of algebras with hemimorphisms" where the above-mentioned operators appear as morphisms, and recall how functoriality of the Kleisli construction (see) can be used to deduce in a uniform manner that these categories are dually equivalent to full subcategories of the Kleisli category of (variants of) the Vietoris monad $\mathbb{V}$;
- employ a formal analogy between order sets and topological spaces to describe these Vietoris monads as the "covariant presheaf monad" which then allows the introduction of metric (and other) generalisations;
- describe the Kleisli category of these monads;
- use general results of to conclude that these categories "of algebras with hemimorphisms" are also dually equivalent to categories of certain algebras of $\mathbb{V}$.

References

1 M. M. Bonsangue, A. Kurz, and I. M. Rewitzky, *Coalgebraic representations of distributive lattices with operators*, Topology Appl., 154 (2007), pp. 778–791.
2 B. A. Davey and J. C. Galati, *A coalgebraic view of Heyting duality*, Studia Logica, 75 (2003), pp. 259–270.
3 P. R. Halmos, *Algebraic logic*, Chelsea Publishing Co., New York, 1962.
4 C. Kupke, A. Kurz, and Y. Venema, *Stone coalgebras*, Theoret. Comput. Sci., 327 (2004), pp. 109–134.
5 D. Pumplün, *Eine Bemerkung über Monaden und adjungierte Funktoren*, Math. Ann., 185 (1970), pp. 329–337.
6 R. Rosebrugh and R. J. Wood, *Split structures*, Theory Appl. Categ., 13 (2004), pp. No. 12, 172–183.
7 G. Sambin and V. Vaccaro, *Topology and duality in modal logic*, Ann. Pure Appl. Logic, 37 (1988), pp. 249–296.
8 L. Vietoris, *Bereiche zweiter Ordnung*, Monatsh. Math. Phys. **32**(1) (1922), 258–280.

3.11 New Directions in Categorical Logic, for Classical, Probabilistic and Quantum Logic

Bart Jacobs (Radboud University Nijmegen, NL)

Main reference B. Jacobs, "New Directions in Categorical Logic, for Classical, Probabilistic and Quantum Logic," arXiv:1205.3940v2 [math.LO].
URL http://arxiv.org/abs/1205.3940v2

Traditionally in categorical logic predicates on an object/type X are represented as subobjects of X. Here we break with that tradition and use maps of the form p : X –> X + X with [id, id] o p = id as predicates. This new view gives a more dynamic, measurement-oriented view on predicates, that works well especially in a quantitative setting. In classical logic (in the category of sets) these new predicates coincide with the traditional ones (subsets, or characteristic maps X –> 0,1); in probabilistic logic (in the category of sets and stochastic matrices), the new predicates correspond to fuzzy predicates X –> [0,1]; and in quantum logic (in Hilbert spaces) they correspond to effects (positive endomaps below the identity), which may be understood as fuzzy predicates on a changed basis. It is shown that, under certain conditions about coproducts +, predicates p : X –> X + X form effect algebras and carry a scalar multiplication (with probabilities). Suitable substitution functors give rise to indexed/fibred categories. In the quantum case the famous Born rule – describing the probability of observation outcomes – follows directly from the form of these substitution functors: probability calculation becomes substitution in predicate logic. Moreover, the characteristic maps associated with predicates provide tests in a dynamic logic, and turn out to capture measurement in a form that uniformly covers the classical, probabilistic and quantum case. The probabilities incorporated in predicates (as eigenvalues) serves as weights for the possible measurement outcomes.

3.12 Programming with Coinductive Types

Dexter Kozen (Cornell University – Ithaca, US)

Joint work of Kozen, Dexter; Jean-Baptiste Jeannin; Alexandra Silva

We present CoCaml, a functional programming language extending OCaml, which allows us to define functions on coinductive datatypes parameterized by an equation solver. We provide numerous examples that attest to the usefulness of the new programming constructs, including operations on infinite lists, infinitary lambda-terms and p-adic numbers.

3.13 Tutorial on relators

Paul Blain Levy (University of Birmingham, GB)

Relators (also known as relational extensions and lax relational extensions of a functor) play a key role in the coalgebraic study of bisimulation and simulation.

Just as a functor goes between categories, a relator goes between framed categories, so we beging by looking at these. We see examples including relations, corelations, and bimodules between preordered sets. We explore some properties of framed categories, in particular tabulations and cotabulations.

Then we look at the required properties of a relator: monotonicity, lax functoriality, and preservation of inverse images. We consider several variations of these requirements. In particular, we see that some relators preserve identities, some composition and some both.

Finally we give four "functor theorems" showing that a relator of a particular kind can be encoded as a functor, bringing together several notions and results from the literature.

3.14 A special discussion session on coalgebraic predicate formalisms

Tadeusz Litak (Universität Erlangen-Nürnberg, DE)

Joint work of Litak, Tadeusz; Pattinson, Dirk; Sano, Katsuhiko; Schröder, Lutz
Main reference T. Litak, D. Pattinson, K. Sano, L. Schröder, "Coalgebraic predicate logic," in Proc. of the 39th Int'l Colloquium on Automata, Languages and Programming (ICALP'12) – Volume II, pp. 299–311, Springer, LNCS, Vol. 7392, 2012.
URL http://dx.doi.org/10.1007/978-3-642-31585-5_29

In our ICALP 2012 paper, Dirk Pattinson, Katsuhiko Sano, Lutz Schröder and myself proposed the Coalgebraic Predicate Logic (CPL) – a one-sorted language for ordinary first-order models enriched with a coalgebraic structure. In the neighbourhood setting, a notational variant of this formalism has been first investigated by C. C. Chang in early 1970's as a "logic for social situations" or as a simplification of Montague's "pragmatics". Later on, its restriction to topological spaces has been rediscovered as a relatively weak language for topological model theory (Ziegler, Makowsky, Flum, Sgro ...) but remained largely unknown or forgotten elsewhere.

Our generalization to arbitrary Set-coalgebras has been based, as may be expected, on the notion of predicate lifting; a variant of the language based on Moss' nabla would also be conceiveable. There are also other, more expressive possible choices: one of them found in FoSSaCS 2010 paper of Schroeder and Pattinson. These more expressive variants require at least a sort for neighbourhoods, possibly also a sort for elements of the transition structure and more involved syntax in general. Furthermore, it is not clear at all whether some of our positive results, such as natural Henkin-style axiomatization or (in a follow-up paper) syntactic proofs of cut-elimination for restricted classes of functors and predicate liftings could be found for too powerful extensions of CPL. Nevertheless, let us not forget that, e.g. first-order formalisms employed in topological model theory are usually stronger than CPL (restricted to topological spaces as a subclass of coalgebras for the neighbourhood functor).

There are also more radically different "coalgebraic predicate languages". Under a sufficiently broad understanding of the notion, one can even include here Jacobs' recent work on predicate formalism for the Kleisli category of a monad. Its relationship to either the formalism of FoSSaCS 2010 or to the one of ICALP 2012 seems an open question to everybody involved; similarly with other formalisms used in categorical logic.

So with all this, what – if any – is the "right" coalgebraic predicate formalism? And more importantly, what sort of results and applications one would expect from such a beast? Does not the very idea of formalism not invariant under bisimulation or behavioural equivalence

go against the main thrust of research in coalgebraic logic? In short: where is coalgebraic predicate logic going and should it go anywhere at all?

These are serious questions, worthy of a public debate. I am convinced that a genuine discussion session on the subject would be more beneficial to us and to the community than one more talk advertising the results of the ICALP 2012 paper and its follow-up.

Our (that is, at least that of Lutz Schroeder and myself) personal belief is that the most fruitful line of research may lie in investigating further the connection with finite model theory and preservation results. We already have suitable variants of the Van Benthem-Rosen theorem for several flavors of coalgebraic predicate formalisms. A natural next step is to attack the only other existing major preservation result surviving in the finite model theory context: invariance of existential-positive formulas under homomorphism (see Rossman in LiCS 2005 and ACM 2008). The key to robustness of these two results seems to be lie in the fact that their proofs rely heavily on notions such as Gaifman graphs – and so does the coalgebraic Van Benthem-Rosen theorem (at least in the FoSSaCS 2010 paper). There seems to be a tantalizing slogan lurking in the background that "preservation results survive in the finite model theory context iff they survive in the coalgebraic context" and its full implications are yet to be understood. The bigger challenge here is developing finite model theory (or "metafinite model theory", as in the paper of Gradel and Gurevich) for non-relational structures.

Yde Venema and the Amsterdam group have already done some work on the generalization of another preservation and characterization result – the Janin-Walukiewicz theorem (which is itself a generalization of the van Benthem-Rosen to the second-order case). All this should lead to a more complete version of "abstract coalgebraic model theory". So far, for example, the only existing coalgebraic variants of the Lindstroem theorem focused on the modal propositional language. Clearly, it is not what the original Lindstroem theorem was about. But what is the right notion of E-F games in the coalgebraic case? We do in fact have E-F games for CPL (developed with Lutz Schroeder, yet unpublished) – are they likely to be of general interest? Are there some unexpected potential applications?

3.15 On the specification of operations on the rational behaviour of systems

Stefan Milius (TU Braunschweig, DE)

Joint work of Bonsangue, Marcello; Milius, Stefan; Myers, Rob; Rot, Jurriaan
Main reference M.M. Bonsangue, S. Milius, J. Rot, "On the specification of operations on the rational behaviour of systems," in Proc. of EXPRESS/SOS 2012. Electron. Proc. Theoret. Comput. Sci. 89 (2012), 3–18.
URL http://dx.doi.org/10.4204/EPTCS.89.2

Structural operational semantics can be studied at the general level of distributive laws of syntax over behaviour. This yields specification formats for well-behaved algebraic operations on final coalgebras, which are a domain for the behaviour of all systems of a given type functor. We introduce a format for specification of algebraic operations that restrict to the *rational fixpoint* of a functor, which captures the behaviour of *finite* systems. Our format can be seen as a generalization of Aceto's simple GSOS format from process algebra to the realm of distributive laws. We show that rational behaviour is closed under operations specified in our format. As applications we consider operations on regular languages, regular processes

and finite weighted transition systems. We also obtain a generalization of Aceto's theorem stating that for a transition system specification in the simple GSOS format the associated LTS is regular.

3.16 Modal proximity lattices and modal compact Hausdorff spaces

M. Andrew Moshier (Chapman University – Orange, US)

Joint work of Moshier, M. Andrew; Nick Bezhanishvili

Thanks to a well-known completeness theorem, normal modal logic can be regarded as a specification language for non-deterministic transition systems modelled as compact, zero dimensional state spaces equipped with a coalgebra for the Vietoris functor. The zero dimensionality requirement, however, severely limits potential applications. After all, this rules out such state spaces as spheres, tori, and other garden variety compact Hausdorff spaces.

In this talk we consider how to generalize normal modal logic to account for general compact Hausdorff state spaces. The result is again a completeness theorem for the generalized normal logic. We then prove that Sahlqvist's Theorem still works in this generalization, provided we replace Sahlqvist formulae with a suitable notion of Sahlqvist inference rule.

3.17 Eilenberg's Theorem Coalgebraically

Rob Myers (TU Braunschweig, DE)

Eilenberg's theorem is one of the central theorems in algebraic automata theory. It describes an isomorphism between the lattice of varieties of finite monoids and the lattice of varieties of regular languages. Recent work by Gehrke, Grigorieff and Pin has shown this theorem arises locally as a duality. Our contribution is that this duality is inherently coalgebraic, to the extent that the entire theorem can be proved using canonical constructions. Since our approach is parametric in a functor we obtain many new theorems and unify much previous work. For example we not only cover the version involving ordered monoids and idempotent semirings, but we also obtain new examples involving associative algebras and modules.

3.18 The Generic Kleene Theorem

Rob Myers (TU Braunschweig, DE)

Kleene theorems are usually proved relative to particular operations satisfying particular equations. The message of this talk is that one can prove them parametric in an arbitrary finitary functor on an arbitrary finitary variety. We justify this by providing many examples

such as boolean automata, subsequential transducers, context free grammars and linear automata over arbitrary semirings. We also discuss an ongoing application of this approach, namely the first definition of the minimal nondeterministic automaton accepting a regular language.

3.19 Monoidal computer and coalgebras

Dusko Pavlovic (RHUL – London, GB)

Main reference D. Pavlovic, "Monoidal computer I: Basic computability by string diagrams," arXiv:1208.5205v2 [cs.LO].
URL http://arxiv.org/abs/1208.5205v2

Church's Thesis is great, but low level programming of Turing Machines, and of lambda terms, makes the bridge between theoretical computer science and practice often longer than one would expect. E.g., the task of measuring the logical distance between algorithms (which I recently put forward in "Gaming security by obscurity" – http://arxiv.org/abs/1109.5542) quickly leads to unreasonably verbose low level programming. To overcome this, we need a high level language for complexity theory, algorithmic information, and cryptorgraphic constructions. The structure of monoidal computer is an effort to formalize the diagrammatic language that I have been using for this purpose informally. The first step is in the uploaded paper. Modeling protocols and Interactive Proof Systems in monoidal computer naturally leads to coalgebras, which will be elaborated in a sequel paper.

3.20 Nominal coalgebriac data types

Daniela Petrisan (University of Leicester, GB)

Pitts and Gabbay proved structural recursion and induction principles for syntax with binding and further introduced nominal algebraic data types. This talk is about nominal coalgebraic data types. In particular we will discuss final coalgebras for functors obtained from a binding signature. Applications include an alpha-corecursion principle for the infinitary lambda calculus and corecursive definitions of infinite normal forms. This talk is based on joint work with Alexander Kurz, Paula Severi and Fer-Jan de Vries.

3.21 Actuality in Coalgebraic Modal Logic

Katsuhiko Sano (JAIST – Nomi, JP)

This talk reports a current ongoing work on coalgebraic modal logic with the actuality operator, originally invented by Kamp and Kaplan. Semantically, the addition of the actuality operator to coalgebraic modal logic corresponds to an addition of an initial state

to a given coalgebra (i.e., pointed coalgebra). First, we observe that this addition of the actuality operator still does not increase the expressive power with respect to truth at the initial state. This is done by a generalization of a recent study on the actuality operator in Kripke and neighborhood semantics by Hazen, Rin, and Wehmeier. Second, we demonstrate how to convert a sequent calculus of coalgebraic modal logic into the one with the actuality operator. For this aim, we employ the framework of sequent calculus by Pattinson and Schröeder (2011).

References

1 Hazen, A., Rin, B., and Wehmeier, K. 'Actuality in Propositional Modal Logic', *Studia Logica*, Online First, 2012. Pattinson, D. and Schröder, L. "Generic Modal Cut Elimination Applied to Conditional Logics," *Logical Methods in Computer Science*, Vol.7, pp.1-28, 2011.

3.22 Coalgebraic Logic and Self-Reference

Lutz Schroeder (Universität Erlangen-Nürnberg, DE)

Decidability of modal logics tends to break down quickly when features for self-reference are added, such as the down-arrow binder of hybrid logic, or its single-variable version popularized by Marx as the I-me construct. We have shown in earlier work that decidability (and in fact low complexity) of logics with I-me is regained if the number of modal operators between between each use of me and its enclosing I is bounded by two; these results are stable under adding graded modalities . Here, we report on ongoing work aimed at a coalgebraic generalization of the algorithmic principles involved, in particular a PSPACE upper bound for local reasoning.

References

1 D. Gorín and L. Schröder. Extending ALCQ with bounded self-reference. In S. Ghilardi and L. Moss, eds., *Proc. Advances in Modal Logic 2012, AiML 2012*. College Publications, 2012.

2 D. Gorín and L. Schröder. Narcissists are easy, stepmothers are hard. In *Foundations of Software Science and Computation Structures, FoSSaCS 2012*, vol. 7213 of *LNCS*, pp. 240–254. Springer, 2012.

3.23 Brzozowski's algorithm (co)algebraically

Alexandra Silva (Radboud University Nijmegen, NL)

Joint work of Bonchi, Filippo; Bonsangue, Marcello; Hansen, Helle; Panangaden, Prakash; Rutten, Jan; Silva, Alexandra
Main reference F. Bonchi, M.M. Bonsangue, J.J.M.M. Rutten, A. Silva, "Brzozowski?s Algorithm (Co)Algebraically," in R.L. Constable, A. Silva, (eds), Logic and Program Semantics – Essays Dedicated to Dexter Kozen on the Occasion of His 60th Birthday, LNCS, Vol. 7230, pp. 12–23, 2012.
URL http://dx.doi.org/10.1007/978-3-642-29485-3_2

We give a new presentation of Brzozowski's algorithm to minimize finite automata, using elementary facts from universal algebra and coalgebra, and building on earlier work by Arbib and Manes on the duality between reachability and observability. This leads to a simple proof of its correctness and opens the door to further generalizations. Notably, we derive algorithms to obtain minimal, language equivalent automata from Moore, non-deterministic and weighted automata.

3.24 Congruences of Convex Algebras

Ana Sokolova (Universität Salzburg, AT)

Joint work of Sokolova, Ana; Woracek, Harald
Main reference A. Sokolova, H. Woracek, "Congruences of convex algebras," ASC report 39/2012, TU Vienna.
URL http://www.asc.tuwien.ac.at/preprint/2012/asc39x2012.pdf

We provide a full description of congruence relations of convex, positive convex, and totally convex algebras. As a consequence of this result we obtain that finitely generated convex (positive convex, totally convex) algebras are finitely presentable. Convex algebras, in particular positive convex algebras, are important in the area of probabilistic systems. They are the Eilenberg-Moore algebras of the subdistribution monad.

3.25 Universal properties of finite powersets

Sam Staton (University of Cambridge, GB)

I discussed the two different universal properties of finite powerset functors.

The first universal property is finite powersets that they classify maps that are fibrewise finite, in the sense that to give a function $X \to P(Y)$ is to give a relation $R \subseteq X \times Y$ whose left leg is fibrewise finite. This universal property is similar to the characterization of the Vietoris functor on Stone spaces as the classifier of open maps. One can use this universal property to prove properties of powerset-like functors in an axiomatic way.

The second universal property is that the finite powerset is a free semilattice. This enables us to define maps $X \to P(Y)$ using Moggi's monadic metalanguage. We can get variations on the powerset by varying the algebraic theory. I demonstrated this with a new powerset

functor on a presheaf category which is useful for the operational semantics of programs with free variables.

3.26 Bisimilarity is not Borel

Pedro Sanchez Terraf (Universidad Nacional de Córdoba, AR)

Main reference P. Sánchez Terraf, "Bisimilarity is not Borel," arXiv:1211.0967v1 [math.LO].
URL http://arxiv.org/abs/1211.0967v1

In this work in progress, we prove that the relation of bisimilarity between countable labelled transition systems is not Borel, by reducing bounded classes of countable wellorders continuously to it.

This has an impact on the theory of probabilistic and nondeterministic processes over uncountable spaces, since the proofs of logical characterizations of bisimilarity based on the unique structure theorem for analytic spaces require a countable logic whose formulas have measurable semantics. Our reduction shows that such a logic does not exist in the case of image-infinite process.

References

1 P. Celayes, "Procesos de Markov Etiquetados sobre Espacios de Borel Estándar", Master's thesis, FaMAF, Universidad Nacional de Córdoba (2006).
2 V. Danos, J. Desharnais, F. Laviolette, P. Panangaden, Bisimulation and cocongruence for probabilistic systems, *Inf. Comput.* **204**: 503–523 (2006).
3 P. D'Argenio, N. Wolovick, P. Sánchez Terraf, P. Celayes, Nondeterministic labeled Markov processes: Bisimulations and logical characterization, in: QEST, IEEE Computer Society: 11–20 (2009).
4 P.R. D'Argenio, P. Sánchez Terraf, N. Wolovick, Bisimulations for nondeterministic labelled Markov processes, *Mathematical. Structures in Comp. Sci.* **22**: 43–68 (2012).
5 J. Desharnais, "Labeled Markov Process", Ph.D. thesis, McGill University (1999).
6 J. Desharnais, A. Edalat, P. Panangaden, Bisimulation for labelled Markov processes, *Inf. Comput.* **179**: 163–193 (2002).
7 J. Desharnais, F. Laviolette, A. Turgeon, A logical duality for underspecified probabilistic systems, *Inf. Comput.* **209**: 850–871 (2011).
8 E.E. Doberkat, Semi-pullbacks and bisimulations in categories of stochastic relations, in: ICALP'03: Proceedings of the 30th international conference on Automata, languages and programming, Springer-Verlag, Berlin, Heidelberg: 996–1007 (2003).
9 D. Janin, I. Walukiewicz, On the expressive completeness of the propositional mu-calculus with respect to monadic second order logic, in: U. Montanari, V. Sassone (Eds.), CONCUR, Lecture Notes in Computer Science **1119**, Springer: 263–277 (1996).
10 A.S. Kechris, "Classical Descriptive Set Theory", Graduate Texts in Mathematics **156**, Springer-Verlag (1994).
11 K.G. Larsen, A. Skou, Bisimulation through probabilistic testing, *Inf. Comput.* **94**: 1–28 (1991).
12 D. Scott, Invariant Borel sets, *Fund. Math.* **56**: 117–128 (1964).
13 J. Stern, Évaluation du rang de Borel de certains ensembles, *C. R. Acad. Sci. Paris* **286**: A855–857 (1978).

14 N. Wolovick, "Continuous Probability and Nondeterminism in Labeled Transition Systems", Ph.D. thesis, Universidad Nacional de Córdoba (2012).

3.27 Systematic Construction of Temporal Logics for Dynamical Systems via Coalgebra

Baltasar Trancon y Widemann (Universität Bayreuth, DE)

Joint work of Trancon y Widemann, Baltasar; Hauhs, Michael

Temporal logics are an obvious high-level descriptive companion formalism to dynamical systems which model behaviour as deterministic evolution of state over time. A wide variety of distinct temporal logics applicable to dynamical systems exists, and each candidate has its own pragmatic justification. Here, a systematic approach to the construction of temporal logics for dynamical systems is proposed: Firstly, it is noted that dynamical systems can be seen as coalgebras in various ways. Secondly, a straightforward standard construction of modal logics out of coalgebras, namely Moss's coalgebraic logic, is applied. Lastly, the resulting systems are characterized with respect to the temporal properties they express.

3.28 Two Finitary Functors

Henning Urbat (TU Braunschweig, DE)

The Hausdorff and the Kantorovich functor are widely used to model (probabilistic) nondeterminism from a coalgebraic perspective. We show that both functors are finitary, improving on previous work by van Breugel et. al. In fact, we derive our result from the general observation that all equationally defined free monads are finitary, provided that the underlying category is well-behaved with respect to filtered colimits.

3.29 Regularity and exactness of quasivarieties and varieties of ordered algebras

Jiri Velebil (Czech Technical University, CZ)

Joint work of Kurz, Alexander; Velebil, Jiri

Ordered algebras are algebras for a signature consisting of n-ary operations (n a cardinal) that are interpreted as monotone operations on a poset. Homomorphisms of such algebras are monotone maps preserving the specified operations.

We characterise quasivarieties and varieties of ordered algebras intrinsically. Our characterisation has the same form as in ordinary universal algebra over sets. Namely, we prove the following result:

Theorem: For a category A, the following are equivalent: (i) A is equivalent to a quasivariety (variety, resp.) of ordered algebras. (ii) A is a "regular" ("exact", resp.) category, and there exists an object P such that (a) P has "copowers". (b) P is a "presentable object". (c) P is a "regular projective", "regular generator".

The notions in the theorem above that are in quotes are to be interpreted as notions that are appropriate for category theory enriched over posets. For example, the notion of regularity and exactness of a category enriched in posets is the (suitably modified) notion due to Ross Street .

As an example, the enriched category of posets and monotone maps is an exact category in the above sense (as opposed to an ordinary category of posets: this ordinary category is not even regular in the sense of Michael Barr).

We exemplify the above notions on various examples and we give connections to the categorical notion of monadicity.

Acknowledgement: Jiri Velebil is supported by the grant no. P202/11/1632 of the Czech Science Foundation.

References

1 Michael Barr, Exact categories, in: Exact categories and categories of sheaves, LNM 236, Springer, 1971, 1–120

2 Ross Street, Two-dimensional sheaf theory, J. Pure Appl. Algebra 24 (1982), 251–270

3.30 Automatic sequences as context-free systems.

Joost Winter (CWI – Amsterdam, NL)

Main reference M.M. Bonsangue, J. Rutten, J. Winter, "Defining Context-Free Power Series Coalgebraically," in CMCS 2012: pp. 20–39.

URL http://homepages.cwi.nl/~winter/articles/cmcs12.pdf

We recall some basic results of the coalgebraic approach to the theory of formal languages. We show that all q-automatic sequences are in the class of $\mathbb{F}_q$ context-free streams, and provide a construction of the Thue-Morse sequence as a context-free stream.

Participants

- Samson Abramsky
University of Oxford, GB
- Octavian Vladut Babus
University of Leicester, GB
- Jort Bergfeld
University of Amsterdam, NL
- Marta Bilkova
Charles University – Prague, CZ
- Marcello M. Bonsangue
Leiden University, NL
- Liang-Ting Chen
University of Birmingham, GB
- Vincenzo Ciancia
CNR – Pisa, IT
- Corina Cirstea
University of Southampton, GB
- Josée Desharnais
Université Laval – Québec, CA
- Ernst-Erich Doberkat
TU Dortmund, DE
- Matej Dostal
Czech Technical University, CZ
- Norman Francis Ferns
McGill Univ. – Montreal, CA
- H. Peter Gumm
Universität Marburg, DE
- Helle Hvid Hansen
Radboud Univ. Nijmegen, NL
- Ichiro Hasuo
University of Tokyo, JP
- Dirk Hofmann
University of Aveiro, PT
- Bart Jacobs
Radboud Univ. Nijmegen, NL
- Achim Jung
University of Birmingham, GB
- Klaus Keimel
TU Darmstadt, DE
- Dexter Kozen
Cornell University – Ithaca, US
- Clemens Kupke
University of Oxford, GB
- Alexander Kurz
University of Leicester, GB
- Paul Blain Levy
University of Birmingham, GB
- Tadeusz Litak
Univ. Erlangen-Nürnberg, DE
- Stefan Milius
TU Braunschweig, DE
- M. Andrew Moshier
Chapman Univ. – Orange, US
- Rob Myers
TU Braunschweig, DE
- Alessandra Palmigiano
University of Amsterdam, NL
- Prakash Panangaden
McGill Univ. – Montreal, CA
- Dusko Pavlovic
RHUL – London, GB
- Daniela Petrisan
University of Leicester, GB
- Katsuhiko Sano
JAIST – Nomi, JP
- Lutz Schröder
Univ. Erlangen-Nürnberg, DE
- Alexandra Silva
Radboud Univ. Nijmegen, NL
- Ana Sokolova
Universität Salzburg, AT
- Shashi M. Srivastava
Indian Statistical Institute – Kolkata, IN
- Sam Staton
University of Cambridge, GB
- Pedro Sánchez Terraf
Universidad Nacional de Córdoba, AR
- Baltasar Trancón y Widemann
Universität Bayreuth, DE
- Henning Urbat
TU Braunschweig, DE
- Jiri Velebil
Czech Technical University, CZ
- Yde Venema
University of Amsterdam, NL
- Joost Winter
CWI – Amsterdam, NL
- Chunlai Zhou
Renmin University of China – Beijing, CN

Report from Dagstuhl Seminar 12421

Algebraic and Combinatorial Methods in Computational Complexity

Edited by

Manindra Agrawal[1], Thomas Thierauf[2], and Christopher Umans[3]

1 **Indian Inst. of Technology – Kanpur, IN,** manindra@iitk.ac.in
2 **Hochschule Aalen, DE,** Thomas.thierauf@HTW-Aalen.de
3 **CalTech – Pasadena, US,** umans@cs.caltech.edu

Abstract

At its core, much of Computational Complexity is concerned with combinatorial objects and structures. But it has often proven true that the best way to prove things about these combinatorial objects is by establishing a connection (perhaps approximate) to a more well-behaved algebraic setting. Indeed, many of the deepest and most powerful results in Computational Complexity rely on algebraic proof techniques. The PCP characterization of NP and the Agrawal-Kayal-Saxena polynomial-time primality test are two prominent examples.

Recently, there have been some works going in the opposite direction, giving alternative combinatorial proofs for results that were originally proved algebraically. These alternative proofs can yield important improvements because they are closer to the underlying problems and avoid the losses in passing to the algebraic setting. A prominent example is Dinur's proof of the PCP Theorem via gap amplification which yielded short PCPs with only a polylogarithmic length blowup (which had been the focus of significant research effort up to that point). We see here (and in a number of recent works) an exciting interplay between algebraic and combinatorial techniques.

This seminar aims to capitalize on recent progress and bring together researchers who are using a diverse array of algebraic and combinatorial methods in a variety of settings.

Seminar 14.–19. October, 2012 – www.dagstuhl.de/12421
1998 ACM Subject Classification F.1.3 Complexity Measures and Classes, F.2 Ananlysis of Algorithms and Problem Complexity
Keywords and phrases Computational Complexity, lower bounds, approximazation, pseudorandomness, derandomization, circuits
Digital Object Identifier 10.4230/DagRep.2.10.60
Edited in cooperation with Thomas Thierauf

1 Executive Summary

Manindra Agrawal
Thomas Thierauf
Christopher Umans

The seminar brought together more than 50 researchers covering a wide spectrum of complexity theory. The focus on algebraic and combinatorial methods showed the great importance of such techniques for theoretical computer science. We had 30 talks, most of them lasting

about 40 minutes, leaving ample room for discussions. In the following we describe the major topics of discussion in more detail.

Circuit Complexity

is an area of fundamental importance to Complexity, which has resisted all efforts to prove strong lower bounds. We had several talks on circuit upper and lower bounds.

Valentine Kabanets considered the following compression problem: Given a truth table of an n-variate Boolean function f, find a Boolean circuit C of non-trivial size (less than $2^n/n$) that computes f. The motivation comes from the desire to understand "easy" functions (what property of their truth tables makes such functions compressible), and "hard" functions (once we understand which functions are compressible, we may be able to prove certain functions to require high circuit complexity). As an example, he showed that the class of functions computable by polysize AC^0-circuits, and linear-size de Morgan formulas are compressible.

The Shub and Smale's "tau-conjecture" states that the number of integer roots of a univariate polynomial should be polynomially bounded in the size of the smallest straight-line program computing it. Pascal Koiran proposed a real version of the tau-conjecture in his talk. If this new conjecture is true, then the permanent polynomial cannot be computed by polynomial-size arithmetic circuits.

Fred Green showed that degree-d block-symmetric multivariate polynomials modulo any odd p correlate with parity exponentially better than degree-d symmetric polynomials, for certain values of d. The result is obtained through the development of a theory call spectral analysis of symmetric correlation, which originated in work of Cai, Green, and Thierauf.

Chaudhuri and Radhakrishnan used certifying polynomials to show that Approximate Majority cannot be computed by AC^0-circuits of size $n^{1+o(1)}$. In his talk, Swastik Kopparty extended their technique and showed that Approximate Majority cannot be computed by AC^0[parity]-circuits of size $n^{1+o(1)}$. This implies a separation between the power of AC^0[parity]-circuits of near-linear size and uniform AC^0[parity]-circuits of polynomial size.

Neeraj Kayal talked on the problem of computing the smallest formula for a polynomial given as a blackbox. The complexity of this problem is still unclear. It is conjectured that it is NP-hard. Neeraj presented his very impressive result, a randomized algorithm that given blackbox access to the polynomial f computed by an unknown/hidden arithmetic formula reconstructs, on the average, an equivalent or smaller formula in time polynomial in the size of its output . This is the strongest model of arithmetic computation for which a reconstruction algorithm is presently known, albeit efficient in a distributional sense rather than in the worst case.

Coding Theory

Error-correcting codes, particularly those constructed from polynomials, lie at the heart of many of the most significant results in Computational Complexity (e.g. interactive proofs, PCPS, hardness amplification, explicit constructions, derandomization, etc.) In many of these applications it is evident that the *local-testability/decodability* of the code is critical.

A q-query Locally Decodable Code (LDC) is an error-correcting code that allows to read any particular symbol of the message by reading only q symbols of the codeword. In a completely new approach, Klim Efremenko showed how to construct q-query LDCs from representation theory. Parikshit Gopalan showed an equivalence between locally testable codes and Cayley graphs with certain spectral properties. These Cayley graphs can be viewed

as "derandomized hypercubes" which preserve several important properties of the Boolean hypercube such as small-set expansion, large threshold rank and hypercontractivity.

Shubhangi Saraf talked about the classical theorem of Sylvester-Gallai, which says that, if for every two points there is a third point on the line through them, then all points are on the same line. In the stable versions of the theorem, it is only guaranteed that many triples of points are approximately collinear. Configurations with many approximately collinear q-tuples of points also arise naturally in stable versions of Locally Correctable Codes over the complex numbers. She showed that that such stable codes with constant query complexity do not exist.

Explicit Constructions

Until recently the best-known construction of extractors (and their cousins, *condensers*) was a primarily combinatorial construction of Lu, Reingold, Vadhan, and Wigderson. Then Guruswami, Umans and Vadhan gave an entirely algebraic construction, utilizing the new polynomial error-correcting codes of Parvaresh and Vardy. Amnon Ta-Shma presented a new construction of condensers based on Parvaresh-Vardy codes. Amnons condensers have entropy rate $1 - \alpha$ for subconstant α (in contrast to GUV which required constant α) and suffer only sublinear entropy loss.

Ronen Shaltiel presented new constructions of zero-error seedless dispersers for bit-fixing sources and affine sources. Ronen used these dispersers to construct an algorithm for a problem related to the Write-Once-Memory (WOM) problem in which once we raise a storage cell from zero to one, it is stuck at this value. He gives the first explicit scheme with asymptotically optimal rate.

Anna Gál identified a new class of superconcentrator-like graphs with connectivity properties distinct from previously studied ones. Anna showed that any circuit computing good codes must satisfy such superconcentrator-like properties.

Probabilistic proof systems is a sub-field of complexity theory that investigates questions such as "how can we use randomness to prove and verify assertions?", "what do we gain from using randomness in verification procedures?", and "what assertions can be verified by probabilistic verification procedures?". Research in this area began in the 1980, and has led to several of the most important achievements of complexity theory in those decades.

A line of research from the recent years is aimed at finding alternative "combinatorial" proofs for those key results, i.e., proofs that do not rely on algebra. This line of research is motivated by trying to gain more intuition of those results, as well as to understand the properties of polynomials that make them useful for such constructions. Or Meir gave a very interesting survey talk about this line of research.

Complexity

In a much appreciated talk, Joshua Grochow gave a very interesting survey-type talk on the Geometric Complexity Theory (GCT) program, which was introduced by Mulmuley and Sohoni to attack fundamental lower bound problems in complexity – such as P vs NP – using algebraic geometry and representation theory. Joshua succeeded in explaining very nicely some of the intuition behind the use of algebraic geometry and representation theory in complexity.

Michal Koucký gave a very interesting overview talk on the online labeling problem, where one receives n integers from the set $\{1, \ldots, r\}$ and has to store them in an array of size m. The integers are presented sequentially in an arbitrary order, and must be stored

in the array in sorted order. The complexity measure is essentially the number of times an element has to be moved in to make space for a newly arrived item. Michal showed that various known algorithms in the literature solve the problem asymptotically optimal.

Perfect matching is in P but not known to be in NC. Counting the number of perfect matchings in a graph is #P-complete. In contrast, Vazirani showed that counting the number of perfect matchings in a planar graph is in NC. So in particular, the decision version of perfect matching in planar graphs is in NC. Hence one way to get perfect matching in NC could be to reduce perfect matching to perfect matching in planar graphs. An obvious approach to construct such a reduction is to come up with a *planarizing gadget*. Jochen Messner proved in his talk unconditionally that such a reduction is not possible for the perfect matching problem.

Steve Fenner considered the following two-player game on a finite partially odered set (poset) S: each player takes turns picking an element x of S and removes all $y?x$ from S. The first one to empty the poset wins. Recently, Daniel Grier, an undergrad at the University of South Carolina, has settled the problem and showed that determining the winner of a poset game is PSPACE-complete. The reduction shows, that the game is already PSPACE-complete when the poset has only 3 levels. The complexity of two-level poset games is still open. Steve presented a simple formula allowing one to compute the status for a large class of of two-level poset game.

Conclusion

As is evident from the list above, the talks ranged over a broad assortment of subjects with the underlying theme of using algebraic and combinatorial techniques. It was a very fruitful meeting and has hopefully initiated new directions in research. Several participants specifically mentioned that they appreciated the particular focus on a common class of *techniques* (rather than end results) as a unifying theme of the workshop. We look forward to our next meeting!

2 Table of Contents

3 Overview of Talks

3.1 Noncommutativity makes determinants hard

Markus Bläser (Universität des Saarlandes, DE)

We consider the complexity of computing the determinant over arbitrary finite-dimensional algebras. We first consider the case that A is fixed. We obtain the following dichotomy: If $A/\operatorname{rad} A$ is noncommutative, then computing the determinant over A is hard. "Hard" here means $\#P$-hard over fields of characteristic 0 and $ModP_p$-hard over fields of characteristic $p > 0$. If $A/\operatorname{rad} A$ is commutative and the underlying field is perfect, then we can compute the determinant over A in polynomial time.

We also consider the case when A is part of the input. Here the hardness is closely related to the nilpotency index of the commutator ideal of A. The commutator ideal $operatornamecom(A)$ of A is the ideal generated by all elements of the form $xy - yx$ with $x, y \in A$. We prove that if the nilpotency index of $operatornamecom(A)$ is linear in n, where $n \times n$ is the format of the given matrix, then computing the determinant is hard. On the other hand, we show the following upper bound: Assume that there is an algebra $B \subseteq A$ with $B = A/\operatorname{rad}(A)$. (If the underlying field is perfect, then this is always true.) The center $Z(A)$ of A is the set of all elements that commute with all other elements. It is a commutative subalgebra. We call an ideal J a complete ideal of noncommuting elements if $B + Z(A) + J = A$. If there is such a J with nilpotency index $o(n/\log n)$, then we can compute the determinant in subexponential time. Therefore, the determinant cannot be hard in this case, assuming the counting version of the exponential time hypothesis.

3.2 Limits of provable security for homomorphic encryptions

Andrej Bogdanov (Chinese University of Hong Kong, HK)

Joint work of Bogdanov, Andrej; Lee, Chin Ho
Main reference unpublished manuscript

We show that public-key bit encryption schemes that support weak homomorphic evaluation of parity (or majority) cannot be proved message indistinguishable beyond AM intersect coAM via general (adaptive) reductions, and beyond statistical zero-knowledge via reductions of constant query complexity.

Previous works on the limitation of reductions for proving security of encryption schemes make restrictive assumptions about the encryption algorithm (Brassard, Goldreich and Goldwasser, Akavia et al.) or about the reduction (Feigenbaum and Fortnow, Bogdanov and Trevisan, Akavia et al.) Our first result makes no assumptions of either sort.

Towards these results, we show that any homomorphic evaluator for parity or majority over sufficiently many inputs can be used to obtain statistical rerandomization of ciphertexts.

3.3 Testing of Boolean Function Isomorphism

Sourav Chakraborty (Chennai Mathematical Institute, IN)

Testing Isomorphism among various objects is a very important problem is Computer Science. We consider the problem of testing whether two given functions are isomorphic under permutation of the inputs. It is one of the most well studied problem in Property Testing and in the past couple of year we have made significant progress in understanding the problem. We know various classes of functions for which testing isomorphism can be done by looking at only a constant number of bits of the truth table. These new understanding on this problem also helps in testing of other function properties.

3.4 Regular Languages are Church-Rosser Congruential

Volker Diekert (Universität Stuttgart, DE)

Joint work of Diekert, Volker; Kufleitner, Manfred; Reinhardt, Klaus; Walter, Tobias
Main reference V. Diekert, M. Kufleitner, K. Reinhardt, T. Walter, "Regular Languages are Church-Rosser Congruential," arXiv:1202.1148v1 [cs.FL]; Proc. ICALP 2012, Warwick, UK, LNCS 7392, pp. 275–286, 2012.
URL http://arxiv.org/abs/1202.1148
URL http://dx.doi.org/10.1007/978-3-642-31585-5_19

I report on the solution to a long standing conjecture in formal language theory. It states that all regular languages are Church-Rosser congruential. The class of Church-Rosser congruential languages was introduced by McNaughton, Narendran, and Otto in 1988. A language L is Church-Rosser congruential, if there exists a finite confluent, and length-reducing semi-Thue system S such that L is a finite union of congruence classes modulo S. It was known that there are deterministic linear context-free languages which are not Church-Rosser congruential, but on the other hand it was strongly believed that all regular language are of this form.

The key step for the solution has been an algebraic proof for more general result about finite semigroups.

The talk is based on a joint paper with Manfred Kufleitner, Klaus Reinhardt, and Tobias Walter which was presented at ICALP 2012 (Best paper award, Track B).

3.5 From Irreducible Representations to Locally Decodable Codes

Klim Efremenko (Tel Aviv University, IL)

Main reference From Irreducible Representations to Locally Decodable Codes

Locally Decodable Code (LDC) is a code that encodes a message in a way that one can decode any particular symbol of the message by reading only a constant number of locations, even if a constant fraction of the encoded message is adversarially corrupted.

In this paper we present a new approach for the construction of LDCs. We show that if there exists an irreducible representation (ρ, V) of G and q elements $g_1, g_2, \ldots, g_q$ in G

such that there exists a linear combination of matrices $\rho(g_i)$ that is of rank one, then we can construct a q-query Locally Decodable Code $C: V \to F^G$.

We show the potential of this approach by constructing constant query LDCs of sub-exponential length matching the parameters of the best known constructions.

3.6 Two-level poset games

Stephen A. Fenner (University of South Carolina, US)

We consider the complexity of determining the winner of a game played on a finite two-level partially ordered set . This is a natural question, as it has been shown recently that determining the winner of a finite three-level poset game is PSPACE-complete. We give a simple formula allowing one to compute the status of a type of two-level poset game that we call, "parity-uniform." This class includes significantly more easily solvable two-level games than was known previously. We also establish general equivalences between various two-level games. This implies that for any n, only finitely many two-level posets with n minimal elements need be considered. We show a similar result for posets with n maximal elements.

3.7 Error-correcting codes vs. superconcentrator graphs

Anna Gál (University of Texas at Austin, US)

Joint work of Gál, Anna; Hansen, Kristoffer; Koucký, Michal; Pudlák, Pavel; Viola, Emanuele
Main reference A. Gál, K.A. Hansen, M. Koucký, P. Pudlák, E. Viola, "Tight bounds on computing error-correcting codes by bounded-depth circuits with arbitrary gates," STOC 2012: 479–494
URL http://dx.doi.org/10.1145/2213977.2214023

We prove tight bounds on the number of wires in constant depth (unbounded fan-in) circuits computing asymptotically good error-correcting codes. We show that quasilinear number of wires is sufficient for computing good codes already in depth 2 circuits with parity gates. This implies that a (necessarily dense) generator matrix for the code can be written as the product of two sparse matrices. For depth 2, our $\Omega(n(\log n/\log\log n)^2)$ lower bound gives the largest known lower bound for computing any linear map.

Furthermore, we identify a new class of superconcentrator-like graphs with connectivity properties distinct from previously studied ones. We show that any circuit computing good codes must satisfy such superconcentrator-like properties.

3.8 The Complexity of Grid Problems

William Gasarch (University of Maryland – College Park, US)

Joint work of Gasarch, William; Lawler, Kevin

A c-coloring of an $n \times m$ grid is a mapping of $n \times m$ into $\{1, \ldots, c\}$ such that no four corners forming a rectangle have the same color. Consider the following problem: Given a partial c-coloring of an $n \times m$ grid, can it be extended to a full c-coloring? We show that this problem is NP-complete. We discuss algorithms for fixed c. We also phrase the statement "$n \times m$ is c-colorable' as a propositional formlua and show that, when its fails, any tree resolution proof of it takes size exponential in c.

3.9 Locally testable codes and Cayley graphs

Parikshit Gopalan (Microsoft Research – Mountain View, US)

Joint work of Gopalan, Parikshit; Boaz Barak; Johan Hastad; Raghu Meka; Prasad Raghavendra; David Steurer; Salil Vadhan; Yuan Zhou

We show an equivalence between locally testable codes and Cayley graphs with certain spectral properties. These Cayley graphs can be viewed as "derandomized hypercubes" which preserve several important properties of the Boolean hypercube such as small-set expansion and hypercontractivity.

3.10 Block-Symmetric Polynomials Correlate with Parity Better than Symmetric

Frederic Green (Clark University – Worcester, US)

Joint work of Green, Frederic; Kreymer, Daniel; Viola, Emenuele

We show that degree-d block-symmetric polynomials in n variables modulo any odd p correlate with parity exponentially better than degree-d symmetric polynomials, if $n > d^3$ and $0.98p^t <= d < p^t$ for some $t >= c$ where c is some constant. For these infinitely many degrees, our result solves an open problem raised by a number of researchers including Alon and Beigel (Computational Complexity Conference 2001). The only case for which this was previously known was $d = 2$ and $p = 3$ (Green, Computational Complexity Conference 2002).

The result is obtained through the development of a theory we call spectral analysis of symmetric correlation, which originated in works of Cai, Green, and Thierauf, MST 1996. In particular, our result follows from a detailed analysis of the correlation of symmetric polynomials, which is determined up to an exponentially small relative error when $d = p^t - 1$.

We give a partial complement to these results by showing that for degree $d = p^t$, p prime, block-symmetric polynomials correlate exponentially worse than symmetric, assuming that the blocks are large enough which is the case above. Moreover we show the same holds for

every d in the case of polynomials modulo $p = 2$ vs. the Mod_3 function. In this setting we present computational evidence that symmetric polynomials may in fact be optimal.

This work builds on a study of correlation using computer search by the authors which gave unexpected results. The latter are here explained analytically. We advocate further use of computer search in complexity theory.

3.11 Introduction to Geometric Complexity Theory

Joshua A. Grochow (University of Toronto, CA)

The Geometric Complexity Theory (GCT) program was introduced by Mulmuley and Sohoni to attack fundamental lower bound problems in complexity – such as P vs NP – using algebraic geometry and representation theory. In addition to presenting the basic structure of the GCT program, I will discuss some of the intuition behind the use of algebraic geometry and representation theory in complexity. This is an expository talk; the only mathematical background presumed is a basic familiarity with group actions and polynomial rings.

3.12 Compression of Boolean functions

Valentine Kabanets (Simon Fraser University – Burnaby, CA)

We consider the following natural compression problem: Given a truth table of an n-variate Boolean function (from some class C of 'easy" functions), we want to find a Boolean circuit C of non-trivial size (less than $2^n/n$) that computes f. For lossless compression, the circuit C must compute f everywhere. For lossy compression, we allow C to approximate f. The compression algorithm must be a deterministic algorithm running in time $\mathrm{poly}(2^n)$.

The motivation comes from the desire to understand "easy" functions (what property of their truth tables makes such functions compressible), and "hard" functions (once we understand which functions are compressible, we may be able to prove certain functions to require high circuit complexity).

We show that the class of functions computable by polysize AC^0 circuits, and linear-size de Morgan formulas are compressible. This uses ideas from the Circuit-SAT algorithms for the corresponding circuit classes, which in turn use the method of random restrictions. On the negative side, we show that for any circuit class $C \subseteq \mathrm{P/poly}$, any nontrivial compression of C implies the circuit lower bounds of the form $\mathrm{NEXP} \not\subseteq C$. However, we believe that the latter implication may be used to prove existing lower bounds (e.g., $\mathrm{NEXP} \not\subseteq \mathrm{ACC}^0$ of Williams) and new lower bounds.

3.13 Random Arithmetic Formulas Can be Reconstructed Efficiently

Neeraj Kayal (Microsoft Research India – Bangalore, IN)

Joint work of Gupta, Ankit; Kayal, Neeraj; Qiao, Youming
Main reference A. Gupta, N. Kayal, Y. Qiao, "Random Arithmetic Formulas can be Reconstructed Efficiently," in Electronic Colloquium on Computational Complexity (ECCC), Report No. 33 (2012), 33 pp.
URL http://eccc.hpi-web.de/report/2012/033/

Informally stated, we present here a randomized algorithm that given blackbox access to the polynomial f computed by an unknown/hidden arithmetic formula reconstructs, on the average, an equivalent or smaller formula in time polynomial in the size of its output .

Specifically, we consider arithmetic formulas wherein the underlying tree is a complete binary tree, the leaf nodes are labelled by affine forms (i.e. degree one polynomials) over the input variables and where the internal nodes consist of alternating layers of addition and multiplication gates. We call these alternating normal form (ANF) formulas. If a polynomial f can be computed by an arithmetic formula of size s, it can also be computed by an ANF formula, possibly of slightly larger size $s^{O(1)}$. Our algorithm gets as input blackbox access to the output polynomial f (i.e. for any point x in the domain, it can query the blackbox and obtain $f(x)$ in one step) of a random ANF formula of size s (wherein the coefficients of the affine forms in the leaf nodes of are chosen independently and uniformly at random from a large enough subset of the underlying field). With high probability (over the choice of coefficients in the leaf nodes), the algorithm efficiently (i.e. in time $s^{O(1)}$) computes an ANF formula of size s computing f. This then is the strongest model of arithmetic computation for which a reconstruction algorithm is presently known, albeit efficient in a distributional sense rather than in the worst case.

3.14 A Wronskian approach to the real tau-conjecture

Pascal Koiran (ENS – Lyon, FR)

Joint work of Koiran, Pascal; Portier, Natacha; Tavenas, Sébastien
Main reference P. Koiran, N. Portier, S. Tavenas, "A Wronskian Approach to the real ?-conjecture," arXiv:1205.1015v1 [cs.CC].
URL http://arxiv.org/abs/1205.1015v1

According to the real tau-conjecture, the number of real roots of a sum of products of sparse polynomials should be polynomially bounded in the size of such an expression. It is known that this conjecture implies a superpolynomial lower bound on the arithmetic circuit complexity of the permanent. In this paper, we use the Wronksian determinant to give an upper bound on the number of real roots of sums of products of sparse polynomials. The proof technique is quite versatile; it can in particular be applied to some sparse geometric problems that do not originate from arithmetic circuit complexity. The paper should therefore be of interest to researchers from these two communities (complexity theory and sparse polynomial systems).

3.15 Certifying Polynomials for AC0(parity) circuits, with applications

Swastik Kopparty (Rutgers Univ. – Piscataway, US)

Joint work of Kopparty, Swastik; Srikanth Srinivasan

I will talk about the method of "certifying polynomials" for proving AC^0[parity] circuit lower bounds.

We use this method to show that Approximate Majority cannot be computed by AC^0[parity] circuits of size $n^{1+o(1)}$. This implies a separation between the power of AC^0[parity] circuits of near-linear size and uniform AC^0[parity] (and even AC^0) circuits of polynomial size. This also implies a separation between randomized AC^0[parity] circuits of linear size and deterministic AC^0[parity] circuits of near-linear size.

Our proof using certifying polynomials extends the deterministic restrictions technique of Chaudhuri and Radhakrishnan, who showed that Approximate Majority cannot be computed by AC^0 circuits of size $n^{1+o(1)}$. At the technical level, we show that for every AC^0[parity] circuit C of near linear size, there is a low degree variety V over F_2 such that the restriction of C to V is constant.

We also prove other results exploring various aspects of the power of certifying polynomials. In the process, we show an essentially optimal lower bound of $(\log s)^{\Omega(d)} \log(1/epsilon)$ on the degree of epsilon-approximating polynomials for AC^0[parity] circuits of size s and depth d.

3.16 An Algebraic Version of Constant Depth Complexity

Klaus-Joern Lange (Universität Tübingen, DE)

Circuit classes of constant depth are known to be equivalent to first order formulas. Less well known is the equivalent transformation of these into an algebraic framework in terms of recognition of languages by morphisms. These connections are surprisingly tight as demonstrated for example by the equivalence of linear sized circuits to two variable logics and to the algebraic restriction of being weakly blocked.

The logical-algebraic approach does not relativize and enforces polynomial size on the circuit side. The algebraic formulation seems to be the most natural one since the underlying questions (like parity not in AC^0) are of an algebraic nature.

The talk tries to demonstate how depth reduction could look like in the algebraic formulation.

3.17 NC^0 proof systems

Meena Mahajan (The Institute of Mathematical Sciences – Chennai, IN)

Joint work of Beyersdorff, Olaf; Datta, Samir; Krebs, Andreas; Mahajan, Meena; Scharfenberger-Fabian, Gido; Sreenivasaiah, Karteek; Thomas, Michael; Vollmer, Heribert
Main reference O. Beyersdorff, S. Datta, A. Krebs, M. Mahajan, G. Scharfenberger-Fabian, K. Sreenivasaiah, M.l Thomas, H. Vollmer, "Verifying Proofs in Constant Depth," in Electronic Colloquium on

Computational Complexity (ECCC), Report No. 79 (2012), 27 pp.
URL http://eccc.hpi-web.de/report/2012/079

Every language L in NP is expressible as the range of some honest P-computable function f. We can think of the argument to f as encoding a candidate string $w \in L$, and a proof x of the fact that w is indeed in L. The function f verifies the proof: if it is fine, then f outputs w, otherwise f outputs some default string in L. The function f is referred to as a proof system for L. We explore the situation where f is required to be computed in NC^0. This requires the proof to be, in a sense, "locally checkable" and "locally correctable". We attempt to understand what kind of languages have proofs possessing these properties. We show that languages with NC^0 proof systems slice vertically across complexity classes.

Based on joint work with Olaf Beyersdorff, Samir Datta, Andreas Krebs, Gido Scharfenberger-Fabian, Karteek Sreenivasaiah, Michael Thomas, and Heribert Vollmer, part of which appears as ECCC TR12-079 (preliminary version in MFCS 2011).

3.18 Themes in Algebraic and Combinatorial Constructions of Probabilistic Proof Systems

Or Meir (Institute of Advanced Study – Princeton, US)

Joint work of Meir, Or; Dinur, Irit; Goldreich, Oded

Probabilistic proof systems is a sub-field of complexity theory that investigates questions such as "how can we use randomness to prove and verify assertions?", "what do we gain from using randomness in verification procedures?", and "what assertions can be verified by probabilistic verification procedures?". Research in this area began in the 1980, and has led to several of the most important achievements of complexity theory in those decades. Many of the key results in this area rely on sophisticated use of low degree polynomials.

A line of research from the recent years is aimed at finding alternative "combinatorial" proofs for those key results, i.e., proofs that do not rely on algebra. This line of research is motivated by trying to gain more intuition of those results, as well as to understand the properties of polynomials that make them useful for such constructions.

In this talk, we will survey this line of research, and focus on a few themes that are shared by this line of work and the algebraic constructions.

3.19 Planarizing Gadgets for Perfect Matching Do not Exist

Jochen Messner (Hochschule Aalen, DE)

Joint work of Gurjar, Rohit; Korwar, Arpita; Messner, Jochen; Straub, Simon; Thierauf, Thomas
Main reference R. Gurjar, A. Korwar, J. Messner, S. Straub, T. Thierauf, "Planarizing Gadgets for Perfect Matching Do not Exist," in Mathematical Foundations of Computer Science 2012. Springer, LNCS, Vol. 7464, pp. 478–490, 2012.
URL http://dx.doi.org/10.1007/978-3-642-32589-2_43

To reduce a graph problem to its planar version, a standard technique is to replace crossings in a drawing of the input graph by planarizing gadgets. We show unconditionally that such

a reduction is not possible for the perfect matching problem and also extend this to other related problems like Mod_k-PM for $k \geq 3$.

3.20 One algorithm to rule them all: One join query at a time

Atri Rudra (SUNY – Buffalo, US)

Joint work of Ngo, Hung; Porat, Ely; Re, Christopher; Rudra, Atri
Main reference H.Q. Ngo, E. Porat, C. Ré, A. Rudra, "Worst-case optimal join algorithms," PODS 2012: 37–48.
URL http://dx.doi.org/10.1145/2213556.2213565

We present a recent algorithm (PODS 2012) that is the first provably optimal (worst-case) algorithm to compute database joins.

As a special case, we show that this join algorithm implies

(i) The first algorithmic versions of some well-known geometric inequalities due to Loomis and Whitney (and their generalizations by Bollobas and Thomason);

(ii) Algorithmically list recoverable codes that work with parameters that no known algorithmic list recovery result work with (e.g. those based on the Reed-Solomon codes) and an application of this result in designing sublinear time decodable compressed sensing schemes;

(iii) Worst-case optimal algorithm to list all occurrences of any fixed hypergraph H in a given large hypergraph G.

We believe that this algorithm should find many more applications.

This talk will focus on (i) and (ii) and is based on joint works with Gilbert, Ngo, Porat, Re and Strauss.

3.21 Lower Bounds against Weak Uniformity and Sublinear Advice

Rahul Santhanam (University of Edinburgh, GB)

Joint work of Santhanam, Rahul; Lance Fortnow; Ryan Williams

Hierarchy theorems give unconditional lower bounds for explicit problems against strongly (DLOGTIME) uniform circuits. There are a couple of natural ways of relaxing the uniformity condition - (i) Allowing a small amount of advice in the lower bound against strongly uniform circuits (ii) Using a weaker notion of uniformity (eg., P- uniformity).

We prove new circuit lower bounds for P and NP with these relaxed uniformity conditions. Among other results, we show that or every constant k

(i) NP is not in $\text{NTIME}(n^k)/n^{o(1)}$

(ii) P does not have P-uniform deterministic circuits of size n^k.

(iii) NP does not have NP-uniform non-deterministic circuits of size n^k.

Based on joint works with Lance Fortnow and Ryan Williams.

3.22 Rank bound for design matrices and applications to incidence theorems and locally correctable codes

Shubhangi Saraf (Rutgers Univ. – Piscataway, US)

Consider a finite set of points in R^n. The classical theorem of Sylvester-Gallai says that, if for every two points there is a third point on the line through them, then all points are on the same line. In this talk I will describe several extensions to this theorem – quantitative versions, high dimensional versions, and average case versions. The main component of our proofs is an improved lower bound on the rank of design matrices, which are matrices over the complexes with certain zero-nonzero patterns. We use our improved lower bounds on the rank to get improved analyses for several questions in incidence geometry. These results build upon and extend a recent work of Barak, Dvir, Wigderson and Yehudayoff.

I will also talk about stable versions of the Sylvester-Gallai Theorem, where we are only guaranteed many triples of points which are approximately collinear. Configurations with many approximately collinear q-tuples of points also arise naturally in stable versions of Locally Correctable Codes over the complex numbers. We show that that such stable codes with constant query complexity do not exist. No impossibility results were known in any such local setting for more than 2 queries.

Based on joint works with Albert Ai, Zeev Dvir and Avi Wigderson

3.23 Invertible zero-error dispersers and defective memory with stuck-at errors

Ronen Shaltiel (University of Haifa, IL)

Joint work of Gabizon, Ariel; Shaltiel, Ronen
Main reference A. Gabizon, R. Shaltiel, "Invertible Zero-Error Dispersers and Defective Memory with Stuck-At Errors," in Proc. of the 16th Int'l Workshop on Randomization and Approximation Techniques in Computer Science, (RANDOM), pp. 553–564, 2012.
URL http://cs.haifa.ac.il/~ronen/online_papers/defects_full.pdf

Let $x = (x_1, \ldots, x_n)$ be a memory with n bit cells where a subset $S \subseteq [n]$ containing at most s out of the n cells are 'stuck' at certain values and cannot be modified. The goal is to store a long string z in memory x, so that at a later point it would be possible to read x and retrieve z, even without knowing which of the cells are stuck. This problem is related to, and harder than, the Write-Once-Memory (WOM) problem (in which once we raise a cell x_i from zero to one, it is stuck at this value).

We give explicit schemes which store $n - s - o(n)$ bits (note that the trivial lower bound is $n - s$). This is the first explicit scheme with asymptotically optimal rate. We are able to guarantee the same rate even if following the encoding, the memory x is corrupted in $o(\sqrt{n})$ adversarially chosen positions.

Our approach utilizes a recent connection observed by Shpilka between the WOM problem and linear seeded extractors for bit-fixing sources. We generalize this observation and show that memory schemes for stuck-at memory are equivalent to zero-error seedless dispersers for bit-fixing sources. It turns out that explicitness of the disperser is not sufficient for the explicitness of the memory scheme. We also need that the disperser is efficiently invertible.

In order to construct our memory schemes, we give new constructions of zero-error seedless dispersers for bit-fixing sources and affine sources. These constructions improve upon previous work: For sources with min- entropy k, they

(i) achieve larger output length $m = (1 - o(1)) \cdot k$ whereas previous constructions did not, and

(ii) are efficiently invertible, whereas previous constructions do not seem to be easily invertible.

3.24 Better condensers and extractors from Parvaresh-Vardy codes

Amnon Ta-Shma (Tel Aviv University, IL)

We give a new construction of condensers based on Parvaresh-Vardy codes. Our condensers have entropy rate $1 - \alpha$ for subconstant α (in contrast to GUV which required constant α) and suffer only sublinear entropy loss.

Known extractors can be applied to the output to extract all but a subconstant fraction of the minentropy. The resulting (k, ϵ)-extractor has output length $m = (1 - \alpha)k$ with $\alpha = 1/\text{polylog}(n)$, and seed length $d = O(\log n)$ when $\epsilon > 1/2^{\log^{\beta} n}$ for any constant $\beta < 1$. Thus we achieve the same "world-record" extractor parameters as DKSS, with an (arguably) simpler construction, while being able to handle smaller error.

3.25 A perspective on arithmetic circuit lower bounds

Amir Yehudayoff (Technion – Haifa, IL)

We discussed general approaches for proving lower bounds for arithmetics circuits. We mainly focus on the following:

1. Prove a structural statement for arithmetic circuits, and
2. find weakness of structure to prove lower bound.

Several structural results are know for general circuits:

(i) Valiant el al. proved that they can be balanced to have depth order $\log(s)\log(r)$, where s is size and r is degree, and

(ii) this was used by Agrawal and Vinay to show a general non-trivial reduction to depth 4.

We do not know, however, how to use these structural results to prove lower bounds.

For multilinear formulas, this approach turned out to be extremely useful. The structural theorem for multilinear formulas is that they can be written as a sum of highly-reducible, variable-disjoint polynomials. The main breakthrough in this context came in the work of Raz who identified a concrete weakness of multilinear formulas, that is based on this structure.

Finally, we discussed other approaches for proving lower bounds.

3.26 Pseudorandomness from Shrinkage

David Zuckerman (University of Texas at Austin, US)

Joint work of Impagliazzo, Russell; Meka, Raghu; Zuckerman, David
Main reference R. Impagliazzo, R. Meka, and D. Zuckerman, "Pseudorandomness From Shrinkage," FOCS 2012.
URL http://eccc.hpi-web.de/report/2012/057/

One powerful theme in complexity theory and pseudorandomness in the past few decades has been the use of lower bounds to give pseudorandom generators (PRGs). However, the general results using this hardness vs. randomness paradigm suffer a quantitative loss in parameters, and hence do not give nontrivial implications for models where we don't know super-polynomial lower bounds but do know lower bounds of a fixed polynomial. We show that when such lower bounds are proved using random restrictions, we can construct PRGs that are essentially best possible without in turn improving the lower bounds.

More specifically, say that a circuit family has shrinkage exponent Γ if a random restriction leaving a p-fraction of variables unset shrinks the size of any circuit in the family by a factor of $p^{\Gamma+o(1)}$. Our PRG uses a seed of length $s^{1/(\Gamma+1)+o(1)}$ to fool circuits in the family of size s. By using this generic construction, we get PRGs with polynomially small error for the following classes of circuits of size s and with the following seed lengths:

1. For de Morgan formulas, seed length $s^{1/3+o(1)}$;
2. For formulas over an arbitrary basis, seed length $s^{1/2+o(1)}$;
3. For read-once de Morgan formulas, seed length $s^{0.234\ldots}$;
4. For branching programs of size s, seed length $s^{1/2+o(1)}$.

The previous best PRGs known for these classes used seeds of length bigger than $n/2$ to output n bits, and worked only when the size $s = O(n)$.

Participants

- Farid Ablayev
Kazan State University, RU
- Manindra Agrawal
Indian Inst. of Technology – Kanpur, IN
- Eric Allender
Rutgers Univ. – Piscataway, US
- Vikraman Arvind
The Institute of Mathematical Sciences – Chennai, IN
- David A. Mix Barrington
University of Massachusetts – Amherst, US
- Markus Bläser
Universität des Saarlandes, DE
- Andrej Bogdanov
Chinese Univ. of Hong Kong, HK
- Harry Buhrman
CWI – Amsterdam, NL
- Sourav Chakraborty
Chennai Mathematical Inst., IN
- Arkadev Chattopadhyay
TIFR Mumbai, IN
- Samir Datta
Chennai Mathematical Inst., IN
- Volker Diekert
Universität Stuttgart, DE
- Klim Efremenko
Tel Aviv University, IL
- Stephen A. Fenner
University of South Carolina, US
- Lance Fortnow
Georgia Inst. of Technology, US
- Anna Gál
University of Texas at Austin, US
- William Gasarch
University of Maryland – College Park, US
- Parikshit Gopalan
Microsoft Research – Mountain View, US
- Frederic Green
Clark University – Worcester, US
- Joshua A. Grochow
University of Toronto, CA
- Steve Homer
Boston University, US
- Valentine Kabanets
Simon Fraser University – Burnaby, CA
- Neeraj Kayal
Microsoft Research India – Bangalore, IN
- Pascal Koiran
ENS – Lyon, FR
- Swastik Kopparty
Rutgers Univ. – Piscataway, US
- Michal Koucký
Academy of Sciences – Prague, CZ
- Matthias Krause
Universität Mannheim, DE
- Klaus-Jörn Lange
Universität Tübingen, DE
- Sophie Laplante
University Paris-Diderot, FR
- Bruno Loff
CWI – Amsterdam, NL
- Meena Mahajan
The Institute of Mathematical Sciences – Chennai, IN
- Pierre McKenzie
University of Montreal, CA
- Or Meir
Institute of Advanced Study – Princeton, US
- Jochen Messner
Hochschule Aalen, DE
- Natacha Portier
ENS – Lyon, FR
- Atri Rudra
SUNY – Buffalo, US
- Chandan Saha
IISc – Bangalore, IN
- Rahul Santhanam
University of Edinburgh, GB
- Shubhangi Saraf
Rutgers Univ. – Piscataway, US
- Uwe Schöning
Universität Ulm, DE
- Rocco Servedio
Columbia University, US
- Ronen Shaltiel
University of Haifa, IL
- Simon Straub
Universität Ulm, DE
- Amnon Ta-Shma
Tel Aviv University, IL
- Thomas Thierauf
Hochschule Aalen, DE
- Jacobo Toran
Universität Ulm, DE
- Christopher Umans
CalTech – Pasadena, US
- Virginia Vassilevska Williams
Stanford University, US
- Nikolay K. Vereshchagin
Moscow State University, RU
- Ryan Williams
Stanford University, US
- Amir Yehudayoff
Technion – Haifa, IL
- David Zuckerman
University of Texas at Austin, US

Report from Dagstuhl Seminar 12431

Time-of-Flight Imaging: Algorithms, Sensors and Applications

Edited by

James Davis[1], Bernd Jähne[2], Andreas Kolb[3], Ramesh Raskar[4], and Christian Theobalt[5]

1 **University of California – Santa Cruz, US,** `davis@cs.ucsc.edu`
2 **Universität Heidelberg, DE**
3 **Universität Siegen, DE,** `andreas.kolb@uni-siegen.de`
4 **MIT – Cambridge, US,** `raskar@media.mit.edu`
5 **MPI für Informatik – Saarbrücken, DE,** `theobalt@mpi-inf.mpg.de`

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 12431 "Time-of-Flight Imaging: Algorithms, Sensors and Applications". The seminar brought together researchers with diverse background from both academia and industry to discuss various aspects of Time-of-Flight imaging and general depth sensors. The executive summary and abstracts of the talks given during the seminar as well as the outcome of several working groups on specific research topics are presented in this report.

Seminar 21.–26. October, 2012 – www.dagstuhl.de/12431
1998 ACM Subject Classification I.2.10 Vision and Scene Understanding, I.4.1 Digitization and Image Capture, H.5.2 User Interfaces
Keywords and phrases Time-of-Flight, Kinect^{TM}, depth sensor
Digital Object Identifier 10.4230/DagRep.2.10.79
Edited in cooperation with Kwang In Kim

1 Executive Summary

James Davis
Bernd Jähne
Andreas Kolb
Ramesh Raskar
Christian Theobalt

In recent years, Time-of-Flight (ToF) depth imaging technology has seen immense progress. Time-of-Flight imaging is based on measuring the time that light, emitted by an illumination unit, requires to travel to an object and back to a detector. From this time, scene depth and possibly additional information that can not be measured by traditional intensity imaging, is inferred. While early ToF cameras were merely lab prototypes to prove a concept, recent sensor designs are at the edge of becoming operative products for mass market applications. A wide range of research disciplines is able to benefit from reliable and fast depth imaging technology, such as computer vision, computer graphics, medical engineering, robotics and computational photography, to name a few. Easy availability of affordable depth cameras will

open the door for many new applications. The commercial success of the Microsoft™ Kinect device – a depth sensor based on an alternative measurement principle – gives a first impression on this.

Currently, manufacturers of ToF systems mainly focus on sensor technology and on the design of cameras. Sensor design has seen great advancements, but the data delivered by the cameras remain challenging and are affected by many types of systematic distortions and difficult scene dependencies. ToF data are thus hardly usable out-of-the-box and it takes proper mathematical modeling and algorithmic processing to apply the data in practical imaging and reconstruction scenarios. Algorithm design for ToF imagers, however, is still in its early days and many challenges remain. In this seminar, we plan to discuss and extend the state of the art in ToF imaging algorithms and applications with leading researchers in the field.

Also, currently, there is little dialogue between researchers developing ToF algorithms and sensor designers. Therefore, the seminar also strongly supported the manufacturers in getting up to date with all relevant research results and, even more importantly, it offered the opportunity to establish long-term partnerships and research collaborations. We also believe that this stronger interaction will lead to more advanced sensor designs, as well as more powerful algorithmic solutions at the same time.

Description of the Seminar: Topics, Goals and Achievements

General Motivation

Time-of-Flight technology is based on measuring the time that light, emitted by an illumination unit, requires to travel to an object and back to a detector. This allows to measure distances with high precision and high speed. Recently, this principle has been the basis for the development of new range-sensing devices realized in standard CMOS and CCD technology and which are called ToF cameras, as well as in the context of photogrammetry Range Imaging (RIM) sensors. Unlike other 3D systems, the ToF camera is a very compact device. It has the potential of being one of the first low-price, off-the-shelf system to provide full-range distance information in at video rate.

Today the community using Time-of-Flight technology is scattered over many research disciplines without intense communication across research areas. Such communication is necessary, however, to fuse results from sensor technology, low–level ToF data processing and high–level image processing. Each of the above research disciplines that employs time-of-flight imaging has to develop algorithmic solutions to these very same core problem areas. Additionally, there are new hot topics that currently do not make use of this new technology but might benefit from it in the future, which further underlines the importance of ToF algorithm design.

In this seminar, we exploited this multi-disciplinarity, and brought researchers from computer vision, computer graphics, computational photography, image processing and engineering disciplines together that work with ToF imagers. Together, we defined the current state of the art in core algorithmic questions that ToF imaging researchers are confronted with (additionally to the seminar by an edited book on the main results). We also contributed advancing the field by identifying current limitations, important future research directions, and by enabling a closer dialogue between algorithm and hardware designers to discuss future sensor designs.

Topics

Time-of-Flight imaging devices can measure scene depth largely independently of scene appearance and are generally based on extensions of standard video intensity camera hardware. ToF sensors can thus be used for static and dynamic scene capture. However, the data of these sensors suffer from a variety of deficiencies, such as low resolution, strong random noise, and non-trivial systematic distortions. These challenges have to be algorithmically addressed before ToF cameras become mainstream in any field of application. The main topic of this seminar was the definition and extension of the state of the art in ToF imaging problems in three core areas of algorithm and technology development that are described in the following.

Low level data processing, calibration and characterization

Researchers in computer vision, computer graphics and image processing only just started to mathematically model the measurement characteristics of ToF sensors [29]. This is a fundamental prerequisite for calibration [6], as well as for well-founded design of low level ToF data processing.

The phase-based Time-of-Flight technology suffers from some specific problems that cause systematic calibration errors and parameter correlation issues. Due to the physical realization of light modulation in the emitting LEDs, the ideal sine-waveform light emittance is approximated by a band-limited rectangular waveform. This causes nonlinear depth distortions, called *wiggling errors*. In addition, there are several non-linear effects depending on multi-path light propagation, for example in the optical system or due to multiple reflections in the scene. Some effects are well-understood, but there are still open issues in depth calibration [20]. In addition, the calibration of external camera parameters suffers from strong correlation, since typically the cameras have limited field of view and low image resolution. Solutions to this problem can be found if a synchronous multi-camera calibration with rigidly coupled color and range camera rigs are investigated [28]. Coupling of high-resolution color video cameras with ToF cameras is hence an issue of further investigation. Latest ideas on sensor calibration will be reviewed and augmented in the seminar.

The knowledge gained through sensor calibration can also be exploited to create sensor simulations of high fidelity in software. This will be an invaluable tool test new algorithms. Proper sensor modeling also enables detailed sensor comparison and evaluation, and eventually even certification. A couple of research initiatives are underway to build in-depth mathematical sensor model of ToF imagers which will be discussed at the seminar [12].

Low level sensor calibration and sensor modeling enables more efficient and effective design of algorithms for low-level TOF processing. For instance, first low-level ToF filtering [35, 2] and ToF 3D superresolution approaches have been proposed [30, 31]. Most of these approaches have already demonstrated that a proper sensor model can be exploited for higher quality processing. In the seminar, we reviewed latest low-level processing techniques, and evaluated how new and better filtering and data enhancement techniques can be developed, also for rarely considered depth camera artifacts, such as ToF motion blur. We also discussed how such techniques can be integrated on the sensor and how the gained understanding of sensor characteristics can benefit the design of future sensors.

High level data processing for 3D reconstruction, understanding and recognition

Low-level ToF imaging builds the foundations for the higher-level processing tasks that researchers and practitioners from many disciplines are confronted with. In most cases, such higher level processing aims to recover high-quality 3D models of static and/or dynamic

scenes that should be displayed, analyzed, interactively modified, or used for recognition and scene understanding.

One major field of research using higher-level ToF image processing is computer graphics. Here, efficient acquisition of geometric models of static and dynamic scenes is of tremendous importance, and has many applications in interactive 3D rendering, geometric modeling and product design, 3D human computer interaction, cultural heritage, as well as professional media and game productions. ToF sensors can be an important asset here in order to replace the costly, highly specialized, complex and often intrusive acquisition technology currently used for such tasks. Static scene acquisition is mostly performed based on active scanners, using structured light or laser-based triangulation. Dynamic scene capture can also be achieved with structured light devices, and specialized optical systems that track fiducial markers exist for capturing motion. Being able to solve similar reconstruction tasks with only ToF cameras would be a big step ahead and eventually make 3D acquisition technology available to a wider range of users.

For a long time computer vision researchers have successfully developed 3D reconstruction approaches from single or multiple cameras that exploit certain photometric or radiometric cues. Many of them have in common that they are computationally expensive and that they only succeed under certain scene conditions, such as if scenes are sufficiently textured. An enormous potential lies in the fusion of ToF sensors with standard sensors for computer vision and robotics problems. Most areas in computer vision benefit from depth or range information; however, due to the difficulty in reconstruction of robust depth maps in real–world environments — especially in real–time applications — most state of the art solutions in areas like object recognition, gesture and action recognition in man-machine communication, pedestrian detection, and low–level tasks like segmentation just rely on 2D intensity information. Available depth and shape cues in real–time together with intensity information will open new possibilities to improve quality and robustness of algorithms and systems in such areas [25, 10, 13, 11, 24, 21]. In this context, there are several open problems, which were discussed during this seminar: do we need to define new features to be extracted from Time-of-Flight data and which feature will lead to a gain in quality compared to nowadays state of the art solutions? How can we deal with resolution and noise level of such cameras to complement normal 2D intensity information? Will we need to fuse Time-of-Flight information with 2D intensity data of standard CCD cameras, or are there applications, that can benefit from Time-of-Flight cameras by itself?

Another area in which ToF imaging will play a major role in future, is video processing, in particular 3D video and 3D TV. The analysis of dynamic 3D scenes from video requires the simultaneous processing of color video and range data. While traditional approaches using multi-view video are already quite successful, the advent of ToF range technology allows novel insights, novel applications and ease of acquisition. Traditional multi-view depth reconstruction requires sufficiently textured scenes, which might not be the case for arbitrary scenes, especially in indoor environments. This might lead to incomplete reconstruction results. ToF range acquisition has the potential for handling range data in dynamic video, but still many issues need to be solved and discussed by experts: in particular the challenging noise, uncertainty in the measurements, and low resolution of current ToF cameras represent a challenge. First applications handling video-rate HD-TV depth processing can be found in systems for 3D-Television capture [7] or in general computer graphics applications [17].

In many other areas, for instance computational photography, computational videography and medical engineering, researchers are facing similar reconstruction problems and can benefit from ToF sensors. For instance, in medical engineering, ToF cameras have been used

to detect patient position [26] and respiratory motion in radiotherapy [27, 23].

The above list of examples shows that the algorithmic problems to be solved for making ToF sensors usable for high level reconstruction in different areas are very similar. The main challenge will be to enable high quality reconstruction despite strongly distorted and low-resolution raw ToF sensor output. Several strategies have been explored to attack these problems: Sensor fusion approaches combine depth and intensity cameras, spatio-temporal reconstruction approaches recover higher detail by accumulating and aligning measurements over time, superresolution and alignment can be combined to enable high-quality 3D reconstruction. Given such better quality reconstructions, the captured data can be employed as scene models ore further analyzed for capturing motion and gestures, for recognizing activities, for recognizing objects, or for analyzing the environment in a navigation scenario. The seminar therefore reviewed latest algorithms for static and spatio-temporal 3D reconstruction from ToF data. We have also discussed how they need to be tuned for specific applications, such as motion capture and recognition. Finally, we discussed ways to better integrate low-level and high-level processing.

Sensor technology and new depth sensor designs

While algorithm design for low-level and high-level TOF imaging were the main focus of this seminar, we also initiated to enable a dialogue between hardware manufacturers and algorithm designers. On the one hand this familiarized hardware designers with the state-of-the-art in ToF data processing, and sensibilized them for the existing challenges and specific application requirements. In return, algorithm designers deepened their knowledge about the fundamental physical principles of ToF imaging and gain a better understanding for the physical origins of sensor characteristics.

It is possible that relatively simple changes to the ToF hardware would result in the possibility of new sensor designs. ToF cameras make use of a CMOS sensor that is an enhanced version of a normal camera with extra circuitry at each pixel, and a structured IR illuminator. A great deal of prior research exists on using “normal” CMOS cameras together with triangulation based structured light to recover depth. The structured illuminator in these two research areas makes use of different principles, and the internal frame rate of the ToF camera is much higher, but the hardware components are broadly similar, suggesting that sharing of ideas might be fruitful.

Importantly, ToF and triangulation have complementary error characteristics, strengths, and weaknesses. For example, ToF sensors tend to perform better at a distance, and triangulation tends to perform better at close range. This leaves open the possibility of new sensor designs that make use of ideas from both ToF and structured light, with greatly improved robustness and accuracy. For example: chips could be designed with both “normal” and “ToF” pixels, the ToF light source could have a focusing lens and spatial pattern, the modulated light used with the ToF sensor could be similar to structured light patterns, the data from ToF could be used as a rough guess to disambiguate phase/depth in structured light when there are not enough patterns.

We are convinced that through a dialogue between hardware and algorithm designers, both sides can benefit. An example for a related research area in which such a dialogue has already resulted in great advancements is the area of computational photography. There, algorithm designers and hardware manufacturers have worked together on new designs for optical systems and processing algorithms that open up new ways of digital imaging, e.g., through high dynamic range imaging, wave front coding etc. We believe that the advent of ToF depth imaging technology is a further boost to this development, as it was already

shown by new ideas on space-time imaging [16]. We also believe that ToF designs can have a similar impact in the emerging field of computational videography where future video sensors and processing paradigms are developed. We believe that the seminar served as a platform to initiate such developments by bringing together key players in the field. In this context, the pros and cons of alternative depth measurement sensors, such as IR-based active stereo cameras, have also been discussed.

Goals and Achievements of the Seminar

The overall goal of this seminar was to bring together researchers from several TOF-related disciplines, review the state-of-the-art in ToF imaging on both the algorithmic and hardware side, and develop new concepts for algorithms and devices that advance the field as a whole. The seminar was not intended to be a classical workshop or conference where mostly finished research is presented. We wanted the seminar to be a platform for identifying and discussing the big open research questions and challenges. More specifically, the following is a list of challenges that have been discussed at the seminar, since they form the basis of low-level and applied research with Time-of-Flight cameras:

- Low-level processing
  - Basic mathematical modeling of ToF cameras: image formation model, noise modeling, calibration of the sensor and optics.
  - Low-level image processing problems: resolution enhancement through superresolution and sensor fusion, data filtering, feature extraction under random and systematic distortions.
- High-level processing
  - Static shape scanning: high-quality geometry scanning, 3d superresolution, alignment approaches, probabilistic methods for reconstruction and alignment under noise.
  - Dynamic shape scanning: Spatio-temporal filtering, multi-sensor fusion approaches, model-based dynamic scene reconstruction, unsupervised dynamic scene reconstruction (joint model-building and motion reconstruction), marker-less motion and performance capture, 3d video.
- Improvements of sensor design: pixel design, light source design and arrangement, Time-of-Flight measurement principles: amplitude modulation vs. shutter. In this context we will also discuss standardization questions.

The seminar was very successful with respect to the set goals and initiated great interaction between researchers from different domains which had never happened in this way at other conferences or workshops.

In order to best initiate this interaction, we decided to organized a multi-faceted scientific programme. It consisted of a variety of different presentation formats. In particular, we had a series of research talks on the different research problems which we wanted to address in the seminar. When selecting the research talks, we planned for having a mix of presentations by junior and senior researchers, as well as balance of different topics. Presenters dedicated at least half the presentation time to address open research problems in order to spawn new research projects and collaborations. In order to further initiate discussion between researchers with different backgrounds, and in order to very practically identify potential research projects, we also organized working groups in which small teams discussed certain focus topics. Finally, the seminar participants organized very informal evening sessions in

which special cross-disciplinary research topics were discussed in a very informal way. Finally, a demo session enables researchers and hardware specialists to showcase their latest results.

As an outcome of this, a very lively discussion and interaction was started between participants, and many concrete research projects were defined. Most fruitful discussions started on the topics of: 1) how to better exploit existing hardware and software systems; 2) the limitation of existing sensors and how to break them; 3) new combinations of existing (heterogeneous) sensors; 4) technical and economical limitations of hardwares.

To achieve sustainability beyond the seminar the organizers will edit a book summarizing the main methods, applications, and challenges in the context of ToF technology based on the presentations and discussions during the seminar. Such a book is currently missing in the community and the seminar itself shall also act as catalyzer for such a project. For more rapid dissemination of ideas and results, the organizers also created Wiki[1] which will be eventually relocated and maintained permanently.

[1] http://www.dagstuhl.de/wiki/index.php?title=12431

2 Table of Contents

3 Overview of Talks

Research talks addressed specific algorithmic problems in Time-of-Flight imaging. Each presenter dedicated a lot of his presentation time to talk about big open research challenges that the community should look into.

3.1 Benchmarking Time-of-Flight Data for Specific Application Demands

Michael Balda (Metrilus GmbH – Erlangen, DE)

Joint work of Balda, Michael; Schaller, Christian; Placht, Simon

Depth data acquired with Time-of-Flight (ToF) sensors suffers from many typical measurement artifacts such as motion artifacts, intensity related depth error, flying pixels, temperature drift, interference between multiple ToF cameras or effects caused by multi-path reflections and many more. Some of these issues can be addressed on chip or illumination level, others can be reduced with proper post-processing methods or, of course, hybrid approaches.

In this talk we outline the influence of these artifacts in practical medical and industrial ToF-applications such as robotics and gesture interaction.From these practical experiences we derive some of the requirements on countermeasures for specific scenarios. When developing new algorithms that process ToF-data and deal with ToF-artifacts it is of course necessary to quantify their performance in specific scenarios in a reproducible way. We suggest some selected benchmarks to evaluate the efficiency of existing countermeasures in standardized scenarios and give a short overview on how the currently available sensors perform in these benchmarks.

Furthermore, we would like to discuss ideas for benchmarking ToF in general and identify possible drawbacks and improvements for benchmarks and find necessary prerequisites to ensure a fair comparison of different sensors and algorithms. These prerequisites could for instance cover the influence of background light or reasonable camera resp. illumination warm-up periods.

3.2 Capturing and Visualizing Light in Motion

Christopher Barsi (MIT – Cambridge, US)

We show a technique to capture ultrafast movies of light in motion and synthesize physically valid visualizations. The effective exposure time for each frame is under two picoseconds. Capturing a 2D video with such a high time resolution is highly challenging, given the extremely low SNR associated with a picosecond exposure time, as well as the absence of 2D cameras that can provide such a shutter speed. We re-purpose modern imaging hardware to record an ensemble average of repeatable events that are synchronized to a streak tube, and we introduce reconstruction methods to visualize propagation of light pulses through macroscopic scenes. Capturing two-dimensional movies with picosecond resolution,

we observe many interesting and complex light transport effects, including multi bounce, delayed mirror reflection, and sub-surface scattering. We notice that the time instances recorded by the camera, i.e. "Camera time" is different from the time of the events as they happen locally at the scene location, i.e. "world time". We introduce a notion of time warp between the two space-time coordinate system, and rewarp the space-time movie for a different perspective. This technique offers support for image-based rendering of relativistic events.

3.3 Frequency Analysis of Transient Light Transport with Applications in Bare Sensor Imaging

Christopher Barsi (MIT – Cambridge, US)

Light transport has been extensively analyzed in both the spatial and the frequency domain; the latter allows for intuitive interpretations of effects introduced by propagation through free space and optical elements, as well as for optimal designs of computational cameras capturing specific visual information. We relax the common assumption that the speed of light is infinite and analyze free space propagation in the frequency domain considering spatial, temporal, and angular light variation. Using this analysis, we derive analytic expressions for cross-dimensional information transfer and show how this can be exploited for designing a new, time-resolved bare sensor imaging system.

3.4 Gesture-based interaction with ToF cameras

Erhardt Barth (Universität Lübeck, DE)

I will base my talk on the experience with our startup company gestigon (www.gestigon.de). But do not worry, this will not be any kind of commercial. Rather, the startup endeavor tells you in a clear way, which can hurt, what the current limitations of the technology are and what future developments are required. If you need to track all degrees of freedom of two hands with very little hardware, if you need to do that through windows, in bright sunlight, and in cars, you are faced with a number of challenges, for example to (i) invent simple and robust algorithms, (ii) talk to the users and define use cases, (iii) talk to the camera people and jointly optimize hardware and algorithm design. I will briefly sketch our approach to hand- and body-skeleton tracking and discuss the main challenges. In addition to those mentioned above, one of the main technical challenges is to obtain a tight coupling between the user and the application. On top of that you need to understand user intent and a basic alphabet of gestures. It seems worth discussing how such an alphabet could be defined. It would be nice if we could set up an interdisciplinary, international interest group for TOF-based gesture technology.

3.5 Mitigating common distortion sources, and exploring alternative applications, for Time-of-Flight cameras

Adrian Dorrington (University of Waikato, NZ)

The Chronoptics research group has more then ten years experience in the field of Time-of-Flight (ToF) imaging. We have developed several technologies to improve the quality of ToF cameras (see more detail at http://www.chronoptics.com). Some of these technologies are well developed, but others suffer from practical limitations. This talk will introduce the following techniques, and call for collaborators to help address their limitations.

We have developed a Mixed Pixel Separation technique that can resolve multiple returns detected by a single pixel. This is useful for correcting edge effects such as mixed, or so-called "flying", pixel distortion, and for rejecting multi-path distortion. Published and unpublished results demonstrate the efficacy of this algorithm when the phase difference between the multiple returns is large and the signal-to-noise ratio is high, but the algorithm fails with small phase differences or when the measured depth precision is poor.

The combination of "Fluttered shutter" and optical flow techniques have allowed us to detect and quantify motion independently for multiple objects and to correct local motion blur. Although directly quantifying individual object velocity and direction is of interest in many fields, this technique requires further work to improve computational complexity and to automatically enumerate moving objects.

ToF sensors have potential for applications other than distance measurement. For example, the process of Diffuse Optical Tomography (DOT) data acquisition for internal medical imaging is very similar to ToF distance measurement, only the illumination and detection is in contact with the subject's skin and the data is processed in a very different way. We have demonstrated proof-of-principle showing that ToF cameras can be used for non-contact DOT using the NIRFast software package. Due to the multidisciplinary nature of this project, it would benefit significantly from a collaborative approach.

3.6 Difficulties and novel applications in a low-cost multi-view depth camera setting

Martin Eisemann (TU Braunschweig, DE)

Joint work of Eisemann, Martin; Berger, Kai; Ruhl, Kai; Guthe Stefan; Klose, Felix; Lipski, Christian; Hell, Benjamin; Magnor, Marcus
URL http://www.cg.cs.tu-bs.de/publications/

High-quality ToF cameras are still expensive nowadays, ranging from only a few to several thousand dollars. While less expensive solutions exist, these come at the cost of a higher signal to noise ratio and lower resolution. In this talk we will take a look at the difficulties, applications and our solutions for such low-cost depth cameras in a multi-view setting.

In this setting we treat the problem of calibration using mirrors, gas reconstruction using depth-images, super-resolution for IR sensors and integrating approximate depth data into dense image correspondence estimation.

Hopefully, these examples give rise to some fruitful discussion on new application fields for depth cameras besides the typical 3D scene reconstruction in the later part of the talk.

3.7 Will Depth Cameras Have a Long-term Impact on Computer Vision Research?

Juergen Gall (MPI für Intelligente Systeme – Tübingen, DE)

Depth cameras have become a commercial success and their popularity in the research community increased with the drop of sensor prices. Since many approaches focus on applying techniques that are well-known from 2D image/video analysis or stereo vision, it is time to discuss if depth sensors will open new research directions in computer vision that will have a long-term impact. To this end, I will review recent publications that appeared at computer vision workshops or conferences and made use of depth cameras for high-level computer vision tasks. Finally, I would like to start a discussion of the future of depth cameras in high-level computer vision research.

3.8 Capturing and Visualizing Light in Motion

Diego Gutierrez (University of Zaragoza, ES)

We show a technique to capture ultrafast movies of light in motion and to synthesize physically valid visualizations. The effective exposure time for each frame is under two picoseconds (ps). Capturing a 2D video with this time resolution is highly challenging, given the low signal-to-noise ratio (SNR) associated with a picosecond exposure time, as well as the absence of 2D cameras that can provide such a shutter speed. We re-purpose modern imaging hardware to record an ensemble average of repeatable events that are synchronized to a streak tube, and we introduce reconstruction methods to visualize both propagation of light pulses through macroscopic scenes, as well as relativistic effects of moving bodies.

Capturing two-dimensional movies with picosecond resolution, we observe many interesting and complex light transport effects, including multibounce scattering, delayed mirror reflections, and subsurface scattering. We notice that the time instances recorded by the camera, i.e., "camera times" are different from the time of the events as they happen locally at the scene location, i.e., "world times". We introduce the notion of time unwarping between the two space-time coordinate systems.

3.9 Open questions in full-body motion estimation with depth cameras

Thomas Helten (MPI für Informatik – Saarbrücken, DE)

The analysis and recording of full-body human motion data is an important strand of research with applications to movie and game productions, sport sciences, and human computer interaction.In the recent years, the availability of cheap range sensors, such as the Microsoft Kinect has boosted the research on tracking human motions from monocular depth images. Despite the promising approaches in this field there are still unsolved challenges such as (self) occlusions or ambiguities. In this talk, I want to elaborate on the reasons for these challenges and ideas to approach them.

3.10 Can we reconstruct the shape of a mirror-room from multi-bounce ToF measurements?

Ivo Ihrke (Universität des Saarlandes, DE)

I will discuss our recent progress in answering this question. We assume that we are given the measurements of a tempo-angularly resolved receiver recording the response of the room to a spherical pulse source. The receiver and the source are inside the room but at separate locations. I will show initial positive results for convex polyhedral rooms in two dimensions. Our method can deal with limited angular and/or temporal data. Also, it is not necessary to know the bounce order of a received pulse. It is however, difficult to establish performance bounds and reconstruction guarantees.

3.11 Deformable Object Detection in Underwater ToF Videos

Slobodan Ilic (TU München, DE)

The aquaculture industry has been continuously thriving since the 1980s. As the fish farming grows, it becomes important to develop a remote monitoring system to estimate the biomass of a large number of fishes bred in cages. Since around 80% of all sales of farmed fish are arranged pre-harvest, the profit on the sale directly depends on correct estimations of weight, size distribution and totalbiomass. Therefore, the goal of this research is to build an automated and relatively affordable tools for biomass estimation.

Here we will rely on ToF camera images acquired underwater, that are supposed to film fishes in the cage for certain period of time. In order to estimate the biomass the volume of the fish has to be estimated. This can be achieved by first detecting the fishes in every range image of the incoming video stream and then fitting a 3D model to these detections. To find the algorithm that is in line with our problem, we need to understand the challenges in detecting fishes. They include the motion of the fish which makes the object of interest

deformable, the location of the fish with respect to the camera and occlusions caused by having multiple fishes in every available frame.

In this talk I will present our approach to this problem mainly addressing high-level processing task summarized in developed algorithm for deformable object detection. In addition I would like to briefly introduce the technical challenges related to data acquisition using ToF camera underwater and get opinions of ToF experts about constructing reliable acquisition device underwater.

3.12 Efficient Deformation Reconstruction from Depth and Color Images using Analysis by Synthesis

Andreas Jordt (Universität Kiel, DE)

The reconstruction of deformations has always been a difficult problem due to the lack of a generic deformation model. Hence, 3d reconstruction of deforming objects ever since can be separated into two classes: Those using an explicit deformation model, e.g. skeletal models, – and those heavily relying on feature movement or optical flow.

Depth sensors like ToF cameras and or the Kinect depth sensor provide valuable scene information but do not provide a stable base for optical flow or feature movement calculation. Approaches associating these depth values with optical flow or feature movement from color images try to circumvent this problem but suffer from the fact that color features are often generated at edges and depth discontinuities, areas in which depth sensors deliver inherently unstable data. This talk introduces how the full potential of depth and color can be tapped by direct methods such as analysis by synthesis, utilizing the complete image data directly to calculate the result. A set of generic and specialized deformation models are introduced as well as an efficient way to synthesize and to optimize high dimensional models. The resulting reconstruction algorithms range from real-time deformation reconstruction methods to very accurate deformation retrieval using models of 100 dimensions and more.

3.13 Efficient Gaussian Process Regression-based Image Enhancement

Kwang In Kim (MPI für Informatik – Saarbrücken, DE)

Many computer vision and computational photography applications essentially solve an image enhancement problem. The image has been deteriorated by a specific noise process that we would like to remove, such as aberrations from camera optics and compression artifacts. In this talk, we discuss an algorithm for learning-based image enhancement. At the core of the algorithm lies a generic regularization framework that comprises a prior on natural images, as well as an application-specific conditional model based on Gaussian processes (GPs). To overcome the high computational complexity of GPs, an efficient approximation scheme of large-scale GPs are presented. This facilitates instantly learning task-specific degradation models from sample images. The efficiency and effectiveness of our approach is demonstrated by applying it to an example enhancement application: single-image super-resolution.

3.14 Real Time Handling of Depth Data

Andreas Kolb (Universität Siegen, DE)

The availability of depth data at interactive frame rates poses the challenge of handling a large amount of 3D data at nearly the same speed in order to realize interactive applications.

This talk presents recent results in handling large sets of streamed range data, taking into account the questions of how to reduce the amount of data and how to efficiently store range data. Here, also the quest of handling scene dynamics and of varying range data quality plays a role.

3.15 Automated classification of therapeutical face exercises using the Kinect

Cornelia Lanz (TU Ilmenau, DE)

The presentation is going to propose an approach for the topic of therapeutical facial exercise recognition using depth images recorded with the Kinect. In cooperation with speech-language therapists, we determined nine exercises that are beneficial for the therapy of patients suffering from dysfunction of facial movements. Extracted depth features comprise the curvature of the face surface and characteristic profiles that are derived using distinctive landmark points. The presentation will focus on the evaluation of the features. This comprises:

- their discriminative power concerning the classification of nine therapeutical exercises.
- their suitability for a fully automated real-world scenario. This requires features that are robust with respect to slightly varying feature extraction regions.

3.16 Enhancing ToF measurements: current work, evaluation with ground truth and open problems

Frank Lenzen (Universität Heidelberg, DE)

In 2010, the research project 'Algorithms for low cost depth imaging' started at the Heidelberg Collaboratory for Image Processing(HCI), co-financed by the Intel Visual Computing Institute (IVCI) in Saarbrücken. We report on the ongoing work within this project. In particular we consider the topic of denoising ToF data. In order to evaluate the quality of our approaches, we use a ToF data set which was created within this project and is annotated with ground truth. This dataset will be made publicly available.

Moreover, we discuss open problems we encountered during our research and which are of interest for the community.

3.17 Patch Based Synthesis for Single Depth Image Super-Resolution

Oisin Mac Aodha (University College London, GB)

Joint work of Mac Aodha, Oisin; Campbell, Neill; Nair, Arun; Brostow, Gabriel J.
Main reference O. Mac Aodha, N. Campbell, A. Nair, G.J. Brostow, "Patch Based Synthesis for Single Depth Image Super-Resolution," ECCV (3), 2012, 71–84.
URL http://dx.doi.org/10.1007/978-3-642-33712-3_6

We present an algorithm to synthetically increase the resolution of a solitary depth image using only a generic database of local patches. Modern range sensors measure depths with non-Gaussian noise and at lower starting resolutions than typical visible-light cameras. While patch based approaches for upsampling intensity images continue to improve, this is the first exploration of patching for depth images.

We match against the field of each low resolution input depth patch, and search our database for a list of appropriate high resolution candidate patches. Selecting the right candidate at each location in the depth image is then posed as a Markov random field labeling problem. Our experiments also show how important further depth-specific processing, such as noise removal and correct patch normalization, dramatically improves our results. Perhaps surprisingly, even better results are achieved on a variety of real test scenes by providing our algorithm with only synthetic training depth data.

3.18 Can ToF Cameras Enable Dynamic Interactive Ubiquitous Displays?

Aditi Majumder (University of California – Irvine, US)

Large dynamically changing surface geometry lighted seamlessly at a very high resolution by multiple projectors allowing interaction from multiple users makes displays truly ubiquitous–available to anyone anywhere. It is a dream harbored by many communities including computer graphics and vision; human computer interaction; and virtual, mixed and augmented reality. These can have tremendous applications in education, entertainment, simulation and training.

Several inroads have been made in the past in this direction, including a big body of work from our lab at UCI. Multiple aspects of this problem have been studied including fast and accurate surface reconstruction from multiple sensors (potentially uncalibrated); cross-validation across multiple devices to achieve robust calibration; fast and accurate 3D gesture recognition of multiple users from multiple sensors; centralized and distributed paradigms to achieve modularity in system design and improvement in efficiency, performance and ease in deployment; and efficient data management to handle large data sets.

However, SAR on very large and dynamically changing surfaces which people can interact with is still limited. Capturing depth from multiple cameras is still not fast enough and limits dynamism and interactivity. The inaccuracies in the estimated depth, especially in the presence of textures, limit the seamless registration of projected imagery on the surface. Both of these can be significantly alleviated by ToF Cameras. However, using multiple time

of flight (ToF) cameras in the same system bring in a different set of challenges in terms of interference with one another and background noise.

In this talk I will first present the large amount of work done in our lab at UCI in making large dynamic and multi-user interactive display systems a possibility. Then I will briefly discuss the motivation and challenges in using ToF cameras in this setting. It seems that many of these challenges overlap with those faced by other communities and I hope to make important connections so that we can work together and reuse findings in multiple domains to make such ubiquitous display systems a reality of the future.

3.19 TOF Ground Truth Generation

Rahul Nair (Universität Heidelberg, DE)

With the eve of low cost depth imaging techniques such as Kinect and TOF the generation of ground truth for vision applications should not be reserved to those who can afford expensive equipment. For large parts of computer vision ground truth generation means the measurement of geometric (and radiometric) properties of the scene. With these new possibilities to provide cheap ground truth with lower accuracy it is crucial to start specifying GT accuracy. Otherwise we cannot benchmark methods against such sequences. Although there are physically correct TOF noise models in literature, many computer vision researchers prefer Kinect rather than TOF cameras because of its systematic errors such as multipath effects caused by interreflections. If we could overcome these errors TOF imaging has the same capability of reaching the mass markets and being used by vision researchers worldwide. We will describe how starting from a precise sensor characterization and physical model we try to tackle both these tasks. By combining this noise model with state of art techniques from computer graphics we are able to simulate the raw image acquisition process in the camera. This enables us to simulate systematic errors such as multipath for further studies. We also show how we produce ground truth data using TOF combined with other modalities with a confidence in each pixel such that this "weak" ground truth may still be used to test other vision algorithms.

3.20 Real-world 3D video production with ToF cameras

Shohei Nobuhara (Kyoto University, JP)

Main reference T. Matsuyama, S. Nobuhara, T. Takai and T. Tung, "3D Video and Its Applications," Springer-Verlag, 2012.
URL http://dx.doi.org/10.1007/978-1-4471-4120-4

This talk first introduces essential design factors on building 3D video production systems with multiple-cameras for lab environment. It covers camera arrangement, background design, illumination, etc for robust silhouette extraction, 3D shape reconstruction, and texture generation. Then it presents some half-baked ideas on how to utilize ToF cameras to improve the production pipeline. It covers simultaneous multi-view silhouette extraction in real environment, and high-fidelity rendering with view-dependent 3D shape optimization.

3.21 Time-of-Flight cameras for computer-assisted interventions: opportunities and challenges

Alexander Seitel (DKFZ – Heidelberg, DE)

Minimally-invasive procedures are increasingly gaining in importance for cancer diagnosis and treatment. To date, computer-based assistance systems mainly rely on external or internal markers and optical or electromagnetic tracking systems for assessment of patient position and movement. Often, these approaches are combined with intra-operative imaging that exposes the patient to additional radiation. With the Time-of-Flight (ToF) camera technique, a markerless and radiation-free approach for transferring planning data acquired before the intervention to the situation at the patient during the intervention is possible.

This talk will present challenges and opportunities of the application of ToF cameras for computer-assisted medical interventions. It will firstly summarize methods for calibration of ToF cameras for use in the medical environment and registration of pre- and intra-operatively acquired surfaces and point out difficulties in correctly evaluating those algorithms due to the lack of adequate ground truth. Furthermore, the feasibility of applying a ToF camera for intra-operative imaging is shown and exemplary applied in an application for navigated percutaneous needle insertions. Lastly, there will be an overview on potential future medical applications, e.g. in the field of ToF-endoscopy, with focus on requirements and potential difficulties for the use of ToF cameras for ToF to be used in the medical environment.

3.22 SoftKinetic DepthSensing and 3D gesture recognition technologies

Julien Thollot (SoftKinetic-Brussels, BE)

What Do SoftKinetic Do?

SoftKinetict's vision is to give everyone the freedom to control, explore and enjoy the entire digital world through the most natural and intuitive user interfaces and machine interactions. SoftKinetic is the leading provider of gesture-based platforms for the consumer electronics and professional markets. The company offers a complete family of 3D imaging and gesture recognition solutions, including patented 3D CMOS time-of-flight sensors and cameras(DepthSense®, formerly Optrima), multi-platform and multi-camera 3D gesture recognition middleware and tools (iisu®as well as games and applications from SoftKinetic Studios.

With over 10 years of R&D on both hardware and software, SoftKinetic solutions have already been successfully used in the field of interactive digital entertainment, consumer electronics, health care and other professional markets such as digital signage and medical systems.

For more information on any of our products and services, please contact us at: sales@softkinetic.com

- SoftKinetic Solutions link: http://www.softkinetic.com/Solutions/iisuSDK.aspx

- SoftKinetic Depthsensor chip link:
  http://www.softkinetic.com/en-us/solutions/depthsensesensors.aspx
- SoftKinetic DepthSense ToF Cameras link:
  RGBZ ToF cameras (image registration included)
  DS311 : 160*120 Z, 720p RGB sensor + audio, Close interaction (0.1-1m)
  DS325 : 320*240 Z, 720p RGB sensor + audio, Close&far (0.1-1&0.5-5m)
  http://www.softkinetic.com/en-us/solutions/depthsensecameras.aspx
- SoftKinetic iisu Middleware link (gesture recognition and user or hand feature)
  http://www.softkinetic.com/en-us/solutions/iisusdk.aspx
- Video and demo:
  - iisu middleware + DS311 close interaction mode + arduino:
    http://www.youtube.com/user/Softkinetic
  - iisu 3.5 (full body skeleton tracking + close range hand interactions):
    http://www.youtube.com/watch?v=5LvhdFudp50&
    list=UUS7kIRSSm_cXBvnszuegUoA&index=2&feature=plcp
  - Corporate video:
    http://www.youtube.com/watch?v=Xfz_uRoJGjE&feature=relmfu
- Perceptual computing SDK solutions by intel (SoftKinetic embedded) including DS325 ToF camera custom build (Creative branded) at 149$:
  http://software.intel.com/en-us/vcsource/tools/perceptual-computing-sdk

3.23 Frequency Analysis of Transient Light Transport with Applications in Bare Sensor Imaging

Gordon Wetzstein (MIT – Cambridge, US)

Light transport has been extensively analyzed in both the spatial and the frequency domain; the latter allows for intuitive interpretations of effects introduced by propagation in free space and optical elements as well as for optimal designs of computational cameras capturing specific visual information. We relax the common assumption that the speed of light is infinite and analyze free space propagation in the frequency domain considering spatial, temporal, and angular light variation. Using this analysis, we derive analytic expressions for cross-dimensional information transfer and show how this can be exploited for designing a new, time-resolved bare sensor imaging system.

3.24 3D Modeling and Motion Analysis from a Single Depth Camera

Ruigang Yang (University of Kentucky, US)

3D has become a hot topic recently, partly due to two recent technical innovations: 3D TVs and commodity depth cameras–the Kinect camera from Microsoft. In this talk, I will first present an approach to create a complete dynamic 4D (space + time) model from a RGB+depth video sequence. Unlike traditional Structure from motion or point cloud

merging algorithm, our approach can deal with deformable subjects. Then I will talk about an approach that estimates skeleton motion using a single depth camera. Trading speed for accuracy, our approach reduces the average motion estimation error from 50 mm to be less than 10mm. Finally I will present a sensor-fusion approach that combines photometric stereo with active stereo (e.g., Kinect) to significantly improve the quality of the depth map. Unlike previous fusion approaches, we model depth discontinuity and occlusion explicitly.

4 Working Groups

4.1 Non-standard usage of ToF hardware – Brainstorming

James Davis (University of California– Santa Cruz, US)

At this workshop we are studying Time-Of-Flight Cameras, which implies the relatively narrow goal of obtaining depth using a measurement of time. However the hardware itself is a device which obtains multiple photonic measurements in rapid succession, and perhaps the device could be used for a purpose other than obtaining depth, or perhaps depth could be obtained through some principle other than strict time estimates. This alternative sessions goal is to brainstorm in these areas:

- alternative applications for the basic hardware
- modifications or flexibility that software researchers would like to see in the hardware
- modifications that hardware researchers would be happy to make, but don't yet know a suitable application

- 15 min – Intro of brainstorming session and example ideas:
  - Use ToF hardware with 4 time slots for triangulation structured light instead of depth phase estimation
  - Currently using only phase, joint coding with structured light source to use amplitude also?
  - "Sophisticated" image processing on the raw data, rather than the "simple" already computed depth
  - Sweep laser and get intersect time as intensity, using modified subpixel activation timing
  - I could build this thing with 8-tap super-pixels, does anyone want that?
- 30 min – Groups of 5 people brainstorm at least one non-standard purpose/method to abuse the hardware.
- 10 min – Sketch some slides/diagrams on overhead transparencies for the best brainstorm idea(s) in each group.
- 45 min – Groups report on their best ideas (About 8 groups with 5 minutes each).
- 5 min – Session wrap up and plan for continuity (Wiki to have areas for ideas and contact info for people potentially interested)

4.2 Time of Flight Cameras vs. Kinect

Seungkyu Lee (SAIT, South Korea)

Recently, many researchers have used either ToF sensor or Kinect for various applications. Many of them ask which type of depth sensor is best for their own applications. Actually, this is one of the most frequent and critical question for beginners of these sensors but the answer is not simple. In principle, both ToF and Kinect sensors have respective pros and cons. In this session, inputs from diverse experienced researchers and practitioners can be collected and shared. They can share what was the problem in using ToF (or Kinect) sensor in their applications and how about if they replace the sensor by Kinect (or ToF) sensor. We may not conclude which one is better than the other, but we can get better understanding and comparison on both sensing principles for future use.

- 15min Opening– start with a short intro./instruction for this topic including basic knowledge on both principles.
- 45min Brainstorming– divide the group into 3 4 along with their experiences or interests, such as interaction, imaging or 3D reconstruction, low level processing etc. ToF users and Kinect users (if available) can be mingled in each group. Let them share their experiences and thoughts on the sensors; what is good, what is bad, what is main obstacle for their app., and why is that. And they can discuss; 1) which characteristic of the sensor has to be improved and 2) what if they replace their ToF sensor by Kinect or vice versa. Each group makes a list/slides of pros-cons of ToF or Kinect for specific application.
- 40min Discussion – Each group report their lists and issues raised and discuss. If someone can advise on a point of the list, that can be added at each list and refine them.
- 5 min – Session wrap-up.

4.3 Real-world 3D video production with ToF cameras

Shohei Nobuhara (Kyoto University, Japan)

Conventional 3D video (or 4D modeling of dynamic 3D surface) production systems utilize multi-view 2D cameras, and reconstruct 3D surfaces based on shape-from-silhouettes (SFS) and wide-baseline stereo (WBS). SFS stably provides a rough but full 3D geometry (visual hull), and WBS refines it where WBS can be confident by prominent textures. This strategy is known to work well (sub-centimeter resolution of 3D human in motion) for controlled environments such as green/blue-backgrounds, but it is not directly applicable for real-world / outdoor scenes because its stability depends on the accuracy of the multi-view silhouettes which is not easily available for such environments. The motivation of this alternative session is to discuss about how ToF cameras can help 3D video production be robust in real-world.

Plan:

- 15 min– introduction of this session and example of ideas.
  - Accurate 2D multi-view silhouette acquisition with ToF cameras,
  - Direct full 3D reconstruction mainly by color cameras but with help of ToF cameras,

- Direct full 3D reconstruction by ToF cameras.

- 30 min– Groups of 5 people brainstorm at least one non-standard purpose/method to abuse the hardware.
- 10 min– Sketch some slides/diagrams on overhead transparencies for the best brainstorm idea(s) in each group.
- 45 min– Groups report on their best ideas (About 8 groups with 5 minutes each)
- 5 min– Session wrap up and plan for continuity (Wiki to have areas for ideas and contact info for people potentially interested)

References

1. Naveed Ahmed, Christian Theobalt, Christian Roessl, Sebastian Thrun, and Hans-Peter Seidel. Dense correspondence finding for parametrization-free animation reconstruction from video. In *Proc. of IEEE Intl. Conf. on Computer Vision and Pattern Recognition (CVPR)*, 2008.
2. Derek Chan, Hylke Buisman, Christian Theobalt, and Sebastian Thrun. A noise-aware filter for real-time depth upsampling. In *Proc. of ECCV Workshop on Multi-camera and Multi-modal Sensor Fusion Algorithms and Applications*, 2008.
3. Ryan Crabb, Colin Tracey, Akshaya Puranik, and James Davis. Real-time foreground segmentation via range and color imaging. *Computer Vision and Pattern Recognition Workshop*, 0:1–5, 2008.
4. Yan Cui, Sebastian Schuon, Derek Chan, Sebastian Thrun, and Christian Theobalt. 3d shape scanning with a time-of-flight camera. In *Proc. of IEEE Intl. Conf. on Computer Vision and Pattern Recognition (CVPR)*, 2010.
5. James Davis and Hector Gonzalez-banos. Enhanced shape recovery with shuttered pulses of light. In *IEEE Workshop on Projector-Camera Systems*, 2003.
6. M. Erz and B. Jähne. Radiometric and Spectrometric Calibrations, and Distance Noise Measurement of TOF Cameras. In R. Koch and A. Kolb, editors, *3rd Workshop on Dynamic 3-D Imaging*, volume 5742 of *Lecture Notes in Computer Science*, pages 28–41. Springer, 2009.
7. A Frick, B Bartczack, and R Koch. 3d-tv ldv content generation with a hybrid tof-multicamera rig. *3DTV-Conference: The True Vision - Capture, Transmission and Display of 3D Video (3DTV-CON), 2010*, pages 1 – 4, 2010.
8. Hector Gonzalez-Banos and James Davis. Computing depth under ambient illumination using multi-shuttered light. *Computer Vision and Pattern Recognition, IEEE Computer Society Conference on*, 2:234–241, 2004.
9. Doaa Hegazy and Joachim Denzler. Combining appearance and range based information for multi-class generic object recognition. In *CIARP*, pages 741–748, 2009.
10. Doaa Hegazy and Joachim Denzler. Generic 3d object recognition from time-of-flight images using boosted combined shape features. In *Proceedings of International Conference on Computer Vision, Theory and Applications (VISAPP 09)*, 2009.
11. Olaf Kähler, Erik Rodner, and Joachim Denzler. On fusion of range and intensity information using graph-cut for planar patch segmentation. *International Journal of Intelligent Systems Technologies and Applications*, 5(3/4):365–373, 2008.
12. M. Keller and A. Kolb. Real-time simulation of time-of-flight sensors. *J. Simulation Practice and Theory*, 17:967–978, 2009.
13. Michael Kemmler, Erik Rodner, and Joachim Denzler. Global context extraction for object recognition using a combination of range and visual features. In R. Koch and A. Kolb, editors, *Proceedings of the Dynamic 3D Imaging Workshop*, volume 5742 of *Lecture Notes in Computer Science*, pages 96–109. Springer, 2009.

14 Young Min Kim, Derek Chan, Christian Theobalt, and Sebastian Thrun. Design and calibration of a multi-view tof sensor fusion system. In *IEEE CVPR Workshop on Time-of-flight Computer Vision*, 2008.

15 Young-Min Kim, Christian Theobalt, James Diebel, Jana Kosecka, Branislav Micusik, and Sebastian Thrun. Multi-view image and tof sensor fusion for dense 3d reconstruction. In *Proc. of 3DIM*, 2009.

16 Ahmed Kirmani, Tyler Hutchison, James Davis, and Ramesh Raskar. Looking around the corner using transient imaging. In *ICCV*, pages 159–166, 2009.

17 A. Kolb, E. Barth, R. Koch, and R. Larsen. Time-of-flight cameras in computer graphics. *COMPUTER GRAPHICS forum, vol. 29, no. 1*, pages 141 – 159, 2010.

18 M. Lindner and A. Kolb. Lateral and depth calibration of pmd-distance sensors. In *Proc. Int. Symp. on Visual Computing*, LNCS, pages 524–533. Springer, 2006.

19 M. Lindner, A. Kolb, and K. Hartmann. Data-fusion of PMD-based distance-information and high-resolution RGB-images. In *Int. Sym. on Signals Circuits & Systems (ISSCS), session on Algorithms for 3D TOF-cameras*, pages 121–124. IEEE, 2007.

20 Marvin Lindner, Ingo Schiller, Andreas Kolb, and Reinhard Koch. Time-of-flight sensor calibration for accurate range sensing. *Computer Vision and Image Understanding*, 114(12):1318 – 1328, 2010. Special issue on Time-of-Flight Camera Based Computer Vision.

21 Christoph Munkelt, Michael Trummer, Peter Kuehmstedt, Gunther Notni, and Joachim Denzler. View planning for 3d reconstruction using time-of-flight camera data. In J. Denzler, G. Notni, and H. Suesse, editors, *DAGM 2009*, volume 5748 of *352–361*. Springer, 2009.

22 Jochen Penne, Kurt Höller, Michael Stürmer, Thomas Schrauder, Armin Schneider, Rainer Engelbrecht, Hubert Feußner, Bernhard Schmauss, and Joachim Hornegger. Time-of-Flight 3-D Endoscopy. In G.-Z. Yang et al., editor, *MICCAI 2009, Part I, LNCS 5761*, volume 5761, pages 467–474, Berlin / Heidelberg, 2009.

23 Jochen Penne, Christian Schaller, Joachim Hornegger, and Thorsten Kuwert. Robust Real-Time 3D Respiratory Motion Detection Using Time-of-Flight Cameras. *Computer Assisted Radiology and Surgery 2008*, 3(5):427–431, 2008.

24 Martin Rapus, Stefan Munder, Gregory Baratoff, and Joachim Denzler. Pedestrian recognition using combined low-resolution depth and intensity images. In Martin Rapus, editor, *IEEE Intelligent Vehicles Symposium*, pages 632–636, Eindhoven University of Technology Eindhoven, The Netherlands, June 2008.

25 Erik Rodner, Doaa Hegazy, and Joachim Denzler. Multiple kernel gaussian process classification for generic 3d object recognition from time-of-flight images. In *Proceedings of the International Conference on Image and Vision Computing*, 2010.

26 Christian Schaller, Andre Adelt, Jochen Penne, and Joachim Hornegger. Time-of-flight sensor for patient positioning. In Ehsan Samei and Jiang Hsieh, editors, *Proceedings of SPIE*, volume 7258, 2009.

27 Christian Schaller, Jochen Penne, and Joachim Hornegger. Time-of-Flight Sensor for Respiratory Motion Gating. *Medical Physics*, 35(7):3090–3093, 2008.

28 Ingo Schiller, Christian Beder, and Reinhard Koch. Calibration of a pmd camera using a planar calibration object together with a multi-camera setup. In *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, volume Vol. XXXVII. Part B3a, pages 297–302, Beijing, China, 2008. XXI. ISPRS Congress.

29 M. Schmidt and B. Jähne. A physical model of time-of-flight 3d imaging systems, including suppression of ambient light. In R. Koch and A. Kolb, editors, *3rd Workshop on Dynamic 3-D Imaging*, volume 5742 of *Lecture Notes in Computer Science*, pages 1–15. Springer, 2009.

30 Sebastian Schuon, Christian Theobalt, James Davis, and Sebastian Thrun. High-quality scanning using time-of-flight depth superresolution. In *IEEE CVPR Workshop on Time-of-flight Computer Vision*, 2008.

31 Sebastian Schuon, Christian Theobalt, James Davis, and Sebastian Thrun. Lidarboost: Depth superresolution for tof 3d shape scanning. In *In Proc. of IEEE Intl. Conf. on Computer Vision and Pattern Recognition (CVPR)*, 2009.

32 A. Seitel, T. Santos, S. Mersmann, J. Penne, R. Tetzlaff, and H.-P. Meinzer. Time-of-flight kameras für die intraoperative oberflächenerfassung. In *Proc BVM*, pages 11–15, 2010.

33 Savil Srivastava, Ashutosh Saxena, Christian Theobalt, Sebastian Thrun, and Andrew Ng. i23 - rapid interactive 3d reconstruction from a single image. In *Proc. of VMV*, 2009.

34 Oliver Wang, Jonathan Finger, Qingxiong Yang, James Davis, and Ruigang Yang. Automatic natural video matting with depth. In *Proceedings of the 15th Pacific Conference on Computer Graphics and Applications*, pages 469–472, Washington, DC, USA, 2007. IEEE Computer Society.

35 Qingxiong Yang, Ruigang Yang, James Davis, and David Nister. Spatial-depth super resolution for range images. *Proc. CVPR*, pages 1–8, 2007.

36 Jiejie Zhu, Liang Wang, Ruigang Yang, James E. Davis, and Zhigeng pan. Reliability fusion of time-of-flight depth and stereo for high quality depth maps. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 99(PrePrints), 2010.

37 J.J. Zhu, L. Wang, R.G. Yang, and J. Davis. Fusion of time-of-flight depth and stereo for high accuracy depth maps. In *Proc. CVPR*, pages 1–8, 2008.

Participants

- Michael Balda
Metrilus GmbH – Erlangen, DE
- Christopher Barsi
MIT – Cambridge, US
- Erhardt Barth
Universität Lübeck, DE
- Sebastian Bauer
Univ. Erlangen-Nürnberg, DE
- James E. Davis
University of California – Santa Cruz, US
- Adrian Dorrington
University of Waikato, NZ
- Martin Eisemann
TU Braunschweig, DE
- Peter Eisert
Fraunhofer-Institut – Berlin, DE
- Jürgen Gall
MPI für Intelligente Systeme – Tübingen, DE
- Marcin Grzegorzek
Universität Siegen, DE
- Diego Gutierrez
University of Zaragoza, ES
- Uwe Hahne
SICK AG – Waldkirch, DE
- Thomas Helten
MPI für Informatik – Saarbrücken, DE
- Ivo Ihrke
Universität des Saarlandes, DE
- Slobodan Ilic
TU München, DE
- Shahram Izadi
Microsoft Research UK – Cambridge, GB
- Bernd Jähne
Universität Heidelberg, DE
- Andreas Jordt
Universität Kiel, DE
- Thomas Kilgus
DKFZ – Heidelberg, DE
- Kwang In Kim
MPI für Informatik – Saarbrücken, DE
- Reinhard Klein
Universität Bonn, DE
- Andreas Kolb
Universität Siegen, DE
- Daniel Kondermann
Universität Heidelberg, DE
- Jens Kubacki
Mesa Imaging AG – Zürich, CH
- Cornelia Lanz
TU Ilmenau, DE
- Seungkyu Lee
SAIT – South Korea, KR
- Damien Lefloch
Universität Siegen, DE
- Frank Lenzen
Universität Heidelberg, DE
- Oisin Mac Aodha
University College London, GB
- Aditi Majumder
Univ. of California – Irvine, US
- Rahul Nair
Universität Heidelberg, DE
- P. J. Narayanan
IIIT – Hyderabad, IN
- Shohei Nobuhara
Kyoto University, JP
- Martin Profittlich
PMD Technologies – Siegen, DE
- Ramesh Raskar
MIT – Cambridge, US
- Christian Schaller
Metrilus GmbH – Erlangen, DE
- Andreas Schilling
Universität Tübingen, DE
- Alexander Seitel
DKFZ – Heidelberg, DE
- Christian Theobalt
MPI für Informatik – Saarbrücken, DE
- Julien Thollot
SoftKinetic-Brussels, BE
- Gordon Wetzstein
MIT – Cambridge, US
- Giora Yahav
Microsoft – Haifa, IL
- Ruigang Yang
University of Kentucky, US

Report from Dagstuhl Seminar 12441

Foundations and Challenges of Change and Evolution in Ontologies

Edited by

James Delgrande[1], Thomas Meyer[2], and Ulrike Sattler[3]

1 **Simon Fraser University, Burnaby, CA,** jim@cs.sfu.ca
2 **Meraka Institute & University of KwaZulu-Natal, ZA,** tmeyer@csir.co.za
3 **University of Manchester, GB,** sattler@cs.man.ac.uk

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 12441 "Foundations and Challenges of Change and Evolution in Ontologies", held from 28 October to 2 November 2012. The aim of the workshop was to bring together researchers working in the areas of logic-based ontologies, belief change, and database systems, along with researchers working in relevant areas in nonmonotonic reasoning, commonsense reasoning, and paraconsistent reasoning. The workshop provided a forum for discussions on the application of existing work in belief change, nonmonotonic reasoning, commonsense reasoning, and databases to logic-based ontologies. Overall the intent was to provide an interdisciplinary (with respect to computer science and mathematics) workshop for addressing both theoretical and computational issues in managing change and evolution in formal ontologies.

Seminar 28. October–02. November, 2012 – www.dagstuhl.de/12441
1998 ACM Subject Classification I.2 Artificial intelligence, I.2.4 Knowledge representation formalisms and methods, I.2.3 Nonmonotonic reasoning and belief revision, F.4.1 Computational logic, H.2.1 Logical design
Keywords and phrases Artificial intelligence, Belief change, Ontologies, Description logics
Digital Object Identifier 10.4230/DagRep.2.10.105
Edited in cooperation with Ivan Varzinczak

1 Executive Summary

James Delgrande
Thomas Meyer
Ulrike Sattler

An ontology in computer science is an explicit, formal specification of the terms of a domain of application, along with the relations among these terms. An ontology provides a (structured) vocabulary which forms the basis for the representation of general knowledge. Ontologies have found extensive application in Artificial Intelligence and the Semantic Web, as well as in areas such as software engineering, bioinformatics, and database systems.

Research in ontologies in Artificial Intelligence has focussed on description logics (DL), where a description logic can be regarded as a (decidable) fragment of first order logic. Historically a DL is divided into two components, a so-called TBox, for expressing concepts and their interrelationships, and an ABox that contains assertions about specific individuals

and instances. Thus, the TBox characterises a domain of application while the ABox contains information on a specific instance of a domain. A key point in description logics is that, via their limited expressiveness, one obtains "good", ideally tractable, inference algorithms. The number of description logics is large, with several prominent families of logics, and the complexity of description logics has been well studied. Research in ontology languages and related reasoning services, most notably in description logics, has also spurred work into logics that are weaker than classical systems, as well provided a substantial impetus for research into modal logic. Moreover, there has been substantial interaction with the database community.

The success of this work has led to an increasing demand for a variety of reasoning services, both classical and non-classical. Crucially, an ontology will be expected to evolve, either as domain information is corrected and refined, or in response to a change in the underlying domain. In a description logic, such change may come in two different forms: the background knowledge, traditionally stored in the TBox, may require modification, or the ground facts or data, traditionally stored in the ABox, may be modified. In the former case, the process is akin to theory revision, in that the underlying background theory is subject to change. In the latter case, one cannot simply update instances, as is done in a relational database, since any set of instances must accord with the potentially rich structure imposed by the TBox. The result is that one must be able to deal with changing ontologies, as well as related notions from commonsense reasoning, including nonmonotonic reasoning and paraconsistent reasoning.

The issues mentioned are of common interest to the ontology, belief change, and database communities. While there has been some interaction between researchers in these communities, there has not been a comprehensive meeting to address notions of change in ontologies in a broad or comprehensive fashion.

The aim of the workshop was to bring together researchers working in the areas of logic-based ontologies, belief change, and database systems, along with researchers working in relevant areas in nonmonotonic reasoning, commonsense reasoning, and paraconsistent reasoning. Hence the workshop's goal was to facilitate discussions on the application of existing work in belief change, nonmonotonic reasoning, commonsense reasoning, and related areas on the one hand, to logic-based ontologies on the other. There has been extensive input and interest from the database community, which also has in interest in these problems. Overall the intent was to provide an interdisciplinary (with respect to computer science and mathematics) workshop for addressing both theoretical and computational issues in managing change in ontologies. In particular, the workshop has given participants a deeper understanding of the concepts, terminologies, and paradigms used in the three areas involved, and in their latest achievements and challenges. Examples of these were the distinction between data and schema level, the relation between different revision operators and justifications, the role of less expressive description logics, to name a few.

The workshop consisted of a five-day event with the following program: On the first day there were three introductory talks by a representative in each of the areas of belief change and nonmonotonic reasoning, description logics, and databases. The purpose of these introductory talks was to come to a shared understanding (and terminology) of these areas, and provide a glimpse of the state-of-the-art and current research challenges in all three areas. On day 2, three breakout groups were created and participants were assigned to them based on their expertise but also in such a way as to have representatives of the three main areas in each group. The groups were 'Foundations and Techniques', 'Applications', and 'Perspectives and Future Directions', and their purpose was that of fostering discussions on

the three fundamental components at the intersection of the above mentioned areas. Day 3 consisted of a report back from each of the groups followed by further discussion. On the fourth day there were presentations on overlapping areas and discussions of problems and issues of mutual interest for the different communities. Day 5 had a wrap-up session with a discussion on the overlap among the different areas, future challenges and next steps in this workshop series.

2 Table of Contents

3 Overview of Talks

3.1 Ontology Views and Evolution

Franz Baader (TU Dresden, DE)

We consider two different topics related to the overall theme of the seminar: views and evolution. For the purpose of this talk, a view on an ontology is a subset of the ontology. The challenge is to pre-compute consequences of such views without doing this for every subset separately. Two instances of this overall challenge have been addressed in our work on pinpointing [2, 5, 6] and on lattice-based access control [8]. Regarding evolution, we consider the situation where an ontology represents an evolving "world" in an incomplete way. The challenge is to decide whether a certain temporal property, e.g., expressed in the temporal Description Logic $\mathcal{ALC}$-LTL [7], holds in all possible evolutions of the world. We have considered both the case where the evolution is due to a black-box "system" [3] that can only be observed and where it is due to applying actions defined in a Description Logic action theory [1, 4].

References

1 F. Baader, C. Lutz, M. Miličić, U. Sattler, and F. Wolter. Integrating description logics and action formalisms: First results. In M. Veloso and S. Kambhampati, editors, *Proceedings of the 20th National Conference on Artificial Intelligence (AAAI-05)*, Pittsburgh, Pennsylvania (USA), 2005. AAAI Press.

2 F. Baader, R. Peñaloza, and B. Suntisrivaraporn. Pinpointing in the description logic $\mathcal{EL}^+$. In *Proceedings of the 30th German Annual Conference on Artificial Intelligence (KI 2007)*, volume 4667 of *Lecture Notes in Artificial Intelligence*, pages 52–67, Osnabrück, Germany, 2007. Springer-Verlag.

3 F. Baader, A. Bauer, and M. Lippmann. Runtime verification using a temporal description logic. In S. Ghilardi and R. Sebastiani, editors, *Proceedings of the 7th International Symposium on Frontiers of Combining Systems (FroCoS 2009)*, volume 5749 of *Lecture Notes in Artificial Intelligence*, pages 149–164, Trento (Italy), 2009. Springer-Verlag.

4 F. Baader, H. Liu, and A. ul Mehdi. Verifying properties of infinite sequences of description logic actions. In H. Coelho, R. Studer, and M. Wooldridge, editors, *Proceedings of the 19th European Conference on Artificial Intelligence (ECAI10)*, pages 53–58. IOS Press, 2010.

5 F. Baader and R. Peñaloza. Automata-based axiom pinpointing. *J. Automated Reasoning*, 45(2):91–129, 2010.

6 F. Baader and R. Peñaloza. Axiom pinpointing in general tableaux. *J. Logic and Computation*, 20(1):5–34, 2010.

7 F. Baader, S. Ghilardi, and C. Lutz. LTL over description logic axioms. *ACM Trans. Comput. Log.*, 13(3), 2012.

8 F. Baader, M. Knechtel, and R. Peñaloza. Context-dependent views to axioms and consequences of Semantic Web ontologies. *J. Web Semantics*, 12:22–40, 2012.

3.2 Facilitating Ontology Refinement through Nonmonotonic DL

Piero Andrea Bonatti (University of Napoli, IT)

Joint work of Bonatti, Piero Andrea; Faella, Marco; Sauro, Luigi
Main reference P.A. Bonatti, M. Faella, L. Sauro, "EL with Default Attributes and Overriding," ISWC 2010: 64–79.
URL http://dx.doi.org/10.1007/978-3-642-17746-0_5

The process of ontology authoring and maintenance requires suitable support at different levels: tools (eg. versioning systems) as well as language extensions (eg. native support to exceptions and overriding). In this talk we argue that suitable nonmonotonic constructs for description logics may contribute to address these needs. We provide a few examples using Circumscription-based DLs, that prove to be promising in terms of expressiveness and scalability.

3.3 Handling Inconsistency of Rules Accessing Ontologies

Thomas Eiter (TU Wien, AT)

Joint work of Eiter, Thomas; Dao-Tran, Minh; Fink, Michael; Krennwallner, Thomas

Rules have been considered in order to increase the expressiveness and usage of ontologies, be it to cater for nonmonotonic inferences or to access ontologies in declarative problem solving. In this talk, we review a taxonomy of different formalisms for rules plus ontologies, and then hex-programs and dl-programs, which are extensions of answer set programming to access external sources of computation and querying ontologies in description logics, respectively. We will present issues regarding inconsistency in answer set programs and these extensions, some approaches to handle them and point out connections to theory change and ontology management, which pose open issues for future research.

3.4 An Approach for Reasoning about Typicality in Description Logics

Laura Giordano (University of Western Piemont – Alessandria, IT)

Joint work of Giordano, Laura; Gliozzi, Valentina; Olivetti, Nicola; Pozzato, Gian Luca
Main reference L. Giordano, V. Gliozzi, N. Olivetti, G.L. Pozzato, "A Non Monotonic Description Logic for Reasoning about Typicality," Artificial Intelligence, in press, 2012.
URL http://dx.doi.org/10.1016/j.artint.2012.10.004

The talk describes an approach for defining non-monotonic extensions of Description Logics, for reasoning about prototypical properties of individuals, based on a typicality operator T plus a minimal model semantics. For any concept C, T(C) singles out the instances of C that are considered as "typical" or "normal". The typicality operator T is essentially characterized by the core properties of nonmonotonic reasoning, axiomatized by preferential logic P. The approach we propose combines the use of the typicality operator with a minimal model semantics, similar in spirit to circumscription. The minimal model mechanism allows to

perform useful nonmonotonic inferences by minimizing the "non typicality" of individuals. The presentation shortly describes the non-monotonic extension of ALC (ALC+Tmin), as well as the non-monotonic extension of some low complexity DLs (namely, DL-lite-core and $EL^{\perp}$). For these extensions, tableau calculi for deciding entailment have been developed. The presentation also points out at some complexity results.

References

1 L. Giordano, V. Gliozzi, N. Olivetti, G.L. Pozzato. ALC + T: A preferential extension of description logics. *Fundamenta Informaticae* 96(3), pages 341-372, 2009.

2 L. Giordano, V. Gliozzi, N. Olivetti, G.L. Pozzato. A Non Monotonic Description Logic for Reasoning about Typicality. *Artificial Intelligence*, to appear, 2012.

3 L. Giordano, V. Gliozzi, N. Olivetti, G.L. Pozzato. Reasoning about typicality in low complexity DLs: the logics EL⊥Tmin and DL-litecTmin. In T. Walsh, ed., Proceedings of the 22nd International Joint Conference on Artificial Intelligence, pages 894-899, 2011.

4 L. Giordano, V. Gliozzi, N. Olivetti, G.L. Pozzato. Preferential Low Complexity Description Logics: Complexity Results and Proof Methods. In Y. Kazakov and F. Wolter, eds., Proceedings of the 25th International Workshop on Description Logics, 2012.

3.5 Nonmonotonic Reasoning – Survey, Perspectives, and Challenges

Gabriele Kern-Isberner (TU Dortmund, DE)

From the idea of giving up monotonicity in logic-based reasoning to comply better with the requirements of everyday life, a plethora of methods have emerged. On the one hand, from the classical logical side, default logics aim at taking the possibility of exceptions explicitly into account, or at loosening the strict link between antecedent and consequent in logical rules. On the other hand, from the probabilistic side, quantitative information was based on qualitative, logic-like structures. In between, semi-quantitative approaches like ranking functions (alternatively, possibilistic theory) and Dempster-Shafer's evidence theory were proposed to (hopefully) bridge the gap between symbolic and fully quantitative theories. Moreover, belief revision theory came into being as "the other side of uncertain reasoning", aiming at catching epistemic changes when new information arrives.

The aim of this talk is to give a survey on some prevalent approaches to nonmonotononic reasoning, distinguishing between those that use rules with default assumptions, and those that are based on defeasible rules, or conditionals. As a powerful semantics for nonmonotonic reasoning that uses both qualitative and quantitative information, we briefly recall Spohn's ranking functions. Moreover, the inference rules of system P are presented as a syntactical guideline, or calculus, for nonmonotonic reasoning. We also illustrate the nonmonotonic fallacies of probabilistic reasoning and propose Bayesian networks and the principle of maximum entropy as approaches providing high quality and efficient probabilistic reasoning. Finally, we mention very briefly the link to belief revision that is established by considering total preorders (more specifically: ranking functions) as a semantics for (iterated) belief revision.

References

1 E.W. Adams. *The Logic of Conditionals.* D. Reidel, Dordrecht, 1975.

2 C.E. Alchourrón, P. Gärdenfors, and P. Makinson. On the logic of theory change: Partial meet contraction and revision functions. *Journal of Symbolic Logic*, 50(2):510–530, 1985.

3 A.P. Dempster. Upper and lower probabilities induced by a multivalued mapping. *Ann. Math. Stat.*, 38:325–339, 1967.

4 D. Dubois, J. Lang, and H. Prade. Possibilistic logic. In D.M. Gabbay, C.H. Hogger, and J.A. Robinson, editors, *Handbook of Logic in Artificial Intelligence and Logic Programming*, volume 3. Oxford University Press, 1994.

5 J. Delgrande and P. Peppas. Revising Horn theories. In T. Walsh, editor, *Proceedings Twenty-Second International Joint Conference on Artificial Intelligence, IJCAI'11*, pages 839–844, Menlo Park, CA, 2011. AAAI Press.

6 P. Gärdenfors. Belief revision and nonmonotonic logic: Two sides of the same coin? In *Proceedings European Conference on Artificial Intelligence, ECAI'92*, pages 768–773. Pitman Publishing, 1992.

7 M. Gelfond and N. Leone. Logic programming and knowledge representation – the A-prolog perspective. *Artificial Intelligence*, 138:3–38, 2002.

8 M. Goldszmidt and J. Pearl. Qualitative probabilities for default reasoning, belief revision, and causal modeling. *Artificial Intelligence*, 84:57–112, 1996.

9 P. Gärdenfors and H. Rott. Belief revision. In D.M. Gabbay, C.H. Hogger, and J.A. Robinson, editors, *Handbook of Logic in Artificial Intelligence and Logic Programming*, pages 35–132. Oxford University Press, 1994.

10 G. Kern-Isberner. A note on conditional logics and entropy. *International Journal of Approximate Reasoning*, 19:231–246, 1998.

11 G. Kern-Isberner. *Conditionals in nonmonotonic reasoning and belief revision.* Springer, Lecture Notes in Artificial Intelligence LNAI 2087, 2001.

12 S. Kraus, D. Lehmann, and M. Magidor. Nonmonotonic reasoning, preferential models and cumulative logics. *Artificial Intelligence*, 44:167–207, 1990.

13 D. Makinson. General patterns in nonmonotonic reasoning. In D.M. Gabbay, C.H. Hogger, and J.A. Robinson, editors, *Handbook of Logic in Artificial Intelligence and Logic Programming*, volume 3, pages 35–110. Oxford University Press, 1994.

14 D. McDermott and J. Doyle. Non-monotonic logic I. *Artificial Intelligence*, 13:41–72, 1980.

15 J.B. Paris. *The uncertain reasoner's companion – A mathematical perspective.* Cambridge University Press, 1994.

16 Jeff Paris. Common sense and maximum entropy. *Synthese*, 117:75–93, 1999.

17 J. Pearl. *Probabilistic Reasoning in Intelligent Systems.* Morgan Kaufmann, San Mateo, Ca., 1988.

18 D. Poole. A logical framework for default reasoning. *Artificial Intelligence*, 36:27–47, 1988.

19 R. Reiter. A logic for default reasoning. *Artificial Intelligence*, 13:81–132, 1980.

20 G. Shafer. *A mathematical theory of evidence.* Princeton University Press, Princeton, NJ, 1976.

21 W. Spohn. Ordinal conditional functions: a dynamic theory of epistemic states. In W.L. Harper and B. Skyrms, editors, *Causation in Decision, Belief Change, and Statistics, II*, pages 105–134. Kluwer Academic Publishers, 1988.

3.6 The History of the Semantic Web

Peter F. Patel-Schneider (Nuance Communications – Mountain View, US)

This personal account describes the genesis and unfolding of the Semantic Web from its beginning to Anno Semantici Webi 22.

3.7 DL-Lite Ontology Changes

Zhe Wang (University of Oxford, GB)

Joint work of Wang, Zhe; Wang, Kewen; Topor, Rodney
Main reference Z. Wang, K. Wang, R. Topor, "A new approach to DL-Lite knowledge base revision," in Proc. of 24th AAAI Conf. on Artificial Intelligence (AAAI'10), pp. 369–374, 2010.
URL http://www.aaai.org/ocs/index.php/AAAI/AAAI10/paper/view/1786

Changing ontologies in description logics (DLs) in a syntax-independent manner is an important and challenging problem for ontology management. In this talk, we present a framework for adapting classical model-based belief change techniques to DL-Lite. Unlike propositional logic, a DL ontology may have infinitely many models with complex and often infinite structures, which introduce complexity to the definition of model distances, make computation via models impossible, and cause expressibility problems. For this reason, we first present an alternative semantic characterisation for DL-Lite by introducing the concept of features as approximations to classical DL models, and then define specific revision and merging operators for DL-Lite ontologies based on features. We present the desired properties possessed by these operators, as well as algorithms for computing the result of changing in DL-Lite. Remarkably, the complexity of the proposed operations in DL-Lite is on the same level as major belief change operators in propositional logic. Finally, prototype implementations of these operators are briefly presented.

4 Breakout Groups

4.1 Report of the Foundations Group

James P. Delgrande (Simon Fraser University – Burnaby, CA)

URL http://www.cs.sfu.ca/ jim/Foundations.pdf

The Foundations group was made up of a diverse group of 15 people, with areas of research including description logics, belief change, nonmonotonic reasoning, and database systems. Ten topics for discussion were identified, of which four were immediately put on hold. There was lively discussion on the remaining issues – ABox and TBox change, first-order issues, relevance, nonmonotonic subsumption, and the role of views.

There was agreement on some issues, for example that belief change needs to go beyond propositional accounts if it is to be useful for dealing with change in description logics; moreover a semantics and/or methodology is needed for change in description logics.

There was also recognition of common problems, notably relevance. If any overall conclusion can be drawn, it is that the 3 areas (BR, DL, DB) have somewhat different aims and methodologies on the one hand, yet broadly common problems on the other hand. While the communities are on the whole separate, it was worthwhile to get together and, moreover, it would be useful to continue meeting, perhaps focussing on a narrower topic.

4.2 Report of the Applications Group

Ulrike Sattler (University of Manchester, GB)

URL http://www.cair.za.net/node/115/Applications.pptx

In the Applications breakout group, we exchanged our views

1. on current developments,
2. new trends and challenges,
3. novel solution or coping techniques, and
4. general paradigms

in applications of the 3 different areas.

We had lively discussions and exchanged interesting and telling stories, partly concerned with (overcoming) communication difficulties between (end) users and tool developers and the usual chicken-and-egg difficulties of getting hold of suitable test data for tool development and optimisation. We had the impression that the three different communities had quite different quality criteria, paradigms, and evaluation approaches to their tools, and also value them in quite different ways: exchanging these different views and approaches is set to be useful in future collaborations, but also for exchanging and learning from each other.

4.3 Report of the Perspectives Group

Thomas Meyer (Meraka Institute & University of KwaZulu-Natal, ZA)

URL http://www.cair.za.net/sites/default/files/downloads/Perspectives.pdf

The brief of the Perspectives breakout group was to consider the following three aspects of each of the areas of databases, belief revision/nonmonotonic reasoning, and description logic:

1. Exciting developments
2. Pressing issues and open problems
3. Challenging areas

What followed was a vigorous discussion, culminating in a (perhaps surprisingly) fair level of consensus on these three points. More details can be found in the slides summarising the work of this breakout group. All participants agreed that one of the most valuable

developments of the breakout session was the opportunity to gain a better understanding of the details, as well as the perceived successes and problems of those areas in which they are not experts. This may well form the basis of increased collaborative efforts between the different areas.

Participants

- Marcelo Arenas
Univ. Catolica de Chile, CL
- Franz Baader
TU Dresden, DE
- Leopoldo Bertossi
Carleton Univ. – Ottawa, CA
- Meghyn Bienvenu
Université Paris Sud, FR
- Alexander Bochman
Holon Inst. of Techn., IL
- Piero Andrea Bonatti
University of Napoli, IT
- Diego Calvanese
Free Univ. Bozen-Bolzano, IT
- David Carral Martínez
Wright State University – Dayton, US
- Giovanni Casini
Meraka Institute – Pretoria, ZA
- James P. Delgrande
Simon Fraser University – Burnaby, CA
- Thomas Eiter
TU Wien, AT
- Eduardo Fermé
Univ. of Madeira – Funchal, PT
- Giorgos Flouris
FORTH – Heraklion, GR
- Laura Giordano
University of Western Piemont – Alessandria, IT
- Birte Glimm
Universität Ulm, DE
- Andreas Herzig
Paul Sabatier University – Toulouse, FR
- Ian Horrocks
University of Oxford, GB
- Aaron M. Hunter
British Columbia Institute of Technology – Burnaby, CA
- Ryutaro Ichise
NII – Tokyo, JP
- Gabriele Kern-Isberner
TU Dortmund, DE
- Marcel Lippmann
TU Dresden, DE
- Carsten Lutz
Universität Bremen, DE
- Robert A. Meersman
Vrije Universiteit Brussel, BE
- Thomas Meyer
CSIR Meraka & University of KwaZulu-Natal, ZA
- Jeff Z. Pan
University of Aberdeen, GB
- Peter F. Patel-Schneider
Nuance Communications – Mountain View, US
- Rafael Penaloza
TU Dresden, DE
- Marcio Moretto Ribeiro
University of Sao Paulo, BR
- Riccardo Rosati
University of Rome "La Sapienza", IT
- Ulrike Sattler
University of Manchester, GB
- Stefan Schlobach
VU – Amsterdam, NL
- Matthias Thimm
Universität Koblenz-Landau, DE
- David Toman
University of Waterloo, CA
- Leon van der Torre
University of Luxembourg, LU
- Ivan José Varzinczak
Meraka Institute – Pretoria, ZA
- Kewen Wang
Griffith Univ. – Brisbane, AU
- Zhe Wang
University of Oxford, GB
- Renata Wassermann
University of Sao Paulo, BR
- Grant Weddell
University of Waterloo, CA
- Emil Weydert
University of Luxembourg, LU
- Frank Wolter
University of Liverpool, GB

Report from Dagstuhl Seminar 12442

Requirements Management – Novel Perspectives and Challenges

Edited by

Jane Cleland-Huang[1], Matthias Jarke[2], Lin Liu[3], and Kalle Lyytinen[4]

1 **DePaul University – Chicago, US,** `jhuang@cs.depaul.edu`
2 **RWTH Aachen and Fraunhofer FIT, DE,** `jarke@cs.rwth-aachen.de`
3 **Tsinghua University Beijing, CN,** `linliu@tsinghua.edu.cn`
4 **Case Western Reserve University – Cleveland, US,** `kalle@case.edu`

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 12442 "Requirements Management – Novel Perspectives and Challenges". Changes in computational paradigms and capabilities that draw upon platform strategies, web services, and virtualization of both application services and development platforms have significant implications for views of modularity and requirements evolution, complexity of RE tasks, and the economics of system development and operations. The aim of the seminar was to bring together experts from multiple fields to discuss models and theories around these changes. Three key challenges and associated solution ideas were addressed, namely (1) to better deal with context changes and business goal management to reduce the "black swan" rate of badly failed large projects, (2) to exploit recent theories of technological and institutional evolution to understand better how to control complexity and leverage it for innovation at the same time, and (3) the demand for runtime re-organization of existing large-scale systems with respect to new operational goals such as energy efficiency. Future RE must see itself as the marketplace where responsibility for all these complexities and evolutionary steps is traded.

Seminar 28.–31. October, 2012 – www.dagstuhl.de/12442
1998 ACM Subject Classification D.2.1 Requirements, D.2.2 Design Tools and Techniques, D.2.11 Software Architectures
Keywords and phrases requirements engineering, system complexity, software evolution, socio-technical systems
Digital Object Identifier 10.4230/DagRep.2.10.117
Edited in cooperation with Anna Hannemann (RWTH Aachen, DE)

1 Executive Summary

Matthias Jarke

Since its inception in the 1970s, much of the research in requirements engineering (RE) has focused on the development of formal notations and protocols to represent requirements and to analyze their properties, such as consistency, correctness, completeness, and validity. Some work has analyzed the impacts of these requirements on downstream development tasks (e.g., traceability), or managing and reconciling conflicts in the requirements process.

Much of requirements research has also assumed that the scope of RE is isolated to a specific project or even a specific stage of that project. The demand for a shift in focus is dictated by changes in computational paradigms and capabilities that draw upon platform strategies, web services, and virtualization of both application services and development platforms. These trends have significant implications for views of modularity and requirements evolution, complexity of RE tasks, and the economics and costs related to application and service use and development. The aim of the seminar was to bring together experts from multiple fields to discuss models and theories around these changes, focusing on a series of interrelated question such as:

- How to theorize and study complexity within RE tasks?
- What theoretical perspectives can inform how and why requirements knowledge evolves as it is generated, validated, and distributed?
- How do requirements, system evolution, and environmental change interact?
- How do different types of knowledge interact to shape requirements and their evolution?
- What are the origins and flows of influence of requirements knowledge? How can non-linear influences be effectively managed in RE evolution?
- What is the effect of speed and scale in requirements processes?
- What is the role of goals and constraints and their complex interactions in RE?

In particular we sought better integration of theories of socio-technical system evolution, distributed cognition, models of RE and design knowledge and their economic effects, the impact of strategy and related knowledge endowments in RE processes (e.g., explorative vs. exploitative processes of requirements discovery), and the role of ambiguity, uncertainty and complexity in managing requirements knowledge. Attention was also placed on new research approaches and methods that can be brought to bear in addressing these problems. The seminar thus built and expanded on some of the critical themes that had been brought up five years earlier in two NSF-sponsored workshops in Cleveland [5] and Dagstuhl [4], [3]. The seminar brought together 33 researchers (exactly one third female) from 12 countries in four continents, with 22% industry participation. Participants felt that this unusually high diversity together with a good mix of junior and senior people of different disciplines, interests and expertise contributed strongly to lively and fruitful discussions. Several cooperative projects have emerged from these discussions. Selected results of the discussions and presentations will be published in a special issue of the ACM Transactions on Management Information Systems in 2014.The program of the seminar was organized into four panels with plenary talks and discussion, five parallel working groups with central reporting, and a final reflection session. With the parallel Dagstuhl seminar on "Foundations and Challenges of Change and Evolution of Ontology" we moreover organized a crossover plenary panel session in which we tried to converge to a better mutual understanding of the different perspectives on Evolution in AI and RE and explored possibilities for future cooperation. Several individual researchers later got together to agree on specific cooperative research. In the final reflection session, the main results, issues and challenges, also taking into account the ontology perspective, can be summarized as follows.

Jackson and Zave [2] have formulated an AI-inspired formalization of the traditional RE viewpoint as a kind of model-based diagnosis: Given a set of domain assumptions D and a set of requirements R, find a suitable specification S such that S, $D \Rightarrow R$. In RE research, the R have often been interpreted as goals, to be refined and satisfied in some extended $AND-OR$ graph structure.

From a social science and business informatics perspective, however, requirements engineering (RE) is in essence a boundary spanning task between the developers and the

other stakeholders (users, management, regulators, ...) concerning the goals, functions and constraints of a system. The traditional viewpoint, where RE is just seen as an "early phase" (resulting in a contract) and the "last phase" (where acceptance testing takes place) is far too narrow. The following citation by Robert Glass wonderfully characterizes the situation RE has entered since the turn of the century: *"Walking on water, and programming according to specifications is easy – as long as both of them are frozen"* At least three key challenges to research and practice were identified in the seminar, together with counter-strategies where promising first steps for solutions were observed: Firstly, *large-scale projects* encounter changes in D, R, and the technology underlying S is shifting. As a consequence,

- 90% of these projects run over budget and time (this is similar to other big engineering projects, so not a drama in itself)
- One sixth so-called *Black Swan* projects show budget overruns of 70% and time overruns of 200% (this is true only for 1% of other engineering projects, so this is a real drama of software engineering).

A central cause is politically motivated over-ambitious goals with systematic under-estimation of the nature and scope of requirements, budget, and cost both on the side of customers and vendors, as well as poor change tracking. As a consequence, we strongly recommend to not just consider goals of stakeholders but also social structures and strategic dependencies in initial system analysis. Moreover, customer and other stakeholder requirements must be continuously monitored during the development process (and sometimes beyond). To ensure product and process compliance and effectively assess the impact of change, requirements traceability should be focused by using trace patterns to maintain transparency and keep the monitoring effort acceptable and feasible.

Secondly, we need architectural mechanisms that *constrain, but also leverage complexity.* In the seminar, John King pointed out the difference between "complicated" and "complex" problems. Complicated problems can be solved by experienced, highly competent engineers with foreseeable effort. In contrast, complex problems can only be explored with uncertain results; thus, taking on a project that tries to solve a complex problem in one shot is bound to lead to disaster – and apparently, it is exactly the tendency to take on such nice-sounding complex projects that leads to the unusually high share of Black Swans in software projects. Theories like Arthur's theory of Technology Evolution [1] or Thornton's theory of institutional evolution [6] were cited in the seminar as showing a way forward, which we can also observe in practice. Platform strategies offer complicated but manageable base solutions that are now being offered both by open source communities and by big players in different sectors, such as IBM, Google, Facebook, and mobile phone vendors/operators. With a uniform infrastructure, they limit complexity. But by enabling innovation at the margin, e.g. end-user developed app's, they at the same time also leverage new complexity at the higher level. The easy entry, combined with ruthless selection of a very small percentage of truly successful apps, then offers a hotbed of complex evolutionary change. Which eventually will grow into, or be replaced again by yet another layer of platforms, as pointed out by both Brian Arthur and the earlier book by Thomas Friedman "The World is Flat". Beyond such market selection mechanisms, software vendors employ various mechanisms to participate in this game in a more controlled way. We mention here the now broad area of software product families, but also Google's 70 : 20 : 10 work rule where employees are free to spend a significant part of their work time on their own ideas, thus fostering continuous internal innovation. Methods for runtime requirements monitoring and requirements mining from usage patterns can be important contributions of the RE field in this context. Last not least, the future will not reduce the challenges of complexity and evolution. Our seminar

understood information systems as socio-technical systems, but in fact many of today's systems are neither truly social nor truly technical. From a social perspective, there is the new question for sustainability of systems, with the demand for re-optimization from the viewpoint of user rights (e.g. asymmetric information and market powers, privacy, data ownership, copyright vs. freedom of information), energy efficiency, and environmental footprint. From a technical perspective, the explosive expected growth of Cyberphysical Systems (Internet of Things) in business, engineering and science is not just an approach to monitor and actuate at a much more fine-grained level, but a significant source of more complexity and evolutionary challenges. Generating and implementing e.g. the visions of smart cities is just but one example. Rather than just talking grand new visions here, methods for how to get there step-by-step in an "only" complicated way – without exposing whole city to the chaos caused by over-ambitious "complex" systems – are urgently needed.In our world of more and more ubiquitous computing, where the impact and complexity of systems continuously seem to grow, *RE is the marketplace where responsibility is traded*, as communication, mutual understanding, and transparent well-structured information management are at the heart of this field.

References

1 B. Arthur (2009). The Nature of Technology: What it is and how it Evolves. Free Press.
2 M. Jackson, P. Zave (1995): Deriving specifications from requirements: an example. Proc. 17th ICSE.
3 M. Jarke, K. Lyytinen, eds. (2010): High Impact Requirements Engineering. Special Issue, Wirtschaftsinformatik/BISE 52, 3.
4 M. Jarke, P. Loucopoulos, K. Lyytinen, J. Mylopoulos, W.N. Robinson (2011): The brave new world of design requirements. Information Systems 36(7): 992–1008.
5 K. Lyytinen, P. Loucopoulos, J. Mylopoulos, W.N. Robinson, eds. (2009). Design Requirements Engineering – A Ten-Year Perspective. Springer LNBIP 14.
6 P. Thornton, W. Occasio, M. Lounsbury (2012). The Institutional Logics Perspective: A New Approach to Culture, Structure, and Process. Oxford University Press.

2 Table of Contents

Working Groups

3 Overview of Talks

3.1 Requirements for Digital Infrastructure Innovation: Three Broad Strategies for Organizations

Nicholas Berente (University of Georgia, US)

Trends in requirements engineering are shifting from a focus on discrete software projects for a particular user community in a particular organization to broad co-evolving and interdependent ecosystems of hardware, software, communications, social practices, business processes, and organizational structures ([7]). This shift is reflected in the increased emphasis on architectures, platforms, and integration that enable ongoing emergent and unpredictable phenomena ([5]; [7]). Contemporary artifacts are increasingly infrastructural, and innovation on digital infrastructures is a fundamentally different sort of thing from the discrete software engineering context around which the requirements engineering discipline grew up. According to Tilson, Lyytinen and Sorensen:

"digital infrastructures can be defined as shared, unbounded, heterogeneous, open, and evolving sociotechnical systems comprising of an installed base of diverse information technology capabilities and their user, operations, and design communities." ([11] p. 748-749, based on [6])

Many organizations – of a variety of different stripes – are looking to participate in and capitalize on digital infrastructure innovation. Organizations do this for a variety of reasons, including:

- Direct Return (examples: Microsoft Office; Apple's platform) – ownership of infrastructures such as platforms as a key element of their product strategy, and associated competitive and profitability issues ([12]);
- Indirect Return (examples: Red Hat Linux; Yahoo! and Hadoop) – building competencies and access to resources which enable indirect business models associated with competitiveness in other domains or complementary products ([4]; [2]);
- Infrastructural Stewardship (examples: U.S. Cyberinfrastructure Centers; Apache and Hadoop) – the organization's mission is to tend to and guide (i.e. "steward") the emergence of a particular digital infrastructure domain ([2]).

Although organizations do look to participate in digital infrastructure innovation, this is not so simple a task. Digital infrastructures are complex and emergent , which poses a number of challenges to their design and management ([6]; [12]). It is simply not possible to specify requirements for an entire infrastructure because of this complexity, and also because of the open, layered generativity that accompanies digital innovation ([13]; [11]). Given this complexity, at this point there is no clear guidance for how organizations who wish to participate in digital infrastructure innovation should go about their requirements activity to define the scope of such innovation.

To begin addressing this situation, we draw upon research into U.S. cyberinfrastructure centers [2] and how they handle requirements for infrastructural innovation. We find three broad strategies that go from less to more centrally controlled: (1) a problem solving strategy; (2) a portfolio & market strategy; and (3) an institutional shift strategy. Next we briefly address the challenges of digital infrastructure innovation and present these three strategies with brief examples from our research. We conclude with a discussion on the merits of the portfolio and market strategy for organizations wishing to engage in digital infrastructure

innovation and motivate the need to understand what requirements for this form of innovation look like.

References

1. Berente, N., Claggett, J., Howison, J. Knobel, C. and Rubleske, J., (2012) "Managing CI Centers: An Agenda for Organizational Scholarship and Cyberinfrastructure Innovation," report on the workshop: 'Managing CI Centers.' Available at SSRN (August 14, 2012):http://ssrn.com/abstract=2128872.
2. Dahlander, L. and Magnusson, M. How do Firms Make Use of Open Source Communities? Long Range Planning 41, 6 (2008), 629–649.
3. Edwards, P., Jackson, S., Bowker, G., and Knobel, C. (2007). Report to the NSF of a Workshop on "History and Theory of Infrastructures: Lessons for new scientific infrastructures." University of Michigan, School of Information.
4. Fitzgerald, B. (2006). The transformation of Open Source Software. MIS Quarterly, 30(4).
5. Hansen, S., Berente N. and Lyytinen, K., (2009) "Requirements in the 21st Century: Current Practice & Emerging Trends," in Lyytinen, Loucopoulos, Mylopoulos, Robinson eds, Design Requirements Engineering: A Ten-Year Perspective, Springer-Verlag (Lecture Notes in Business Information Processing Series Vol.14), 2009.
6. Hanseth, O., and Lyytinen, K. (2010). Design theory for dynamic complexity in information infrastructures: the case of building internet. Journal of Information Technology, 25, 1–19.
7. Jarke, M. (2009) "On Technology Convergence and Platforms: Requirements Challenges from New Technologies and System Architectures," in Lyytinen, Loucopoulos, Mylopoulos, Robinson eds, Design Requirements Engineering: A Ten-Year Perspective, Springer-Verlag (Lecture Notes in Business Information Processing Series Vol.14), 2009.
8. Mitra, S. (2005). Information technology as an enabler of growth in firms: An empirical assessment. JOURNAL OF MANAGEMENT INFORMATION SYSTEMS, 22(2), 279–300.
9. Ribes, David, and Finholt, T. A. (2009). The Long Now of Technology Infrastructure: Articulating Tensions in Development. Journal of the Association for Information Systems, 10(5), 375–398.
10. Star, S., and Ruhleder, K. (1996). Steps toward an ecology of infrastructure: Design and access for large information spaces. INFORMATION SYSTEMS RESEARCH, 7(1), 111-134.
11. Tilson, D., Lyytinen, K., and Sorensen, C. (2010). Digital Infrastructures: The Missing IS Research Agenda. INFORMATION SYSTEMS RESEARCH, 21(4), 748-759. doi:10.1287/isre.1100.0318
12. Tiwana, A., Konsynski, B., and Bush, A.A. 2010. "Platform Evolution: Coevolution of Platform Architecture, Governance, and Environmental Dynamics," Information Systems Research (21:4), pp 685–687.
13. Yoo, Y., Henfridsson, O., and Lyytinen, K. (2010). The New Organizing Logic of Digital Innovation: An Agenda for Information Systems Research. Information Systems Research, 4(21), 724–735.

3.2 Models of Institutional Evolution for Requirements Engineering

Nicholas Berente (University of Georgia, US)

Requirements engineering as a discipline is fundamentally concerned with change. Certain sociotechnical practices, however, are deeply entrenched in organizational contexts and, as a result, can be quite difficult to change. As the quotes above indicate, practices can be reinforced from a number of sources: ,"the way we do things around here," implies cognitive economizing; professional pressures imply norms that are driven by identities; and compliance with government mandates implies regulatory pressures. These three forces for deeply entrenching sociotechnical practices are often described as the "pillars" of institutional analysis ([8]). Cognitive, normative, and regulatory sources for institutional persistence and stability.

Sometimes people resist just because they don't want to change. Other times, however, users resist change efforts because there are powerful 'social' forces (of the cognitive, normative, and regulatory variety) that may be reinforcing the existing situation. The former may just be an issue of convincing the person to change and perhaps appeal to their self-interest, whereas the latter may require substantially rethinking the situation. In these situations that are more deeply at odds, it is sometimes useful to investigate whether the "institutional logics" ([5]) that guide the action are consistent between the local context and the change. Institutional logics are the symbolically shaped goals and assumptions implied by patterns of action in a particular domain ([9]). Institutional logics embody the "rules of the game" so to speak ([2]). Organizational contexts are institutionally plural ([6]) and are rife with multiple, often contradictory institutional logics. In cases where the resistance to change is more deeply grounded in contrasting goals, values and assumptions about particular actions that might undermine user identities, the institutional logics of the local context and the change are contradictory ([2]). When business analysts and software engineers go about eliciting requirements for a sociotechnical change, it is important understand those "social" forces that may lead people to resist what appears to be a perfectly reasonable change from the perspective of the development team.

Just as some of these institutional forces tend to reinforce existing situation, new institutional pressure can also help drive change in ways consistent with prevailing or dominant institutions. Organizational actors respond to coercive, normative, and mimetic mechanisms for change ([3]). Thus we can see institutional pressure as simultaneously either a force for stability and a force for change of existing sociotechnical patterns of action. The clash of contradictory institutions is a key driver for bringing about institutional change ([7]). Individuals who draw upon alternative logics to change existing institutions are often described as "institutional entrepreneurs" ([4]; [9]).

Given the stability of organizational contexts borne of entrenched institutions, how can requirements professionals thus navigate this institutional landscape of persistence an isomorphic change? In this essay, we briefly introduce the recent model for institutional evolution following the new "institutional logics perspective" of institutional change ([9]) and reflect on how this model may be relevant for requirements engineering.

References

1 Berente, N. and Yoo, Y. (2012) "Institutional Contradictions and Loose Coupling: Post-Implementation ofNASA's Enterprise Information System," Information Systems Research, Vol.23, No. 2.

2 Bourdieu, P. and Wacquant, L.J.D. (1992) An Invitation to Reflexive Sociology, University of Chicago Press.
3 DiMaggio, P.J., and Powell, W.W. (1983). The Iron Cage Revisited – Institutional Isomorphism andCollective Rationality in Organizational Fields. American Sociological Review, 48(2), 147–160.
4 DiMaggio, P. (1988) "Interest and Agency in Institutional Theory," In L. Zucker (ed) Institutional Patternsand Organizations,Balinger Pub.
5 Friedland, R., and Alford, R.R. (1991) "Bringing Society Back In: Symbols, Practices, and InstitutionalContradictions," in Powell, W.W., and DiMaggio, P.J. eds (1991), The New Institutionalism inOrganizational Analysis, The University of Chicago Press, 1991.
6 Kraatz, M.S. and Block, E.S. (2008) "Organizational Implications of Institutional Pluralism." In R. Greenwood, et al (eds.) Handbook of Organizational Institutionalism, London: Sage
7 Seo, M.G. and Creed, W.E.D. (2002) "Institutional contradictions, praxis, and institutional change: Adialectical perspective." Academy of Management Review, v. 27 issue 2, 2002, p. 222.
8 Scott, W.R. (2008) Institutions and Organizations, third edition, Sage Publications, 2008.
9 Thornton, P.M., Ocasio, W., and Lounsbury, M. (2012) The Institutional Logics Perspective: A New Approach to Culture, Structure, and Process, Oxford University Press.

3.3 Has Time Stood Still in Requirements Engineering?

Richard Berntsson Svensson (Lund University, SE)

Since the inception of requirements engineering in the 1970s, a major shift has taken place. This shift is not only related to, e.g. changes in globalization, but also changes in economic activities and the merge of traditional industries and technology industries. Just as the industrial revolution replaced agriculture as the dominant economic activity, the 'creativity age' is replacing the 'information age' as the next dominant global economic activity. Although the importance of creativity in requirements engineering is argued, both by empirical evidence and that creativity has received more attention in requirements engineering research in the last couple of years, relatively little requirements engineering research has addressed creativity. I believe that economic and market trends imply that requirements engineering will have to become significantly more creative to realize the potential of future software applications. These changes lead to that the complexity and size of software-intensive systems continues to increase. Hence, scaling software in a controlled and efficient way may become a crucial competitive advantage. How many requirements can an industrial system development organization manage with available requirements engineering processes? This is hard to know as requirements engineering research often falls short in characterizing the scalability of proposed methods.

3.4 Requirements Engineering for Requirements Engineering

Joerg Doerr (Fraunhofer IESE – Kaiserslautern, DE)

Joint work of Doerr, Joerg; Hess, Anne
Main reference A. Gross, J.Doerr, "What You Need Is What You Get! The Vision of View-Based Requirements Specifications," in Proc. of 20th IEEE Int'l Requirements Engineering Conf. (RE), pp. 171-180, 2012.
URL http://dx.doi.org/10.1109/RE.2012.6345801

Software requirements specifications play a crucial role in software development projects. Especially in large projects, these specifications serve as a source of communication and information for a variety of roles involved in downstream activities like architecture, design, and testing. The Dagstuhl Workshop claims that there is a major shift in how we need to approach the RE task due to changes in computational paradigms and to development of organizational capabilities. This position paper argues that our RE community has currently little knowledge about what our stakeholders, i.e., the stakeholders of requirements specifications want to see in requirements specifications and that this will even be worse in the light of the prospected major shift to RE. It argues that in order to create high-quality requirements specifications that fit the specific demands of successive document stakeholders, our research community needs to better understand the particular information needs of requirements specification's stakeholders, but especially the downstream development roles like architects and testers. So more Requirements Engineering for Requirements Engineering needs to take place.

3.5 Requirements Management for Service Providers: the Case of Services for Citizens

Xavier Franch (UPC – Barcelona Tech – Barcelona, ES)

Main reference X. Franch, "Requirements Management for Service Providers: the Case of Services for Citizens," arXiv:1301.4600v1 [cs.SE], 2013.
URL http://arxiv.org/abs/1301.4600

Take the Internet of Things, a piece of cloud computing, a handful of smart cities, don't forget social platforms, flavor it with mobile technologies and ever-changing environments, shake it up and... voilà! What a wonderful service! Oops! Wait a minute, where did my requirements go?

3.6 The Importance of Continuous Value Based Project Management in the Context of Requirements Engineering

Gilbert Fridgen (Universität Augsburg, DE) and Julia Heidemann (McKinsey & Company, DE / Universiät Regensburg, DE)

Joint work of Fridgen, Gilbert; Heidemann, Julia
Main reference G. Fridgen, J. Heidemann, "The Importance of Continuous Value Based Project Management in the Context of Requirements Engineering," arXiv:1301.5438v1 [cs.SE], 2013.
URL http://arxiv.org/abs/1301.5438

Despite several scientific achievements in the last years, there are still a lot of IT projects that fail. Researchers found that one out of five IT-projects run out of time, budget or value. Major reasons for this failure are unexpected economic risk factors that emerge during the runtime of projects. In order to be able to identify emerging risks early and to counteract reasonably, financial methods for a continuous IT-project-steering are necessary, which as of today to the best of our knowledge are missing within scientific literature.

3.7 Requirements Engineering Discovery in Open Source Software Projects

Anna Hannemann (RWTH Aachen, DE)

Open source software (OSS) presents a class of successful community-driven systems. Software engineering (SE) in OSS is a subject of many studies. The researchers discover, investigate, and even simulate the organization of development processes within open-source communities using data from publicly available OSS code repositories and communication platforms. However, organization of requirements engineering (RE) in OSS is seldom addressed. The requirements in OSS are not explicitly defined. They are intertwined into the development and communication process of open-source community members.

By analyzing RE in OSS, we can learn, how different layers within communities are integrated in OSS development process. Does their voice matter? Which structural and organizational changes do influence significantly an OSS project in general and organization of RE in particular? Are there different participation model in terms of requirements negotiation? The answers to these and other related research questions can help us to design community-oriented RE for development of complex, socio-technical systems within interdisciplinary, distributed teams.

3.8 Requirements Engineering as a Distributed Cognitive Process

Sean Hansen (Rochester Institute of Technology, US)

Effective requirements engineering has remained a persistent impediment to the success of information systems projects. In this research, we undertake a novel reframing of requirements

engineering as a socio-technical distributed cognitive process in which diverse stakeholders collaborate to reach a collectively-held and feasible understanding of design requirements. This pursuit of shared understanding represents the 'computing' of a closure on a requirements set based on distributed representations. We draw upon the theory of distributed cognition to analyze the ways in which requirements processes become distributed across social, structural, and temporal boundaries and how the requirements computation unfolds in diverse development environments. In this position paper, we highlight the complementarities and challenges that a distributed cognitive perspective presents for long-standing topics in requirements engineering research. In addition, we posit a number of new lines of inquiry that this approach engenders.

3.9 Orthogonal Perspectives on Taming Complexity

Jane Cleland-Huang (DePaul University – Chicago, US)

This position paper discusses several different forms of software complexity. It describes a variety of techniques for managing, embracing, and living-with complexity throughout the software development life-cycle. Finally, the paper advocates creating strategic traceability links that can be used to generate comprehensible and meaningful views that slice the system and provide the stakeholders with the information they need to perform specific tasks.

3.10 Walk Before You Run: A Dialogue with Three US Developers on "Within" Complexity of Requirements

Jane Huffmann Hayes (University of Kentucky, US)

When considering how to manage complexity within requirements, it is prudent to understand industry opinion. Toward that end, three developers were consulted, one from IBM, one from HP (a startup bought by HP), and one from a small industrial programming company (use some automation to accomplish manufacturing). Based on their feedback, it is the position of this author that much of Industry is still attempting to ensure capture and use of requirements; we may be asking them to run before they walk if we 'push' techniques aimed at managing complexity. The questions and industry responses follow. A suggestion of a first step toward addressing complexity closes out the paper.

3.11 Complexity Explained

John Leslie King (University of Michigan – Ann Arbor, US)

The title for this was assigned to me. As my colleague said when the assignment was made, "I'm sure you can talk about this." Hmmm. Turns out he was right: I can talk about it. And it is important.

People use the term "complexity" a lot in requirements, but there is more to it than meets the eye. What people often talk about as complex is, in fact, complicated. What is the difference? Complicated means lots of parts, and perhaps lots of causal connections between the parts. Complicated might be hard to understand but it can be understood. Complex, in contrast, typically means things that are changing, evolving, becoming something that is at once similar to and different from the thing it used to be. The important issue is control. We typically at least can control things that are complicated; we typically cannot control things that are complex. This does not mean that we cannot understand complex things, we sometimes can. But it is hubris to think that just because we understand something we can control it. And it is worse than hubris to think we can control things we do not understand.*

This brings us to the issue of requirements. I used to think that requirements engineering was a way to help us address complexity. I have changed my mind on that. I think that requirements engineering can be useful when helping us to create systems that address complicated problems, but the moment we cross from complicated into complex, requirements engineering fails us. Put simply, we can build software that deals with complicated things, but we cannot build software that deals with complex things. And requirements engineering – or any other methods-based approaches to improving software development – will save us from this fact. The smart requirements engineer, therefore, keeps the effort focused on dealing with the complicated, and out of the complex. Complicated is hard enough. Complex is impossible. Maybe this should be a new tenet of requirements engineering: keep it complicated, but not complex.

*We deal all the time, and often successfully, with things we do not understand at some level. We have managed to control many kinds of physical materials without fully understanding the nature of matter. We have applied 'fuzzy logic' to making things work even though we do not completely understand them. Good workarounds allow us to work around problems. Also, what we can control changes over time, as we come to understand things or create workarounds.

3.12 Where is the human mind in requirements engineering (research) and what do we think and know of it?

Kim Lauenroth (adesso AG – Dortmund, DE)

We have to reconsider our theories, methods, models and tools taking into account the limitations and abilities of the human mind on both sides, the requirements engineer's

side and the stakeholder's side. Without a profound understanding of our own mind, the development of requirements engineering theories, methods, models, techniques etc. is not optimal since we are developing 'software' for a machine that have not understood properly.

3.13 Software Requirements Are Soft

Julio Cesar Leite (PUC-Rio de Janeiro, BR)

Software requirements and the engineering of software requirements stands upon the name require and the suffix: ment, which according to the Online Etymology Dictionary means: "suffix forming nouns, originally from French and representing L. -mentum, which was added to verb stems sometimes to represent the result or product of the action.". It occurs that the result of the action require, in this context, is a fuzzy one. As such, the construction of software suffers from a basic hard problem, an unstable soil. Dealing with environment instability is hard. We are studying the concept of requirements awareness as a way of tackling environment instability in order to support software evolution policies.

3.14 The evolution of requirements: towards an ecological theory

Kalle Lyytinen (Case Western Reserve University – Cleveland, US)

This paper addresses long waves and changes in the requirements engineering environments similar to punctuated shifts studied in organization theory or Kondratieff waves in macroeconomics. The is issue at stake is are the tectonic shifts how the requirement work is expected to conducted. My answer is yes. The key is that requirements engineers face a larger context, a larger multitude of mechanisms and new dynamics in which design spaces and solution spaces interact - the key target of requirements work. While the old world of requirements engineering was largely engaged in digitizing the cowpaths and where the movement was from existing task or function to a isolated computer solution. Here the key challenges were cognitive, economic (cost/risk) and technological and requirements were carried out to estimate the failure to execute the plan. In the new world the design and solution spaces are recursively and dynamically organized and involve a constant orchestration of largely existing digital assets to come to a wholly new computational solution which does not have counterpart in the past. The key question to ask is : "What will you do when you can compute anything?" In such situations it is assumed that the effect size of technology increases as variation in combining technological assets increases (Arthur 2010). Overall, this means that the mutation rate of technologies and solutions change resulting in shifts in ecologies where solutions and problems are matched. The key question what requirements engineers must address is to find applications/system that match technological capability and stakeholder needs often in radical/disruptive manner. This is a generative model which assumed multiple evolutionary paths for software and system evolution through functions of informating, embedding into new contexts, and expansion of technological capabilities. The key drivers for variation are classic forms of evolutionary change: code and task mutation,

selection, retention mechanisms. The key form of RE is Exploration where analysts seeks to minimize the risk of failing to discover.

The main challenges are entrenchment and related cognitive barriers, speed at generating variety which requires experimentation, understanding the effects of asset ecologies and forms of platformization (architectural control), and the effects of network externalities on software asset use. I offered an example from the evolution of music industry and related digital assets how new software and service solutions have emerged over the last 20 years.

3.15 Interactive Traceability Querying and Visualization for Coping With Development Complexity

Patrick Maeder (TU Ilmenau, DE)

Main reference P. Mäder, "Interactive Traceability Querying and Visualization for Coping With Development Complexity," arXiv:1301.5363v1 [cs.SE], 2013.
URL http://arxiv.org/abs/1301.5363

Requirements traceability can in principle support stakeholders coping with rising development complexity. However, studies showed that practitioners rarely use available traceability information after its initial creation. In the position paper for the Dagstuhl seminar 1242, we argued that a more integrated approach allowing interactive traceability queries and context-specific traceability visualizations is needed to let practitioner access and use valuable traceability information. The information retrieved via traceability can be very specific to a current task of a stakeholder, abstracting from everything that is not required to solve the task.

3.16 Requirements Complexity and Evolution: A Computational Perspective

John Mylopoulos (University of Toronto, CA)

Joint work of Ernst, Neil; Borgida, Alexander; Mylopoulos, John; Jureta, Ivan
Main reference E. Neil, A. Borgida J. Mylopoulos, I. Jureta, "Agile Requirements Evolution via Paraconsistent Reasoning", in Proc. of 24th Int'l Conf. on Advanced Information Systems Engineering (CAiSE'12), Gdansk, LNCS, Vol. 7328, pp. 382–397, Springer, 2012.
URL http://dx.doi.org/10.1007/978-3-642-31095-9_25

We review the requirements problem as defined by Jackson and Zave [2]. We then discuss how computational complexity creeps in and how to cope with it. In addition, we sketch some approaches for dealing with requirements evolution, adopted from the PhD thesis of Neil Ernst [1].

References

1 N. Ernst, A. Borgida, J. Mylopoulos, I. Jureta (2012) Agile Requirements Evolution via Paraconsistent Reasoning, Proc. 24th Int. Conference on Advanced Information Systems Engineering (CAiSE'12), Gdansk, June 2012.
2 M. Jackson, P. Zave (1995). Deriving specifications from requirements: an example. Proc. 17th ICSE.

3.17 Large Scale Business System Evolution

Andreas Oberweis (KIT – Karlsruhe Institute of Technology, DE)

Business systems are sociotechnical systems, which are embedded in an organization. The organization itself is embedded in supplier, customer and/or technical markets. Business systems usually contribute to an organization's (strategic) goal.

In the literature several definitions for the term "evolution" have been proposed, sometimes inspired by the interpretation of this term in biology. In practice of business systems the term evolution can be found in different variants: evolution as the result of a proactive plan for sequences of change, evolution as a sequence of some spontaneous or random change events, and evolution as reactions to environmental changes.

Business systems evolve in evolution cycles (or life cycles). However, the business system evolution cycle is strongly related to the evolution cycles of business process, business objects, organizational structures, markets, and legal systems. A business system consists of components, each one possibly having an evolution cycle of its own.

Business systems are individually implemented or results of customizing a standard software system. In case of standard software systems there are overlapping evolution cycles of the standard business system (under responsibility of the software vendor) and of the customized business system (under responsibility of the software buyer). Some important challenges of complex business system evolution are:

- Develop mechanisms to support synchronization of different evolution cycles (the term "synchronization" still has to be clarified).
- Find optimization criteria for synchronization efforts (besides cost).
- Decide between central and decentral control of evolution (if possible).
- Manage (reduce?) complexity of relationships between different evolution cycles.
- Decide between system replacement and system evolution. Can an evolving business system finally die?
- Develop languages to model and methods to analyze system evolution and evolution cycle synchronization.

3.18 Requirements Engineering Intelligence: Dealing with Complexity and Change

Barbara Paech (Universität Heidelberg, DE)

Similarly to business intelligence, requirements engineering intelligence captures data about software and its development, operation and use, and leverages intelligent mechanisms such as mining and analytics for decision support in requirements engineering and management. In this paper we distinguish usage, system and operation, and development process data capturing either plan, rationale or execution. We discuss open issues in answering the following questions based on this data: what is the current situation of the system and its usage,what changes to the system are necessary and why, what is the impact of a change, when should which change be executed.

3.19 Managing Requirements Evolution in Software Product Lines

Xin Peng (Fudan University – Shanghai, CN)

A software product line (SPL) is a set of similar applications that share a common, managed set of features and are developed from a common set of core assets. A produce line evolves when existing applications change, core assets evolve, or new applications are derived. In an ideal setting, applications always keep consistent with the core assets in the evolution of a product line. However, in real product lines, it is often the case that applications evolve independently to some extent and may deviate from core assets. Therefore, for SPL evolution management, there is a need to balance independent application evolution for quick response and the desire of SPL evolving as a whole. To this end, SPL evolution management needs to monitor and track the evolution trends of core assets and applications and conduct periodic synchronization among them.

3.20 Software evolution in complex environments

Barbara Pernici (Politecnico di Milano, IT)

Evolution of software can be considered from several different points of view. First of all, evolution can be an issue in service-based systems, where services adapt themselves on the basis of a set of available adaptation actions. For instance, service compositions can select different components, or Quality of Service requirements for invoked service may vary.

A wider perspective is given when complex environments are considered, in which external factors are involved, as in the case of software running in variable contexts or changing users' requirements.

Project such as the S-Cube (the European Network of Excellence in Software Services and Systems, http://www.s-cube-network.eu/) have studied the impact on the software life cycle of adaptive environments, where services adapt to changes. The life cycle in this case is composed of two cycles, one focusing on design for adaptation, the other one on adaptation at execution time, where monitoring is the basis for identifying contexts which require adaptation to satisfy requirements in a changing environment. Adaptation includes strategies such as dynamic service selection, substitution, repair, and so on. When available adaptation strategies are not sufficient to meet the requirements, a redesign of the application can be considered, thus evolving the existing system.

However, one of the goals in adaptive systems is to minimize this evolution and to perform it only when necessary, minimizing change in the system, As a consequence, research goals are to study the areas of designing applications for adaptation, trying to improve their dependability, to minimize evolution, and to identify adaptation contexts and patterns.

On the other hand, evolution has often to be analyzed in the context of complex environments, including not only software components, but also users and business level requirements and the underlying physical infrastructure. In this case, evolution is based on monitoring and control at different levels, and several factors need to be taken into account:

- considering multiple instances and multiple applications

- goals might be variable and context-dependent
- the effect of adaptation decisions may be not always clear.

As an example, adaptation of services and systems with the goal of reaching energy efficiency and optimizing the environmental impact of IT (e.g., as considered in the European projects GAMES – http://www.green-datacenters.eu/ – and ECO2Clouds – http://eco2clouds.eu), requires to consider multiple layers at the same time: applications, services, and infrastructure layers.

In this case many conflicting goals might be present, and actions intended to reach a set of goals might have a negative impact on other ones.

Therefore, when considering complex environments, evolution should take into consideration different aspects:

- rather than considering single applications, patterns of usage of applications should be taken into account
- user behavior can change, also considering feedback from the monitoring system
- the definition of requirements in a multi-layer and adaptive system needs a redefinition of the way requirements are usually specified and considered
- in addition to requirements on functionalities and quality of service, data usage requirements should also be considered.

From the discussion in the workshop, ideas emerged on dealing with manageable evolution (distinguishing between complicated and complex systems) and the need of managing requirements at different abstraction levels.

3.21 Boundary Spanning in RE

Balasubramaniam Ramesh (Georgia State University, US)

Joint work of Ramesh, Balasubramaniam; Mohan, Kannan

Boundary spanning is a central activity in requirements engineering. Research on viewpoint management, requirements traceability and development methods provide several mechanisms that facilitate boundary spanning by suggesting boundary objects and boundary spanning roles. Our research examines the role of boundary spanning in three different contexts: collaborative development, projects characterized by cognitive conflicts and mixed motive conflicts. Our findings suggest that boundary spanning practices must be tailored to the specific project context. In addition, the evolving nature of boundaries due to changes in the external, organizational, and project context necessitates adaptations/evolution of RE tools/processes that fit the context.

3.22 Dealing with uncertainty and iterations in design processes: An entrepreneurial perspective

Isabelle Reymen (TU Eindhoven, NL)

This abstract aims to question the relation between requirements management and two important characteristics of design processes, namely the iterative character and dealing with uncertainty about the environment. It brings forward the entrepreneurial effectuation theory [6] as a perspective that might inform requirements management.

An important characteristic of design processes is iteration [4]. Much of the complexity of design processes is due to iterations [10]. A recent study focusing on long-term process dynamics in design processes in a real-life context [1] found that the iterativity of designing occurs along multiple dimensions, at multiple levels of analysis, and on multiple different time scales. Another important characteristic of design processes is dealing with uncertainty about the environment. Simon [9] already noted the importance of dealing with changing complexities in the outer environment.

Effectuation theory is a recent entrepreneurship theory developed by Sarasvathy [6]. The creation of new ventures is a process characterized by the need to decide and take action in the face of uncertainty. The entrepreneurship literature to date has advanced two contrasting approaches to decision-making (so-called decision-making logics) under uncertainty. The first logic aims to lower uncertainty based on prediction and is termed "causation" by Sarasvathy [6]. Cuastion is contrasted with a second logic labeled "effectuation". Effectuation allows to control uncertainty by being adaptive, seeking feedback and leveraging existing means and stakeholder contacts. The most important principles behind the effectuation logic are means orientation (instead of goal orientation), affordable loss (instead of expected return), strategic alliances (instead of competitive analyses) and exploiting contingencies (instead of preexisting knowledge).

Effectual logic is thus especially useful for (design) decision making under situations of high uncertainty, leaving also room for much iteration in the design process. What can we learn from this decision making logic for managing requirements in complex design processes? It would be worth trying to apply the effectuation principles for designing complex processes. Agile methods, and especially the agile design method Scrum [8] comes really close to the effectuation principles and are already used in (software) design processes in practice. Evaluation of these processes from an effectuation perspective can give insight in the pros and cons of applying effectual principles in design practice, more specifically, under which conditions does they work, and which type of iterations are supported in the process.

When finding inspiration for the requirements process in using effectuation logic, it is important to realize that recent studies point at the combined use of effectuation and causation in practice. Whereas effectual and causal logics were often contrasted in the literature, there is some empirical evidence that individual entrepreneurs use both logics [7], [3]. The combination of effectuation and causation was also found empirically in innovation/design processes in small firms [2]. In addition, Sarasvathy suggests that ventures should switch between effectual and causal logics depending on the degree of uncertainty the venture is confronted with. A recent study [5] focuses on the potential shifts in effectual and causal decision-making over time (in new venture development processes). Such a dynamic perspective is necessary for moving beyond the discussion of causation and effectuation as contrasting approaches. It can shed light on whether, how and why both approaches are

alternated or combined over time. These insights can then also be applied to the requirements managing field, ultimately retrieving guidelines for how to organize requirements processes taking into account increasing complexity and allowing for several type of iterations in the design process.

Concluding, ingredients for finding a relation between requirements management and two important characteristics of design processes, namely the iterative character and dealing with uncertainty about the environment are discussed, thereby making use of the entrepreneurial effectuation theory; but the relations are not yet clear. I hope at least some food for thought was offered that initiates nice discussions on these topics.

References

1 Berends, H., Reymen, I.M.M.J., Stultiens, R.G.L., Peutz, M. (2011) External designers in product design processes of small manufacturing firms. Design Studies, 32(1), pp. 86-108.
2 Berends, H., Jelinek, M., Reymen, I.M.M.J., Stultiens, R.G.L. (2012) Product Innovation Processes in Small Firms: Combining entrepreneurial effectuation and managerial causation, Journal of Product Innovation Management. (forthcoming)
3 Dew, N., Read, S., Sarasvathy, S.D., Wiltbank, R. (2009) Effectual versus predictive logics in entrepreneurial decision-making: Differences between experts and novices. Journal of Business Venturing, 24: 287-309.
4 Dorst, K., & Cross, N. (2001) Creativity in the design process: co-evolution of problem-solution. Design Studies 22, 425-437.
5 Reymen, I.M.M.J., Andries, P., Berends, H., Mauer, R., Stephan, U., van Burg, J.C. (2012) Dynamics of Effectuation and Causation in Technology- based New Ventures, Proceedings of the 2012 Academy of Management Annual Meeting, August 3-7, 2012, Boston, Massachusetts. (pp. 1-39). Boston: Academy of Management.
6 Sarasvathy, S.D.(2001) Causation and effectuation: Toward a theoretical shift from economic inevitability to entrepreneurial contingency, Academy of Management Review, 26(2), pp. 243-263.
7 Sarasvathy, S.D. (2008) Effectuation: Elements of entrepreneurial expertise. Northampton, MA: Edward Elgar.
8 Schwaber, K. and Beedle, M. (2002) Agile Software Development with SCRUM, Upper Saddle River, NJ, Prentice-Hall.
9 Simon, H.A. (1996) The sciences of the artificial, 3rd ed, MIT Press, Cambridge, Massachusetts.
10 Smith, R. P., & Morrow, J.A. (1999) Product development process modelling. Design Studies 20, 237-261.

3.23 Understanding Software System Evolution through Requirements Monitoring

William N. Robinson (Georgia State University, US)

Main reference W.N. Robinson, S. Fickas, "Designs Can Talk: A Case of Feedback for Design Evolution in Assistive Technology," in Design Requirements Engineering: A Ten-Year Perspective, K. Lyytinen, P. Loucopoulos, J. Mylopoulos, and W. Robinson, Eds., pp. 215–237, LNBIP, Vol. 14, Springer-Verlag, 2009.
URL http://dx.doi.org/10.1007/978-3-540-92966-6_12

This paper presents the challenge of understanding system behaviors. Software systems are complex, and we do need the traditional computing techniques, such as requirements

discovery, modeling, simulation, and automation. Improvements in these traditional areas will significantly improve software and software development. New approaches may also be beneficial. Herein, we consider the relatively new approach of requirements systems monitoring (not to be confused with traditional techniques of systems monitoring or telemetry). Requirements monitoring is fundamentally an interpretation problem: What is the system doing?, as expressed in high-level behaviors and qualities. This perspective can be applied to software execution or to software development, where the system is the community of developers. In both contexts, we want to know if the system is meeting its requirements and moving toward a successful conclusion. Monitoring includes specific techniques, but also includes the philosophy that continuous monitoring enables continuous improvement, which is fundamental to successful systems in uncertain and evolving environments.

3.24 Getting to the Shalls: Facilitating Sense-Making in Requirements Engineering

Christoph Rosenkranz (Goethe-Universität Frankfurt am Main, DE)

Knowledge transfer, communication, and shared understanding between project stakeholders are critical, problematic factors in requirements engineering (RE). Yet, specifying complete and unambiguous requirements in the face of the complexity inherent in RE remains a significant challenge. There is a lack of systematic procedures that facilitate a structured analysis of the qualitative data in RE. We propose the use of a procedural approach to fill this gap that builds on Linguistic Analysis and Grounded Theory Method.

3.25 Platforms wars as a source of complexity

Matti Rossi (Aalto University, FI)

For last 15 years most end-user applications have been developed for Windows and server software for various flavors of UNIX. There were other platforms, but they were niches. This made certain platform constraints easy to deal with and more or less fixed.

All this has changed in last 5 years. A proliferation of mobile platforms and totally new user interaction forms has created a maze of options to work with. It would be easy if everyone just developed software and services using HTML5 as a standard rendering platform and browser as an execution platform. However, the major operating systems are shifting and it is not Chrome the browser that is the largest operating system, but rather Android that competes with iOS. This creates a wealth of issues.

First issue to choose is whether to develop a user interface for desktop, mobile or tablet form factor. Then one has to decide whether to use mouse, touch, menus etc. All this and still the actual execution platform and its exact form factor and API's have to be selected. When these are done, one can choose a distribution channel (store) and perhaps an in-app payment method. If the choices are right and the developers have luck and good timing, they have an instant potential and addressable market of tens or even hundreds of millions devices

and users. However, at the same time the platforms are on the mercy of fashion and fads. So if wrong constraints are acknowledged in the start and/or development is delayed, it could be that a new killer app is deployed against last season's platform, which is no longer viable.

To understand the platform risks and constraints, there should be more research on path dependencies and whether we are moving towards hardware or software platforms. Furthermore, the economics of moving to fragmented and closed versus open platforms should be studied to understand the long term evolution.

3.26 Extreme Requirements: The Challenge of Ultra Large Scale Systems

Alistair G. Sutcliffe (Univ. of Manchester, GB)

I review the drivers of complexity in very large scale systems arguing that human unpredictability, exception conditions in social systems, functional bloat, environmental change, and increasing connectivity are inescapable trends creating over complex, global scale systems which current RE methods can not address. Dealing with complex systems is confounded by long development times in changing worlds and communication problem within groups of developers. Possible solutions for large scale socio-technical systems are explored, ranging from simulations to understanding the constraints on high level system goals, to evolutionary approaches which generate and test solutions, where requirements become fitness criteria for surviving in operational environments. Finally I propose a challenge for developing a sound abstraction theory to bridge requirements to conceptual system architectures and argue that abstraction theory will be necessary to effectively 'divide and conquer' requirements problems in complex systems.

3.27 A general-to-specific architectural design for managing requirements evolution

Fan Yang-Turner (University of Leeds, GB)

Deriving requirements from users to support issues with cognitive complexity (such as sense making or creative thinking) or social complexity (such as trust enhancement or culture awareness) are difficult. Applications that support these complex issues are often developed in a fast prototyping manner. The requirements are constantly evolving because of the interaction between the users and designers catalyzed by the prototype. Meanwhile, few theories or conceptual models from cognitive science or social science have been reused to the level of design or development. To manage requirements evolution for cognitive or social complex issues, I posit a general-to-specific architectural design underpinned by theoretical models. In this paper, I illustrate this design in a development project, which creates a platform that facilitates sense making and decision making in data-intensive and cognitively-complex settings.

3.28 Modeling and (social) complexity – a perspective from conceptualizing the BI-enabled adaptive enterprise

Eric S. Yu (University of Toronto, CA)

Is complexity good? Is complexity bad? Modern living takes for granted numerous conveniences that are built upon layers upon layers of complexity, most of which are hidden from us.

Complexity is good, as long as someone else takes care of it. Complex societies derive value from complexity. We are all benefitting from complexity. Social complexity is achieved through mechanisms of social organization, such as division of labour, specialization, trust, commitment, delegation, exchange, markets, power, and politics. Complexity is hidden by exploiting locality, but is exposed when the locality boundary fails, resulting in (side-)effects propagating across boundaries.

Requirements arise at the boundary between localized social units (abstract social actors), as dependencies from service consumer to service provider. Requirements are inherently distributed. There are numerous consumer/provider interfaces in a society or in an enterprise. In the classical requirements paradigm, the focus is on the one-time activity of obtaining a set of high-quality requirements for a single "system". This paradigm applies only in the context of inflexible, slow-moving, and monolithic service providers. This no longer works in the "brave new world" [1].

Requirements dynamics result from dynamics in the service consumer and in the service provider. Since consumer and provider each evolves at its own pace, driven by different forces and varying degrees of uncertainty, misalignment can be expected between what is wanted by the consumer and what is offered by the provider. Perfect alignment, or perfect achievement of requirements despite ongoing change, is unrealistic in the brave new world. Instead, requirements complexity should be addressed by architecting the enterprise (or society, or relevant ecosystems) so as to minimize misalignment at the boundaries between the various social units, taking into account the abilities (and limits) that each unit has in adapting to its environment.

This perspective on requirements derives from a project on "BI-enabled Adaptive Enterprise Architecture", a project within the Business Intelligence Network (BIN), a Canadian academic-industry collaborative research network. The project aims to position BI and data analytics within a conception of the adaptive enterprise [2].

References

1 M. Jarke, P. Loucopoulos, K. Lyytinen, J. Mylopoulos, and W. Robinson (2011). The brave new world of design requirements. Inf. Syst. 36, 7 (November 2011), 992-1008. http://dx.doi.org/10.1016/j.is.2011.04.003

2 E. Yu, S. Deng and D. Sasmal (2012). Enterprise Architecture for the Adaptive Enterprise. Proc. 7th Workshop on Trends in enterprise architecture research (TEAR). at The Open Group Conference 2012, Barcelona, Spain, October 23–24, 2012. http://dx.doi.org/10.1007/978-3-642-34163-2_9

3.29 A Feature Model Centric Approach to Requirements Management and Reuse

Haiyan Zhao (Peking University, CN)

As a critical component of software reuse, requirements reuse provides organizations with the ability to share requirements across projects without absorbing unnecessary duplication of artifacts. The key issue in requirements reuse is *how to make the requirements reusable*. Requirements are reusable only if they can be easily configurable with respect to the needs and preference of users in the sense that the requirements should be highly customizable following the principles of loose-coupling and high-cohesion. To this end, this talk proposes and discusses an integrated framework for managing and reusing requirements, which adopts feature models as the centric representations to organize and manage the reusable requirements. It encompass 1) the structures of feature models and the mechanism for requirements family evolution; 2) the construction of traceability between feature models and other artifacts, such as use cases and software architecture; 3) the reuse of requirements through feature model customization.

3.30 Requirements Issues in SoC and SoS

Andrea Zisman (City University – London, GB)

Main reference A. Zisman, "Requirements Issues in SoC and SoS," arXiv:1301.5470v1 [cs.SE], 2013.
URL http://arxiv.org/abs/1301.5470

This position paper "Requirements Issues in SoC and SoS" outlines some of the existing issues and challenges concerned with the complexity of the requirements for service-oriented computing and systems-of-systems applications.

3.31 A quest for building theories of requirements evolution

Didar Zowghi (Univ. of Technology – Sydney, AU)

Main reference V. Gervasi, D. Zowghi, "On the Role of Ambiguity in RE," in Proc. of the 16th Int'l Working Conf. on Requirements Engineering, Foundations for Software Quality (REFSQ'10), LNCS, Vol. 6182, pp. 248–254, 2010.
URL http://dx.doi.org/10.1007/978-3-642-14192-8_22

The primary productive force in information capitalism is the human mind and its cognitive, linguistic, and creative capacities. New systems of production and exchange, and new orders of power and control are built to harness, enclose, and exploit what humans can do naturally: think, communicate, problem-solve, and create etc. Software systems are unique artefacts both produced by, and helping to produce, informational capitalism. Similar to the larger systems of power in which software is situated and embedded, it can often be unstable, uncertain, unpredictable, and prone to disruption and failure. Yet paradoxically, each new software application developed carries the hopes of human users for order and certainty,

offering a technological solution that will effectively solve a specific problem or support a specialized activity or process. No matter how often software systems might under-perform or fail given the weight of collective and sometimes unrealistic expectations, software users remain optimistic that 'this time it will be different!'

What role should requirements engineering research and practice play in increasing the confidence of users of future systems that their voices will be heard and their needs will be met better than it has been over 6 decades of software systems development? More importantly, how could effective RE practices decrease the likelihood of future system failures, disruptions, and disorder in everyday life? What we as a community have achieved in RE research thus far that has produced a quantum leap in that direction? These are some of the questions that many of us would like answered.

I have been exploring some old and recent research questions and issues (summarized below) that I hope may contribute to responding to some of the above questions.

User involvement in RE and software development

On the one hand, software development processes often focus on a small number of representative users to give input and feedback in requirements related activities and later during user acceptance testing. On the other hand, user feedback mechanisms in software systems are not standardized and remain rather ad hoc. Typically base line features of software approved by management are perceived to be more important than those requested or needed by less frequent or less powerful users. Communication channels that allow for effective collaboration among users or between users and developers are usually decoupled from software systems and their development infrastructure. Research involves conducting field studies of software development and software usage, so that we can collect valuable data through observation of software development tasks and interactions through interviews with as many relevant stakeholders as possible within the entire software development lifecycle.

The aim is to employ Grounded Theory throughout this longitudinal research project in order to increase our understanding of the evolution of requirement knowledge generated by users involvement. We are specifically interested in building theories of generation, negotiation, validation and sustainability of requirements knowledge through the lens of users participation. From a management perspective, we wish to develop a sufficiently deep analysis of the evolution of the role of users involvement in software development and how this is managed by development teams.

Properties of Requirements Specifications (RS) are attributes that can be associated with the documented requirements. Properties are important because they enable us to assess whether an RS is in some way "good" or "better" than another RS. Knowing this, one can decide when to declare the requirements process complete, how to estimate the cost of a development effort, and so on. I have studied factors such as inconsistency, incompleteness, and ambiguity and investigated their evolution and management within the RE process. An individual cannot inspect or examine a requirements specification and determine its level of ambiguity, consistency, completeness, etc., without referring to external bodies of knowledge such as other related documents, business processes, organizational strategy, other systems, and so on. Many external bodies are highly volatile while others are slow to change while others are completely static. There is a need to develop sound theories that describe the dependencies between RS properties, requirements and external bodies of knowledge, and show how a number of common phenomena (and related properties) can be expressed and modeled by that theory. In particular, modeling the interdependencies and interrelationships between these attributes that determine the overall quality of the RS. Here I mention three of such properties:

Consistency

Every phenomenon that has its ultimate roots in human subjectivity is liable to possible change in the future. In practice it often happens that revision of requirements comes either from strikingly new and different needs which demand that the conceptual model be revised in order to account for them, or from some unexpected conclusions which are deduced from the conceptual model itself and which may contradict some of the already known requirements [2]. The problem of managing changing requirements and maintaining the consistency of evolving requirements throughout software development life cycle is one of the most significant issues in requirements engineering.

Completeness

The boundary between the real world and the application domain is necessarily a leaky interface because the individuals and predicates continue to be discovered and captured during requirements evolution and hence this boundary is volatile. Therefore, at any point in the evolution of a system, one cannot claim with absolute certainty that all the items of interest and their relationships have been captured completely, because the application domain itself (where the requirements are situated), is indeed an evolving entity. This argument suggests that absolute completeness of requirements specifications can never be established and completeness remains only as a relative measure [2], [3].

Ambiguity

Ambiguity has long been considered as one of the worst defects in requirements specifications whose identification and removal should be given higher priority. More recently the nature of ambiguity has been subject of research that advocates that the simplistic view of ambiguity as merely a "defect" that has to be avoided at all costs does not do justice to the complexity of this phenomenon [1].

References

1 Gervasi, V. and Zowghi D., (2010), On the Role of Ambiguity in RE, Proceedings of the 16th International Working Conference on Requirements Engineering, Foundations for Software Quality (REFSQ'10), Essen, Germany.

2 Zowghi D. and Gervasi V., (2002), The Three Cs of Requirements: Consistency, Completeness and Correctness, proceedings of 8th International Workshop on Requirements Engineering: Foundation for Software Quality, (REFSQ'02), Essen, Germany.

3 Zowghi D., and Gervasi V., (2004), On the Interplay Between Consistency, Completeness, and Correctness in Requirements Evolution, Journal of Information and Software Technology, 46(11):763-779.

4 Working Groups

4.1 Managing Complexity within Requirements

Andrea Zisman (City University – London, GB)

Joint work of Zisman, Andrea; Maeder, Patrick; Hayes, Jane; King, John; Lauenroth, Kim; Mylopoulos, John; Ramesh, Bala

In this working group we discussed the main topic of how to manage complexity within requirements. We started with some initial presentations from the members of the group

about (i) cognition effects of the human mind and how these effects can influence requirements engineering activities; (ii) industrial experience with requirements; (iii) difference between complicated and complex; (iii) use of traceability queries and visualization; and (iv) requirements issues when developing SoC and SoS. We also discussed what could be the causes of complexity, and how to manage complexity within requirements. Some of the ideas that have been proposed to manage complexity within requirements are: (a) identification of dependencies and opportunities in requirements, (b) use of test-driven development, (c) use structural levels of constructions, (d) use of specific terminology, and (e) keep the project out of the complex space and contain its scope.

4.2 Requirements Discovery and Negotiation in Complex Environments: Work Group Discussion

Gilbert Fridgen (Universität Augsburg, DE)

Joint work of Fridgen, Gilbert; Hansen, Sean W.; Reymen, Isabelle M.M.J.; Rosenkranz, Christoph; Svensson, Richard Berntsson; Yu, Eric S.; Zowghi, Didar

During the discussion we structured the topic in four areas that have to be considered for requirements discovery and negotiation in complex environments: The role of humans, the design attitude, the difficulties that come with complexity, and the challenges through evolution.As for human beings, we first have to distinguish between software engineers who have to deal with complexity during development and end-users who have to cope with a possible insufficient system. Both stakeholders can be parts of complex systems of power and politics that can hinder any project, especially if it comes to negotiation. While users are today by far more involved through participatory design (e.g. with agile methods), observed use, misuse, or non-use can be an important indicator for the quality of requirements. To improve communication between software developers and users we have to develop their skill set to enable boundary spanning between disciplinary knowledge. User observation is also an important interlink between to role of human beings and the design attitude. It can be one means of creativity to foster the exploration of user needs that have not been addressed by a requirements specification before. Especially the focus on processes instead of products is important here: Users do not need a certain product for itself; they rather need support in fulfilling their respective processes. To identify and support these processes, software engineers require a design thinking in contrast to a decision oriented thinking, iteratively improving their solutions. This can be reached through multiple cycles of divergence/convergence, effectuation/causation, freezing/unfreezing, and exploration/exploitation.For complexity itself, it is important to consider that it is only a perception by humans and that different individuals can perceive it differently, especially if you differentiate between software engineers and end-users. Modularity seems still to be a powerful means to break down and manage complexity. Successful strategies to overcome this issue are furthermore "markets" for innovative ideas like e.g. implemented by Google who reserve only 70% of the time for work that generates direct revenue, 20% for any project they want and 10% for own idea. It is consequently a means to manage the complexity of many employees having various ideas. Therefore, complexity can be crucial, it can be the source of innovation that needs to be leveraged.Regarding the evolution of systems and their surroundings we have to be aware that we are only partially able to drive evolution and that much evolution

will just happen by itself requiring systems to react. We therefore need to identify areas in which we can control evolution and areas in which we have to be prepared e.g. by implementing a certain amount flexibility. The architectural concept of solid cores and flexible boundaries seems to be a promising strategy to prepare systems for a controlled evolution.Out of these challenges we identified to following four research topics to be the most pressing but currently neglected:First, we need to do more shift our research from a product to a process focus. Second, we need to explore the dynamics of power and politics in software development projects to implement corresponding governance structures. Third, we need to improve human-centered discovery techniques, especially including (fourth) improved feedback mechanisms.

4.3 Managing complexity through requirements

Anna Hannemann (RWTH Aachen, DE)

Joint work of Xavier Franch (chair); Hannemann, Anna (scribe); Cleland-Huang, Jane; Doerr, Joerg; Heidemann, Julia; Leite, Julio; Rossi, Matti

The discussion addressed questions along different dimensions: requirements nature (requirements for RE, Jackson's problem frames), techniques (social network analysis), domains (services for citizens, OSS communities) and architectural issues (constraints on mobile technologies, agile vs. traditional architectural model).

In terms of RE organization (e.g., generic vs. OSS projects, services for systems), different iteration cycles can be observed. Different frequency of change requires different approaches to handle the resulting complexity. For example, the complexity of services for mobile systems consists of: too different users, too different context, too different applications, too many sensors. The complexity arising during development and evolution of services can be approached by tailoring the requirement specifications to the development roles and even individuals. First, define the whole picture of the process, roles and tasks. Second, provide every participating engineer with a personalized view of his/her role within the development process. We argue, that the increase of general awareness is one way to improve the understanding of complexity and, thus, to handle it. Social network analysis can be applied in order to make not only technical but also social complexity transparent to the process participants. Socio-technical representation should not only be based on RE related data, but also incorporate communication and interaction aspects within the whole development process.

In terms of reducing the complexity of requirements, prioritizing appears to be an appropriate strategy. The essential (cannot avoid it) complexity can be distinguished from accidental (this comes from the method). The existence of complex requirements may help tackling more complex problems (e.g., constraints to model platform variability) on the one hand. On the other hand, complex requirements are more complex to handle, e.g. to trace. Prioritizing presents a challenging process and can eventually lead to information loss. Especially, considering community-driven systems the open questions to answer are: "Where is the boundary of the system?" and "How to handle the requirements form the long-tail of community".

In terms of RE environments, more prescriptive and modular systems can reduce the complexity of requirements negotiation among multiple stakeholders, different in their views,

knowledge and needs. However, knowledge innovation is believed to be a result of a creative, non-restricted process of idea finding. When and why more traditional RE or a generative model is more suitable – an open question.

In terms of complexity of interactions between architectures and requirements, we need to understand what the information needs of our architects are. Then we can elicit and transfer the information to architects. A subset of requirements known as architecturally significant requirements (ASR) drive architectural design, while at the same time existing architectural design constrains new functions (requirements) that the system can implement. This is a cost issue. Almost any new requirements can be accepted, but they will cost more or less according to the necessary refactoring.

4.4 Managing Complex Systems Evolution with Requirements Models

Matthias Jarke (RWTH Aachen and Fraunhofer FIT, DE)

Joint work of Matthias Jarke (scribe), Xin Peng, Barbara Pernici, Alistair Sutcliffe, Hayian Zhao (chair)

The workgroup addressed three major questions from different perspectives:

- Alignment of model types with complex systems and their evolution: models should be aligned to the required and available depth of knowledge; to support evolution, they should be simulatable, but also enable ex-post change through traceability
- Careful management of model incompleteness: requirements scenarios should be modeled at different levels of granularity and timescales, with or without consideration of aspects such as causality or feedback loops; they not only at design time but also at runtime because of constant change; but all these submodels cannot necessarily be fully connected to each other. Especially phenomena models beyond the actual system design are of necessity incomplete, but purpose-focussed traceability patterns may help not to forget critical aspects that someone has thought about before.
- Modeling requirements variation and evolutionary branches: clutter in variation modeling should be avoided using recent solution approaches such as product families even at the RE level; similarly, empirical research should identify process patterns of requirements evolution that can perhaps be standardized.

Alistair Sutcliffe presented Extreme Requirements as the challenge of ultra-large socio-technical systems to illustrate their typical problems: overambition by desire to improve existing systems when transferring them to new settings; the tendency of political lobbying to complicate regulations with endless exceptions; the unpredictability of human users, developers, and especially decision makers; the evolution of technology combined with multiple layers of connectivity and thus sources of additional complexity. He stressed the importance of simulations as well as of not just deterministic but also stochastic goal and obstacle analysis, and the helpful nature of requirements patterns. Hayian Zhao advocated a feature-centric approach to RE as a possible answer to many of these challenges. Features abstract away complexity and evolution in a manner that is relatively easy to communicate among stakeholders. He, as also Matthias Jarke in his brief talk, stressed the role of standard platforms and standard software in combining complexity reduction with richness of innovation. Features are also claimed to provide patterns for traceability, such that Zhao even proposed to replace domain models altogether by feature models. Barbara Pernici

focused her talk on the rarely discussed but practically eminently important aspects of evolving systems operation requirements, using the example of high-performance systems in scientific computing. For example, how to make an expensive ocean-simulation environment more energy-efficient, how to re-balance workload between mobile devices and static servers in different phases of battery life. New parameters must be introduced into requirements models to capture these aspects, e.g. frequency of use, data and usage stability, etc.

Finally, Xin Peng focused on the evolution and complexity aspect of socio-technical systems, claiming that traditional systems that separate human and technical components to much are neither social nor technical. In the future, we shall face a deeper integration of human, software, and technical world, but it is unclear how to represent and manage requirements on such ambient and deeply integrated systems. The group concluded that RE must become a bit more quantitative, dynamic, and adaptive in its analyses, in many cases get much more deeply into the modeling of domains which were traditionally outside the IT world. When attacking complex projects in the sense of John King, requirements engineers, developers, and also management stakeholders moreover must be prepared to get into deep research and very major, time-consuming and expensive conceptual and systems revisions as unexpected phenomena are bound to arise during such projects, unless they are very lucky. A stepwise approach to taking on and evaluating such systems in relatively simple steps is therefore strongly recommended, but unfortunately often prevented by the nature of the political debate.

4.5 Understanding Evolution: Biological, Cultural and Technological Perspectives

Lin Liu (Tsinghua University Beijing, CN)

Joint work of Liu, Lin; Myloupolous, John; Li, FengLin; Wang, Jun
Main reference L. Gabora, "The Origin and Evolution of Culture and Creativity,"Journal of Memetics – Evolutionary Models of Information Transmission, 1. 1997.

More and more software systems are required to cope with an ever- changing and evolving environment. These changes and evolutions could take place in the users needs and demands, in the capacity and availability of software assets, in the emergence of new technologies, and in the dimension of time and location, in the physical, systematical and social context of the operational environments. It has imposed great challenges for requirements engineering researchers to develop useful techniques to bridge the gap between intuitive user objective statements to concrete design constraints that is understandable and implementable by designers. In order to understand the evolution of systems and discuss requirements engineering strategies and techniques in response to the needs of evolution, we need to answer questions such as: what are the key challenges in requirements engineering for adaptation and evolution? What are the appropriate models for capturing changes? What are the levels of abstraction that should be used in light of adaptation and evolution? What are the possible types of adaptation and evolution? What are the appropriate strategies and mechanisms supporting requirements and systems co-evolution? I would set out from example evolution models in biological systems and cultural systems to give my observation on the general model of requirements and systems co-evolution.

5 Joint Panel with the Dagstuhl Seminar on "Foundations and Challenges of Change and Evolution in ontologies"

5.1 "When worlds collide: Requirements evolution and ontologies"

Matthias Jarke (RWTH Aachen and Fraunhofer FIT, DE) and Ulrike Sattler (University of Manchester, UK)

When we found out that in parallel to our seminar, another one with a very similar theme "Foundations and Challenges of Change and Evolution of Ontologies" would be organized by the knowledge representation/description logic community, we were excited to propose a joint session of both seminars to investigate how complexity, change, and evolution had been studied in these usually almost disjoint communities. We also hoped that some people from both seminars might identify joint topics they could collaborate on.

The joint session took the form of an open discussion with two introductory talks by Matthias Jarke and Ulrike Sattler. Matthias Jarke tried to establish the link from the RE side by pointing out the well-known formalization of RE by Jackson and Zave (1995) which was obviously inspired by the then very active AI community on model-based diagnosis : Given a set of domain assumptions D and a set of requirements R, find a suitable specification S such that $S, D \Rightarrow R$. In RE research, the R have often been interpreted as goals, to be refined and satisfied in some extended AND-OR graph structure. Matthias pointed out that reasoning in goal graphs is now well understood, and can in simple cases be reduced to SAT propositional reasoning. The fashionable research topic of provable compliance to regulations adds to the relevance of such approaches. As an even more direct bridge between RE and ontology, domain assumptions D are nowadays often described as more or less formal ontologies, at least in their static part. Thus, there seems to be a significant share of formalisms that seem relevant to both sides. However, since 1995, the problems in RE have shifted significantly, because the complexity and dynamics of systems has enormously increased. The dynamics especially in the business sector leads to frequent radical changes in the way domains are seen and modeled; witness the fashion industry as an extreme and obvious example, but also the new business models in the Internet, and the blurring of boundaries between hitherto separate industries e.g. in the Telekom sector. The RE seminar has identified three key challenges resulting from this growing complexity and change rate, which it would also like to pose to the ontology colleagues: At least the following key challenges to research and practice were identified in the seminar, together with counter-strategies where promising first steps for solutions:

- In large-scale projects, continuous changes in D and R lead to a shockingly high share of "black swan" projects that exceed budget by more than 70% and schedule more than 200%. A central cause are often politically motivated over-ambitious goals, with systematic under-estimation of requirements and resource needs, as well as poor change tracking. As a consequence, we strongly recommend not just to model the domain but also model and continuously monitor stakeholder goals, social structures and strategic dependencies during the development process, and even beyond. Monitoring and decision tracing should be supported by formal patterns (a kind of change ontologies?) to ensure compliance and effectively assess the impact of proposed changes.
- In the seminar, John King pointed out the difference between "complicated" and "complex" problems. Complicated problems can be solved by experienced, highly competent engineers with foreseeable effort. In contrast, complex problems can only be explored with uncertain results; thus, taking on a project that tries to solve a complex problem in one shot is bound

to lead to disaster. Platform strategies offer architectural mechanisms that constrain, but also leverage complexity. They constrain complexity because they offer a very large number of users and developers a uniform base understanding at a level of technology which is already well understood. They leverage complexity in that they allow end user-driven innovation on their top, witness e.g. the development of a huge app ecosystem on the iPhone platform. It could be interesting to see how ontologies might help to capture what the platforms offer, but one could also imagine data mining methods that would generalize an ontology of what is (successfully or not successfully) innovated by the huge chaos of apps.

After the social software revolution, few people would doubt that information systems need to be seen, and modeled, as socio-technical systems. But many traditional software systems are anything but social, and in the future, the upcoming cyberphysical systems reaching out to the real world with billions of sensors/actuators will teach us that our systems understanding so far is not sufficiently technical, either. The challenges mentioned above are therefore likely to increase in the near future, rather than being reduced. Perhaps a bit too immodestly, we claim that RE is the marketplace where responsibility is traded, and we need all the formalisms and tools we can get to help that task. Communication and mutual understanding is also the stated key goal of ontologies, so ontology evolution could of great interest of RE as well if a common language of interaction between the communities could be found.

Ulrike Sattler introduced the goals of the Ontology seminar. The knowledge representation/description logic community has focused on precise semantics for shared ontologies, supported by automated reasoning mechanisms with guaranteed time and space complexity, and a model theory that can operate purely at the schema level (possible worlds), or including instance-level real-world facts. One important specific objective has been to characterize precisely what kind of knowledge about the real world can or cannot be expressed by a specific ontology formalism. Research on change and evolution of ontologies has for a long time been a rather marginal part of the field, but is growing in importance in the last years. Four different formal approaches are being pursued:

- Calculating the difference between two ontologies (not just their syntactic structure, but also the derivable properties)
- Modeling timelines how concepts change over multiple versions of an ontology; as an example: In the fishery domain, the definition of what a salmon is has changed many times over the past 50 years; is it still possible to make, and formally justify a statistical statement whether the population of salmon has been growing or shrinking in this period?
- Belief revision within an ontology after new facts become known: numerous methods from databases (view maintenance, view updates) and knowledge representation (non-monotonic and paraconsistent reasoning) have been explored for cases where consistent repair of the overall beliefs is possible, or even where unrepairable inconsistencies remain.
- Reasoning about actions: Explicit modeling of actions and their effects aims at integrating the modeling of dynamic aspects into ontologies, thus supporting also tasks like planning and prediction from observed or modeled history.

In the subsequent discussion, many possible overlaps of interest were discussed. One example of shared interest is the law domain which has been a very interesting subject for ontology modelers for quite a while, and has become of great interest to requirements engineers due to the growing importance of all kinds of compliance in current systems. A second example is the question of dealing with paradigm change in fields such as biology, medicine, or even fashion, where the same data (biological specimen, medical observations, clothing colors and designs) need to be re-interpreted under new world views or ontologies – a problem

also known in the field of databases as consistent query processing under schema evolution). A third interesting question is the comparison of virtual vs. materialized dependencies among domain and system concepts. Ontologies based on description logics that allow to represent also some aspects of incomplete or negative knowledge, might on the one hand help with automated reasoning about the relationships between requirements, or between requirements and designs, especially where the impact analysis of proposed requirements changes is concerned. On the other hand, traceability research in RE seems very advanced in materializing effectively the dependency knowledge where virtual reasoning would not be helpful because of human design decisions, or experience-based dependency structures for which no general logical description is available. One possible joint follow-up project which was envisioned in the seminar, could therefore be to find a new solution that combines the strengths of the KR and RE approaches in this field.

Participants

- Nicholas Berente
University of Georgia, US
- Richard Berntsson Svensson
Lund University, SE
- Jörg Dörr
Fraunhofer IESE – Kaiserslautern, DE
- Xavier Franch
UPC – Barcelona Tech – Barcelona, ES
- Gilbert Fridgen
Universität Augsburg, DE
- Anna Hannemann
RWTH Aachen, DE
- Sean Hansen
Rochester Institute of Technology, US
- Julia Heidemann
McKinsey & Company – München / Universiät Regensburg
- Jane Cleland-Huang
DePaul University – Chicago, US
- Jane Huffmann Hayes
University of Kentucky, US
- Matthias Jarke
RWTH Aachen, DE
- John Leslie King
University of Michigan – Ann Arbor, US
- Kim Lauenroth
adesso AG – Dortmund, DE
- Julio Cesar Leite
PUC-Rio de Janeiro, BR
- Lin Liu
Tsinghua University Beijing, CN
- Kalle Lyytinen
Case Western Reserve University – Cleveland, US
- Patrick Mäder
TU Ilmenau, DE
- John Mylopoulos
University of Toronto, CA
- Andreas Oberweis
KIT – Karlsruhe Institute of Technology, DE
- Barbara Paech
Universität Heidelberg, DE
- Xin Peng
Fudan University – Shanghai, CN
- Barbara Pernici
Politecnico di Milano, IT
- Balasubramaniam Ramesh
Georgia State University, US
- Isabelle Reymen
TU Eindhoven, NL
- William N. Robinson
Georgia State University, US
- Christoph Rosenkranz
Goethe-Universität Frankfurt am Main, DE
- Matti Rossi
Aalto University, FI
- Alistair G. Sutcliffe
Univ. of Manchester, GB
- Fan Yang-Turner
University of Leeds, GB
- Eric S. Yu
University of Toronto, CA
- Haiyan Zhao
Peking University, CN
- Andrea Zisman
City University – London, GB
- Didar Zowghi
Univ. of Technology – Sydney, AU