An Intuitionistic Analysis of Size-change Termination

Silvia Steila

Dipartimento di Informatica, Università degli studi di Torino
Corso Svizzera 185 Torino, Italy
steila@di.unito.it

Abstract

In 2001 Lee, Jones and Ben-Amram introduced the notion of size-change termination (SCT) for first order functional programs, a sufficient condition for termination. They proved that a program is size-change terminating if and only if it has a certain property which can be statically verified from the recursive definition of the program. Their proof of the size-change termination theorem used Ramsey's Theorem for pairs, which is a purely classical result. In 2012 Vytiniotis, Coquand and Wahlsteldt intuitionistically proved a classical variant of the size-change termination theorem by using the Almost-Full Theorem instead of Ramsey's Theorem for pairs. In this paper we provide an intuitionistic proof of another classical variant of the SCT theorem: our goal is to provide a statement and a proof very similar to the original ones. This can be done by using the H-closure Theorem, which differs from Ramsey's Theorem for pairs only by a contrapositive step. As a side result we obtain another proof of the characterization of the functions computed by a tail-recursive SCT program, by relating the SCT Theorem with the Termination Theorem by Podelski and Rybalchenko. Finally, by investigating the relationship between them, we provide a property in the "language" of size-change termination which is equivalent to Podelski and Rybalchenko's termination.

1998 ACM Subject Classification F.4.1 Mathematical Logic, F.3.1 Specifying and Verifying and Reasoning about Programs

Keywords and phrases Intuitionism, Ramsey's Theorem, Termination

Digital Object Identifier 10.4230/LIPIcs.TYPES.2014.288

1 Introduction

An important topic in theoretical computer science is determining whether a program is terminating on a given input by studying its source code. Even if in general this problem, known as Halting problem, is undecidable, in some special cases this can be done. In 2001 Lee, Jones and Ben-Amram introduced the notion of size-change termination. A first order functional program $\mathcal{P}$ is SCT if for any infinite sequence of calls which follows the control of $\mathcal{P}$ there exists a variable whose value has to decrease infinitely many times. If the domain of the values of $\mathcal{P}$ is well-founded this condition guarantees the termination. In [14] the authors prove that any first order functional program is SCT if and only if it satisfies some combinatorial property which can be statically verified from the recursive definition of the program. We will call this result the SCT Theorem. In order to prove this theorem the authors use Ramsey's Theorem for pairs [19]. This result states that given any coloring over the edges of the complete graph with infinitely many nodes in finitely many colors, there exists an infinite "homogeneous" set. A set of nodes of a colored graph is said "homogeneous" when any two elements of the set are connected with the same color. It is well-known that Ramsey's Theorem for pairs is not an intuitionistically valid result. To be precise, we need

20th International Conference on Types for Proofs and Programs (TYPES 2014).
Editors: Hugo Herbelin, Pierre Letouzey, and Matthieu Sozeau; pp. 288–307
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

the law of excluded middle for Σ^0_3 formulas in order to prove the fragment of this theorem which can be expressed as a schema of first order statements [5].

The SCT Theorem is not the only result which characterizes the termination of some class of programs by using Ramsey's Theorem for pairs. In 2004 Podelski and Rybalchenko introduced the notion of transition invariant. T is a transition invariant for a transition-based program $\mathcal{R}$ if T contains the transitive closure of the transition relation of $\mathcal{R}$. In [18] the authors proved their Termination Theorem: a while-if program is terminating if and only if there exists a transition invariant which satisfies certain properties. We refer to Section 2 for details. The proof of the Termination Theorem uses Ramsey's Theorem for pairs, as it is the case for the SCT Theorem.

The Termination Theorem is intuitionistically provable if we consider inductive well-foundedness instead of well-foundedness (see Section 2). Intuitionistic proofs of this theorem are given in [20] and [6]. In both the proofs Ramsey's Theorem for pairs is replaced by some intuitionistic result. In the first one it is replaced by the Almost-full Theorem [9] by Coquand, while in the second one it is replaced by the H-closure Theorem [6]. Both of them are classically (but not intuitionistically) equivalent to Ramsey's Theorem for pairs. They keep the combinatorial strength of Ramsey's Theorem for pairs required in the proof of the Termination Theorem but they drop the classical part.

In this paper we prove some intuitionistic version of the SCT Theorem. From the intuitionistic proof we extract an upper bound for the number of steps needed by an SCT program to terminate. In Section 3 we define a variant of SCT, which we call SCT* and which is classically equivalent but intuitionistically more informative. SCT* is defined by taking a contrapositive and, as in the case of the Termination Theorem, by using the inductive version of well-foundedness. Thanks to it, in Section 4, we may prove the SCT Theorem without using classical principles. We will use the H-closure Theorem instead of Ramsey's Theorem for pairs. This is not the first intuitionistic proof of the SCT Theorem since Vytiniotis, Coquand and Wahlsteldt in [20] intuitionistically proved this result by using the Almost-Full Theorem. However since we find no way to intuitionistically deduce the H-closure Theorem from the Almost-Full Theorem, there are no apparent relationships between the proofs.

In [3] Ben-Amram proved that any tail-recursive SCT functional program is primitive recursive. In Section 5 we give a completely different proof of this result based on the bounds found for the Termination Theorem in [4] and [11]. We can use these bounds since the SCT Theorem and the Termination Theorem are strictly related. Heizmann, Jones and Podelski proved that size-change termination is a property strictly stronger than termination [13]. By applying an argument similar to the one used in [13] we will get the bound for a tail-recursive SCT program from the one for the Termination Theorem provided in [11]. As a corollary of the results presented in [13], in Section 6, we find a property in the "language" of size-change termination which is equivalent to the termination with transition invariants.

In this paper we will work in Heyting Arithmetic (HA); all the proofs are intuitionistic.

2 Transition Invariants and the H-closure Theorem

In this section we summarize the main definitions and properties of transition invariants. Transition invariants are used by Podelski and Rybalchenko in [18] in order to characterize terminating programs. The Termination Theorem by Podelski and Rybalchenko states that a transition-based program $\mathcal{R}$ is terminating if and only if there exists a disjunctively well-founded transition invariant for $\mathcal{R}$. The proof of this result was classical since the authors use Ramsey's Theorem for pairs in order to prove it. However we can modify the definition of termination with a classically equivalent one and show that the theorem is intuitionistically true ([20] and [6]).

2.1 Transition Invariants

In this subsection we recall the definition of transition invariant and the Termination Theorem. For all details we refer to [18].

▶ **Definition 1** (Transition Invariants). As in [18]:

- A transition-based program $\mathcal{R} = (S, I, R)$ consists of:
  - S: a set of states,
  - I: a set of initial states, such that $I \subseteq S$,
  - R: a transition relation, such that $R \subseteq S \times S$.
- A computation is a maximal sequence of states $s_0, s_1, \ldots$ such that
  - $s_0 \in I$,
  - $(s_{i+1}, s_i) \in R$ for all $i \in \mathbb{N}$.
- The set Acc of accessible states consists of all states that appear in some computation.
- The transition-based program $\mathcal{R}$ is terminating if and only if $R \cap (\mathrm{Acc} \times \mathrm{Acc})$ is well-founded.
- A transition invariant T is a set which contains the transitive closure of the transition relation R restricted to the accessible states Acc. Formally,

  $$R^+ \cap (\mathrm{Acc} \times \mathrm{Acc}) \subseteq T.$$

- A relation T is disjunctively well-founded if it is a finite union $T = T_0 \cup \cdots \cup T_{n-1}$ of well-founded relations.

Being well-founded is not preserved under binary unions, therefore a disjunctively well-founded relation can be ill-founded. We represent each state as a finite map s which provides the values of the variables and the location of s (for an introduction to these concepts see [13, pag 8]). Given a state s and a variable x we will write $s(x)$ to mean the value of x in the state s, while $s(\mathrm{pc})$ is the current location of s.

The main result by Podelski and Rybalchenko is the following.

▶ **Theorem 2** (Termination Theorem, Theorem 1 [18]). *The transition-based program $\mathcal{R}$ is terminating if and only if there exists a disjunctively well-founded transition invariant for $\mathcal{R}$.*

By unfolding definitions Theorem 2 states that a binary relation R is well-founded if and only if there exist a natural number n and n-many well-founded relations $R_0, \ldots, R_{n-1}$ whose union contains the transitive closure of R. This is non trivial since in general a disjunctively well-founded relation can be ill-founded. The fact that a transitive binary relation which is the union of two well-founded relations is well-founded has been remarked before Podelski and Rybalchenko (for instance see [12, pag 31]).

Let us see as example one simple application of the Termination Theorem.

▶ **Example 3.** Examine the following transition-based program which computes $\exp = x^y$ whenever $x, y > 0$ and $\exp = 1$ at the beginning.

```
while($y > 0$)
    {
     $l$ : temp $= 0$; $z = x$;
     while($z > 0$)
          {temp $=$ temp $+$ exp; $z = z - 1$; }
     $l'$ : $y = y - 1$; exp $=$ temp;
    }
```

This program terminates since there exists a disjunctively well-founded transition invariant for it:

$$T := \{(s', s) \mid s'(z) < s(z)\} \cup \{(s', s) \mid s'(y) < s(y)\} \cup \{(s', s) \mid s'(\mathrm{pc}) = l \ \wedge \ s(\mathrm{pc}) = l'\}\,.$$

Observe that, in this case, it would not be difficult to directly prove termination by using the lexicographic ordering.

From the Termination Theorem Cook, Podelski and Rybalchenko extracted an algorithm which produces disjunctively well-founded transition invariants for some terminating programs [8], as in the example above.

2.2 Overview on inductive well-foundedness

In this subsection we recall the main results about well-foundedness which we require in this paper. All the results presented in this subsection are presented in previous work [6], we refer to it for details. From now on we consider the inductive definition of well-foundedness as in [1, 2], which is classically equivalent to the usual one if we assume the Axiom of Dependent Choice.

Classically a binary relation R over a set S is well-founded if there are no infinite decreasing R-chains. We say that $x \in S$ is classically R-well-founded if there are no infinite decreasing R-chains from x. Here we are interested in the inductive definition of well-foundedness, which is classically, but not intuitionistically, equivalent to the classical one. Hence we say that a binary relation R over S is inductively well-founded if and only if every element of S belongs to any R-inductive property X:

$$\forall x \forall X((\forall y((\forall z(zRy \implies z \in X)) \implies y \in X)) \implies x \in X).$$

We say that $x \in S$ is inductively R-well-founded if $x \in X$ holds for any R-inductive property X. For short, when clear from the context, we will say well-founded instead of inductive well-founded.

An important tool for proving that a relation is well-founded are simulations [16]. A simulation relation is a binary relation which connects two other binary relations. Intuitively a simulation of a binary relation $R \subseteq S^2$ into a binary relation $R' \subseteq S'^2$ is a way of associating, step by step, any R-decreasing sequence to some R'-decreasing sequence.

▶ **Definition 4.** Let R be a binary relation on S and R' be a binary relation on S'. Let U be a binary relation on $S \times S'$, and let $\circ$ denote the composition between two relations.

- U is a simulation of R in R' if and only if $R \circ U \subseteq U \circ R'$; i.e.

$$\forall x, z \in S \ \forall y \in S' \left((xUy \wedge zRx) \implies \exists w \in S' \left(wR'y \wedge zUw\right)\right)$$

- A simulation relation U of R in R' is total if $\mathrm{dom}(U) = \{x \in S \mid \exists y \in S'(xUy)\} = S$.
- R is simulable in R' if there exists a total simulation relation U of R in R'.

The next proposition shows that the simulation relations “preserve” inductively well-foundedness: it is a generalization of the preservation of well-foundedness by inverse image [17].

▶ **Proposition 5.** *Let R be any binary relation on S, and let R' be a binary relation on S'.*

1. *For any $x \in S$:*

$$x \textit{ is } R\textit{-well-founded } \iff \forall y (yRx \implies y \textit{ is } R\textit{-well-founded }).$$

2. *If U is a simulation of R in R' and if xUy and y is R'-well-founded, then x is R-well-founded.*
3. *If U is a simulation of R in R' and R' is well-founded, then* $\mathrm{dom}(U)$ *is R-well-founded.*
4. *If R is simulable in R' and R' is well-founded, then R is well-founded.*

Let R be a binary relation over a set S. We say that a function $f : S \to \mathbb{N}$ is a weight function if for any $x,\ y \in S$

$$xRy \implies f(x) < f(y).$$

R has height ω if and only if R has a weight function.

By using the total simulation $U = \{(x, f(x)) \mid x \in \mathrm{dom}(R)\}$ we can easily prove that if R has height ω then it is inductively well-founded. Moreover if R is inductively well-founded and finitely branching, then $f(x) = \sup \{f(y) + 1 \mid yRx\}$ is a weight function for R.

We also need to recall a well-known result about finite relations. Let R be a binary relation on any finite set $\{x_i \mid i \leq k\}$. A R-cycle is a finite sequence $\langle x_{i_0}, \ldots, x_{i_n} \rangle$ for some $n \in \mathbb{N}$, such that and $i_j \leq k$ for any $j \leq n$, and

$$x_{i_0} = x_{i_n} R x_{i_{n-1}} R \ldots R x_{i_1} R x_{i_0}.$$

If $n = 0$ we ask that $x_{i_0} R x_{i_0}$ and we call x_{i_0} a loop of R.

▶ **Proposition 6.** *Let R be any binary relation on a finite set S.*

- *R is well-founded if and only if there are no R-cycles.*
- *If R is a strict order then R is well-founded.*

2.3 H-closure Theorem

The H-closure Theorem, where H stands for “homogeneous”, is the result used in [6] to give an intuitionistic proof of the Termination Theorem. The statement of the H-closure Theorem was obtained from Ramsey’s Theorem for pairs by taking a contrapositive and it is intuitionistically provable. The two theorems are equivalent in RCA_0 [7], the base system of Reverse Mathematics which consists of recursive comprehension and Σ^0_1-induction. We may define H-closure as follows.

Let $\succ$ denote the one-step expansion between finite sequences; i.e.

$$\langle y_0, \ldots, y_{m-1} \rangle \succ \langle x_0, \ldots, x_{n-1} \rangle \iff m = n + 1 \wedge \forall i < n(x_i = y_i).$$

We call an R-homogeneous sequence any finite transitive decreasing R-chain. We say that R is homogeneous-well-founded, just H-well-founded for short, if the relation $\succ$ on the set of R-homogeneous sequences is well-founded. Being H-well-founded is weaker than being well-founded, as we will see in a moment. Formally, the definition runs as follows.

▶ **Definition 7** (H-well-foundedness)**.** Let R be a binary relation on S.

- $H(R)$, the set of R-homogeneous sequences, is the set of the R-decreasing transitive finite sequences on S:

$$\langle x_0, \dots, x_{n-1}\rangle \in H(R) \iff \forall i, j < n\ (i < j \implies x_j R x_i).$$

- R is H-well-founded if $H(R)$ is $\succ$-well-founded.

From the previous definition follows that R is classically H-well-founded if and only if there are no infinite decreasing transitive R-chains. It also follows that if R is decidable then also $H(R)$ is. If S is finite, then we may describe the difference between well-foundedness and H-well-foundedness as follows: R is well-founded if and only if R has no cycles, while R is H-well-founded if and only if R has no loops (there is no $x \in S$ such that xRx). There is a strong connection between well-foundedness and H-well-foundedness, described in the following proposition.

▶ **Proposition 8** (Proposition 1 [6])**.** *Let R be a binary relation.*

1. *If R is well-founded then R is H-well-founded.*
2. *If R is H-well-founded and R is transitive then R is well-founded.*

A last example. Consider $R = \{(n + 1, n) \mid n \in \mathbb{N}\}$. It is straightforward to check that it is not well-founded and it is H-well-founded since

$$H(R) = \{\langle\rangle\} \cup \{\langle n\rangle \mid n \in \mathbb{N}\} \cup \{\langle n, n+1\rangle \mid n \in \mathbb{N}\}\,.$$

The H-closure theorem states that H-well-foundedness is closed under finite unions. Formally

▶ **Theorem 9** (H-closure Theorem, Theorem 2 [6])**.** *Let $R_0, \dots, R_{n-1}$ be binary relations. If $R_0, \dots, R_{n-1}$ are H-well-founded then $R_0 \cup \dots \cup R_{n-1}$ is H-well-founded.*

Classically, and if we take a contrapositive, the H-closure Theorem states: if there is some infinite $R_0 \cup \dots \cup R_{n-1}$-homogeneous sequence then for some $i < n$ there is some infinite R_i-homogeneous sequence. From this remark we may classically check that the H-closure Theorem is but a variant of Ramsey's Theorem for pairs [19]. However, the H-closure Theorem is intuitionistically provable, while Ramsey's Theorem for pairs is not [6].

In [6] from the H-closure Theorem we obtained an intuitionistic proof of the Termination Theorem. Furthermore, by analysing this intuitionistic proof, in [4] the authors got a characterization of the Termination Theorem via the primitive recursive functions.

▶ **Theorem 10.** *Assume that the transition relation of the program $\mathcal{R}$ is the graph of a primitive recursive function restricted to a primitive recursive subset. If $\mathcal{R}$ has a disjunctively well-founded transition invariant whose relations are primitive recursive and have height ω then it computes a primitive recursive function.*

For short we say that a transition invariant has height ω if the relations which compose it have height ω. In [11] there is another proof of this result based on the Dickson Lemma. With both approaches we can characterize the level of the primitive recursive hierarchy reached by the transition-based program $\mathcal{R}$. We denote with $\mathcal{F}_k$ the usual k-class of the Fast Growing Hierarchy [15]. Define

$$F_0(x) = x + 1$$
$$F_{k+1}(x) = F_k^{(x+1)}(x).$$

Then $\mathcal{F}_k$ is the closure under limited recursion and substitution of the set of functions composed of constant, projections, sum and F_h for any $h \leq k$.

As shown in [11] if $\mathcal{R}$ is a program such that

- its transition relation R is the graph of a function in $\mathcal{F}_2$;
- there exists a transition invariant for $\mathcal{R}$ which is the union of k relations, all having weight functions in $\mathcal{F}_1$.

Then the function computed by $\mathcal{R}$ is in $\mathcal{F}_{k+1}$.

3 From SCT to SCT*

In this section after a brief summary on the original definition of SCT presented in [13], we introduce a variant of SCT, which we call SCT*, and which is classically equivalent to SCT. Thanks to this definition we can intuitionistically prove the SCT Theorem. This is similar to what we did in the previous section: in order to intuitionistically prove the Termination Theorem we had to consider a classical equivalent of the termination property which is intuitionistically easier to prove. We obtain SCT* from SCT by taking the contrapositive and by considering the inductive well-foundedness instead of the classical one.

From now on we will deal with a language for functions on $\mathbb{N}$ with call-by-value semantics considered in [14]. We use the recursive definitions and notations for maps $f : \mathbb{N}^n \to \mathbb{N}$ which Heizmann, Jones and Podelski present in their paper, for details see [13, pages 2-4]. Another useful reference is [3].

3.1 Size-change Termination

Here we recall the definition of SCT. If the reader is familiar with this definition, he may skip this subsection.

Informally, a recursive definition of a function has the SCT property if in every infinite sequence of function calls there is some infinite sequence of values of arguments which is weakly decreasing, and strictly decreasing infinitely many times. In the case the domain of the function is $\mathbb{N}$, there is no such sequence of values, and SCT is a sufficient condition for termination. In order to formally express SCT, first of all we need the definition of size-change graph. From now on we fix a recursive definition for a program $\mathcal{P}$ characterized as above. Let f be defined in $\mathcal{P}$ as follows:

$$f(x_0, \dots, x_{n-1}) := \text{if}(\dots) \text{ then } f_1(\dots) \text{ else if}(\dots) \text{ then } f_2(\dots) \text{ else } f_3(\dots).$$

Then we will denote the set $\{x_0, \dots, x_{n-1}\}$ by $\text{Var}(f)$. Given such f, a state is a pair $(f, \mathbf{v})$ where $\mathbf{v}$ is a finite sequence of natural numbers whose length is n. If in the definition of f there is a call

$$\dots \tau : g(e_0, \dots, e_{m-1})$$

we define a state transition $(f, \mathbf{v}) \xrightarrow{\tau} (g, \mathbf{u})$ to be a pair of states such that $\mathbf{u}$ is the sequence of values obtained by the expressions $(e_0, \dots, e_{m-1})$ when f is evaluated with $\mathbf{v}$.

▶ **Definition 11** (Size-change graph)**.** Let f, g be defined in $\mathcal{P}$. A size-change graph $G : f \to g$ for $\mathcal{P}$ is a bipartite directed graph on $(\mathrm{Var}(f), \mathrm{Var}(g))$. The set of edges is a subset of $\mathrm{Var}(f) \times \{\downarrow, \Downarrow\} \times \mathrm{Var}(g)$ such that there is at most one edge for any $x \in \mathrm{Var}(f)$, $y \in \mathrm{Var}(g)$. We say that f is the source function of G and g is the target function of G.

We call $(x, \downarrow, y)$ the decreasing edge, and we denote it with $x \xrightarrow{\downarrow} y$. We call $(x, \Downarrow, y)$ the weakly-decreasing edge, and we denote it with $x \xrightarrow{\Downarrow} y$.

▶ **Definition 12.** Let $f(x_0, \dots, x_{n-1})$ be defined with a call $\tau : g(e_0, \dots, e_{m-1})$ (where $\mathrm{Var}(g) = \{y_0, \dots, y_{m-1}\}$).

- The edge $x_i \xrightarrow{r} y_j$ safely describes the $x_i - y_j$ relation in the call τ, if for any $\mathbf{v} \in \mathbb{N}^n$ and $\mathbf{u} \in \mathbb{N}^m$ such that $(f, \mathbf{v}) \xrightarrow{\tau} (g, \mathbf{u})$, then $r = \downarrow$ implies that $u_j < v_i$ and $r = \Downarrow$ implies that $u_j \leq v_i$.
- The size-change graph G_τ is safe for the call τ if every edge in G_τ is a safe description.
- Set $\mathcal{G}_\mathcal{P} = \{G_\tau \mid \tau \text{ is a call in } P\}$. We say that $\mathcal{G}_\mathcal{P}$ is a safe description of $\mathcal{P}$ if for any call τ, G_τ is safe.

Note that the absence of edges between two variables x and y in the size-change graph G_τ which is safe for τ indicates either an unknown or an increasing relation in the call τ.

▶ **Definition 13.** A multipath $\mathcal{M}$ is a graph sequence $G_0, \dots, G_n, \dots$ such that the target function of G_i is the source function of G_{i+1} for any i. A thread is a connected path of edges in $\mathcal{M}$ that starts at some G_t, where $t \in \mathbb{N}$. A multipath $\mathcal{M}$ has infinite descent if some thread in $\mathcal{M}$ contains infinitely many decreasing edges.

▶ **Definition 14** (SCT program)**.** Let $\mathcal{T}$ be the set of calls in program $\mathcal{P}$. Suppose that each size-change graph $G_\tau : f \to g$ is safe for every call τ in

$$\mathcal{G}_\mathcal{P} = \{G_\tau \mid \tau \in \mathcal{T}\}.$$

$\mathcal{P}$ is size-change terminating (SCT) if, for any infinite call sequence $\pi = \tau_1, \dots, \tau_n, \dots$ that follows $\mathcal{P}$'s control flow, the multipath $M_\pi = G_{\tau_1}, \dots, G_{\tau_n}, \dots$ has an infinite descent.

3.2 Composing size-change graphs

As in [13], given two size-change graphs $G_0 : f \to g$ and $G_1 : g \to h$ we define their composition $G_0; G_1 : f \to h$. The composition of two edges $x \xrightarrow{\Downarrow} y$ and $y \xrightarrow{\Downarrow} z$ is one edge $x \xrightarrow{\Downarrow} z$. In all other cases the composition of two edges from x to y and from y to z is the edge $x \xrightarrow{\downarrow} z$. Formally, $G_0; G_1$ is the size-change graph with the following set of edges:

$$\begin{aligned}
E = \{x \xrightarrow{\downarrow} z \mid \exists y \in \mathrm{Var}(g)\ \exists r \in \{\downarrow, \Downarrow\}\, ((&x \xrightarrow{\downarrow} y \in G_0 \wedge y \xrightarrow{r} z \in G_1) \\
&\vee (x \xrightarrow{r} y \in G_0 \wedge y \xrightarrow{\downarrow} z \in G_1))\} \\
\cup \{x \xrightarrow{\Downarrow} z \mid \exists y \in \mathrm{Var}(g)(x \xrightarrow{\Downarrow} y \in G_0 \wedge y &\xrightarrow{\Downarrow} z \in G_1) \wedge \forall y \in \mathrm{Var}(g) \\
&\forall r, r' \in \{\downarrow, \Downarrow\}\, ((x \xrightarrow{r} y \in G_0 \wedge y \xrightarrow{r'} z \in G_1) \implies r = r' = \Downarrow)\}.
\end{aligned}$$

Observe that the composition operator ";" is associative. Given a finite call sequence $\pi = \tau_0, \dots, \tau_{n-1}$ we define $G_\pi = G_{\tau_0}, \dots, G_{\tau_{n-1}}$. Moreover we say that the size-change graph G is idempotent if $G; G = G$.

Given a finite set of size-change graphs $\mathcal{G}$, $\mathsf{cl}(\mathcal{G})$ is the smallest set which contains $\mathcal{G}$ and is closed by composition. Formally $\mathsf{cl}(\mathcal{G})$ is the smallest set such that

- $\mathcal{G} \subseteq \mathsf{cl}(\mathcal{G})$;
- If $G_0 : f \to g$ and $G_1 : g \to h$ are in $\mathsf{cl}(\mathcal{G})$, then $G_0; G_1 \in \mathsf{cl}(\mathcal{G})$.

Once we fixed the number of variables, there are only finitely many bipartite graphs with two labels for the edges, therefore classically $\mathsf{cl}(\mathcal{G})$ is finite. Moreover we can intuitionistically prove that it is finite thanks to the following proposition.

▶ **Proposition 15.** *Assume that S is a finite set where the equality is decidable and that op: $S \times S \to S$ is a computable map. Then the closure of any finite subset of S is intuitionistically finite.*

In fact if $I \subseteq S$, we can define $I_0 = I$, $I_{k+1} = \{\mathrm{op}(a,b) \mid a, b \in \bigcup\{I_h \mid h \leq k\}\} \setminus \bigcup\{I_h \mid h \leq k\}$. By decidability of equality, we may effectively compute $A \setminus B$ for any A, B finite subsets of S. Therefore we may intuitionistically prove by induction over $S \setminus \bigcup\{I_h \mid h \leq k\}$ that there is a $k \leq |S|$ such that $I_{k+1} = \emptyset$. Thus k defines the closure of I.

3.3 Definition of SCT*

As seen above, $\mathcal{P}$ is SCT if and only if

for any infinite call sequence π that follows $\mathcal{P}$, M_π has an infinite descent.

Now we want to apply some classical step in order to obtain a statement SCT* classically equivalent to SCT but intuitionistically easier to prove. From the definition of SCT, by taking a contrapositive, we obtain

for any call sequence π which follows $\mathcal{P}$,
M_π has no infinite descents implies that π is not infinite.

This is the sentence from which we will obtain our definition. Formally a call sequence which follows $\mathcal{P}$ is a function $\pi : \mathbb{N} \longrightarrow \{\tau \mid \tau \text{ is a call in } \mathcal{P}\} \cup \{\emptyset\}$ such that

- if $\pi(n) = \emptyset$ for some $n \in \mathbb{N}$, then $\forall m > n(\pi(m) = \emptyset)$;
- if $\pi(n+1) = \tau$, then τ is a call which appears in the definition corresponding to the call $\pi(n)$.

Observe that π is infinite in this notation means that $\forall n(\pi(n) \neq \emptyset)$. In order to keep the notation of [14] for any natural number n we denote $\tau_n = \pi(n)$.

We introduce two binary relations, π^+ on $\mathbb{N}$ and R_π on $\mathbb{N} \times \mathrm{Var}$. Then we translate "$M_\pi$ has no infinite descents" with "R_π is inductively well-founded" and "π is not infinite" with "π^+ is inductively well-founded".

Let $\mathcal{P}$ be a program and let π be a call sequence which follows $\mathcal{P}$. We define a binary relation π^+ on $\mathbb{N}$ by:

$$m\pi^+n \iff m > n \wedge \tau_m \neq \emptyset.$$

Observe that if π is infinite then $m\pi^+n$ holds if and only if $m > n$, while if l is the minimum number such that $\pi(l) = \emptyset$ then $m\pi^+n$ holds if and only if $l > m > n$.

Now, we define a binary relation R_π on $\mathbb{N} \times \mathrm{Var}$. Here $(m, y)R_\pi(n, x)$ holds if and only if y becomes strictly smaller than x when we step from τ_n to τ_{m-1} along the call sequence π.

▶ **Definition 16.** Given a sequence π that follows $\mathcal{P}$, R_π is defined as:

$$(m, y)R_\pi(n, x) \iff m\pi^+n \wedge x \xrightarrow{\downarrow} y \in G_{\tau_n}; \ldots G_{\tau_{m-1}},$$

where G_τ is the size-change graph associated to τ.

From R_π and π^+ we define SCT*.

▶ **Definition 17** (SCT* program)**.** $\mathcal{P}$ is SCT* if and only if for any call sequence π which follows $\mathcal{P}$: R_π is (inductively) well-founded implies that π^+ is (inductively) well-founded.

We highlighted the use of the inductive definition of well-foundedness instead of the classical one, since as seen it is crucial in order to give an intuitionistic proof of the SCT Theorem. However for short, from now on we will write well-foundedness instead of inductive well-foundedness.

4 Proving SCT* Theorem

The goal of this section is to intuitionistically prove that the SCT Theorem by Lee et al. holds providing we use SCT* instead of SCT. The SCT Theorem states that a program $\mathcal{P}$ is SCT if and only if for any idempotent $G \in \mathsf{cl}(\mathcal{G}_\mathcal{P})$ there exists a variable x in the source of G such that $x \xrightarrow{\downarrow} x \in G$. Recall that in the classical proof of the SCT Theorem the main ingredient is Ramsey's Theorem for pairs. In the classical proof the authors suppose by contradiction that there exists an infinite call sequence π which follows $\mathcal{P}$. Then they define a coloring $h : [\mathbb{N}]^2 \to \mathsf{cl}(\mathcal{G}_\mathcal{P})$ which associates to any pair of natural numbers $n < m$ the size-change graph which corresponds to $G_{\tau_n}; \dots; G_{\tau_{m-1}}$. Since $\mathsf{cl}(\mathcal{G}_\mathcal{P})$ if finite and by applying Ramsey's Theorem for pairs they obtain an infinite homogeneous chain and therefore a contradiction.

We will prove that also in this case we can use the H-closure Theorem instead of Ramsey's Theorem for pairs. In order to do that we need to introduce a binary relation π_G^+ for any $G \in \mathsf{cl}(\mathcal{G}_\mathcal{P})$ and for any call sequence π which follows $\mathcal{P}$. We have that $m\pi_G^+n$ holds if and only if the size-change graph associated to $\tau_n, \dots, \tau_{m-1}$ is G.

▶ **Definition 18.** Let π be a call sequence which follows $\mathcal{P}$ and let $G \in \mathsf{cl}(\mathcal{G}_\mathcal{P})$. Define $\pi_G^+ \subseteq \mathbb{N}^2$ as:

$$m\pi_G^+n \iff m\pi^+n \wedge G_{\tau_n}; \dots; G_{\tau_{m-1}} = G.$$

Observe that π_G^+ is decidable since G_{τ_i} is finite and π^+ is decidable. Moreover, as remarked in Subsection 3.3, if R is decidable then $H(R)$ is.

▶ **Lemma 19.** *Let π be a call sequence which follows $\mathcal{P}$ and let $G \in \mathsf{cl}(\mathcal{G}_\mathcal{P})$. Then both π_G^+ and $H(\pi_G^+)$ are decidable.*

By applying the H-closure Theorem to the relations π_G^+, for $G \in \mathsf{cl}(\mathcal{G}_\mathcal{P})$, we can intuitionistically prove the SCT* Theorem.

▶ **Theorem 20** (SCT* Theorem)**.** *Every idempotent graph in $\mathsf{cl}(\mathcal{G}_\mathcal{P})$ has an edge $x \xrightarrow{\downarrow} x$ if and only if $\mathcal{P}$ is* SCT**.*

Proof. "⇒": Assume that any idempotent graph in $\mathsf{cl}(\mathcal{G}_\mathcal{P})$ has an edge $x \xrightarrow{\downarrow} x$. Let π be a call sequence which follows $\mathcal{P}$ such that R_π is well-founded. We want to prove that π^+ is well-founded.

▶ **Claim.** *For any G in $\mathsf{cl}(\mathcal{G}_\mathcal{P})$, π_G^+ is H-well-founded.*

Proof of the Claim. Since "G is idempotent" is a decidable statement we can consider two cases.

- If G is not idempotent, then each $L \in H(\pi^+_G)$ has length at most 2. Otherwise assume that $\langle n, m, l\rangle \in H(\pi^+_G)$ for some $n < m < l$. By definition, this would imply that $m\pi^+_G n$, $l\pi^+_G m$ and $l\pi^+_G n$, therefore we would have

  $$G; G = G_{\tau_n}; \dots; G_{\tau_{m-1}}; G_{\tau_m}; \dots; G_{\tau_{l-1}} = G.$$

  This means that G is idempotent. Contradiction. Hence we have $\neg\exists n, m, l(\langle n, m, l\rangle \in H(\pi^+_G))$, and so $\forall n, m, l(\langle n, m, l\rangle \notin H(\pi^+_G))$ follows by Lemma 19. Hence π^+_G is H-well-founded.
- If G is idempotent, then there exists $x \xrightarrow{\downarrow} x \in G$. Define the following binary relation

  $$U_x = \{(n, (n, x)) \mid n \in \mathbb{N}\}.$$

  Then U_x is a simulation of π^+_G in R_π. In fact assume that

  $$m\pi^+_G n \ \wedge \ nU_x(n, x),$$

  Therefore, since $x \xrightarrow{\downarrow} x \in G = G_{\tau_n}; \dots; G_{\tau_{m-1}}$, we have

  $$mU_x(m, x) \wedge (m, x)R_\pi(n, x).$$

  Since by hypothesis R_π is well-founded, then by Proposition 5 also π^+_G is well-founded. By Proposition 8 it is H-well-founded. ◀

Now observe that

$$\pi^+ = \bigcup \left\{\pi^+_G \mid G \in \mathsf{cl}(\mathcal{G}_\mathcal{P})\right\},$$

since every $G_{\tau_n}; \dots; G_{\tau_{m-1}}$ equates some $G \in \mathsf{cl}(\mathcal{G}_\mathcal{P})$ by definition of $\mathsf{cl}(\mathcal{G}_\mathcal{P})$. Hence by applying both the H-closure Theorem (Theorem 9) and finiteness of $\mathsf{cl}(\mathcal{G}_\mathcal{P})$ we obtain also π^+ is H-well-founded. Moreover it is transitive by definition, then it is well-founded by Proposition 8 and we are done.

"$\Leftarrow$": Suppose that $\mathcal{P}$ is SCT* and let G_τ be an idempotent size-change graph. By idempotency if we define the call sequence π such that $\pi(n) = \tau$ for any $n \in \mathbb{N}$, then it is an infinite call sequence which follows $\mathcal{P}$. In particular π^+ is not well-founded. Since $\mathcal{P}$ is SCT*, R_π is not well-founded. In this case, we may observe that:

$$(m, y)R_\pi(n, x) \iff x \xrightarrow{\downarrow} y \in G_{\tau_n}; \dots; G_{\tau_{m-1}} = G_\tau; \dots; G_\tau = G_\tau$$

Then $(m, y)R_\pi(n, x) \iff x \xrightarrow{\downarrow} y \in G_\tau$. Define

$$y\tilde{R}_\pi x \iff x \xrightarrow{\downarrow} y \in G_\tau,$$

Observe that if $\tilde{R}_\pi$ is well-founded, then also R_π is. We can prove it by using the simulation

$$U = \{((n, x), x) \mid n \in \mathbb{N}, x \text{ a variable in the source of } G_\tau\}.$$

Hence $\tilde{R}_\pi$ is not well-founded. Since $\tilde{R}_\pi$ is not well-founded and it is finite, thanks to Proposition 6, it has a cycle for some variable z:

$$z = z_n\tilde{R}_\pi z_{n-1}\tilde{R}_\pi \dots \tilde{R}_\pi z_0 = z.$$

Moreover $\tilde{R}_\pi$ is transitive: in fact if $x \xrightarrow{\downarrow} y \in G_\tau$ and $y \xrightarrow{\downarrow} z \in G_\tau$, then $x \xrightarrow{\downarrow} z \in G_\tau; G_\tau = G_\tau$. Since $\tilde{R}_\pi$ is transitive, hence $z\tilde{R}_\pi z$. Therefore

$$z \xrightarrow{\downarrow} z \in G_\tau.$$

We have proved that if G_τ is idempotent, then $z \xrightarrow{\downarrow} z \in G_\tau$. ◀

By comparing the classical proofs of the termination theorems, the version of Ramsey's Theorem for pairs used in the proof of the Termination Theorem is weaker then the one used in the proof of the SCT Theorem. In fact in order to prove the Termination Theorem it is sufficient to have an infinite homogeneous chain (i.e. an ordered set $\{x_i \mid i \in \mathbb{N}\}$ such that each pair of consecutive elements has the same color) instead of an infinite homogeneous set. This result which is an infinite version of Erdős–Szekeres's Theorem [10] is called also Weak Ramsey's Theorem for pairs and it is strictly weaker than Ramsey's Theorem for pairs in two colors in RCA_0 [7]. We can stress this difference also in the intuitionistic proofs. In fact the proof of the Termination Theorem in [6] uses:

if $R_0, \dots, R_{n-1}$ are well-founded then $\bigcup\{R_i \mid i < n\}$ is H-well-founded,

where the hypothesis is stronger than in the H-closure Theorem, by Proposition 8. On the other hand the proof of the SCT* Theorem above uses the whole H-closure Theorem.

Let us conclude this section with an example of an SCT* program.

▶ **Example 21.** Let us consider the following functional program, where $*$ denotes any value.

$$\begin{aligned}
g(x, y, \mathrm{temp}, \mathrm{exp}, z) :=& \text{if } (z = 0) \quad 0\\
& \text{else if } (z = 1) \quad \mathrm{temp}\\
& \text{else } \tau_0 : g(*, *, \mathrm{temp} + \mathrm{exp}, \mathrm{exp}, z - 1)\\
f(x, y, \mathrm{temp}, \mathrm{exp}, z) :=& \text{if } (y = 0) \quad 1\\
& \text{else if } (y = 1) \quad \mathrm{exp}\\
& \text{else } \tau_1 : f(x, y - 1, *, g(x, y, 0, \mathrm{exp}, x)), *)
\end{aligned}$$

As in Example 3, $f(x, y, 0, 1, z)$ computes x^y. The idempotent graphs in $\mathsf{cl}(\mathcal{G})$ are $G_{\tau_0} : g \to g$ and $G_{\tau_1} : f \to f$ (since the source and the target of the other size-change graphs are different). G_{τ_0} is composed of $z \xrightarrow{\downarrow} z$ and $\mathrm{exp} \xrightarrow{\Downarrow} \mathrm{exp}$, while G_{τ_1} is composed of $y \xrightarrow{\downarrow} y$ and $x \xrightarrow{\Downarrow} x$. Hence this program is SCT* since it satisfies the condition of the SCT* Theorem.

5 Tail-recursive SCT* programs compute exactly primitive recursive functions

In this section we compare size-change termination and transition invariant termination. As Heizmann, Jones and Podelski did, we restrict the domain of the programs we consider in order to match transition invariants termination and SCT*. In fact SCT (and so SCT*) is defined for functional programs, while Podelski and Rybalchenko's termination is defined for transition-based programs. As they did from now on we consider just tail-recursive functional programs (where all functions use the same variables), for which there exists a direct transition-based translation into while-if programs. We refer to [13] for details. The reader has to keep in mind that along all this section we have at the same time a functional program, which we denote by $\mathcal{P}$, and its translation as a transition-based program $\mathcal{R}_{\mathcal{P}}$. The only property we use of the translation $\mathcal{R}_{\mathcal{P}}$ is that $\mathcal{R}_{\mathcal{P}}$ consists of: while, if, a program counter and the values of the variables of $\mathcal{P}$. If $\mathcal{P}$ were recursive but not tail-recursive, $\mathcal{R}_{\mathcal{P}}$ should include also a stack, but we explicitly assume that this is not the case. We will derive a characterization of $\mathcal{P}$ from a characterization of $\mathcal{R}_{\mathcal{P}}$.

The goal of this section is to prove, by using the result obtained in [4], that the functional programs which are tail-recursive and are SCT* compute exactly the primitive recursive functions. Ben-Amram in [3] already proved that the tail-recursive SCT programs compute primitive recursive functions, however we present a completely different proof which uses an analysis of the intuitionistic proof of the Termination Theorem, in the case of a transition invariant of height ω. In fact we intuitionistically prove that if a program $\mathcal{P}$ is SCT* then $\mathcal{R}_\mathcal{P}$ has a transition invariant of height ω.

First of all we recall some definitions and results useful to compare size-change termination and Podelski and Rybalchenko's termination. Each state in the transition-based program $\mathcal{R}_\mathcal{P}$ which corresponds to the tail-recursive functional program $\mathcal{P}$ is a tuple s composed of the location $s(\mathrm{pc})$ of the program instruction and a value $s(x)$ for any variable x. We define a relation $\Phi(G)$ on states saying that whenever G includes a decreasing edge $x \xrightarrow{\downarrow} y$ then the value of y in the second state is smaller than the value of x in the first state, and similarly for any weakly-decreasing edge.

▶ **Definition 22** (Transition relation of a size-change graph, Definition 26 [13]). Given a size-change graph $G : f \to g$, define the binary relation over states $\Phi(G) \subseteq S \times S$ as follows: $s'\Phi(G)s$ if and only if $s(\mathrm{pc}) = f$, $s'(\mathrm{pc}) = g$ and

$$\bigwedge \left\{ s(z_i) \geq s'(z_j) \mid (z_i \xrightarrow{\Downarrow} z_j) \in G \right\} \wedge \bigwedge \left\{ s(z_i) > s'(z_j) \mid (z_i \xrightarrow{\downarrow} z_j) \in G \right\}.$$

The transition relation ρ_τ associated to the transition

$$f(x_0, \ldots, x_{n-1}) = \ldots \tau : g(e_0, \ldots, e_{n-1}), \ldots,$$

is defined as follows:

$$\rho_\tau = \left\{ ((f, \mathbf{v}), (g, \mathbf{u})) \mid (f, \mathbf{v}) \xrightarrow{\tau} (g, \mathbf{u}) \right\}.$$

Observe that if G_τ is the size-change graph assigned to the call τ of program $\mathcal{P}$, G_τ is safe for τ if and only if the inclusion $\rho_\tau \subseteq \Phi(G_\tau)$ holds.

▶ **Lemma 23** (Lemma 29 [13]). *The composition of the two size-change graphs $G_1 : f \to g$ and $G_2 : g \to h$ overapproximates the composition of the relations they define, i.e.*

$$\Phi(G_1) \circ \Phi(G_2) \subseteq \Phi(G_1; G_2).$$

The authors of [13] proved the following lemma about the connection between G and $\Phi(G)$.

▶ **Lemma 24** (Lemma 31 [13]). *Let G be a size-change graph such that source and target of G coincide. If G has an edge of form $x \xrightarrow{\downarrow} x$ then the relation $\Phi(G)$ is well-founded.*

They also noticed that the vice versa does not hold in the general case, however we prove that if G is idempotent this equivalence holds.

▶ **Lemma 25.** *Let G be an idempotent size-change graph. Then G has an edge of form $x \xrightarrow{\downarrow} x$ if and only if the relation $\Phi(G)$ is well-founded.*

Proof.
"$\Rightarrow$": It follows from Lemma 24.
"$\Leftarrow$": Observe that "there exists a variable x in the source of G, $x \xrightarrow{\downarrow} x \in G$" is a decidable statement, since G is finite. Therefore either G has some edge of the form $x \xrightarrow{\downarrow} x$, or G has no edge of this form. In the first case we are done, in the second one we will prove a contradiction, that $\Phi(G)$ is not well-founded. This argument intuitionistically shows the

thesis, because from a contradiction we may derive everything. Let V be the set of the variables in the source of G. Define the following preorder on V:

$$x \precsim y \iff x = y \ \vee\ y \overset{\downarrow}{\to} x \ \vee\ y \overset{\Downarrow}{\to} x.$$

It is reflexive by definition and it is transitive since G is idempotent: if $y \overset{r}{\to} x \in G$ and $z \xrightarrow{r'} y \in G$ then $z \xrightarrow{r''} x \in G$ for some $r'' \in \{\downarrow, \Downarrow\}$.

Let us consider the quotient X of V with respect to the equivalence relation

$$x \sim y \iff x \precsim y \ \wedge\ y \precsim x.$$

In X, $\precsim$ is an order since it is also antisymmetric. Moreover X is finite then, by Proposition 6, $\precsim$ is well-founded on X. Hence for any equivalence class $[x] \in X$ we can define $h([x])$ to be the height of $[x]$ with respect to $\precsim$ in X: i.e. the number of elements $[y] \in X$ such that $[y] \precsim [x]$.

Then we can define a state s as follows: for any $x \in V$, $s(x) = h([x])$. We claim that $s\Phi(G)s$. In fact

- if $y \overset{\Downarrow}{\to} x \in G$ then $x \precsim y$ and we have two possibilities: if $[x] = [y]$ in X then $s(x) = s(y)$, otherwise $h([x]) < h([y])$ and so $s(x) < s(y)$;
- if $y \overset{\downarrow}{\to} x \in G$ then $x \precsim y$. Moreover $y \precsim x$ is false, otherwise by case analysis from $y \overset{\downarrow}{\to} x \in G$ and $x = y \vee x \overset{\downarrow}{\to} y \in G \vee x \overset{\Downarrow}{\to} y \in G$ we deduce $x \overset{\downarrow}{\to} x \in G$, contradicting the hypothesis. Hence $h([x]) < h([y])$ and so $s(x) < s(y)$.

Then $s\Phi(G)s$ and so $\Phi(G)$ is ill-founded. Contradiction. ◀

Thanks to the SCT* Theorem and the lemma above, we may observe that if $\mathcal{P}$ is tail-recursive, $\mathcal{P}$ is SCT* if and only if for every $G \in \mathsf{cl}(\mathcal{G}_\mathcal{P})$ idempotent $\Phi(G)$ is well-founded.

Our next goal is to prove that any tail-recursive program which is SCT* computes a primitive recursive function. In order to do that we modify the proof by Heizmann, Jones and Podelski of "$\bigcup\{\Phi(G) \mid G \in \mathsf{cl}(\mathcal{G}_\mathcal{P})\}$ is a transition invariant". We will prove that it is a transition invariant of height ω. In order to do this we need the following lemmas.

▶ **Lemma 26.** *Every finite semigroup G has an idempotent element.*

Proof. Let $x \in G$ and consider the following chain

$$x \mapsto x^2 \mapsto (x^2)^2 = x^4 \mapsto \ldots \mapsto x^n \mapsto (x^n)^2 \mapsto \ldots.$$

Since G is finite, there exists y in the previous chain such that $y^k = y$, for some $k \geq 2$. Put $z = y^{k-1}$, then

$$z \cdot z = y^{k-1} \cdot y^{k-1} = y^k \cdot y^{k-2} = y \cdot y^{k-2} = y^{k-1} = z.$$ ◀

Even if the previous definitions and results can be stated for any functional program, we highlight now that we need tail-recursive functional programs in order to have the translation $\mathcal{R}_\mathcal{P}$ of $\mathcal{P}$. In this case each state of $\mathcal{R}_\mathcal{P}$ is composed of the location of the program and the values in $\mathbb{N}$ of the variables.

▶ **Lemma 27.** *Let G be a size-change graph. Let k be a positive natural number. If G^k is such that $x \overset{\downarrow}{\to} x$ for some x then $\Phi(G)$ has height ω.*

Proof. Assume that $x \overset{\downarrow}{\to} x$ in G^k. We distinguish the cases $k = 1$ and $k \geq 2$.

If $k = 1$, let $f : \mathrm{dom}(\Phi(G)) \to \mathbb{N}$ be such that $f(s) = s(x)$. Since If $s'\Phi(G)s$, then by $x \overset{\downarrow}{\to} x \in G$ we deduce $s'(x) < s(x)$, hence $f(s') < f(s)$. Thus f is a weight function for $\Phi(G)$.

Assume now that $k \geq 2$, since $x \overset{\downarrow}{\to} x$ in G^k, then there exist $y_0, \dots, y_{k-2}$ such that

$$x \to y_0 \to \cdots \to y_{k-2} \to x$$

where at least one of these arrows is strictly decreasing. Then define a function $f : \mathrm{dom}(\Phi(G)) \to \mathbb{N}$ by

$$f(s) = \sum_{i=0}^{k-2} s(y_i) + s(x).$$

Hence if $s'\Phi(G)s$ then each of the $s'(y_i)$ and $s'(x)$ is less or equal to the ones of s. Moreover one of these is strictly less, since at least one of the edges of G is strictly decreasing. So $f(s') < f(s)$ and this means that f witnesses that $\Phi(G)$ has height ω. ◀

By using the results above we can modify the Theorem Idempotence and well-foundedness [13, Theorem 32] which states that if for any $G \in \mathsf{cl}(\mathcal{G}_\mathcal{P})$ idempotent $\Phi(G)$ is well-founded, then $\Phi(G)$ is well-founded for any $G \in \mathsf{cl}(\mathcal{G}_\mathcal{P})$.

▶ **Theorem 28.** *If*

$$\forall G \in \mathsf{cl}(\mathcal{G}_\mathcal{P})(G; G = G \implies \Phi(G) \textit{ is well-founded})$$

then $\Phi(G)$ has height ω for every graph in $\mathsf{cl}(\mathcal{G}_\mathcal{P})$.

Proof. Let $G \in \mathsf{cl}(\mathcal{G}_\mathcal{P})$ be a size-change graph. There are two possibilities. On the one hand, if the source and target of G do not coincide, then $\Phi(G) \circ \Phi(G) = \emptyset$, therefore $\Phi(G)$ has height ω. On the other hand, assume that source and target of G coincide. Then G^n is defined for any $n \in \mathbb{N}$. Since the semigroup $(\{G^n \mid n > 0\}, ;)$ is finite, by Lemma 26 it has an idempotent element G^k. Since $\Phi(G^k)$ is well-founded by hypothesis we obtain, by applying Lemma 25, that $x \overset{\downarrow}{\to} x \in G^k$ for some x. By Lemma 27 $\Phi(G)$ has height ω and we are done. ◀

▶ **Corollary 29** (Corollary 33 [13]). *If the program $\mathcal{P}$ is size-change terminating for a set of size-change graphs $\mathcal{G}_\mathcal{P}$ that is a safe description of $\mathcal{P}$, then the relation defined by its closure* $\mathsf{cl}(\mathcal{G}_\mathcal{P})$

$$\bigcup \{\Phi(G) \mid G \in \mathsf{cl}(\mathcal{G}_\mathcal{P})\}$$

is a disjunctively well-founded transition invariant for $\mathcal{R}_\mathcal{P}$.

Therefore, thanks to Theorem 28, all $\Phi(G)$ have height ω: by definition, the transition invariant has height ω. In [4] and [11] it is proved that if $\mathcal{R}$ has a transition invariant of height ω then it computes a primitive recursive function.

We apply this result to the while-if program $\mathcal{R}_\mathcal{P}$ which translates the tail-recursive program P. We obtain:

▶ **Proposition 30.** *Each tail-recursive program which is* SCT* *is primitive recursive.*

This result was already proved by Ben-Amram in [3] using the classical definition of SCT. He proved that in general SCT programs compute multiple recursive function. As a corollary, by observing that if you do not use nested recursive calls a multiple recursive function is primitive recursive, he obtained that any tail-recursive SCT program computes a primitive recursive function.

By using our proof we can easily obtain a bound whose class is given by the number of relations of the transition invariant. In fact the weight function provided in Lemma 27 is in $\mathcal{F}_1$, since $f(s) < |s| \cdot F_0(\max(s))$ and for any program $|s|$ is fixed. Therefore by applying the bound provided in [11] we have that if the transition relation of $\mathcal{R}_\mathcal{P}$ is the graph of a function in $\mathcal{F}_n$, there is a bound in $\mathcal{F}_{k+n-1}$ where k is the number of the relations which compose the transition invariant whose weight functions are in $\mathcal{F}_1$. Therefore by Corollary 29, we can conclude that if the transition relation is in $\mathcal{F}_2$, the function is in $\mathcal{F}_{|\mathsf{cl}(\mathcal{G}_\mathcal{P})|+1}$. Unfortunately $\mathsf{cl}(\mathcal{G}_\mathcal{P})$ is exponential in $\mathcal{G}_\mathcal{P}$, so this bound is huge. We have also another bound on the number of variables. In fact in the proof of Theorem 28 we saw that for any G there exists $k > 0$ such that G^k is idempotent. Let us consider the minimum such k. Then, by following the proof of Lemma 27 there exists either a $x \overset{\downarrow}{\to} x$ for some x or a chain

$$x \to y_0 \to \cdots \to y_{k-2} \to x$$

for some variables, where at least one arrow is strict. Observe that all the variables in the chain are different: there is not a path which connect some y_i to itself, by minimality of k. The weight function we built for $\Phi(G)$ is given by the sum of the values which corresponds to these variables. This means that if we have n-many variables, the number of possible weight functions f of this kind is

$$\sum_{i=k}^{n} \binom{n}{k} = 2^n - 1.$$

Since if R and R' have the same weight function, then also $R \cup R'$ have this weight function, we can merge the relations in the transition invariant found in such a way their number is less or equal to the number of the possible weight functions. Unfortunately also this bound is exponential (in the number of variables), so it is huge too.

▶ **Example 31.** The program considered in Example 21 is tail-recursive. Observe that

$$\Phi(G_{\tau_0}) = \{s'\Phi(G)s \mid s'(\mathrm{pc}) = s(\mathrm{pc}) = g \ \wedge \ s'(z) < s(z) \ \wedge \ s'(\exp) \le s'(\exp)\}\,;$$
$$\Phi(G_{\tau_1}) = \{s'\Phi(G)s \mid s'(\mathrm{pc}) = s(\mathrm{pc}) = f \ \wedge \ s'(y) < s(y) \ \wedge \ s'(x) \le s'(x)\}\,;$$
$$\Phi(G_{\tau_2}) = \{s'\Phi(G)s \mid s'(\mathrm{pc}) = f \ \wedge \ s(\mathrm{pc}) = g\}\,.$$

Then $\Phi(G_{\tau_0}) \cup \Phi(G_{\tau_1}) \cup \Phi(G_{\tau_2})$ is already a transition invariant of height ω for the transition-based program which corresponds to it (Example 3 where $l = g$ and $l' = f$). Trivially, also $\bigcup\{\Phi(G) \mid G \in \mathsf{cl}(\mathcal{G}_\mathcal{P})\}$ is a transition invariant and the function computed is primitive recursive.

Furthermore we can observe that each primitive recursive function has a tail-recursive implementation which is SCT*.

▶ **Proposition 32.** *Each primitive recursive function has an implementation which is* SCT*.

Proof. By induction on the primitive recursive functions.

- For the constant function, successor function and the projection function it is trivial since we can write tail-recursive first order functional programs which have no idempotent size-change graphs.
- Assume that the primitive recursive functions $g_0, \dots, g_{n-1}$ and f have an implementation which is SCT*. By using them it is straightforward to show that the standard program which computes their composition

  $$h(x_0, \dots, x_{k-1}) = f(g_0(x_0, \dots, x_{k-1}), \dots, g_{n-1}(x_0, \dots, x_{k-1}))$$

  is SCT*. In fact each idempotent size-change graph corresponds to some call in the definitions either of g_i for some $i < k$ or of f.
- Assume that the primitive recursive functions f and g have a SCT* program which computes it. Then, by using these programs we can define a standard tail-recursive SCT* program which computes

  $$h(x_0, \dots, x_{k-1}, y) = \begin{cases} f(x_0, \dots, x_{k-1}) & \text{if } y = 0 \\ g(h(x_0, \dots, x_{k-1}, y-1), y) & \text{otherwise.} \end{cases}$$

  As observed in the previous point each size-change graph which corresponds to some call either in f or in g, has the desired property. There is only one new size-change graph $G \in \mathsf{cl}(\mathcal{G}_\mathcal{P})$ derived from the definition of h. Since $y \xrightarrow{\downarrow} y \in G$, we are done. ◀

6 Transition Invariants Termination as a property of size-change graphs

In the previous section we proved that if a tail-recursive program is SCT* then it has a transition invariant of height ω. In this section we will see a statement on functional programs strictly weaker than SCT* which is equivalent to the definition of termination by Podelski and Rybalchenko, so it is equivalent to have a transition invariant of general height.

Thanks to Lemma 25, we saw that if $\mathcal{P}$ is tail-recursive, $\mathcal{P}$ is SCT* if and only if for every $G \in \mathsf{cl}(\mathcal{G}_\mathcal{P})$ idempotent $\Phi(G)$ is well-founded. Recall that Podelski and Rybalchenko analyse the termination of while-if programs, and in order to have a simple relationship with while-if program we restrict the functional programs to be tail-recursive. Here we prove that a tail-recursive program $\mathcal{P}$ has a disjunctively well-founded transition invariant if and only if for any $G \in \mathsf{cl}(\mathcal{G}_\mathcal{P})$ idempotent $\Phi(G) \cap R^+$ is well-founded, where R is the transition relation of $\mathcal{R}_\mathcal{P}$. The proof of "for any G idempotent $\Phi(G) \cap R^+$ is well-founded implies termination" follows, with some little changes, the proof of Corollary 29 studied in [13, Corollary 33].

The first step is to intuitionistically prove another version of the Theorem Idempotence and well-foundedness [13, Theorem 32]. In order to do that we need the following lemma.

▶ **Lemma 33.** *Let R be a binary relation on I and $k \in \mathbb{N}$ and T a transitive binary relation. If $R^k \cap T$ is well-founded then $R \cap T$ is well-founded.*

Proof.
- Let $k = 2$. Induction on x with respect to R^2. Assume that

  $$\forall z (z(R^2 \cap T)x \implies z \text{ is } (R \cap T)\text{-well-founded }).$$

  By two applications of point 1 of Proposition 5,

  $$\begin{aligned} x \text{ is } (R \cap T)\text{-well-founded} &\iff \forall y (y(R \cap T)x \implies y \text{ is } (R \cap T)\text{-well-founded}) \\ &\iff \forall y (y(R \cap T)x \implies (\forall z (z(R \cap T)y \implies z \text{ is } (R \cap T)\text{-well-founded}))). \end{aligned}$$

Observe that since $z(R\cap T)y$ and $y(R\cap T)x$ then $z(R^2\cap T)x$. This implies by inductive hypothesis that z is $(R\cap T)$-well-founded. So for every $x\in I$, x is $(R\cap T)$-well-founded.

- The idea of the proof for $k>2$ is to prove it by induction on x with respect to R^k and to repeat the same argument providing in the case above, by using k-many steps following point 1 of Proposition 5 in order to get $z(R^k\cap T)x$. By applying the inductive hypothesis we will obtain our thesis. ◀

▶ **Theorem 34.** *If*

$$\forall G\in \mathsf{cl}(\mathcal{G}_\mathcal{P})(G;G=G \implies \Phi(G)\cap R^+\cap(\mathrm{Acc}\times\mathrm{Acc})\ \textit{well-founded}\ )$$

then $\Phi(G)\cap R^+\cap(\mathrm{Acc}\times\mathrm{Acc})$ *is well-founded for every graph in* $\mathsf{cl}(\mathcal{G}_\mathcal{P})$.

Proof. Let $G\in\mathsf{cl}(\mathcal{G}_\mathcal{P})$ be a size-change graph. We have two cases. On the one hand, if the source and target of G do not coincide, then $\Phi(G)\circ\Phi(G)=\emptyset$, therefore $\Phi(G)\cap R^+\cap(\mathrm{Acc}\times\mathrm{Acc})$ is well-founded. On the other hand, assume that source and target of G coincide. In this case G^n is defined for all $n\in\mathbb{N}$. Since the semigroup $(\{G^n\mid n\in\mathbb{N}\},;)$ is finite, by Lemma 26 it has an idempotent element G^k. By Lemma 23 the inclusion $\Phi(G)^k\subseteq\Phi(G^k)$ holds. Then

$$\Phi(G)^k\cap R^+\cap(\mathrm{Acc}\times\mathrm{Acc})\subseteq\Phi(G^k)\cap R^+\cap(\mathrm{Acc}\times\mathrm{Acc})$$

By hypothesis, since G^k is idempotent we have: $\Phi(G^k)\cap R^+\cap(\mathrm{Acc}\times\mathrm{Acc})$ is well-founded. Then $\Phi(G)^k\cap R^+\cap(\mathrm{Acc}\times\mathrm{Acc})$ is well-founded by Lemma 23 and therefore by Lemma 33 also $\Phi(G)\cap R^+\cap(\mathrm{Acc}\times\mathrm{Acc})$ is well-founded. ◀

Therefore we obtain the corresponding version of Corollary 29.

▶ **Corollary 35.** *Let* $\mathcal{P}$ *be a program and let* $\mathcal{G}_\mathcal{P}$ *be a set of size-change graphs that is a safe description of* $\mathcal{P}$. *If for every* $G\in\mathsf{cl}(\mathcal{G}_\mathcal{P})$ *idempotent,* $\Phi(G)\cap R^+\cap(\mathrm{Acc}\times\mathrm{Acc})$ *is well-founded, then the relation defined by its closure* $\mathsf{cl}(\mathcal{G}_\mathcal{P})$

$$\bigcup\{\Phi(G)\cap R^+\cap(\mathrm{Acc}\times\mathrm{Acc})\mid G\in\mathsf{cl}(\mathcal{G}_\mathcal{P})\}$$

is a disjunctively well-founded transition invariant for $\mathcal{R}_\mathcal{P}$.

Proof. Thanks to the proof of Corollary 29 in [13, Corollary 33]

$$R^+\subseteq\bigcup\{\Phi(G)\mid G\in\mathsf{cl}(\mathcal{G}_\mathcal{P})\}\,.$$

Then

$$R^+\cap(\mathrm{Acc}\times\mathrm{Acc})\subseteq\bigcup\{\Phi(G)\cap R^+\cap(\mathrm{Acc}\times\mathrm{Acc})\mid G\in\mathsf{cl}(\mathcal{G}_\mathcal{P})\}\,.$$

Moreover, by hypothesis and thanks to Lemma 34 the relation $\Phi(G)\cap R^+\cap(\mathrm{Acc}\times\mathrm{Acc})$ is well-founded. Hence $\bigcup\{\Phi(G)\cap R^+\cap(\mathrm{Acc}\times\mathrm{Acc})\mid G\in\mathsf{cl}(\mathcal{G}_\mathcal{P})\}$ is a disjunctively well-founded transition invariant for $\mathcal{R}_\mathcal{P}$. ◀

Finally we prove the equivalence, the other implication is trivial.

▶ **Theorem 36.** *Given a program* $\mathcal{P}$ *the followings are equivalent:*

1. *for every* $G\in\mathsf{cl}(\mathcal{G}_\mathcal{P})$ *idempotent,* $\Phi(G)\cap R^+\cap(\mathrm{Acc}\times\mathrm{Acc})$ *is well-founded;*
2. *there is a disjunctively well-founded transition invariant for* $\mathcal{R}_\mathcal{P}$.

Proof. "$\Uparrow$": If 2 holds, then $R^+ \cap (\mathrm{Acc} \times \mathrm{Acc})$ is well-founded. Then for every $G \in \mathsf{cl}(\mathcal{G}_{\mathcal{P}})$

$$\Phi(G) \cap R^+ \cap (\mathrm{Acc} \times \mathrm{Acc}) \subseteq R^+ \cap (\mathrm{Acc} \times \mathrm{Acc}),$$

is well-founded.

"$\Downarrow$": If 1 holds, then by Corollary 35 we obtain the thesis. ◀

To conclude observe that the condition (1) in the previous theorem is strictly weaker than being SCT. To put otherwise: using a transition invariant, we may prove terminating some programs $\mathcal{R}_{\mathcal{P}}$ which are while-if translation of non-SCT tail-recursive programs $\mathcal{P}$. The following basic example explains why.

▶ **Example 37.** Let us consider the following functional program:

$$\begin{aligned} f(x,y) := &\text{if } (x > y) \quad x \\ &\text{else } \tau : f(x+1, y). \end{aligned}$$

It is not SCT since G_τ is idempotent and has no decreasing edges. In particular $\Phi(G)$ is not well-founded. However $\Phi(G) \cap R^+$ is and therefore this program satisfies the condition (1) of Theorem 36, therefore in particular it is terminating.

7 Conclusions

In this work we presented an intuitionistic proof of the SCT* Theorem. This is not the first intuitionistic proof of the SCT Theorem. Vytiniotis, Coquand and Wahlsteldt in [20] intuitionistically proved it by using Almost-Full relations. A binary relation R over a set S is almost-full if the set of finite sequences $x_0, x_1, \ldots, x_n$ on S, such that for no $i < j \leq n$ $x_i R x_j$ holds, is inductively well-founded. Classically, the set of almost-full relations R is the set of relations such that the complement of the inverse of R is H-well-founded. However, we need De Morgan's Law to prove this equivalence. Therefore it is not evident whether the H-closure Theorem may be intuitionistically derived from the Almost-full Theorem, or the other way round. The proof of the SCT Theorem in [20] uses the following facts:

- almost-full relations are closed under finite intersections;
- if R and T are two binary relations such that $T \cap R^{-1} = \emptyset$ and R is almost-full, then T is well-founded.

In our intuitionistic proof, instead, we use H-well-founded relations and:

- H-well-founded relations are closed under finite unions;
- if a binary relation R is H-well-founded and transitive then it is well-founded.

In [6] we showed that we may provide an intuitionistic proof of the Termination Theorem by replacing the use of Ramsey's Theorem for pairs with the use of the H-closure Theorem. In this paper we did the same for the SCT Theorem. Since Ramsey's Theorem for pairs is used in many branches of mathematics, in future works we hope to apply this method to other classical results based on it, in order to obtain intuitionistic proofs.

We proved that the functions which are computed by a tail-recursive SCT* program are exactly the primitive recursive functions. This result fits in with the one by Ben-Amram [3]: he proved that the SCT programs compute primitive recursive functions. More in details, for any tail-recursive SCT program we provided some primitive recursive bound to the number of computation steps given an input. However as discussed in Section 5 the bound obtained in this way is large. An open question is whether we may extract from the intuitionistic proof of the SCT* Theorem a bound stricter than this one.

Acknowledgements. I would like to thank Stefano Berardi for his careful readings, remarks and corrections, and the anonymous referees for their very helpful suggestions.

References

1 Peter Aczel. *Handbook of Mathematical Logic*, volume 90 of *Studies in Logic and the Foundations of Mathematics*, chapter An introduction to inductive definitions, pages 739–782. Elsevier, 1977.

2 Thorsten Altenkirch. A formalization of the strong normalization proof for system F in LEGO. In *TLCA*, pages 13–28, 1993.

3 Amir M. Ben-Amram. General size-change termination and lexicographic descent. In Torben Mogensen, David Schmidt, and I. Hal Sudborough, editors, *The Essence of Computation: Complexity, Analysis, Transformation. Essays Dedicated to Neil D. Jones*, volume 2566 of *LNCS*, pages 3–17. Springer-Verlag, 2002.

4 Stefano Berardi, Paulo Oliva, and Silvia Steila. Proving termination with transition invariants of height omega. *CoRR*, abs/1407.4692, 2014.

5 Stefano Berardi and Silvia Steila. Ramsey theorem for pairs as a classical principle in intuitionistic arithmetic. In *TYPES*, pages 64–83, 2013.

6 Stefano Berardi and Silvia Steila. Ramsey theorem as an intuitionistic property of well founded relations. In *RTA-TLCA*, pages 93–107, 2014.

7 Stefano Berardi, Silvia Steila, and Keita Yokoyama. Notes on H-closure. In preparation.

8 Byron Cook, Andreas Podelski, and Andrey Rybalchenko. Abstraction refinement for termination. In *SAS*, pages 87–101, 2005.

9 Thierry Coquand. A direct proof of Ramsey's Theorem. Author's website, revised in 2011, 1994.

10 Paul Erdős and George Szekeres. A combinatorial problem in geometry. *Compositio Mathematica*, 2:463–470, 1935.

11 Diego Figueira, Santiago Figueira, Sylvain Schmitz, and Philippe Schnoebelen. Ackermannian and primitive-recursive bounds with Dickson's Lemma. In *LICS*, pages 269–278. IEEE Press, 2011.

12 Alfons Geser. Relative termination. PhD thesis, Universitat Passau, 1990.

13 Matthias Heizmann, Neil D. Jones, and Andreas Podelski. Size-change termination and transition invariants. In *SAS*, pages 22–50, 2010.

14 Chin Soon Lee, Neil D. Jones, and Amir M. Ben-Amram. The size-change principle for program termination. In *POPL*, pages 81–92, 2001.

15 M.H. Löb and S.S. Wainer. Hierarchies of number-theoretic functions. i. *Arch. Math. Logic*, 13(1-2):39–51, 1970.

16 David Park. Concurrency and automata on infinite sequences. In *Proceedings of the 5th GI-Conference on Theoretical Computer Science*, pages 167–183. Springer-Verlag, 1981.

17 Lawrence C. Paulson. Constructing recursion operators in intuitionistic type theory. *J. of Symb. Comp.*, 2(4):325–355, 1986.

18 Andreas Podelski and Andrey Rybalchenko. Transition invariants. In *LICS*, pages 32–41, 2004.

19 Frank Plumpton Ramsey. On a problem in formal logic. *Proc. London Math. Soc.*, 30:264–286, 1930.

20 Dimitrios Vytiniotis, Thierry Coquand, and David Wahlstedt. Stop when you are almost-full – adventures in constructive termination. In *ITP*, pages 250–265, 2012.