Size-Change Termination in Reverse Mathematics

Emanuele Frittaion

(joint work with Silvia Steila and Keita Yokoyama)

TAMC 2017

Outline

Termination analysis

- The **verification problem** may be stated as follows: we aim to find an automatic procedure that, given any program, verifies whether or not a given property holds of the program.
- **Termination** in general is undecidable, but sometimes we can tell when a program terminates.
- **Size-change termination** is a property that can be automatically verified and ensures termination.

Termination analysis

$$\begin{aligned}\mathrm{Ack}(m,n) = \;& \textbf{if } m = 0 \textbf{ then } n+1 \\ & \textbf{else if } n = 0 \textbf{ then } \tau_0 : \mathrm{Ack}(m-1, 1) \\ & \textbf{else } \tau_1 : \mathrm{Ack}(m-1, \tau_2 : \mathrm{Ack}(m, n-1))\end{aligned}$$

τ_0, τ_1, τ_2 are the calls of Ack.

Question:

How do we prove that Ack terminates?

Reverse mathematics

Reverse mathematics is a program in the foundations of mathematics. Main question:

What do we need to prove a given theorem?

We formalize theorems in second order arithmetic Z_2, a (first order) theory that extends Peano arithmetic by adding comprehension axioms (for this we need variables for sets of natural numbers)

$$\exists X \forall n (n \in X \iff \varphi(n))$$

and see what we **need** to prove something. Essentially, we need A to prove B if A is equivalent to B (over a **base** system $\subseteq \mathsf{Z}_2$). The typical base system of reverse mathematics is RCA_0, basically what we need to have primitive recursion (the provably total functions of RCA_0 are exactly the primitive recursive ones).

SCT framework

- We consider first-order functional programs. A program is a list of finitely many equations of the form:

$$f(x_0, \ldots, x_{n-1}) = e^f$$

  where e^f is an **expression**.

- A program P specifies an **initial function** f. The idea is that P computes the function $f : \mathbb{N}^n \to \mathbb{N}$, where n is the arity of f.

SCT framework

Expression:

$$
\begin{array}{rll}
\mathrm{Par} \ni x & \text{parameter} & \\
\mathrm{Fun} \ni f & \text{function identifier} & \\
\mathrm{Op} \ni f & \text{primitive operator} & \\
a & \text{arithmetic expression} & ::= \; x \mid x+1 \mid x-1 \mid f(a, \ldots, a) \\
b & \text{boolean expression} & \\
 & ::= \; x = 0 \mid x = 1 \mid x < y \mid x \leq y \mid b \wedge b \mid b \vee b \mid \neg b & \\
e & \text{expression} & ::= \; a \mid \textbf{if } b \textbf{ then } e \textbf{ else } e
\end{array}
$$

SCT framework

- Suppose that in the definition of f

$$f(x_0, \ldots, x_{n-1}) = e^f$$

there is a call τ to a function g

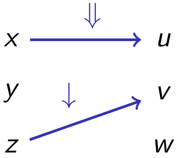
$$\tau : g(e_0, \ldots, e_{m-1}).$$

A **state transition** is given by $(f, \mathbf{u}) \rightarrow_\tau (g, \mathbf{v})$, where

  - $\mathbf{u} = (u_0, \ldots, u_{n-1}) \in \mathbb{N}^n$, $\mathbf{v} = (v_0, \ldots, v_{m-1}) \in \mathbb{N}^m$
  - $\mathbf{v}$ are the values obtained by $e_0, \ldots, e_{m-1}$ when we compute f on input $\mathbf{u}$

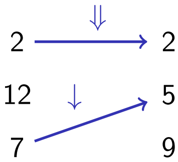
SCT framework

- A **size-change graph** $G : f \to g$ describes a transition relation $\to_G$.
- Formally, $G : f \to g$ is a bipartite graph on $(\mathrm{Par}(f), \mathrm{Par}(g))$.
- $G : f \to g$ looks like:



- f is the **source** function of G and g is the **target** function of G.

SCT framework



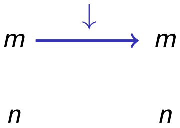
SCT framework

- A **description** of P is a set $\mathcal{G} = \{G_\tau : f \to g \mid \tau : f \to g\}$
- A description $\mathcal{G}$ of P is **safe** if the transition relation induced by every G_τ is compatible with the transition relation of P, i.e., if $\tau : f \to g$ is a call and $(f, \mathbf{u}) \to_\tau (g, \mathbf{v})$ then $(f, \mathbf{u}) \to_{G_\tau} (g, \mathbf{v})$

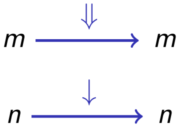
SCT framework

$$\begin{aligned}\mathrm{Ack}(m,n) = {} & \textbf{if } m = 0 \textbf{ then } n+1 \\ & \textbf{else if } n = 0 \textbf{ then } \tau_0 : \mathrm{Ack}(m-1,1) \\ & \textbf{else } \tau_1 : \mathrm{Ack}(m-1, \tau_2 : \mathrm{Ack}(m, n-1))\end{aligned}$$

Description of τ_0 and τ_1



Description of τ_2



SCT framework

- A **multipath** M of $\mathcal{G}$ is a sequence $G_0, \ldots, G_n, \ldots$ such that $G_i \in \mathcal{G}$ and the target function of $G_i : f \to g$ coincides with the source function of $G_{i+1} : g \to h$ for all i.
- An **infinite descent** in an infinite multipath M is a sequence of parameters

  $$x_t, x_{t+1}, x_{t+2}, \ldots, x_i, \ldots$$

  such that $x_i \to x_{i+1} \in G_i$ and for infinitely many i we have $x_i \xrightarrow{\downarrow} x_{i+1} \in G_i$.
- A description $\mathcal{G}$ is **SCT** if every infinite multipath contains an infinite descent

Proving termination

Theorem (SCT soundness; Lee, Jones, Ben Amram 2001)

Let $\mathcal{G}$ be a safe description of a program P. If $\mathcal{G}$ is SCT then P is terminating.

Proof.

If P does not terminate then there exists an infinite state transition sequence. From the corresponding multipath we can extract an infinite descending sequence in $\mathbb{N}$. □

Question:

What do we need to prove the SCT criterion? (work in progress)

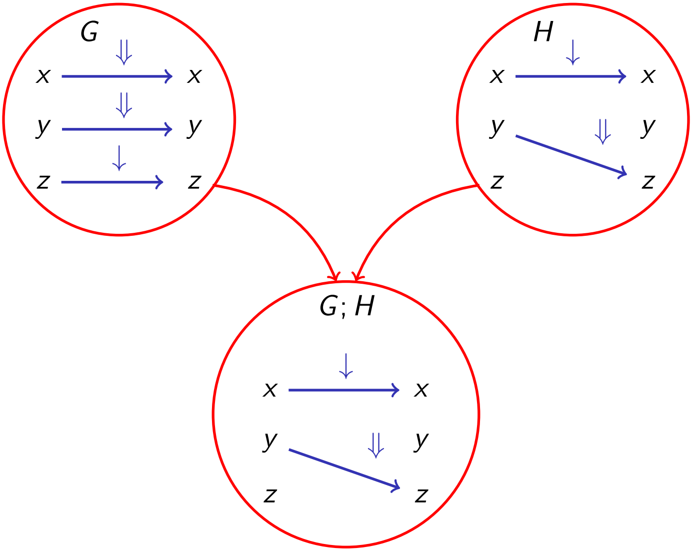
Proving termination

Ack has a safe SCT description. It is easy to verify that every infinite multipath contains an infinite descent.

Deciding SCT

Even though SCT is not even arithmetical, it is equivalent to a decidable property.

Deciding SCT



Deciding SCT

- In $G; H$ the composition of two edges $x \stackrel{\Downarrow}{\rightarrow} y$ and $y \stackrel{\Downarrow}{\rightarrow} z$ is the edge $x \stackrel{\Downarrow}{\rightarrow} z$. In all other cases the composition of two edges from x to y and from y to z is the edge $x \stackrel{\downarrow}{\rightarrow} z$.
- A size-change graph G is **idempotent** if $G; G = G$.
- Given a $\mathcal{G}$, $\mathrm{cl}(\mathcal{G})$ is the smallest set which contains $\mathcal{G}$ and is closed under composition.

Deciding SCT

Theorem (SCT criterion; Lee, Jones, Ben Amram 2001)
Let $\mathcal{G}$ be a description of P. Then $\mathcal{G}$ is SCT iff every idempotent $G \in \mathrm{cl}(\mathcal{G})$ has an arc $x \xrightarrow{\downarrow} x$.

Question:

> *What do we need to prove the SCT criterion?*

Classical proof: Ramsey's theorem for pairs.

Proving SCT criterion

- RCA_0: axioms of arithmetic, Σ^0_1-induction, Δ^0_1-comprehension.
- WKL_0: RCA_0, weak König's lemma
- ACA_0: RCA_0, arithmetical comprehension.
- ATR_0: ACA_0, $X^{(\alpha)}$ exists
- Π^1_1-CA_0: ACA_0, Π^1_1-comprehension.

Γ-induction: for any $\varphi(x)$ in Γ,

$$(\varphi(0) \wedge \forall n(\varphi(n) \implies \varphi(S(n)))) \implies \forall n \varphi(n)$$

Γ-comprehension: for any $\varphi(x)$ in Γ,

$$\exists X \forall n(n \in X \iff \varphi(n))$$

Proving SCT criterion

(RT^1_k) For any $c\colon \mathbb{N} \to k$ there exists $i < k$ such that $c(x) = i$ for infinitely many x

(RT^1) $\forall k \in \mathbb{N}\ \mathrm{RT}^1_k$

(RT^2_k) For any $c : [\mathbb{N}]^2 \to k$ there exists an infinite homogeneous set $X \subseteq \mathbb{N}$, that is $c''[X]^2$ is constant

(RT^2) $\forall k \in \mathbb{N}\ \mathrm{RT}^2_k$

Proving SCT criterion

(Triang_k) For any coloring $c : [\mathbb{N}]^2 \to k$ there exist $i \in k$ and $t \in \mathbb{N}$ such that $c(t, m) = c(t, l) = c(m, l) = i$ for infinitely many pairs $\{m, l\}$

(Triang) $\forall k \in \mathbb{N}\ \mathrm{Triang}_k$

(SPP_k) For any coloring $c\colon \mathbb{N} \to k$ there exists $I \subseteq k$ such that $i \in I$ iff $i < k$ and $c(x) = i$ for infinitely many x

(SPP) $\forall k \in \mathbb{N}\ \mathrm{SPP}_k$

Proving SCT criterion

Theorem (Frittaion, Steila, Yokoyama 2016)

Over RCA_0*:*

- Triang *implies the SCT criterion.*
- *SCT criterion implies* SPP*.*
- $\mathsf{I}\Sigma^0_2$ *implies* Triang*.*

Therefore, we need $\mathsf{I}\Sigma^0_2$ to prove the SCT criterion.

Proving SCT criterion

- One direction of the SCT criterion is already provable in RCA_0 (from multipath SCT to idempotent SCT). One just needs the finite pigeonhole principle. Note that the (full) finite Ramsey's theorem is provable in RCA_0.
- The implication $\mathrm{Triang} \implies$ SCT criterion is basically (but not quite) the original proof.
- The implication $\mathsf{I}\Sigma^0_2 \implies \mathrm{Triang}$ follows from general results.
  - RT^2 is Π^1_1-conservative over $\mathsf{B}\Sigma^0_3$ (Yokoyama and Slaman, unpublished).
  - $\mathsf{B}\Sigma^0_3$ is $\widetilde{\Pi}^0_4$-conservative over $\mathsf{I}\Sigma^0_2$.
  - Triang is $\widetilde{\Pi}^0_4$.

Proving SCT criterion

Sketch of the reversal: SCT criterion $\implies$ SPP.

Warm-up. Suppose we want to show that for every finite coloring $c : \mathbb{N} \to k$ there exists an infinite color, that is, some color $i < k$ such that $c(x) = i$ for infinitely many x.

- Our $\mathcal{G}$ consists of k size-change graphs $G_0, G_1, \ldots, G_{k-1}$ on parameters $z_0, z_1, \ldots, z_{k-1}$.
- The graph G_i has a deacreasing edge $z_i \xrightarrow{\downarrow} z_i$ and a non-increasing edge $z_j \xrightarrow{\Downarrow} z_j$ for every $j \neq i$.

Proving SCT criterion

- Every graph in $\mathrm{cl}(\mathcal{G})$ has an edge $x \overset{\downarrow}{\to} x$. By the SCT criterion, $\mathcal{G}$ is SCT (infinite multipaths have infinite descents)
- Let

$$M = G_{c(0)}, G_{c(1)}, \ldots, G_{c(n)}, \ldots$$

  Say we have an infinite descent starting from parameter z_i. Then the color i is infinite.

Proving SCT criterion

General case. We want to show that for every finite coloring $c : \mathbb{N} \to k$ the set $I^\infty = \{i < k : (\exists^\infty x) c(x) = i\}$ exists.

- We can define for all $x \in \mathbb{N}$ the set $\mathcal{I}_x$ of guesses at stage x. That is, $I \in \mathcal{I}_x$ is a subset of k and $I \subseteq I^\infty$ iff $I \in \mathcal{I}_x$ for infinitely many x.
- We want to define finitely many size-change graphs with the idempotent condition such that any infinite descent in the multipath $M = G_0, G_1, \dots, G_x, \dots$ gives us the right guess, where G_x is defined according to $\mathcal{I}_x$.
- Note that there are finitely many $\mathcal{I} \subseteq \mathcal{P}(k)$.

Proving SCT criterion

- To get the right guess define G_x on parameters z_I for $I \subseteq k$.
- Put a decreasing edge $z_I \xrightarrow{\downarrow} z_I$ if $I \in \mathcal{I}_x$ and $|I|$ is maximal.
- Make sure to put no edge from z_I to z_I if there exists $J \in \mathcal{I}_x$ of bigger size.
- Put no edges from z_I to z_J with I different from J.

Conclusion

Since the SCT criterion is not provable in RCA_0:

- $\mathcal{G}$ is **MSCT** if every infinite multipath has an infinite descent.
- $\mathcal{G}$ is **ISCT** if every idempotent $G \in \mathrm{cl}(\mathcal{G})$ has an arc $x \xrightarrow{\downarrow} x$.

Question:

What do we need to prove that:

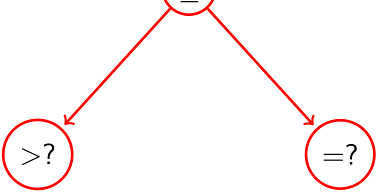
- If P has a safe MSCT description, then P terminates? (MSCT soundness)
- If P has a safe ISCT description, then P terminates? (ISCT soundness)

Conclusion

Hint: SCT programs compute exactly the **multiply-recursive** functions (Ben Amram). The totality of these functions can be proved by using the well-foundedness of $\omega^{\omega^{\omega}}$.

Over RCA_0:

$$\mathsf{WO}(\omega^{\omega^{\omega}}) = \text{ISCT soundness} \geq \text{MSCT soundness} > \mathsf{WO}(\omega^{\omega}).$$



Thanks for your attention.