On Polynomial Secret Sharing Schemes

Anat Paskin-Cherniavsky
Ariel University, Ariél, Israel
anatpc@ariel.ac.il

Radune Artiom
Ariel University, Ariél, Israel
The Open University, Raanana, Israel
tom.radune@gmail.com

Abstract

Nearly all secret sharing schemes studied so far are linear or multi-linear schemes. Although these schemes allow to implement any monotone access structure, the share complexity, SC, may be suboptimal – there are access structures for which the gap between the best known lower bounds and best known multi-linear schemes is exponential.

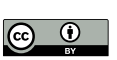
There is growing evidence in the literature, that non-linear schemes can improve share complexity for some access structures, with the work of Beimel and Ishai (CCC '01) being among the first to demonstrate it. This motivates further study of non linear schemes.

We initiate a systematic study of polynomial secret sharing schemes (PSSS), where shares are (multi-variate) polynomials of secret and randomness vectors $\vec{s}, \vec{r}$ respectively over some finite field $\mathbb{F}_q$. Our main hope is that the algebraic structure of polynomials would help obtain better lower bounds than those known for the general secret sharing. Some of the initial results we prove in this work are as follows.

On share complexity of polynomial schemes. First we study degree (at most) 1 in randomness variables $\vec{r}$ (where the degree of secret variables is unlimited). We have shown that for a large subclass of these schemes, there exist equivalent multi-linear schemes with $O(n)$ share complexity overhead. Namely, PSSS where every polynomial misses monomials of exact degree $c \geq 2$ in $\vec{s}$ and 0 in $\vec{r}$, and PSSS where all polynomials miss monomials of exact degree ≥ 1 in $\vec{s}$ and 1 in $\vec{r}$. This translates the known lower bound of $\Omega(n^{\log(n)})$ for multi linear schemes onto a class of schemes strictly larger than multi linear schemes, to contrast with the best $\Omega(n^2/\log(n))$ bound known for general schemes, with no progress since 94'. An observation in the positive direction we make refers to the share complexity (per bit) of multi linear schemes (polynomial schemes of total degree 1). We observe that the scheme by Liu et. al obtaining share complexity $O(2^{0.994n})$ can be transformed into a multi-linear scheme with similar share complexity per bit, for sufficiently long secrets. For the next natural degree to consider, 2 in $\vec{r}$, we have shown that PSSS where all share polynomials are of exact degree 2 in $\vec{r}$ (without exact degree 1 in $\vec{r}$ monomials) where $\mathbb{F}_q$ has odd characteristic, can implement only trivial access structures where the minterms consist of single parties.

Obtaining improved lower bounds for degree-2 in $\vec{r}$ PSSS, and even arbitrary degree-1 in $\vec{r}$ PSSS is left as an interesting open question.

On the randomness complexity of polynomial schemes. We prove that for every degree-2 polynomial secret sharing scheme, there exists an equivalent degree-2 scheme with identical share complexity with randomness complexity, RC, bounded by $2^{poly(SC)}$. For general PSSS, we obtain a similar bound on RC (preserving SC and $\mathbb{F}_q$ but not degree). So far, bounds on randomness complexity were known only for multi linear schemes, demonstrating that $RC \leq SC$ is always achievable. Our bounds are not nearly as practical as those for multi-linear schemes, and should be viewed as a proof of concept. If a much better bound for some degree bound $d = O(1)$ is obtained, it would lead directly to super-polynomial counting-based lower bounds for degree-d PSSS over constant-sized fields. Another application of low (say, polynomial) randomness complexity is transforming polynomial schemes with polynomial-sized (in n) algebraic formulas $C(\vec{s}, \vec{r})$ for each share, into a degree-3 scheme with only polynomial blowup in share complexity, using standard randomizing polynomials constructions.



1st Conference on Information-Theoretic Cryptography (ITC 2020).
Editors: Yael Tauman Kalai, Adam D. Smith, and Daniel Wichs; Article No. 12; pp. 12:1–12:21

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

2012 ACM Subject Classification Theory of computation; Theory of computation → Cryptographic primitives

Keywords and phrases Secret sharing, polynomial, lower bounds, linear program

Digital Object Identifier 10.4230/LIPIcs.ITC.2020.12

Related Version A full version of this article is available at `https://eprint.iacr.org/2019/361`.

Funding *Anat Paskin-Cherniavsky*: This work was supported by The Ariel Cyber Innovation Center in conjunction with the Israel National Cyber directorate in the Prime Minister's Office.

1 Introduction

Secret sharing is a primitive allowing a dealer to share a secret s among n players. The secret sharing scheme implements a (monotone) access structure $\mathcal{A} \subseteq 2^{[n]}$ if any $A \in \mathcal{A}$ can learn the secret from their joint share vector (A is called qualified set), and any set $B \notin \mathcal{A}$ learns nothing about the secret (B is called unqualified set). Secret sharing was introduced in '79 by Shamir [19] and Blakley [9] for threshold access structures, and was followed by thousands of works exploring the primitive itself, and its many applications found since. Quite early on [7,15] put forward a first construction realizing any monotone access structure. As a notable application, secret sharing is used as a key building block in various secure Multi-Party Computation (MPC) constructions [6,12].

Arguably, the most important complexity measure of a secret sharing scheme is its share complexity (SC). Share complexity is the maximum, over the parties' share length, received from the dealer by any of the parties. A somewhat relaxed measure is its information rate, which is the share complexity *per shared bit*. It can be viewed as "amortized" share complexity, which is a useful measure if secrets are allowed to be long.

Unfortunately, there is a huge gap in our understanding of this measure. Namely, the best known lower bound on share complexity for a general scheme is $\Omega(n/\log(n))$ [10], while the best known constructions for certain access structures have exponential complexity $O(2^{0.637n})$ [2]. In [10], techniques from information theory are used, characterizing the existence of a secret sharing scheme in terms of requirements on the entropy of various distributions. The lower bound in [10] is on information rate (making it stronger) and states an explicit access structure for which it holds. It is important to note that counting arguments do not work for general secret sharing schemes.[1]

In spite of extensive research attempting to improve [10]'s lower bound, the best known lower bound for general schemes has not improved since (even for implicit access structures). A major motivation for this work is the hope that departing from previous approaches relying mostly on information theoretic techniques, making use of algebraic techniques could potentially yield improved lower bounds for large classes of schemes, and hopefully eventually for general schemes. See [4] and references therein, for example, for a more thorough discussion of the many positive and negative results on share complexity of secret sharing schemes, as well as their numerous applications.

[1] In a nutshell, even if randomness domain is polynomially bounded in the share complexity, we still get a double-exponential number of secret sharing schemes of share complexity $O(n/\log(n))$, which is about the number of monotone access structures.

(Multi-)linear schemes

On the other hand, much more is known about the share complexity of the well studied family of linear secret sharing schemes, and more generally multi linear secret sharing schemes. In a nutshell, a linear scheme is a scheme, where each share is a linear combination of elements from a finite field $\mathbb{F}$, each of which is either the secret or a random variable, while a multi-linear scheme is a scheme where the secret can be vector of elements from $\mathbb{F}$ and the shares are a linear combination of these elements and the random variables. Linear schemes are relatively easy to design, often exploiting the insights and intuition we have into linear algebra. Perhaps a more important reason for their popularity is their "homomorphic" property. In MPC, for example, linear schemes are a useful building block, as they allow computing a sharing of the sum of shared secrets by locally adding the corresponding shares. Even more importantly, for (multi) linear schemes better lower bounds on share complexity are also known. In particular, counting arguments yield exponential lower bounds for non-explicit access structures, and recently, an exponential lower bound has been obtained on the share complexity of linear schemes for an explicit access structure. See next section for more details. For now, the observation important for discussion is that as well as upper bounds, lower bounds for (multi) linear secret sharing schemes heavily exploit the (linear-)algebraic structure of the sharing scheme.

Motivated by the hope to narrow the gap between upper and lower bounds for share complexity and information rate in secret sharing schemes, in this work, we continue the work of [5], which initiates a study of the power of non-linear secret sharing schemes. The main motivation in [5] for studying non-(multi) linear schemes is that most constructions of secret sharing schemes so far were either linear or multi linear, so new insights both on upper and lower bounds may be gained. Indeed [5] put forward several innovative secret sharing schemes for access structures for which linear schemes of comparable complexity are not known, or even do not exist under reasonable assumptions. In [5] the authors explore both arbitrary non-linear schemes, and a specific generalization of linear schemes, they refer to as *quasi-linear* schemes.

We have the additional motivation of obtaining new lower bounds for a broader class of schemes than linear and multi linear ones, making a step forward towards improved lower bounds for general schemes, which proved notoriously hard so far.

More specifically, we chose to explore the arguably natural extension of multi linear schemes, we call *polynomial schemes*, or PSSS. A PSSS is defined as multi linear scheme over a finite field $\mathbb{F}$, where each share is some polynomial over $\mathbb{F}$ in the secret and randomness elements, rather than necessarily a degree-1 polynomial (corresponding to a multi linear scheme). We hope that the rich algebraic structure of polynomials - especially of polynomials of low degree, say 2, would help develop techniques for lower bounds of more *algebraic* nature, as they proved useful for linear and multi linear schemes. A slightly more general notion of polynomial schemes is one where where the secret domain S is a subset of $\mathbb{F}^k$, rather than the entire set $\mathbb{F}^k$. We refer to such schemes as *generalized* polynomial schemes.

Besides the potential for useful analytic techniques, we believe PSSS is a useful set of schemes to study as it is very broad. In particular, as any function $f : \mathbb{F}^n \to \mathbb{F}$ can be represented by an n-variate polynomial over $\mathbb{F}$, it takes a moment to think why not every secret sharing scheme can be represented by a PSSS with the same share complexity. The reason is that a secret sharing scheme is a randomized mapping $Sh : S \times R \to S_1 \times \ldots \times S_n$, rather than a deterministic function. In Sh, the randomness is uniformly sampled from a finite set R. Now observe that in any PSSS scheme $Sh' : \mathbb{F}_p^s \times \mathbb{F}_p^r$ over a finite field $\mathbb{F}_p$, the probability of outputting any share vector is a multiple of p^{-r}. The straightforward way to

convert from Sh into an equivalent scheme Sh' as above is to embed S and R into $\mathbb{F}_p^s, \mathbb{F}_p^r$ for some s, r respectively, and evaluate the shares as polynomials corresponding to every share $Sh_i(s, r)$ (which are guaranteed to exist). More precisely, arbitrarily partition $\mathbb{F}_p^r$ into $|R|$ equal parts $R'_1, \ldots, R'_{|R|}$, the embedding labels every element of R'_j by r_j and sets Sh' accordingly. The problem with this approach in perfect secret sharing is that p^r may not be divisible by $|R|$ for any prime p and any r. For instance, for $|R| = 6$ in Sh there is no such embedding, as $1/6$ can not be written as $\frac{a}{p^r}$ for any prime p and $a \in \mathbb{N}$. We note that the above approach of transformation into PSSS (over any field $\mathbb{F}_p$) does work for statistical secret sharing, by choosing a sufficiently large r and R_j's of almost equal size, making the privacy "leakage" arbitrarily small, and keeping correctness perfect. In this work we focus on the standard notion of perfect secret sharing schemes, though.

1.1 Our Results

Feasibility and share complexity lens

On the negative side, we show that a large subclass of PSSS with r-degree 1 is equivalent to multi-linear schemes in the sense that for each such scheme, a multi-linear scheme for the same access structure with (almost) the same share complexity per secret bit and over the same field exists.

▶ **Theorem 1** (Informal). *Let $\mathcal{M}$ be a PSSS of degree 1 in $\vec{r}$, where all share polynomials are either missing monomials of (exact) degree $c \geq 2$ in $\vec{s}$ and 0 in $\vec{r}$, or all share polynomials miss monomials of exact degree ≥ 1 in $\vec{s}$ and 1 in $\vec{r}$. Then there exists an equivalent multi linear scheme $\mathcal{M}'$ with share complexity at most n times that of $\mathcal{M}$.*

We conjecture that all schemes with $\vec{r}$-degree 1 are as weak as multi-linear schemes, and leave it as an interesting open problem. See Theorem 9 and Theorem 11 for a formal statement and a proof of the above theorem. The proofs of both theorems are constructive, transforming the r-degree 1 schemes into multi linear schemes. The validity of the constructions is proved by rather simple linear algebraic techniques, but the constructions themselves, especially that of Theorem 9 are somewhat surprising, in our opinion.

Moving to the next natural class of $\vec{r}$-degree 2, we show that a certain natural subclass of such PSSS only allows to implement a small subset of access structures (regradless of share complexity).

▶ **Theorem 2** (Informal). *PSSS of degree exactly 2 in $\vec{r}$ over fields of odd characteristic capture only access structures where all minterms are singletons.*

That is, somewhat intuitively, linear terms are required in degree-2 schemes for implementing useful access structures. The proof here relies on facts regarding the number of solutions of equations of the form $p(x_1, \ldots, x_n) = b$, where b is a quadratic form.

To contrast with the bounds in [14] on functions representable by polynomial-sized randomizing polynomials with r-degree 2 and any constant degree in s (over small fields), indicating the corresponding functions are relatively simple, falling in NC_3. The reason why their bound does not directly imply that PSSS of r-degree 2 and polynomial share complexity works for relatively simple schemes, is that their bound holds for representations polynomial in input size. In particular, they assume the randomness vector's size is polynomially bounded in the input vector's size. For PSSS with $poly(n)$ randomness and share complexity we could indeed obtain a similar bound on the type of access structures for which such PSSS exists.

However, lacking bounds on the randomness complexity (see the following section), assuming only polynomial share complexity does not seem to suffice. [2]

On the positive side, we observe that a surprising recent result indicating all monotone access structures have a scheme construction share complexity $O(2^{0.994n})$ [18] can be replaced with a multi-linear construction (instead of a non-polynomial scheme).

We show that there exists (multi) linear secret sharing schemes based on the multi-linear CDS [1] with information rate O(1) for a certain class (not all) of access structures for a sufficiently large share domain.[3]

▶ **Observation 1.** *Let $n > 0$ be an integer. Then all monotone access structures on n parties admit a multi-linear scheme over $S = \mathbb{F}_2^{O(2^n)}$ with information rate $O(2^{0.994n})$ per party. (in our language, degree-1 polynomial scheme over $\mathbb{F}_2$).*

This observation demonstrates the power of amortization (increasing k) all else kept equal. Additionally, we can obtain a polynomial scheme of (possibly) high degree with the same share complexity.

▶ **Observation 2.** *Let $n > 0$ be an integer. Then all monotone access structures on n parties admit a polynomial scheme over $S = \mathbb{F}_{2^{O(2^n)}}$ with information rate of $O(2^{0.994n})$ per party.*

This is a direct corollary of Theorem 1. This holds due to the simple observation that any polynomial scheme over $\mathbb{F}_q^{k'}$, where q is a prime power (of any degree) can be replaced by a scheme where $S = \mathbb{F}_{q^{k'}}$, (that is, a scheme with $k = 1$) and the sharing polynomials are of possibly higher degree than the original ones. This is done by thinking of the vector of field elements in parties' shares and the vector of random field elements as vectors of elements over $\mathbb{F}_q^{k'}$, and the secret as an element of $\mathbb{F}^{q^{k'}}$. Then, the fact that any finite field $\mathbb{F}$ and function $\mathbb{F}^{1+r'} \to \mathbb{F}$ can be represented as a multi-variate polynomial over $\mathbb{F}$ implies that the original scheme can be implemented as a polynomial scheme with $k = 1$ over $\mathbb{F}_{q^{k'}}$. The overall share complexity overhead of this transformation is at most n, as the overall share complexity is at least $\log_2(|S|)$ to maintain perfect correctness. This general observation implies that there is certain redundancy regarding the usefulness of various parameters ($k, |F|$ and total degree) of polynomial schemes towards reducing share complexity. Namely, if we are free to adjust $\mathbb{F}$ and the degree arbitrarily, then without loss of generality k can be fixed to 1 without loss of generality.

Randomness complexity lens

An additional aspect that we have studied is the randomness complexity of PSSS. Here we study what is the best upper bound on the randomness complexity, as a function of the share complexity of a scheme – $\mathrm{RC}(SC)$. That is, for every scheme in the (sub) class of polynomial schemes with share complexity SC, there exists an equivalent scheme in the class with the same share complexity and randomness complexity at most $\mathrm{RC}(SC)$. For linear

[2] Still, if we had polynomial in share complexity upper bounds on randomness complexity, a modification of [14]'s result would yield bounds on this type of limited constant degree PSSS which are stronger than just counting-based bounds for constant-degree PSSS given suitable bounds on randomness complexity. Namely, not only do access structures that cannot be implemented efficiently exist, but there are candidates in relatively low complexity classes (under standard assumptions). See full version for details.

[3] The following pair of results are simple observations, which may be described and understood within the limits of the introduction, and we think they hope gain intuition on. The full proof of the first observation relies on particular details of [1]'s construction and is deferred to the full version. The proof of the second is simple and appears below.

and multi-linear schemes it is known that their randomness complexity is (without loss of generality) upper bounded by SC (the equivalent scheme is also over the same field). To the best of our knowledge, no such bounds appear in the literature for other broad classes of schemes. In particular, we have not found a bound for general (perfect) secret sharing schemes (we believe it was likely previously known).

In this work we put forward an upper bound for randomness complexity for general secret sharing schemes as well as various types of PSSS.

▶ **Theorem 3** (Informal). *Let $\mathcal{M}$ be a secret sharing scheme. Then, there exists an equivalent scheme $\mathcal{M}'$ with the same share complexity SC and randomness $RC = 2^{poly(SC)}$ such that if $\mathcal{M}'$ is a PSSS of degree 2, then so is $\mathcal{M}'$, and if $\mathcal{M}$ is a PSSS then so is $\mathcal{M}$. Also, in the two latter cases, $\mathcal{M}$ and $\mathcal{M}'$ are defined over the same field.*

The full proof of the theorem appears in the full version. To prove the bound for degree-2 PSSS, we restate the privacy requirements into sets of equality of distributions restrictions for single polynomials obtained using a variant of Vazirani's XOR lemma (already satisfied by $\mathcal{M}$). In particular, we prove there exists (via an explicit construction) a linear mapping from the vector space $span(r_1, \ldots, r_t)$ to a (much) smaller $span(r_1, \ldots, r_{t'})$ and every share polynomial $p(\vec{s}, \vec{r})$ is replaced by $p(\vec{s}, L(r_1), \ldots, L(r_n))$ so that privacy is still satisfied. The proof is based on a somewhat involved case analysis based on the theory on output distributions of quadratic forms. The bound for general secret sharing is proved using the following approach: given a PSSS scheme, we state the correctness and privacy requirements for any secret sharing scheme for the same access structure as an LP. Curiously, the LP formulation makes use of the scheme we already have at hand (with potentially high RC), rather than just a formulation of correctness and privacy. A solution to the LP determines the probabilities of mapping each secret s to each share vector $(\vec{\text{sh}}_1, \ldots, \vec{\text{sh}}_n)$, which easily extends into a PSSS over the same field and same share complexity. Briefly, the LP variables are probabilities $p_{i,k}$ where $\vec{s}_i$ is a secret and $\vec{sh}_k$ is a share vector. Privacy implies that for all maxterms A, and share vectors $\vec{\text{sh}}_A$ it must hold that

$$\sum_{\substack{all\ k\ for\ which\ the\ projection \\ of\ \vec{sh}_k\ on\ A\ is\ \vec{sh}_A}} p_{i,k} - \sum_{\substack{all\ k\ for\ which\ the\ projection \\ of\ \vec{sh}_k\ on\ A\ is\ \vec{sh}_A}} p_{j,k} = 0.$$

From correctness, it follows that for every minterm A, for every value $\vec{\text{sh}}_A$ all but at most $\vec{s}$, the projection value $\vec{\text{sh}}_A$ is seen with probability 0. This constraint would result in a degree-2 inequality in the $p_{\vec{s},\vec{\text{sh}}}$'s. To make it linear, the trick is to require that the 0 probabilities are exactly as in the scheme $\mathcal{M}$. That is, of every $(A, \vec{\text{sh}}_A)$ we require: $\sum_{\substack{all\ k\ for\ which\ the\ projection \\ of\ \vec{sh}_k\ on\ A\ is\ \vec{sh}_A \\ and\ j \notin I}} p_{j,k} = 0$, where I is either $\{i\}$ for some i, or empty, and is fixed according to $\mathcal{M}$. Finally, the requirement that $(p_{i,1}, \ldots, p_{i,l})$ is a probability vector is also expressed by linear inequalities. We look for solutions with small randomness vector length - as the LP has small integer entries, it easily follows that the probabilities are a multiple of some $1/L$, where L is not very large (exponential in LP dimensions). In particular, this implies a scheme with R of size L and same share complexity. This alone, already yields a bound on the randomness complexity ($\log(|R|)$) of general (perfect) secret sharing schemes. Given $\mathcal{M}$ is a PSSS, to obtain a PSSS with the required parameters it is necessary and sufficient that additionally the probabilities in the solution are powers of $q = |\mathbb{F}|$. In Theorem 14 we prove the former part, the proof of the stronger statement for $\mathcal{M}$ which is a PSSS is deferred to the full version.

All of the bounds above are exponential in SC and may serve as a proof of concept. A strong motivation here is that good upper bounds on randomness complexity $\mathrm{RC}(SC)$ for constant-degree PSSS would lead to good existential bounds on the share complexity of such PSSS which we do not currently have (over small enough $\mathbb{F}$). More concretely, for constant $\mathbb{F}$ and $poly(SC)$ randomness complexity there exist access structures with share complexity $2^{\Omega(n)}$ of PSSS over $\mathbb{F}$.

We stress that all our upper bounds on randomness complexity are for *perfect* secret sharing schemes, and are therefore require new techniques even in the general secret sharing and unbounded degree PSSS settings. For general non-PSSS (or PSSS) statistically secure schemes, partial derandomization techniques from the literature can be applied. In more detail, for ϵ-statistical secret sharing, bounds of $\ell(h) = O(SC + \log \epsilon)$ on randomness complexity can be easily obtained by replacing the randomness with the output of a non-boolean PRG (nb-PRG) [11] against the sharing algorithm, mapping from $\ell(h)$ random bits to h random bits as used by the sharing algorithm. By standard analysis similar to that in the proof of Claim 2 in [3]'s full version, a random function from ℓ to h bits is a suitable nb-PRG. Such results however are not useful for lower bounds, however. It is unclear whether nb-PRGs can be applied to constant-degree PSSS to yield even statistical secret sharing schemes, as the resulting sharing scheme does not necessarily remain low-degree (as the nb-PRG itself may be of high degree). Thus, good lower bounds for low-degree PSSS even in the statistical setting are left as an interesting open problem.

Roadmap

In Section 2 we provide the precise (standard) definition of secret sharing that we use, and introduce some new definitions and notations for PSSS. In Section 3, we present our results on feasibility and share complexity. Precise theorems and proofs of the randomness-related results and a broader survey of previous work from the perspective of PSSS implicit in it are deffered to the full version.

1.2 Open questions

In this work we have obtained some preliminary results on PSSS but many fundamental questions remain open.

▶ **Question 1** (Informal). *Do there exist access structures, that have non-polynomial schemes much more efficient than any PSSS?*

See a discussion on this question in the full version, with certain evidence in the positive direction. In a nutshell, it considers secret sharing constructions based on large matching vectors families such as [17], which are known to exist over rings $\mathbb{Z}_m$ of composite size but provably do not exist when m is a prime.

Other interesting questions concern understanding the effect of various parameters of PSSS on their power, in terms of achievable share complexity and information rate. There are various interesting parameters. One useful parameter is k - the length of the vector space $\mathbb{F}^k$ constituting the secret domain S. The distinction between $k = 1$ and arbitrary k is the difference between linear and multi-linear schemes, when considering PSSS of total degree $d = 1$. Generally, as we discuss below, the distinction between small secrets - $k = 1$ (or small k) appears meaningful in terms of achievable information rate - see further discussion in the full version. An Additional question to study is the effect of the particular field $\mathbb{F}_p$ on the power of the induced PSSS class.

A concrete natural question is obtaining lower bounds for low degree PSSS, say of degree $d = O(1)$. A simple approach for $k = 1$ would be to bound $|R|$ as a function of the share complexity, and then rely on the fact that there are few different degree-d polynomials in $R + 1$ variables (exponentially many in the share complexity) for a constant $\mathbb{F}_p$. The number of monotone access structures is double-exponential in n. For linear schemes, it is well known that wlog. $\log(|R|) \leq$ share complexity, leading to a $2^{\Omega(n)}$ lower bound on share complexity of linear schemes over any fixed $\mathbb{F}_p$. However, for any $d > 1$, there are no known explicit bounds on $|R|$ in terms of |share complexity|, so this approach does not currently work. In this work we make a first step in the direction of filling in the missing component, obtaining certain upper bounds on $|R|$ (as a function of share complexity). This leaves the following interesting question open.

▶ **Question 2** (informal). *Fix some finite field $\mathbb{F}_q$, and $d = O(1)$. Does there exist a polynomial bound $h(\cdot)$ on $|R|$ as a function of share complexity, such that any PSSS over $\mathbb{F}_q$ of degree d has an equivalent PSSS over $\mathbb{F}_q$ and degree q with the same share complexity, and $|R| \leq h(SC)$.*[4]

2 Preliminaries

General notation

In this work we consider finite fields $\mathbb{F}$. We write $\mathbb{F}_q$ to denote a field of size q (some prime power). For matrices M_1, M_2 (of the proper sizes) over some field $\mathbb{F}$, we denote by $(M_1|M_2)$ the matrix resulting from concatenating M_2 to the right of M_1, and $(M_1; M_2)$ results from concatenating M_2 below M_1. Vectors are denoted by $\vec{v}$ or just v when there is no risk of confusion (with scalars), and are by default column vectors. We let M_i denote the i'th row of M, and M^i its i'th column. We let M_I (M^I) denote a submatrix with rows (columns) restricted to I. For a matrix $M \in \mathbb{F}^{n\times n}$, we denote by $N \in \mathbb{F}^{m\times m}$ the matrix resulting from removing all row-column pairs such that $M^i = (M_i^T) = \vec{0}$.

Secret sharing

We use standard definitions of secret sharing schemes, following [4].

▶ **Definition 4** ([4]). *Access Structure: For a set of parties $\{p_1, ..p_n\}$ a subset $\mathcal{A} \subseteq 2^{\{p_1,..,p_n\}}$ is called monotone if $B \in \mathcal{A}$ and $B \subseteq C$ implies $C \in \mathcal{A}$. Sets in $\mathcal{A}$ are called authorized and sets not in $\mathcal{A}$ are called unauthorized.*

▶ **Definition 5** ([4]). *Distribution Scheme: Let S,$|S| \geq 2$ be a finite set of secrets. A secret sharing scheme with secrets domain S, is a tuple $\mathcal{M} =< Sh, \mu >$ where μ is a probability distribution over some finite set R (called the set of random strings) and Sh is a mapping from $S \times R$ to a set of n-tuples $S_1 \times S_2 \times \ldots \times S_n$, where S_j is called the domain of shares of p_j. For a set $A \subseteq \{p_1, \ldots, p_n\}$, we denote $Sh(s, r)_A$ as the restriction of $Sh(s, r)$ to its A-entries. Sh satisfies the following properties:*

***Perfect Correctness**. The secret $s \in S$ can be reconstructed by any authorized set of parties. That is, for any set $B \in \mathcal{A}$ (where $B = \{p_{i_1}, \ldots, p_{i_{|B|}}\}$), there exists a reconstruction function $Recon_B : S_{i_1} \times \ldots \times S_{i_{|B|}} \to S$ such that for every $s \in S$,*

$$Pr[Recon_B(Sh(s, r)_B) = s] = 1 \tag{1}$$

[4] A sufficiently small super-polynomial bound on $|R|$ would still imply non-trivial bounds on share complexity, say better than the best known bound of $\Omega(n/\log n)$ for general schemes.

We refer to sets in $\mathcal{A}$ as qualified, and to minimal qualified B in the sense that B is qualified and no $B' \subsetneq B$ is qualified as minterms of $\mathcal{A}$. We refer to maximal unqualified sets, in the sense that B is unqualified but for all $P_i \notin B$, $\{P_i\} \cup B$ is qualified as maxterms of $\mathcal{A}$.

***Perfect Privacy**. Every unauthorized set cannot learn anything about the secret (in the information theoretic sense) from their shares. Formally, for any set $T \notin \mathcal{A}$, for every two secrets $a, b \in S$, and for every possible vector of shares $< \vec{sh}_j >_{p_j \in T}$:*

$$Pr[Sh(a,r)_T =< \vec{sh}_j >_{p_j \in T}] = Pr[Sh(b,r)_T =< \vec{sh}_j >_{p_j \in T}] \tag{2}$$

Observe that wlog., each share polynomial $q_{i,j}$ has free coefficient 0 (as any constant may be locally added by *Recon*). We will assume this implicitly throughout the paper.

Sometimes, we will be interested in ϵ statistical secret sharing, where ϵ error in correctness is allowed, and the distributions $Sh(a,r)_T$ and $Sh(b,r)_T$ are for unqualified T may be at statistical distance up to ϵ. Our default notion throughout the paper is that of perfect secret sharing as in Definition 5.

(Multi)Linear secret sharing schemes

The most studied and most commonly used class of secret sharing schemes is the linear secret sharing schemes class. This class is subclass of multi-linear secret sharing schemes.

A secret sharing scheme is said to be multi-linear, if $S = \mathbb{F}^k, R = \mathbb{F}^m$ for some finite field $\mathbb{F}$, and each share $\vec{\mathrm{sh}}_i$ consists of g linear combinations $l_{i,1}(\mathrm{s}_1, \ldots, \mathrm{s}_k, r_1, \ldots, r_m) \ldots, l_{i,g}(\mathrm{s}_1, \ldots, \mathrm{s}_k, r_1, \ldots, r_m)$ over $\mathbb{F}$. The scheme is called linear if additionally $k = 1$.

Complexity measures of secret sharing schemes

The information rate, IR of a secret sharing scheme $\mathcal{M}$, is the ratio between the maximum length of the shares and the length of the secret. Formally, $IR(\mathcal{M}) = (\max_{i \in [n]} \log(|S_i|))/|\log S|$, where the maximum is taken over all dealer's random strings r.

The share complexity of secret sharing scheme, $\mathcal{M}$, is $SC(\mathcal{M}) = \max_{i \in [n]} \log(|S_i|)$.

We denote the randomness complexity of a secret sharing scheme $\mathcal{M}$ by $\mathrm{RC}(\mathcal{M})) = \lceil \log_2(|R|) \rceil$ - the number of bits required to represent an element of R.

2.1 Polynomials over finite fields

In this work we focus on the set $\mathbb{F}_q[y_1, \ldots, y_n]$ of multivariate polynomials over finite fields. We say a polynomial $p(y_1, \ldots, y_n)$ is of degree i if all monomials in the polynomials have a cumulative degree of at most i. We say p has degree exactly i if all monomials in p are of cumulative degree exactly i. Similarly, for a subset $I \subseteq [n]$, we say p is of degree i in $x_I = \{x_j | j \in I\}$ if every monomial of p has cumulative degree at most i in the variables from x_I (similarly, for exact degree in x_I). In a finite field $\mathbb{F} = \mathbb{F}_{p^\ell}$, where p is prime, let $Tr_{\mathbb{F}}(\alpha) = \sum_{i=0}^{\ell-1} \alpha^{p^i}$ is the *trace* mapping from $\mathbb{F}$ to itself.[5]

2.1.1 Output distributions of degree-2 polynomials

Some of our results require some theory on degree-2 polynomials over finite fields. In particular, we will reduce understanding the output distributions of (various subclasses of) degree-2 PSSS to understanding the output distribution of a *single* degree-2 multivariate

[5] In fact, the image of $Tr_{\mathbb{F}}$ is always contained in $\mathbb{F}_p$.

polynomial. For (any) polynomial in $p(x_1,\ldots,x_n) \in \mathbb{F}_q[x_1,\ldots,x_n]$, we let $N_{f,b}$ denote the number of solutions in $\mathbb{F}_q^n$ for the equation $f(x_1,\ldots,x_n) = b$. Polynomials in $\mathbb{F}[x_1,\ldots,x_n]_q$ where all monomials are of exactly degree 2, called *quadratic forms*. It is convenient to represent quadratic forms $f(x)$, by a matrix $A \in \mathbb{F}_q^{n\times n}$, where $f(x) = x^T Ax$. That is, $A_{i,j}$ is the coefficient of $x_i x_j$. We will need the following existing theory characterizing $N_{f,b}$ for f which are quadratic forms over a finite fields, and general degree-2 polynomials over fields of characteristic 2. All required theory and discussions appears in chapter 6 in [16], and is included here for self containment. Also, some of the theorems we state here are straightforward corollaries of [16], but were not explicitly stated there.

Fields of odd characteristic

Fix some finite field $\mathbb{F}$ of odd charactersitic. We let η denote the quadratic character on $\mathbb{F}^*$. That is, $\eta(x) = 1$ if x is a quadratic residue modulo q, and -1 otherwise. We extend its definition to 0 via $\eta(0) = 0$.

We also let $\nu : \mathbb{F} \to \mathbb{Z}$ be $\nu(b) = -1$ for $b \in \mathbb{F}^*$, and $\nu(0) = q-1$. Recall a quadratic form f over a characteristic field $\mathbb{F}$ in variables $x_1,\ldots,x_n$ is a polynomial where all monomials are of degree exactly 2. It is known that a quadratic form $f(x)$ in variables $x = (x_1,\ldots,x_n)$ has a representation of the form $f(x) = x^T C \cdot M_f \cdot C^T x$, where C is an invertible matrix in $\mathbb{F}^{n\times n}$, and $M_f \in \mathbb{F}_q^{n\times n}$ is diagonal, and all $rank(M_f)$ non-zero elements in the diagonal are at entries $M[i,i]$ for $i \le rank(M_f)$. Such a representation M_f is called canonical. Here, M_f represents a quadratic form $p'(v) = v^T M_f v$ in a new vector $\vec{v} = (v_1,\ldots,v_n)$ of variables, obtained from $\vec{x}$ via $\vec{v} = C^T x$. The number $m \le n$ of non-zero elements on M_f's diagonal is an invariant for all canonical representations of f. The function $\eta(det(M_f^-))$ is another invariant, independent of the concrete canonical representation M_f. (see Theorem 6.21 in [16] and discussion beforehand for more intuition). We denote the type of a quardatric form $f(x_1,\ldots,x_n)$ over $\mathbb{F}_q$ of odd characteristic as (n,m,η), where (m,η) are the corresponding values of the above invariants of equivalent canonical forms.

To understand the expression for $N_{f,b}$ for a quadratic form f, it suffices to understand $N_{g,b}$ for the quadratic form $g(v_1,\ldots,v_n)$ in a new vector of variables $v = (v_1,\ldots,v_n)$, where $g(v) = v^T M_f v$ where M_f is a canonical representation of a quadratic form, as $N_{f,b} = N_{g,b}$ for all $b \in \mathbb{F}_q$. We refer to such g as canonical forms. This holds as $v(x) = C^T x$ is a bijection between the domain of $f(x)$ and the domain of $g(v)$ satisfying $f(x) = g(v(x))$ for all $x \in \mathbb{F}_q^n$. We say that f is equivalent to a canonical form g as above. We define the *type* of a quadratic form $f(x_1,\ldots,x_n)$ of odd characteristic via the triple $(n,m,\eta(\det))$ (with $m,\eta(det)$ invariants of canonical forms equivalent to f).

By the above discussion, we may assume wlog. that $n = m$, and calculate the number of roots in that case. In the general case of f of type (n,m,η), compute the number of roots for an equivalent canonical g of type $(n = m,m,\eta)$, and multiply by q^{n-m}.

The following theorem now follows directly by combining theorems 6.26, 6.27 from [16]. For a quadratic form $f(x)$ we denote the number of solutions to the equation $f(x) = b$ by $N_{f,b}$,

▶ **Theorem 6.** *Let $p(x_1,\ldots,x_n)$ denote a quadratic form over a finite field $\mathbb{F}_q$ of odd characteristic of type (n,m,d). Consider a representation $f(x) = v^T M_f v$ as above, $x = (x_1,\ldots,x_n)$,and the v_i's are (independent, by choice of C) linear combinations of the x_j's. Then*

1. *If m is even, then for every $b \in \mathbb{F}$*

$$N_{f,b} = q^{n-m}(q^{m-1} + q^{(m-2)/2}\nu(b)\eta((-1)^{m/2})d).$$

2. *If m is odd, for every $b \in \mathbb{F}$*

$$N_{f,b} = q^{n-m}(q^{m-1} + q^{(m-1)/2}\eta(b(-1)^{m/2})d).$$

Following Theorem 6, we define the *type* of a quadratic form $f(x_1, \ldots, x_n)$ of odd characteristic via $(m, \det)$. Evidently, the type of f determines the distribution of $f(x)$ when x is picked uniformly from $\mathbb{F}^n$. Here we no longer assume $m = n$.

Fields of characteristic 2

Let $\mathbb{F}$ be a field of characteristic 2. Here we also have a canonical representation of quadratic forms, albeit somewhat less simple. Namely, for every quadratic form $f(x_1, \ldots, x_n)$, there exists a number $m \leq n$, and a non-signular matrix $C \in \mathbb{F}^{n \times n}$ such that $f(x) = x^T C M_f C^T x$, where M_f has one of the following forms:

1. (Type $T = 1$) m is even. M_f has 0's everywhere except for entries $M[2i-1, 2i]$ for $1 \leq i \leq m/2$ for some integer $m \leq n$, which are all 1.
2. (Type $T = 2$) m is even. M_f has 0's everywhere except for entries $M[2i-1, 2i]$ for all $1 \leq i \leq m/2$ for some integer $m \leq n$ which are 1, $M[m-1, m-1] = 1$, and $M[m, m] = a$, where $Tr_{\mathbb{F}}(a) = 1$.
3. (Type $T = 3$) m is odd. M_f has 0's everywhere except for entries $M[2i-1, 2i]$ for $1 \leq i \leq (m-1)/2$ which are all 1, and also $M[m, m] = 1$.

Similarly to the odd characteristic case, we refer to M_f as a canonical representation. By Theorem 6.30 in [16], the number m and T of the canonical M_f is and invariant depending only on f, and not on the particular representation f. Thus, we denote the type of a quadratic form $f(x_1, \ldots, x_n)$ as (n, m, T), according to n and the above invariants. For each type, and $b \in \mathbb{F}$, a characterization of $N_{f,b}$ for quadratic forms is known, as follows from Theorem 6.32 in [16].[6]

▶ **Theorem 7.** *Let $p(x_1, \ldots, x_n)$ denote a quadratic form of type (n, m, T) over a finite field $\mathbb{F}_q$ of characteristic 2. Then*

1. *If $T = 1$, for every $b \in \mathbb{F}_q$, $N_{f,b} = q^{n-m}(q^{m-1} + q^{(m-2)/2}\nu(b))$.*
2. *If $T = 2$, for every $b \in \mathbb{F}_q$, $N_{f,b} = q^{n-m}(q^{m-1} - q^{(m-1)/2}\nu(b))$.*
3. *If $T = 3$, for all $b \in \mathbb{F}_q$, $N_{f,b} = q^{n-1}$.*

2.2 Polynomial Secret Sharing Schemes (PSSS)

In this work, we put forward a natural generalization of (multi)-linear secret sharing schemes - where shares are allowed to be general polynomials of $\vec{s}, \vec{r}$, rather than just linear combinations. Namely:

▶ **Definition 8** (PSSS). *A polynomial secret sharing scheme (PSSS) $\mathcal{M} = (Sh, \mu)$ is a secret sharing scheme specified by $(\mathbb{F}, t, k, Sh)$ where $\mathbb{F}$ is a finite field, $S = \mathbb{F}^k$ is the domain of secrets, μ is uniform over $R = \mathbb{F}^t$, and $t, k \in \mathbb{N}^+$. The sharing function $Sh(\vec{s}; \vec{r})_i$ returns $(p_{i,1}(\vec{s}, \vec{r}), \ldots, p_{i,l_i}(\vec{s}, \vec{r}))$ as the i'th party's share, where each $p_{i,j}(\vec{s}, \vec{r})$ is a (multivariate) polynomial over $\mathbb{F}$.*

[6] The theorem applies to $m = n$, but reasoning similar to the odd characteristic case implies $N_{f,b}$ for general m, n as a simple corollary.

We will denote the corresponding classes of polynomial schemes over $\mathbb{F}$ via $PSSS_{regexp[s,r],\mathbb{F}}$, where $regexp$ is a (variant of) a regular expression in $r, s, 1$. The syntax and semantics of the expression set is defined recursively as follows: r encodes the set of polynomials $\{\sum_{j\in[k]} a_j r_j | a_j \in \mathbb{F}\}$, and s encodes $\{\sum_{j\in[k]} a_j \mathrm{s}_j | a_j \in \mathbb{F}\}$, 1 encodes $\{a | a \in \mathbb{F}\}$. For a pair of regular expressions g_1, g_2; g_1^* encodes the set $\{p_1 \cdot \ldots \cdot p_h | h \in \mathbb{N}, \forall i \in [h], p_i \in g_1\}$; $g_1 + g_2$ encodes $\{p_1 + p_2 | p_1 \in g_1, p_2 \in g_2\}$, and $g_1 \cdot g_2$ encodes the set $\{\sum_{j\in[h]} p_{1,j} \cdot p_{2,j} | h \in \mathbb{N}, \forall j p_{1,j} \in g_1, p_{2,j} \in g_2\}$. g_1^i is a shorthand for $g_1 \cdot \ldots \cdot g_1$ with i appearances of g_1. We also say that a scheme M has degree at most (exactly) d in r (s), if each monomial contains at most (exactly) d r_i's (s_i's).

For polynomial schemes $\mathcal{M}$, we measure share complexity in field elements, rather than in bits. Formally, these measures will be denoted by $SC_{\mathbb{F}}(\mathcal{M}$ etc. (it always the case $IR_{\mathbb{F}}(\mathcal{M}) = IR(\mathcal{M})$, as this measure is normalized by secret size).

Our definition is a generalization of the notion of multi linear secret sharing in a natural direction, which potentially adds power over multi-linear schemes. We try to keep it as close as possible to the definition of multi-linear schemes, and insist that the domain where secrets, randomness and computation are performed is a finite field.[7]

A slightly more general notion of polynomial schemes is one where $S \subseteq \mathbb{F}^k$, rather than the entire set $\mathbb{F}^k$.[8] We refer to such schemes as *generalized* polynomial schemes.

3 On Feasibility and Share Complexity of PSSS

In the next two sections, we present our negative results. Our positive result on the power of multilinear schemes is a rather simple observation based on existing work, and is deferred to the full version.

3.1 Bounds on efficiency of degree 1 in r PSSS

We show that a large sub-class of polynomial schemes of degree at most 1 in r ($PSSS_{s^*\cdot r+s^*}$) are not more powerful than multi-linear schemes, in the sense that they can not reduce share complexity super-polynomially over multi-linear schemes.

Our first result proves that $PSSS_{s^*\cdot r+s}$ can be replaced by a multi-linear scheme without any loss in parametres.

▶ **Theorem 9.** *For every scheme $\mathcal{M} = (\mathbb{F}, t, k, Sh)$ in $PSSS_{s^*\cdot r+s}$, there exists a $PSSS_{s+r}$ scheme $\mathcal{M}' = (\mathbb{F}, t, k, Sh')$ for the same access structure and $\mathcal{A}$ with $SC(\mathcal{M}') = SC(\mathcal{M})$.*

Proof. Somewhat surprisingly, for any scheme $PSSS_{s+r,\mathbb{F}}$ we build an equivalent multi-linear scheme by replacing the coefficient polynomials of the r_i's in the shares (which have the form $p(s)$) by constants resulting from substituting an arbitrary fixed vector $s' \in S$ into the coefficients.

To prove this theorem, let us restate the sharing algorithm Sh more conveniently. For such a scheme, $Sh(s, r)$ can be represented as $Vs + Mr$, where $V \in \mathbb{F}^{a\times k}, M \in \mathbb{F}[\mathrm{s}_1, \ldots, \mathrm{s}_n]^{a\times t}$. Here each entry of M is a formal polynomial $p_{i,j}$ in s, a the total number of polynomials in

[7] Note that some of the schemes appearing in [5] are quite close to "polynomial" schemes, but the domains employed there are rings R which are (crucially) not fields, and the secrets and randomness do not necessarily come from domains of the form R^t, R^k.

[8] If no restriction on the s-degree are made, we may replace the subset S with any other subset of the same size, without affecting the other parameters.

the share vector, and V a constant. M_s is a shorthand for $M(s)$ - substituting a concrete value s as the secret vector, into the matrix of polynomials.

A function $\rho : \{1, ..., a\} \longrightarrow \{p_1, ..., p_n\}$ labels each row by a party, so that party P_i receives the shares corresponding to rows $H_i = j|\rho(j) = i$. For a set A of parties, we abbreviate the submatrix pf M involved in generating A's shares on secret vector s (aka $\cup_{i\in A} H_i$) as $A_s = (V_A|M_{s,A})$.

▷ Claim 10. Let $\mathcal{M} = \{\mathbb{F}, t, k, (V|M)\}$, in $PSSS_{s^*r+s,\mathbb{F}}$, be a secret sharing scheme for an access structure $\mathcal{A}$. The scheme $\mathcal{M}'$ where M is substituted by a constant matrix $M_{\vec{s_1}}$ for some fixed secret $\vec{s_1}$ is a (multi-linear) secret sharing scheme for the same access structure.

Proof. Fix some secret vector $\vec{s_1}$ as in the statement of the claim. We prove the scheme remains valid.

Correctness: Consider any $\vec{s_0} \in \mathbb{F}^k$. Now we will look at authorized set A. Let us look at the two share distributions $(V_A|A_{\vec{s_1}}) \cdot (\vec{s_1}|\vec{r_1})$ and $(V_A|A_{\vec{s_0}}) \cdot (\vec{s_0}|\vec{r_0})$ of secrets $\vec{s_1}$ and $\vec{s_0}$, where $\vec{r_1}, \vec{r_0} \in \mathbb{F}^t$ are independent random vectors. The correctness of $\mathcal{M}$ is equivalent to stating that for all pairs $\vec{r_0}, \vec{r_1}$, we have:

$$\begin{aligned} &(V_A|A_{\vec{s_1}}) \cdot (\vec{s_1}|\vec{r_1}) \neq (V_A|A_{\vec{s_0}}) \cdot (\vec{s_0}|\vec{r_0}) \\ &\qquad\qquad \Downarrow \\ &V_A \cdot (\vec{s_0} - \vec{s_1}) \neq A_{\vec{s_1}} \cdot \vec{r_1} - A_{\vec{s_0}} \cdot \vec{r_0}. \end{aligned} \tag{3}$$

It is correct in particular for $\vec{r_0} = \vec{0}$. Which means that:

$$V_A \cdot (\vec{s_0} - \vec{s_1}) \neq A_{\vec{s_1}} \cdot \vec{r_1} \tag{4}$$

for all $\vec{r_1}$. Due to the fact that Equation 4 is correct for any $\vec{s_0} \in \mathbb{F}^k$ and by the structure of the secret domain, for any two distinct secret vectors $\vec{s_2}, \vec{s_3} \in \mathbb{F}^k$ there exists $\vec{s_0}$ for which $\vec{s_2} - \vec{s_3} = \vec{s_0} - \vec{s_1}$. From equation 4:

$$V_A \cdot (\vec{s_2} - \vec{s_3}) \neq A_{\vec{s_1}} \cdot r_1 \tag{5}$$

For all $\vec{r_1} \in \mathbb{F}^t$. Let $\vec{r_2}, \vec{r_3} \in \mathbb{F}^t$. Writing $\vec{r_1} = \vec{r_3} - \vec{r_2}$ we conclude that (as r_1 in Equation 5 is arbitrary),

$$\begin{aligned} &V_A \cdot (\vec{s_2} - \vec{s_3}) \neq A_{\vec{s_1}} \cdot \vec{r_1} \\ &\qquad\qquad \Downarrow \\ &(V_A|A_{\vec{s_1}}) \cdot (\vec{s_2}|\vec{r_2}) \neq (V_A|A_{\vec{s_1}}) \cdot (\vec{s_3}|\vec{r_3}) \end{aligned} \tag{6}$$

Which is precisely the definition of correctness for the new scheme (as $\vec{r_2}, \vec{r_3}, \vec{s_2} \neq \vec{s_3}$ are otherwise arbitrary).

Privacy: Consider some secret $\vec{s_0} \neq \vec{s_1} \in \mathbb{F}^k$. It follows directly from privacy that for each unauthorized set A, for any $\vec{r_0} \in \mathbb{F}^t$ there exists $\vec{r_1} \in \mathbb{F}^t$ for which:

$$\begin{aligned} &(V_A|A_{\vec{s_1}}) \cdot (\vec{s_1}|\vec{r_1}) = (V_A|A_{\vec{s_0}}) \cdot (\vec{s_0}|\vec{r_0}) \\ &\qquad\qquad \Downarrow \\ &V_A \cdot (\vec{s_0} - \vec{s_1}) = A_{\vec{s_1}} \cdot \vec{r_1} - A_{\vec{s_0}} \cdot \vec{r_0} \end{aligned} \tag{7}$$

In particular this is true for $\vec{r_0} = \vec{0}$. Then for any $\vec{s_0}$ there exists $\vec{r_1} \in \mathbb{F}^t$ for which:

$$V_A \cdot (\vec{s_0} - \vec{s_1}) = A_{\vec{s_1}} \cdot \vec{r_1} \tag{8}$$

Let $\vec{s_2}, \vec{s_3}$ denote a pair of secrets. Fix $\vec{s_0}$ for which $\vec{s_2} - \vec{s_3} = \vec{s_0} - \vec{s_1}$. From 8 it follows there exists $\vec{r_1}$ for which:

$$V_A \cdot (\vec{s_2} - \vec{s_3}) = A_{\vec{s_1}} \cdot \vec{r_1} \tag{9}$$

So for any vector $r_3 \in \mathbb{F}^t$ we get:

$$\begin{aligned} V_A \cdot (\vec{s_2} - \vec{s_3}) &= A_{\vec{s_1}} \cdot r_1 \\ &\Downarrow \\ V_A \cdot (\vec{s_2} - \vec{s_3}) &= A_{\vec{s_1}} \cdot (\vec{r_3} - (\vec{r_3} - \vec{r_1})) \\ &\Downarrow \\ (V_A | A_{\vec{s_1}}) \cdot (\vec{s_2} | \vec{r_3} - \vec{r_1}) &= (V_A | A_{\vec{s_1}}) \cdot (\vec{s_3} | \vec{r_3}) \end{aligned} \tag{10}$$

We prove that this implies privacy. Picking $\vec{r_3}$ at random, the vector $\vec{r_3} - \vec{r_1}$ is a random vector as well. Thus, the left hand size, where $\vec{r_3}$ is picked at random is distributed precisely as the shares seen by A when sharing $\vec{s_2}$ in $\mathcal{M}'$. This value is uniform over the affine subspace $V_A\vec{s_2} + \text{colSpan}(A_{\vec{s_1}})$. Similarly, the right hand side is also a random element of an affine subspace of the form $V_A\vec{s_3} + \text{colSpan}(A_{\vec{s_1}})$, and is distributed precisely as a share of $\vec{s_3}$ seen by A at M'. By Equation 10, these affine subspaces intersect, so they must be the same subspace, since both are cosets of $\text{colSpan}(A_{\vec{s_1}})$. This concludes the proof. ◁

◀

Next, we prove that a $PSSS_{s^*+r}$ scheme can be replaced by a multi-linear scheme up to a small loss in rate due to a small reduction in the dimension k of the secret space. Here, it will be convenient to specify $Sh(s, r)$ by a pair $(v(s), M)$, where $v(s) = (v_1(\mathrm{s}), \ldots, v_\ell(\mathrm{s}))$ is a vector of (multivariate) polynomials in s, and M is a constant matrix, and

$$Sh(s, r) = Mr + \sum_{i \in [k]} \mathrm{s}_i \frac{v^{(i)}}{\mathrm{s}_i}(s) = Mr + v(s) \tag{11}$$

Such an expression exists as we assume all share polynomials have a non-zero free coefficient. Here every $v^{(i)}(s)$ is a vector of formal polynomials, comprised of sums of all monomials in v in which s_i's degree is at least 1, and that were not included in $v^{(j)}$ for $j < i$ (we construct the $v^{(i)}$'s iteratively, starting from $i = 1$).[9] In this representation, s_i appears only in $v^{(j)}$ with $j \leq i$. We will sometimes denote Sh in $PSSS_{s^*+r}$ schemes as a pair (v, M) as above.

▶ **Theorem 11.** *For every scheme $\mathcal{M} = (\mathbb{F}, t, k, (v, M))$ in $PSSS_{s^*+r}$ there exists a multi-linear scheme $\mathcal{M}' = (\mathbb{F}, t, k - n, Sh)$ for the same access structure $\mathcal{A}$ with share complexity $SC(\mathcal{M}') \leq n \cdot SC(\mathcal{M})$.*

Proof. We construct a multi-linear scheme $\mathcal{M}' = (\mathbb{F}, t, k', (V'|M))$, by constructing a basis B for V''s column space, where $Sh(s, r) = (V'|M)(s, r)$ is the sharing algorithm of the multi-linear scheme (note V' here is constant). By Equation 11, for $s' = \vec{0}$, the distribution of $Sh(s', r)$ is therefor uniform over the zero coset of $Mr = colSpan(M)$. We conclude the following:

[9] Unlike in the previous section, it is more convenient to denote the formal polynomial vector by v, rather than v_s, in analog to M_s in the previous section, to simplify notation. We let $v(s)$ denote the evaluation of v on a specific vector s.

▷ Claim 12. For all $s' \in \mathbb{F}^k$ and every unqualified A, the vector $v_A(\mathrm{s}')$ is in $colSpan(M_A)$.

Proof. To see this, consider a representation of Sh as in Equation 11 of the form $Sh(\mathrm{s}', r) = Mr + v(\mathrm{s}')$ as above. Let v_A denote v restricted to entries held by A. We have $v_A(0, \mathrm{s}'_2, \ldots, \mathrm{s}'_k) = v_A(\mathrm{s}') - v_A^{(1)}(\mathrm{s}')$ (since only $v_A^{(1)}$ depends on s_1). Since by privacy of $\mathcal{M}$ both $v_A(s')$ and $v_A(0, s'_2, \ldots, s'_k)$ must belong to $colSpan(M_A)$ (as this holds for $s' = \vec{0}$), so does $v_A^{(1)}(s')$. Since s' is arbitrary, we conclude that $s''_1 v_A^{(1)}(s'')$ is in $colSpan(M_A)$ for all $s' = s''$. Now, comparing $Sh(s', r)$ and $s'' = (s'_1, 0, s'_3, \ldots, s'_k)$, by similar reasoning to the above, we conclude that $v_A^{(2)}(\mathrm{s}')$ is also $\vec{0}$ in $\mathbb{F}^{\#_{rows}(M_A)}/colSpan(M_A)$. This follows from the fact that $v_A^{(j)}$'s for $j > 2$ are independent of s_2, and the fact that $v_A^{(1)}(\mathrm{s}')$ and $v_A^{(1)}(\mathrm{s}'')$ are 0 in $\mathbb{F}^{\#_{rows}(M_A)}/colSpan(M_A)$ as we proved before, so it does not effect the coset. Similarly to the case of $j = 2$, by induction on j we can prove that $v_A^{(j)}(s')$ equals $\vec{0}$ in $\mathbb{F}^{\#_{rows}(M_A)}/colSpan(M_A)$. Now, as $v_A(s') = \sum_i v_A^{(i)}(s')$, it also equals $\vec{0}$, as required. ◁

From Claim 12, it follows that taking any V' with columns in $span(\{v(s')|s' \in \mathbb{F}^k\}$, $(V'|M)$ immediately satisfies privacy. We will indeed pick our basis B out of $span(\{v(s')|s' \in \mathbb{F}^k\}$, so we will only need to worry that the resulting scheme satisfies correctness. The construction is as follows.

1. Initialization: Initialize $B = \phi$ (recall $span(B)$ is $\{\vec{0}\}$).
2. Iteration $i > 0$: Find some $s' \in S$, so that for all minterms $A \subseteq [n]$, $v(s')$ belongs to a coset of $\mathbb{F}^{\#_{rows}(M_A)}/colSpan(M_A)$ that differs from coset(v) for all $v \in span(B)$. Halt if no such s exists. If it does, add one such V^s to B.

We prove by induction that at the end of every iteration $i \leq max(1, k - n)$, we B is a size-i independent set in $\mathbb{F}^{\#_{rows}(M)}$ such that $(B|M)(s, r)$ is correct for $\mathcal{A}$ with secret domain $S = \mathbb{F}^i$ (and private, which we observed before).

First, observe that the above procedure will yield at least a single vector. For every $s' \neq \vec{0}$, and every minterm A, $v_A(s')$ is non zero in $\mathbb{F}^{\#_{rows}(M_A)}/colSpan(M_A)$ by correctness of $\mathcal{M}$. Now, any product $\alpha\vec{s'}$ for $\alpha \in \mathbb{F}$ will yield a different coset in $\mathbb{F}^{\#_{rows}(M_A)}/colSpan(M_A)$, as v_A is non-zero. Thus, we can add $v_s(s')$ to our set. By the inductive hypothesis, at the end of iteration i, we have $|\mathbb{F}|^i$ vectors already in $span(B)$ - for clarity, denote B at the end of iteration i by $B^{(i)}$. We observe that for every minterm A all projections $v_A(s')$ are distinct for different values s' - which follows from correctness of $\mathcal{M}$. Therefor, going over all A's, at most

$$(\text{number of minterms})|\mathbb{F}|^i \leq 2^n|\mathbb{F}|^i \leq |\mathbb{F}|^{i+n}$$

vectors are excluded as candidates for the next $v_s(s')$ to join B. Finally, by the condition imposed on the new vector to join B, it follows that $B^{(i+1)}$ is a size-$i+1$ independent set, as satisfies that $(B|M)$ is correct for secret domain $S = \mathbb{F}^{i+1}$ (the formal argument is similar to the base case, observing that $v_A(s')$ is non-zero as a coset of $(M_A|B_A^{(i)})$). As there are $|\mathbb{F}|^k$ vectors in $\mathcal{M}$'s domain to begin with, we conclude (from the proof of the inductive step above) that at least $k - n$ iterations can be made before running out of vectors to add, which concludes the proof. ◀

3.2 $PSSS_{s^*+s^*r^2}$ is very weak

In this section we will show that if the shares are from the class $PSSS_{s^*+s^*r^2}$ (no r-degree 1 part) captures only the access structures consisting of a set of singletons as its minterms.[10]

▶ **Theorem 13.** *Let $\mathbb{F}$ be a finite field of odd characteristic. Then the class $PSSS_{s*+s*r^2,\mathbb{F}}$ can only implement a simple set of access structures where its minterms are all singletons.*

Indeed, observe that we can not expect a similar result for all fields, as for $\mathbb{F}_2$, for instance, we have $r_i^2 = r_i$, so one can represent any multi linear scheme over $\mathbb{F}_2$ as a $PSSS_{s*+s*r^2,\mathbb{F}}$ scheme, by replacing every variable r_i by r_i^2, which are equal over $\mathbb{F}_2$. However, linear schemes over $\mathbb{F}_2$ do capture all monotone access structures (e.g, via the formula-based construction of [8]). See 2 for required background and notation on quadratic forms.

Furthermore, we have

▶ **Observation 3.** *Let $f_1(x_1,\ldots,x_n), f_2(x_1,\ldots,x_n)$ be two quadratic forms over a field $\mathbb{F}_q$ of odd characteristic of (possibly same) types $(n_1,m_1,d_1),(n_2,m_2,d_2)$ respectively. Then for all $b \in \mathbb{F} - \{0\}$, $Pr_{x\leftarrow\mathbb{F}^n}(f_1(x)=0) \neq Pr_{x\leftarrow\mathbb{F}^n}(f_2(x)=b)$.*

The observation follows by simple case analysis. In some more detail, by Theorem 6, $N(f_1(x=0))$ is either a single q^x or of the form $q^{x_1} \pm q^{x_2} \pm q^{x_3}$ for $x_1 > x_2 > x_3$, while for $b \neq 0$, $N(f_2(x=b))$ is of the form $q^{x_1} \pm q^{x_2}$ for $x_1 > x_2$. So, the probabilities (after dividing both numbers by q^n) must differ. This is regardless of the values of m_1, m_2.

Now, consider a party P_h that receives a share of the form

$$f(\vec{s},\vec{r}) = p(\vec{s}) + \sum_{\substack{i,j\in\{1,..,n\}\\ i\leq j}} p_{i,j}(\vec{s})r_ir_j = p(\vec{s}) + q_{\vec{s}}(\vec{r}).$$

where each $q_{\vec{s}}(\vec{r})$ is a polynomial in $\vec{r}$ with coefficients in the ring $\mathbb{F}_q[s_1,\ldots,s_n]$, and $p(\vec{s})$ is non constant over $\mathbb{F}_q^n$. First consider the case when $p(\vec{s})$ is non-constant over $\mathbb{F}_q^n$. We prove that there exists a pair of secrets $\vec{s_1},\vec{s_2}$ that P_h can distinguish by itself. To see this, fix two vectors $\vec{s_1},\vec{s_2}$ such that $p(\vec{s_1}) \neq p(\vec{s_2})$. By observation 3, it directly follows that the unique probability (over the choice of $\vec{r}$) of $f(\vec{s_1},\vec{r})$ hitting $p(\vec{s_1})$ equals the probability of $q_{\vec{s_1}}(r)$ hitting 0, while the probability of hitting values $b \neq p(\vec{s_1})$, equals the probability of $q_{\vec{s_1}}(r)$ hitting corresponding non-zero values (indeed, adding a constant permutes the distribution). A similar situation occurs with $f(\vec{s_2},\vec{r})$ and the "spacial" point $p(\vec{s_2})$. Thus, the points with the "special 0-probability for the $q_{\vec{s_i}}$-part" for $\vec{s_1}$ and $\vec{s_2}$ differ for $f(\vec{s_1},\vec{r})$ and $f(\vec{s_2},\vec{r})$. We conclude that the two distributions $f(\vec{s_1},r), f(\vec{s_2},r)$ are distinct. To see this, note that the contribution of $b = p(\vec{s_1})$ to the statistical distance between $f(\vec{s_1},r)$ and $f(\vec{s_2},r)$ is $1/2|Pr[q_{\vec{s_1}}(\vec{r})=0] - Pr[q_{\vec{s_2}}(\vec{r}) = p(\vec{s_1}) - p(\vec{s_2})]|$, which is non-zero by Observation 3.

Finally, let us look at all the remaining parties with only shares where $p(\vec{s})$ is constant (zero, wlog. since the free coefficient is 0). Such parties receive only shares of the form $f(\vec{s},\vec{r}) = q_{\vec{s}}(\vec{r})$, where every $q_{\vec{s}}$ is a quadratic form. Therefore, for any $\vec{s} \in S$ we have $f_p(\vec{s},\vec{0}) = 0$. Thus, all these parties together can not reconstruct the secret with probability 1, implying that the singletons above are the only minterms of the access structure. ◀

[10] Note that our results only rule out perfect schemes.

References

1 Benny Applebaum and Barak Arkis. Conditional disclosure of secrets and d-uniform secret sharing with constant information rate. *IACR Cryptology ePrint Archive*, 2018:1, 2018. URL: http://eprint.iacr.org/2018/001.

2 Benny Applebaum, Amos Beimel, Oded Nir, and Naty Peter. Better secret-sharing via robust conditional disclosure of secrets. *Electronic Colloquium on Computational Complexity (ECCC)*, 27:8, 2020. URL: https://eccc.weizmann.ac.il/report/2020/008.

3 Benny Applebaum and Prashant Nalini Vasudevan. Placing conditional disclosure of secrets in the communication complexity universe. In Avrim Blum, editor, *10th Innovations in Theoretical Computer Science Conference, ITCS 2019, January 10-12, 2019, San Diego, California, USA*, volume 124 of *LIPIcs*, pages 4:1–4:14. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2019. doi:10.4230/LIPIcs.ITCS.2019.4.

4 Amos Beimel. Secret-sharing schemes: A survey. In Yeow Meng Chee, Zhenbo Guo, San Ling, Fengjing Shao, Yuansheng Tang, Huaxiong Wang, and Chaoping Xing, editors, *Coding and Cryptology*, pages 11–46, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

5 Amos Beimel and Yuval Ishai. On the power of nonlinear secret-sharing. *IACR Cryptology ePrint Archive*, 2001:30, 2001. URL: http://eprint.iacr.org/2001/030.

6 Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In Janos Simon, editor, *Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA*, pages 1–10. ACM, 1988. doi:10.1145/62212.62213.

7 Josh Cohen Benaloh and Jerry Leichter. Generalized secret sharing and monotone functions. In Shafi Goldwasser, editor, *Advances in Cryptology - CRYPTO '88, 8th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1988, Proceedings*, volume 403 of *Lecture Notes in Computer Science*, pages 27–35. Springer, 1988. doi:10.1007/0-387-34799-2_3.

8 Josh Cohen Benaloh and Jerry Leichter. Generalized secret sharing and monotone functions. In Shafi Goldwasser, editor, *Advances in Cryptology - CRYPTO '88, 8th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1988, Proceedings*, volume 403 of *Lecture Notes in Computer Science*, pages 27–35. Springer, 1988. doi:10.1007/0-387-34799-2_3.

9 G. R. Blakley. One time pads are key safeguarding schemes, not cryptosystems fast key safeguarding schemes (threshold schemes) exist. In *Proceedings of the 1980 IEEE Symposium on Security and Privacy, Oakland, California, USA, April 14-16, 1980*, pages 108–113. IEEE Computer Society, 1980. doi:10.1109/SP.1980.10016.

10 László Csirmaz. The size of a share must be large. In Alfredo De Santis, editor, *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings*, volume 950 of *Lecture Notes in Computer Science*, pages 13–22. Springer, 1994. doi:10.1007/BFb0053420.

11 Bella Dubrov and Yuval Ishai. On the randomness complexity of efficient sampling. In Jon M. Kleinberg, editor, *Proceedings of the 38th Annual ACM Symposium on Theory of Computing, Seattle, WA, USA, May 21-23, 2006*, pages 711–720. ACM, 2006. doi:10.1145/1132516.1132615.

12 Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or A completeness theorem for protocols with honest majority. In Alfred V. Aho, editor, *Proceedings of the 19th Annual ACM Symposium on Theory of Computing, 1987, New York, New York, USA*, pages 218–229. ACM, 1987. doi:10.1145/28395.28420.

13 R. K. Gupta. *Linear Programming*. Krishna Prakashan, 2009. URL: https://books.google.co.il/books?id=Ur2vi5kB5IoC.

14 Yuval Ishai, Eyal Kushilevitz, and Anat Paskin-Cherniavsky. From randomizing polynomials to parallel algorithms. In Shafi Goldwasser, editor, *Innovations in Theoretical Computer*

Science 2012, Cambridge, MA, USA, January 8-10, 2012, pages 76–89. ACM, 2012. doi:10.1145/2090236.2090244.

15 Mitsuru Ito, Akira Saito, and Takao Nishizeki. Secret sharing scheme realizing general access structure. *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, 72:56–64, 1989.

16 Rudolf Lidl and Harald Neiderreiter. *Introduction to finite fields and their applications*. Cambridge University Press, 1997.

17 Tianren Liu, Vinod Vaikuntanathan, and Hoeteck Wee. Conditional disclosure of secrets via non-linear reconstruction. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part I*, volume 10401 of *Lecture Notes in Computer Science*, pages 758–790. Springer, 2017. doi:10.1007/978-3-319-63688-7_25.

18 Tianren Liu, Vinod Vaikuntanathan, and Hoeteck Wee. Towards breaking the exponential barrier for general secret sharing. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part I*, volume 10820 of *Lecture Notes in Computer Science*, pages 567–596. Springer, 2018. doi:10.1007/978-3-319-78381-9_21.

19 Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979. doi:10.1145/359168.359176.

A Bounding the Number of Random Variables in (general) PSSS

In this section we will present a bound on the number of random variables in (perfectly correct and private) PSSS and general secret sharing schemes.

▶ **Theorem 14.** *Let $\mathcal{M}$ denote a secret sharing scheme implementing an access structure $\mathcal{A}$ (with perfect privacy and correctness). Then there exists an equivalent secret sharing scheme with $RC(\mathcal{M}) = 2^{\tilde{O}(SC(\mathcal{M}))}$. Furthermore, if $\mathcal{M} = (\mathbb{F}_{q^d}, t, k, Sh)$ is a PSSS, then there exists an equivalent PSSS scheme $\mathcal{M}' = (\mathbb{F}_{q^d}, t', k, Sh')$ with $SC(\mathcal{M}') = SC(\mathcal{M})$ and $RC(\mathcal{M}') = 2^{poly(SC(\mathcal{M}))}$.*

Notation and some facts on Linear programs

For a PSSS scheme $\mathcal{M} = (\mathbb{F}_{q^d}, t, k, Sh)$, let us denote by sc the number of polynomial evaluations (field elements) output by Sh. Thus, $sc \geq k$ (since the set of sharings must be at least as large as S). We will need some theory of linear programs (LP). Here we will only care about the feasible region of a linear program (LP), and will not have a target function to optimize. Without loss of generality we consider LP's comprised of systems of inequalities of the form $Ax = b, x \geq 0$, where A, b are over $\mathbb{R}$, all b's components are non-negative. We denote such LP's by (A, b). We may also assume without loss of generality that $A \in \mathbb{R}^{m \times n}$, where $m \leq n$, and A has full rank (m). We say that a solution to the system is a basic feasible solution (BFS) if x only has non zero coordinates corresponding to an invertible submatrix of A (taking a subset of columns). For a finite set $B \subseteq \mathbb{R}^m$ of vectors, a convex combination of B is a linear combination $\sum_{b \in B} \alpha_b b$, so that $\sum_{b \in B} \alpha_b = 1$, and $\forall b \in B, \alpha_b \geq 0$. The convex hall of a set $A \subseteq \mathbb{R}^m$ is the set of all linear combinations of finite subsets $B \subseteq A$. We denote it as $CH(A)$. We say a set $A \subseteq \mathbb{R}^m$ is convex if $CH(A) = A$. An extreme point of a convex set A is a point $y \in A$ such that if y is a convex combination of $\{x, z\} \subseteq A$, then either $x = y$ or $z = y$. It is well known that the set of solutions of an LP is convex. We say an LP has a *bounded* solution set X, if there exists an integer N, such that $\ell_\infty(x) \leq N$ for all $x \in X$.

For a set $A = \{a_1, \ldots, a_t\} \subseteq \mathcal{R}^m$, the affine dimension of A, aff(A), is the dimension of $\{a_2 - a_1, \ldots, a_t - a_1\}$. We say that a set A has *full affine dimension* if aff$(A) = |A| - 1$.

▶ **Theorem 15** ([13], chapter 2)**.** *The set of extreme points $\mathcal{B}$ of a bounded non-empty solution set X of an LP $(A, b) \in \mathbb{R}^{m\times n} \times \mathbb{R}^{m\times 1}$ is non empty, and $X = CH(\mathcal{B})$. Furthermore, the set $\mathcal{B}$ is precisely the set of BFS's of (A, b). Furthermore, Any solution p of (A, b) is a convex combination of a subset $\{p_1, \ldots, p_\ell\} \subseteq \mathcal{B}$ of full affine dimension, where $\ell \leq m + 1$.*

▶ **Lemma 16** (Cramer's rule)**.** *Let $A \in \mathcal{R}^{m\times m}$ denote an invertible matrix. Then, $A^{-1}_{i,j} = |A_{i,j}|/|A|$. Here $A_{i,j}$ is the (i, j)'th cofactor of A, obtained from removing the i'th column and j'th row from A.*

▶ **Lemma 17.** *Let $A \in \mathbb{R}^{m\times m}$ denote a matrix whose entries $a_{i,j}$ all satisfy $|a_{i,j}| \in \{0\} \cup [\delta, 1]$ for $0 < \delta$. Then every entry $a'_{i,j}$ in A^{-1} satisfies*

$$|a'_{i,j}| \text{ or } |a'_{i,j}| \geq \delta^m/m^m.$$

Additionally, if the $a_{i,j}$'s are integers, then the $|a'_{i,j}|$'s are multiples of a constant $0 < L \leq m^m$.

The proof of the above lemma follows directly from Lemma 16. In the following we only prove the bound for general schemes. The full proof for PSSS appears in the full version.

Proof of Theorem 14. Let us consider the given polynomial scheme $\mathcal{M}$ as in the theorem statement. We denote $Q = q^d$, $SC = Q^{SC(\mathcal{M})}$, and $sc = \log_Q(SC)$.

We denote the share vector output by Sh for any $\vec{s} \in S$ by $\vec{sh} = (sh_1, ..., sh_n) \in \mathbb{F}_Q^{sc})$. For every secret $\vec{s_i} \in S$, and for every possible $\vec{sh_j} \in \mathbb{F}_Q^{sc}$ let us denote by $p_{i,j}$ the probability to receive $\vec{sh_j}$ as the share vector on input $\vec{s_i}$. (For each $\vec{s_i}$, there are Q^{sc} such probabilities.)

Now we will build a matrix that will hold all the constraints on the probabilities $p_{i,j}$ for a scheme $\mathcal{M}'$ with $S, S_1 \times \ldots \times S_n$ for $\mathcal{A}$. Let $p_{\mathcal{M}}$ denote the probabilities vector induced by $\mathcal{M}$. Our set of requirements will be stronger than stating that $\mathcal{M}'$ is a secret sharing scheme for $\mathcal{A}$, as it will additionally require that $\mathcal{M}'$ is "similar" to $\mathcal{M}$ in a certain way. A solution will be guaranteed to exist, as $p_{\mathcal{M}}$ is such a solution ($\mathcal{M}$ is "similar" to itself).

The constraints are divided into 3 sets:

privacy: For any max unqualified set A, for every two secrets $\mathrm{s}_i, \mathrm{s}_j \in S$ the probability of getting the same shares (for this specific set) should be equal. That is to say, for any two secrets $\mathrm{s}_i, \mathrm{s}_j \in S$ and projection of shares on A, $\vec{sh}'$ (some specific share that parties in A receive).

$$\sum_{\substack{\text{all } k \text{ for which the projection} \\ \text{of } \vec{sh}_k \text{ on } A \text{ is } \vec{sh}'}} p_{i,k} = \sum_{\substack{\text{all } k \text{ for which the projection} \\ \text{of } \vec{sh}_k \text{ on } A \text{ is } \vec{sh}'}} p_{j,k}$$

Reorganizing, we get.

$$\sum_{\substack{\text{all } k \text{ for which the projection} \\ \text{of } \vec{sh}_k \text{ on } A \text{ is } \vec{sh}'}} p_{i,k} - \sum_{\substack{\text{all } k \text{ for which the projection} \\ \text{of } \vec{sh}_k \text{ on } A \text{ is } \vec{sh}'}} p_{j,k} = 0 \tag{12}$$

correctness: For any minimal qualified set A, for every two secrets $\mathrm{s}_i, \mathrm{s}_j \in S$ there are no share $\vec{sh}_k$ for which both $p_{i,k}$ and $p_{j,k}$ are not zero. That is to say, for every two secret $\mathrm{s}_i \in S$ and projection of shares on A $\vec{sh}'$ (some specific share that parties in A receive), for each s_j

so that $Pr(Sh(\mathrm{s}_j, r)_A = \vec{sh}') = 0$

$$\sum_{\substack{\text{all } k \text{ for which the projection} \\ \text{of } \vec{sh}_k \text{ on } A \text{ is } \vec{sh}' \\ \text{and } j \neq i}} p_{j,k} = 0 \tag{13}$$

By correctness, for each $\vec{sh}'$, there are at least $|S| - 1$ such j's.

probability restrictions: For any secret $\vec{\mathrm{s}_i} \in S$

$$\sum_j p_{i,j} = 1 \tag{14}$$

That is to say, that for every secret the sum of all the probabilities to get any share is 1.Another constraint is for every i and j.

$$0 \leq p_{i,j} \tag{15}$$

We stress that the privacy and probability constraints follow from the requirements on any secret sharing scheme implementing $\mathcal{A}$. The correctness constraints are constructed based on the concrete scheme $\mathcal{M}$.

The matrix M_1 defining our LP will be built from these three sets of equations 12, 13, 14, where the variables are the the $p_{i,j}$-s. In addition we will remove all the rows that depend on other rows, so our matrix M_1 will have a full rank. Let us denote:

$$r = 2^n |\mathbb{F}_Q^k| SC \leq SC^3 \tag{16}$$

Here the inequality holds since $n, k \leq sc$. There are at most r columns in M_1 thus and at most r rows.[11]

This LP is solvable since $p_{\mathcal{M}}$ is a solution for it. The right hand side b is the vector obtained from Equations 12, 13, 14 $(0, 0, \ldots, 0, 1, \ldots, 1)$ (with $|S|$ 1's at the end).

▶ **Observation 4.** *In the LP (M_1, b) above, all the entries in M_1 and in b are 1, -1 or 0.*

Now, any solution $\vec{p}'$ to the LP specified by (M_1, b) defines a secret sharing scheme for the desired access structure. Namely, assuming all entries in a solution $\vec{p}$ are multiples of some $1/L$ for some integer, we can set R to be of size L, and an arbitrary mapping Sh from $(\vec{s}, \vec{r})$'s to share vectors in $\mathbb{F}_Q^{sc}$ that agree with the probabilities in $\vec{p}$.

The problem is that if the elements in $\vec{p}'$ will be not multiples of $Q^{-t'}$ for some t' it will be impossible to present this secret sharing scheme with polynomials over $\mathbb{F}_Q$. We know one solution $p_{\mathcal{M}}$ that has probabilities which are multiples of Q^{-t} for some, possibly very large, t (the one induced by $\mathcal{M}$). Now we want to show that there exists $t' = 2^{2^{poly(SC)}}$, for which there is solution p' to (M_1, b) where all probability $p_{i,j}$ are multiples of $Q^{-t'}$, which will prove the theorem. By theorem 15, there is a set of BFS's $G = \{p_1, ..., p_\ell\}$ for the system, so that there exists a solution (the one induced by $\mathcal{M}$) $p_{\mathcal{M}} \in CH(G)$.[12]. Next, we prove that the entries of all $p_i \in G$ are of "low" resolution.

▷ Claim 18. For every $g \in G$, there exists an integer $0 < L \leq r^{2r}$, every entry g_i of g is a multiple of $1/L$.

[11] The second inequality follows from correctness of the scheme.

[12] Note that (M_1, b)'s solution set is indeed bounded, as all coordinates of a solution p are in the range $[0, 1]$.

Proof. This follows from the fact that the BFS in G is of the form $M_{1,H}^{-1}b$, where $M_{1,H}$ is a subset of M_1's columns corresponding to an invertible (square) matrix so that the entries in b corresponding to the other columns are all 0's. As M_1, b have entries in $\{0, 1, -1\}$ by Observation 4, the claim follows from Lemma 17. ◁

For any G, if the resulting scheme $\mathcal{M}'$ is not required to be a PSSS, then we are also done, as we can take (e.g.) $p_1 \in G$ as a basis for the scheme, and set R of size $L \leq 2^{2r}$ as guaranteed by Lemma 18. The randomness complexity of the resulting scheme is $\log_2(L) = 2^{\tilde{O}(SC(\mathcal{M}))}$. Additionally, for the case of $\mathcal{M}$ is a PSSS, $\mathcal{M}'$ is as in the theorem if $|G| = 1$, then p_1 must be a single solution, and its entries are already multiples of q^d, and we are done, as $M \leq r^{2r} \leq 2^{2^{\tilde{O}(SC(\mathcal{M}))}}$. Therefor, the solution vector p_1 induces a PSSS where $t = \log_Q(M) = 2^{\tilde{O}(SC(\mathcal{M}))}$. This is also the case if some BFS $p_i \in G$ happens to have entries which are all multiples of $Q^{-t'}$ for some t'. Otherwise, we prove that $CH(G)$ contains some solution where all entries are multiples of $Q^{-t'}$ where $t' = 2^{poly(SC)}$. See the full version for a proof, which is somewhat technically involved, but uses only some basic number theory. ◀