

Reverse Mathematical Bounds for the Termination Theorem

Silvia Steila

joint work with Keita Yokoyama

University of Bern

Logic, Complexity and Automation

Obergurgl University Center

September 5th, 2016

A first informal question

Assume that a child really likes biscuits, he has z -many biscuits. Assume that his grandmother gave him x -many gold coins and y -many silver coins to buy biscuits by pursuing the following rules at each purchase:

- ▶ the child may spend one silver coin to duplicate his number of biscuits;
- ▶ the child may spend one gold coin and all his silver coins to duplicate his number of biscuits and to get one silver coin for every biscuit he has.

Does the child get infinitely many biscuits?

A first formal question

```
while ( x > 0 AND y > 0 )  
    ( x, y, z ) = ( x, y-1, 2*z )  
OR  
    ( x, y, z ) = ( x-1, 2*z, 2*z )
```

Does this program **terminate** for any x , y and z ?

Transition-based programs

A **transition-based program** $P = (S, I, R)$ 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_2, \dots such that

- ▶ $s_0 \in I$,
- ▶ $(s_{i+1}, s_i) \in R$ for any $i \in \mathbb{N}$.

$$s_i \rightarrow s_{i+1}$$
$$s_{i+1} R s_i$$

The set Acc of **accessible states** is the set of all states which appear in some computation.

Termination Theorem by Podelski and Rybalchenko

- ▶ A program P is **terminating** if its transition relation R restricted to the accessible states is well-founded.
- ▶ A **transition invariant** of a program is a binary relation over program's states which contains the transitive closure of the transition relation of the program; i.e. $T \supseteq R^+ \cap (\text{Acc} \times \text{Acc})$.
- ▶ A relation is **disjunctively well-founded** if it is a finite union of well-founded relations.

Theorem (Podelski and Rybalchenko 2004)

The program P is terminating if and only if there exists a disjunctively well-founded transition invariant for P .

Termination Theorem by Podelski and Rybalchenko

- ▶ A program P is **terminating** if its transition relation R restricted to the accessible states is well-founded.
- ▶ A **transition invariant** of a program is a binary relation over program's states which contains the transitive closure of the transition relation of the program; i.e. $T \supseteq R^+ \cap (\text{Acc} \times \text{Acc})$.
- ▶ A relation is **disjunctively well-founded** if it is a finite union of well-founded relations.

Theorem (Podelski and Rybalchenko 2004)

R is well-founded if and only if there exist $k \in \mathbb{N}$ and k -many well-founded relations R_0, \dots, R_{k-1} such that $R_0 \cup \dots \cup R_{k-1} \supseteq R^+$.

An answer

```
while ( x > 0 AND y > 0 )  
    ( x, y, z ) = ( x, y-1, 2*z )  
OR  
    ( x, y, z ) = ( x-1, 2*z, 2*z )
```

A transition invariant for this program is $R_1 \cup R_2$, where

$$R_1 := \{(\langle x', y', z' \rangle, \langle x, y, z \rangle) \mid y > 0 \wedge y' < y\}$$

$$R_2 := \{(\langle x', y', z' \rangle, \langle x, y, z \rangle) \mid x > 0 \wedge x' < x\}$$

Since each R_i is well-founded, then the program **terminates**.

A second question

```
while ( x > 0 AND y > 0 )  
    ( x, y, z ) = ( x, y-1, 2*z )  
OR  
    ( x, y, z ) = ( x-1, 2*z, 2*z )
```

How many **steps** before the program terminates?

I.e. how many **biscuits** can the child get?

Infinite Ramsey Theorem for pairs

If you have \mathbb{N} -many people at a party then either there exists an infinite subset whose members all know each other or an infinite subset none of whose members know each other.

Theorem (Ramsey 1930)

For any $k \in \mathbb{N}$ and for every k -coloring $c : [\mathbb{N}]^2 \rightarrow k$, there exists an infinite **homogeneous** set H , i.e. there exists $h < k$, such that for any distinct $x, y \in H$, $c(\{x, y\}) = h$.

Complete disorder is impossible

Theodore Samuel Motzkin

How many steps before the program terminates?

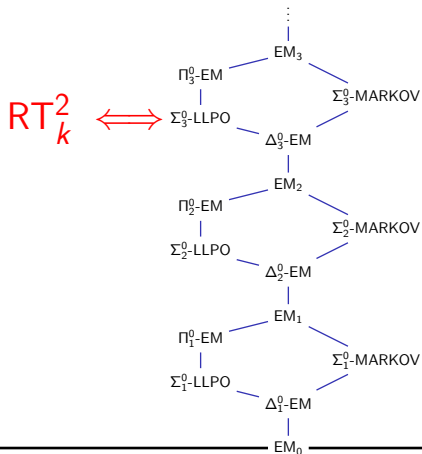
Hard to say, because Ramsey's Theorem is a purely **classical** result. Indeed,

- ▶ In 1969 Specker proved there is one recursive coloring in two colors with **no** recursive infinite homogeneous sets.

- ▶ In 1972 Jockusch proved that it is **not** even possible to recursively find a color for which there is an infinite homogeneous set.

Ramsey's Theorem in the hierarchy of classical principles

Classical Logic



H-closure Theorem

A binary relation R is **H-well-founded** there are no infinite decreasing transitive R -sequences.

Theorem (Berardi and S. 2014)

For any $k \in \mathbb{N}$, if R_0, \dots, R_{k-1} are H-well-founded relations, then $R_0 \cup \dots \cup R_{k-1}$ is H-well-founded.

- ▶ H-closure Theorem is **classically true**, because there exists a simple (i.e. within RCA_0) classical proof of the equivalence between Ramsey's Theorem and H-closure Theorem.
- ▶ By considering the inductive definition of well-foundedness, this result is **intuitionistically provable**.

An intuitionistic proof of the Termination Theorem

Assume that there exists a disjunctively well-founded transition invariant, namely

$$R_0 \cup \dots \cup R_{k-1} \supseteq R^+,$$

- ▶ then R_i is H-well-founded for each $i < k$;
 - ▶ hence $R_0 \cup \dots \cup R_{k-1}$ is H-well-founded;
 - ▶ therefore R^+ is H-well-founded and transitive;
 - ▶ so it is well-founded, and then also R is.
- H-closure

Bounds from H-closure Theorem

A **weight function** for a binary relation $R \subseteq S^2$ is a function $f : S \rightarrow \mathbb{N}$ such that for any $x, y \in S$

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

\mathcal{A} = the class of functions computable by a program for which there exists a disjointively well-founded transition invariant whose relations have **primitive recursive weight functions**.

Proposition (Berardi, Oliva and S. 2014)

$$\mathcal{A} = \text{PR}$$

Might a Reverse Mathematical approach help?

- ▶ Which **bounds** may we get by using Reverse Mathematical tools?
- ▶ (Gasarch) Is there a natural example showing that the Termination Theorem **requires** the full Ramsey Theorem for pairs?
- ▶ (Gasarch) Is the Termination Theorem **equivalent** to Ramsey's Theorem for pairs?

Reverse Mathematics

Given a theorem of ordinary mathematics, what is the weakest subsystem of **second order arithmetic** in which it is provable?

- ▶ RCA_0 : axioms of arithmetic, Σ_1^0 -induction, Δ_1^0 -comprehension.
- ▶ WKL_0 : RCA_0 , Σ_1^0 -separation.
- ▶ ACA_0 : RCA_0 , arithmetical comprehension.
- ▶ ATR_0 : ACA_0 , Σ_1^1 -separation.
- ▶ 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 ,

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

Γ -separation: for any $\psi(x), \varphi(x)$ in Γ which are exclusive,

$$\exists X \forall n((\psi(n) \implies n \in X) \wedge (\varphi(n) \implies n \notin X)).$$

The H -closure Theorem in the Ramsey's zoo

- ▶ R is **well-founded** if there are no infinite R -decreasing sequences.
- ▶ R is **inductively well-founded** if every element in S belongs to every R -inductive set.
- ▶ RT_k^2 . For any $c : [\mathbb{N}]^2 \rightarrow k$, there exists an infinite **homogeneous** set; i.e. there exist $h \in k$ and an infinite $H \subseteq \mathbb{N}$ such that for any two elements x and y in H we have $c(x, y) = h$.
- ▶ k -HCT. Given k -many inductively H -well-founded relations, their union is inductively H -well-founded.

Theorem (S. and Yokoyama 2015)

$$\text{RCA}_0 \vdash \forall k (k\text{-HCT} \iff \text{RT}_k^2).$$

Consequences of Ramsey's Theorem for pairs in two colors

- ▶ WRT_k^2 . For any $c : [\mathbb{N}]^2 \rightarrow k$, there exists an infinite **weakly homogeneous** set; i.e. there exist $h \in k$ and $H = \{x_i : i \in \mathbb{N}\} \subseteq \mathbb{N}$ such that for any $i \in \mathbb{N}$ $c(x_i, x_{i+1}) = h$.
- ▶ **CAC**. Every infinite poset has an infinite chain or antichain.
- ▶ **ADS**. Every infinite linear ordering has an infinite ascending or descending sequence.

$$\begin{aligned} \text{RCA}_0 < \text{ADS} = \text{WRT}_2^2 \leq \text{WRT}_3^2 \leq \dots \\ \leq \text{WRT}_k^2 \leq \text{CAC} < \text{RT}_2^2 = \dots = \text{RT}_k^2. \end{aligned}$$

The Termination Theorem in the Ramsey's zoo

- ▶ WRT_k^2 . For any $c : [\mathbb{N}]^2 \rightarrow k$, there exists an infinite **weakly homogeneous** set; i.e. there exist $h \in k$ and $H = \{x_i : i \in \mathbb{N}\} \subseteq \mathbb{N}$ such that for any $i \in \mathbb{N}$ $c(x_i, x_{i+1}) = h$.
- ▶ **CAC**. Every infinite poset has an infinite chain or antichain.
- ▶ k -**TT**. For any relation R , if there exist R_0, \dots, R_{k-1} such that they are well-founded and $R_0 \cup \dots \cup R_{k-1} \supseteq R^+$, then R is well-founded.

Theorem (S. and Yokoyama 2015)

$$\text{RCA}_0 \vdash \forall k (k\text{-TT} \iff \text{WRT}_k).$$

Answers to questions posed by Gasarch

Theorem (Hirschfeldt and Shore 2007)

CAC plus full induction does not imply RT_2^2 .

Since CAC plus full induction proves $\forall k$ k -TT:

- ▶ Is there a natural example showing that the Termination Theorem requires the full Ramsey Theorem for pairs? **NO!**
- ▶ Is the Termination Theorem equivalent to Ramsey's Theorem for pairs? **NO!**

Hence, which **bounds** may we get by using Reverse Mathematical tools?

Bounds and H-bounds

Let R be a binary relation on S .

- ▶ A **weight function** for R is a function $f : S \rightarrow \mathbb{N}$ such that for any $x, y \in S$

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

- ▶ A **bound** for R is a function $f : S \rightarrow \mathbb{N}$ such that for any R -decreasing sequence $a_{l-1}R \dots Ra_0$, $l \leq f(a_0)$.
- ▶ A **H-bound** for R is a function $f : S \rightarrow \mathbb{N}$ such that for any R -decreasing **transitive** sequence $a_{l-1}R \dots Ra_0$, $l \leq f(a_0)$.

Weight function, bounds, H-bounds

Proposition

In RCA_0 . For any relation $R \subseteq S^2$. If R has a **weight function** then R has a **bound**.

Proposition

The following are equivalent over RCA_0 .

1. WKL_0 .
2. For any relation $R \subseteq S^2$, R has a **bound** then R has a **weight function**.

$R = \{(n+1, n) \mid n \in \mathbb{N}\}$ has no **bound**, but $f : \mathbb{N} \rightarrow \mathbb{N}$ such that $f(n) = 2$ is a **H-bound** for R !

Reverse mathematical bounds

Theorem (Parson 1970 / Paris and Kirby 1977 / Chong, Slaman and Yang 2012)

The class of provable recursive functions of $WKL_0 + CAC$ is exactly the same as the class of primitive recursive functions.

Consequence

Any relation R generated by a **primitive recursive transition function** for which there exist k -many relations R_0, \dots, R_{k-1} with **primitive recursive weight functions** such that $R_0 \cup \dots \cup R_{k-1} \supseteq R^+$ has a **primitive recursive bound**.

Another question

Summing up, if we assume that R, R_0, \dots, R_{k-1} are such that:

- ▶ R is the graph of a primitive recursive function;
- ▶ R_i has a primitive recursive weight function;
- ▶ $R_0 \cup \dots \cup R_{k-1} \supseteq R^+$;

Then R has a primitive recursive bound.

Is there a **correspondence** between the **complexity** of the bound and

- ▶ k ?
- ▶ the **complexity** of the weight functions for R_0, \dots, R_{k-1} ?

Paris-Harrington Theorem for pairs

For given $k \in \mathbb{N}$,

- ▶ PH_k^{*2} : for any infinite set $X \subseteq \mathbb{N}$ and any coloring function $c : [X]^2 \rightarrow k$, there exists a **homogeneous** set H for c such that $\min H < |H|$.
- ▶ WPH_k^{*2} : for any infinite set $X \subseteq \mathbb{N}$ and any coloring function $c : [X]^2 \rightarrow k$, there exists a **weakly homogeneous** set H for c such that $\min H < |H|$.

Fast Growing Hierarchy

Let F_k be the usual k -th **fast growing function** defined as

$$\begin{cases} F_0(x) = x + 1, \\ F_{h+1}(x) = F_h^{(x+1)}(x). \end{cases}$$

Let $\text{Tot}(F_k)$ denote the **totality** of F_k :

$$\forall a \exists b (F_k(a) = b).$$

Let $k\text{-TT}^h$ for weight functions (respectively bounds or H-bounds) be the following statement:

Assume that R, R_0, \dots, R_{k-1} are such that:

- ▶ R is the graph of a function below F_h ;
- ▶ R_i has a weight function (respectively bound or H-bound) below F_h ;
- ▶ $R_0 \cup \dots \cup R_{k-1} \supseteq R^+$.

Then R has a bound.

With Keita Yokoyama, we proved that there is an equivalence over RCA_0^*

- ▶ between $k\text{-TT}^h$ for weight functions, $k\text{-TT}^h$ for bounds and some restricted version of WPH_k^{*2} ($\text{WPH}_k^{h,2}$).
- ▶ $k\text{-TT}^h$ for H-bounds and some restricted version of PH_k^{*2} ($\text{PH}_k^{h,2}$).

From transition invariants to bound

Theorem (Solovay and Ketonen 1981)

In RCA_0^* . $\text{Tot}(F_{k+h+5}) \implies \text{PH}_k^{h,2}$.

Consequence

For any $R, R_0, \dots, R_{k-1} \subseteq \mathbb{N}^2$ such that

- ▶ R is the graph of a function below F_h ,
- ▶ R_i has a H-bound below F_h ;
- ▶ $R_0 \cup \dots \cup R_{k-1} \supseteq R^+$.

R is bounded by F_{k+h+5} .

Is it possible to improve it?

In 2011 Figueira D., Figueira S, Schmitz and Schnoebelen observed that the Termination Theorem is a consequence of **Dickson's Lemma**

Theorem (Dickson 1913)

For any natural number k , every infinite sequence σ of elements in \mathbb{N}^k is **good**; i.e. for any infinite sequence σ of elements in \mathbb{N}^k there exist natural numbers $n < m$ such that $\sigma(n) \leq \sigma(m)$.

Note that given a transition-based program $P = (S, I, R)$, for which there is k -disjunctively well-founded transition invariant composed of relations with weight functions we can define a map:

$$\begin{array}{lcl} \sigma : S & \longrightarrow & \mathbb{N}^k \\ s & \longmapsto & (f_0(s), \dots, f_{k-1}(s)) \end{array} \quad s_i \rightarrow s_{i+1}$$

where f_i is a weight function of R_j .

Any **computation** is mapped in a **bad sequence**!

$$\begin{array}{l} s_{i+1} R_h s_i \\ f_h(s_{i+1}) < f_h(s_i) \\ \sigma(s_i) > \sigma(s_{i+1}) \end{array}$$

Bounding bad sequences

Figueira D., Figueira S., Schmitz and Schnoebelen, provided a bound for the length of the **bad** sequences. As a corollary

Theorem (Figueira D., Figueira S., Schmitz and Schnoebelen 2011)

For any $R, R_0, \dots, R_{k-1} \subseteq \mathbb{N}^2$ such that

- ▶ R is the graph of a function **below** F_h ;
- ▶ R_i has bound **below** F_h ;
- ▶ $R_0 \cup \dots \cup R_{k-1} \supseteq R^+$;

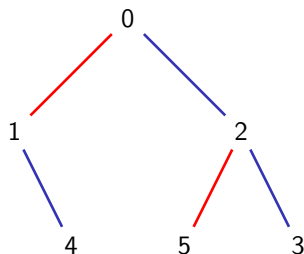
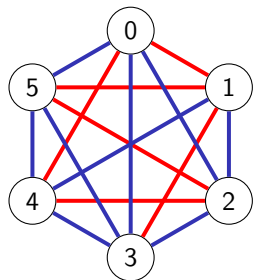
R is bounded by $F_{k+\max\{1, h-1\}}$.

Consequence

In RCA_0^* . $\text{Tot}(F_{k+\max\{1, h-1\}}) \implies \text{WPH}_k^{h,2}$.

Erdős' trees

Assume given a sequence $\langle 0, \dots, 5 \rangle$ such that the coloring between its elements is as follows.



If $x \prec_E y \prec_E z$, then $c(\{x, y\}) = c(\{x, z\})$.

And for H-bounds?

By looking for bounds via Erdős' tree.

Theorem (S. 2015)

In RCA_0^* . For any $R, R_0, \dots, R_{k-1} \subseteq \mathbb{N}^2$ such that

- ▶ R is the graph of a function below F_h ;
- ▶ R_i has a H-bound below F_h ;
- ▶ $R_0 \cup \dots \cup R_{k-1} \supseteq R^+$;

R is bounded by $F_{k+\max\{1, h-1\}}$.

Consequence

In RCA_0^* . $\text{Tot}(F_{k+\max\{h-1, 1\}}) \implies \text{PH}_k^{h, 2}$.

Example of OPTIMAL bounds

```
while (x > 0 AND y > 0)
  if(y > 1)
    (x,y,z) = (x, y-1, 2*z)
  else
    (x,y,z) = (x-1, 2*z, 2*z)
```

A transition invariant for this program is $R_1 \cup R_2$, where

$R_1 := \{(\langle x', y', z' \rangle, \langle x, y, z \rangle) \mid y > 0 \wedge y' < y\}$ Bounded by F_0

$R_2 := \{(\langle x', y', z' \rangle, \langle x, y, z \rangle) \mid x > 0 \wedge x' < x\}$ Bounded by F_0

Then R is well-founded, and R is bounded by F_{2+1} !

It is optimal since for any $x \geq y > 0$, the computation which starts in $(x, y, 1)$ has length greater than $F_2^{x-2}(y)$!

From bounds to transition invariants

Theorem (S. and Yokoyama 2015)

Let $k \in \mathbb{N}$. In RCA_0^* for any **deterministic** binary relation $R \subseteq \mathbb{N}^2$, R is bounded by F_k only if there exists $R_0, \dots, R_{k+1} \subseteq \mathbb{N}^2$ such that $R^+ \subseteq R_0 \cup \dots \cup R_{k+1}$ and each R_i is **bounded** by F_0 .

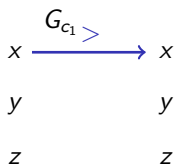
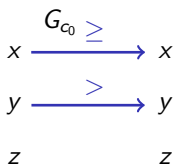
Theorem (S. and Yokoyama 2015)

Let $k \in \mathbb{N}$. In RCA_0^* for any binary relation $R \subseteq \mathbb{N}^2$, R is bounded by F_k only if there exists $R_0, \dots, R_{k+1} \subseteq \mathbb{N}^2$ such that $R^+ \subseteq R_0 \cup \dots \cup R_{k+1}$ and each R_i is **H-bounded** by F_0 .

Size-Change Termination programs

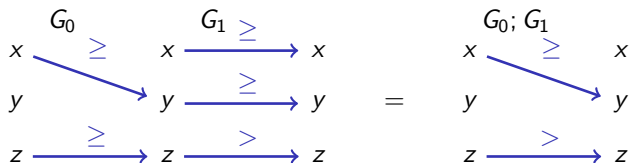
A functional program is **SCT** if for every sequence of calls: the sequence is infinite implies there is some **infinite descent** (i.e. weakly decreasing sequence of values which is strictly decreasing infinitely many times).

```
f(x,y,z) = if (y > 1) c0: f(x,y-1, 2*z)
           else      c1: f(x-1,2*z,2*z).
```



Size-Change Termination Theorem

A size-change graph G is **idempotent** if $G; G = G$, where



Theorem (Lee, Jones, Ben-Amram 2001)

A program is SCT if and only if every idempotent size-change graph of the program has an edge $x \xrightarrow{>} x$.

What we are doing **now**

A **reverse mathematical analysis** of SCT (on going work with Emanuele Frittaion and Keita Yokoyama).

Since the Ackermann function is SCT, it seems that **higher induction** should be use to prove termination from SCT.

What we are doing **now**

A **reverse mathematical analysis** of SCT (on going work with Emanuele Frittaion and Keita Yokoyama).

Since the Ackermann function is SCT, it seems that **higher induction** should be use to prove termination from SCT.

Thank you!