Effective Bounds on the Podelski-Rybalchenko Termination Theorem

Stefano Berardi, Paulo Oliva, and Silvia Steila

Università degli studi di Torino, Queen Mary University of London

PSC

Vienna Summer of Logic 2014

July 17, 2014

Termination Theorem by Podelski and Rybalchenko

- Transition invariants are used by Podelski and Rybalchenko to prove the termination of a program.
- 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. $T \supseteq R^+ \cap (\mathrm{Acc} \times \mathrm{Acc})$.
- A relation is disjunctively well-founded if it is a finite union of well-founded relations.

Theorem (Termination Theorem)

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

Example

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

A transition invariant for this program is $T_1 \cup T_2 \cup T_3$, where

$$T_1 := \{(\langle x, y\rangle, \langle x', y'\rangle) \mid x > 0 \land x' < x\}$$
$$T_2 := \{(\langle x, y\rangle, \langle x', y'\rangle) \mid x + y > 0 \land x' + y' < x + y\}.$$
$$T_3 := \{(\langle x, y\rangle, \langle x', y'\rangle) \mid y > 0 \land y' < y\}$$

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

The proof by Podelski and Rybalchenko requires Ramsey Theorem

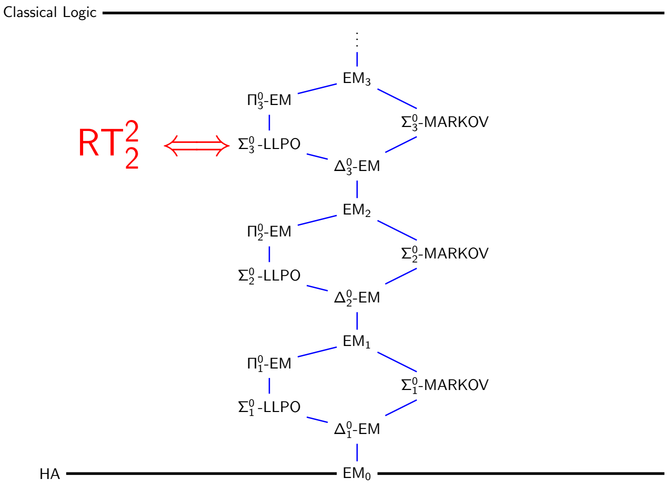
If you have ω people at a party then either there exists an infinite subset whose members all know each other or an infinite subset none of whose members know each other.

Theorem (Ramsey for pairs)

Let $n \in \mathbb{N}$. For any coloring over the edges with n-many colors of the complete graph on $\mathbb{N}$ ($c : \mathbb{N}^2 \to n$), there exists an infinite homogeneous set.

Where a set X is homogeneous with respect a coloring over the edges if every two nodes are connected with the same color.

Ramsey Theorem is a purely classical result.



In the papers

"Stop when you are almost-full - adventures in constructive termination"

and

"Ramsey Theorem as an intuitionistic property of well founded relations"

two proofs of an intuitionistic version of this theorem have been proposed. Here the notion of program being terminating is replaced by an intuitionistically weaker but classically equivalent notion, based on inductively well-foundedness.

Theorem

The program P is (inductively) terminating iff there exists a disjunctively (inductively) well-founded transition invariant for P.

In this result both the hypothesis and the thesis are intuitionistically weaker than the original ones.

In this work we want to intuitionistically prove Podelski and Rybalchenko Termination Theorem considering the classical definition of well-foundedness.

Theorem

Given a program P, with transition relation R, if

$$\exists n \; \exists T_1, \ldots, T_n \; \exists \omega_1, \ldots, \omega_n \; (T_1 \cup \cdots \cup T_n \supseteq R^+ \cap (\mathsf{Acc} \times \mathsf{Acc}) \\ \wedge \; \forall i \in [1, n] \; (\forall \alpha \; \exists j < \omega_i(\alpha) \; \neg(\alpha_j T_i \alpha_{j+1})))$$

then there exists Φ *such that*

$$\forall \alpha \; (\alpha_0 \in S \implies \exists m < \Phi(\bar{T}, \bar{\omega}, \alpha) \; \neg(\alpha_m R \alpha_{m+1})).$$

Transitive Ramsey Theorem

Assume $n = 2$.

Theorem (Infinite Erdős-Szerkeres Theorem)

Let $c : \mathbb{N}^2 \to 2$, then there exists an infinite homogeneous chain.

Proof.

Consider a coloring $c : \mathbb{N}^2 \to 2$. Given a well ordered set X we say that s is the leftmost sequence of X if and only if $s_i \in X$ and

- $s_0 = \min X$;
- $s_{i+1} > s_i$;
- $c(\{s_i, s_{i+1}\}) = 0$;
- $\forall x \in X(s_i < x < s_{i+1} \implies c(\{s_i, x\}) \neq 0)$.

Transitive Ramsey Theorem

Assume $n = 2$.

Theorem (Infinite Erdős-Szerkeres Theorem)

Let $c : \mathbb{N}^2 \to 2$, then there exists an infinite homogeneous chain.

Proof.

Then Blackwell constructs a sequence of sequences as follows:

- w_0 is the leftmost sequence of $\mathbb{N}$.
- w_i is the leftmost sequence of $\mathbb{N} \setminus \bigcup\{w_j : j < i\}$.

Transitive Ramsey Theorem

Assume $n = 2$.

Theorem (Infinite Erdős-Szerkeres Theorem)

Let $c : \mathbb{N}^2 \to 2$*, then there exists an infinite homogeneous chain.*

Proof.

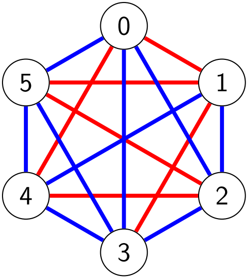
Since $\mathbb{N}$ is infinite, thanks to the Pigeonhole Principle we have either an infinite sequence or infinitely many finite sequences.

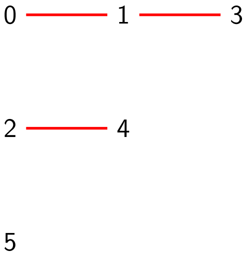
- In the first case we are done.
- In the second case let $\langle b_i : i \in \mathbb{N} \rangle$ be the sequence of the last elements of the sequences w_i. Since it is an infinite sequence of natural numbers we can extract an infinite increasing subsequence. By construction this is an infinite homogeneous set in color 1.

□

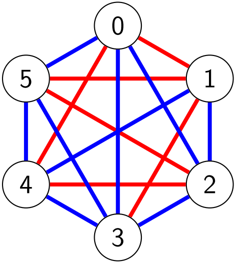
The idea is to consider finite approximations of the tree given by the leftmost sequences of the Blackwell's proof, and work with these approximations.

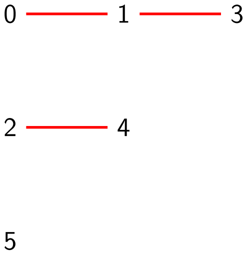
So given a finite sequence s we can define by primitive recursion a function φ which produces the Blackwell's structure.



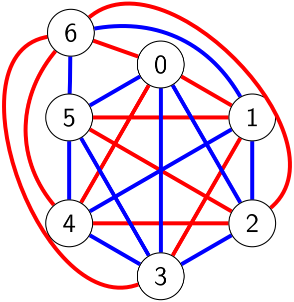


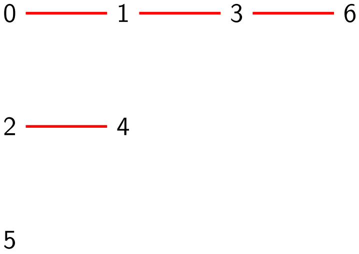
Then we must consider a large enough approximation of the Blackwell tree, so as to make sure that we obtain a counter-example.



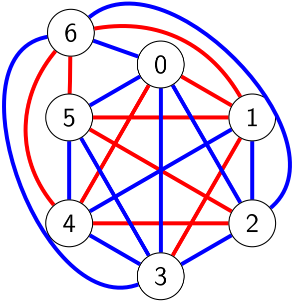


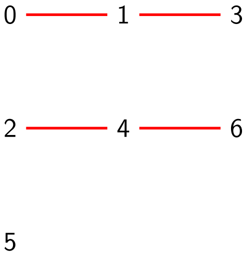
Then we must consider a large enough approximation of the Blackwell tree, so as to make sure that we obtain a counter-example.



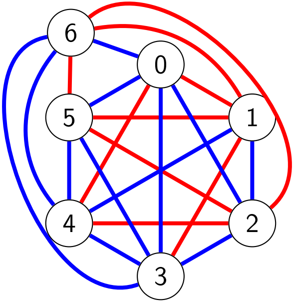


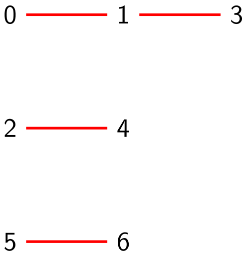
Then we must consider a large enough approximation of the Blackwell tree, so as to make sure that we obtain a counter-example.



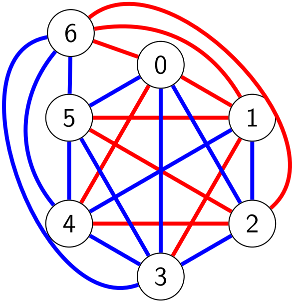


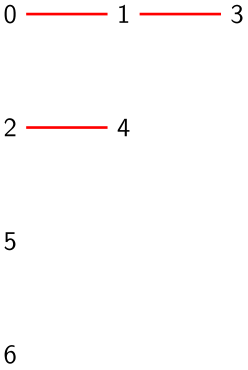
Then we must consider a large enough approximation of the Blackwell tree, so as to make sure that we obtain a counter-example.





Then we must consider a large enough approximation of the Blackwell tree, so as to make sure that we obtain a counter-example.





The following function ξ will check whether it is enough to consider the first m elements of a given sequence α.

Definition

Given α and n let $\varphi(\emptyset, \langle 0, \ldots, m \rangle) = \langle w_i \rangle_{i \leq k}$. Define

$$\begin{aligned} \xi(\alpha, m) &= \begin{cases} m & \text{if } \exists i \leq k(\omega_0(\hat{w}_i) < |w_i|) \\ & \quad \vee\ \omega_1(\sigma(\hat{b})) < |\sigma(b)| \\ \xi(\alpha, m+1) & \text{otherwise} \end{cases} \\ \Phi(\alpha) &= \xi(\alpha, 0). \end{aligned}$$

Where b is the sequence of the last elements of the w_i and $\sigma(b)$ is the increasing subsequence of b starting with the first element.

This function as defined is not primitive recursive!

Is $\Phi(\alpha)$ in T?

- $\Phi(\alpha)$ computes the finite Blackwell's structure $M(\alpha) = \langle w_i \rangle_{i \leq k}$, where each w_i is a maximal Blackwell's leftmost sequence.
- $\Phi(\alpha)$ returns an integer which guarantees that the length of α is finite.
- The definition of $\Phi(\alpha)$ uses the given modulus ω_0, ω_1.

We claim that if ω_0, ω_1 are in T, then also $\Phi(\alpha)$ is.

Is $\Phi(\alpha)$ in T?

We claim that if ω_0, ω_1 are in T, then also $\Phi(\alpha)$ is.

- Firstly we prove that given a sequence γ satisfying certain conditions, we can compute the structure M by primitive recursion.
- Then we will approximate γ via Bar Recursion, and we will prove that such γ is in T.

Therefore $\Phi(\alpha)$ is!

The construction of M given an oracle γ

$$A(i,k,X) := k > i \ \wedge \ c(\{i,k\}) = 0 \ \wedge \ k \notin X.$$

Assume that for any finite set of integers X we have a sequence $\gamma(X)$ such that for all $i \in \mathbb{N}$:

$$\exists k A(i,k,X) \iff A(i,\gamma(X)(i),X) \ \wedge \ \forall j < \gamma(X)(i) \neg A(i,j,X).$$

We can prove that given such sequence the construction of $M(\alpha)$ is effective.

The construction of M given an oracle γ

The idea is the following:

- Let $\gamma^k(X)(i)$ be defined as

$$\gamma^0(X)(i) = i;$$
$$\gamma^{k+1}(X)(i) = \gamma(X \cup \bigcup_{h \leq k} \{\gamma^h(X)(i)\})(\gamma^k(X)(i));$$

- Then we can define the sequence

$$i, \gamma^1(X)(i), \dots, \gamma^k(X)(i), \dots.$$

- By primitive recursion we can find a prefix w of such sequence such that $\omega_0(w) < |w|$.
- So we can build the white Blackwell's sequences. Moreover by considering the increasing subsequence of the last elements, again by primitive recursion we can find a maximal prefix t of such sequence such that $\omega_1(t) < |t|$.

Approximating γ via Bar Recursion

Recall that

$$A(i, k, X) := k > i \ \wedge \ c(i, k) = 0 \ \wedge \ k \notin X.$$

Let $q, \omega : \mathbb{N}^{\mathbb{N}} \to \mathbb{N}$ be such that $q(\gamma) = \omega(\gamma)$ is the greatest element in the finite structure $M(\alpha)$.

Our goal is to build a finite approximation of γ such that for any $i \leq \omega\gamma$:

$$\exists k < q\gamma A(i, k, X) \iff A(i, \gamma(X)(i), X) \ \wedge \ \forall j < \gamma(X)(i) \neg A(i, j, X).$$

And this can be done, by using the product of selection functions and the main theorem of Spector's bar recursion.

Approximating γ via Bar Recursion

Switchtenberg in 1979 proved that each functional defined by Bar Recursion of type 0 or 1 by using primitive recursive functional, is primitive recursive as well.

Thanks to Schwichtenberg's result, by assuming that ω_0 and ω_1 are in T, and since γ is defined by Bar Recursion of type 1, we can conclude that γ is in T and so also $\Phi(\alpha)$ is.

This result can be generalized with n relations.

- Firstly we need to generalize Blackwell's proof for n colors. But it can be done quite easily by induction.
- Then we can define Φ_n as follows:

$$\begin{aligned} \xi_n(\alpha, m) &= \begin{cases} m & \text{if } \exists i \leq k(\omega_0(w_i) < |w_i|) \\ & \quad \vee \ \Phi_{n-1}(\sigma(b)) < |\sigma(b)| \\ \xi_n(\alpha, m+1) & \text{otherwise} \end{cases} \\ \Phi_n(\alpha) &= \xi_n(\alpha, 0). \end{aligned}$$

Since Φ_{n-1} is in T, by using the same argument we used in the case with 2 relations we obtain that also Φ_n is in T.

References

P. Blackwell. An alternative Proof of a Theorem of Erdős and Szekeres. The American Mathematical Monthly, 1971

H. Schwichtenberg. On bar recursion of types 0 and 1. J.S.L., 1979

A. Podelski, A. Rybalchenko. Transition Invariants. LICS, 2004

M.H. Escardó, P. Oliva. Computational interpretations of analysis via products of selections functions. CiE, 2010

Coquand. A direct proof of Ramsey's Theorem. Author's website, 2011

D. Vytiniotis, T.Coquand, D. Wahlstedt. Stop when you are almost-full-adventures in constructive termination. ITP, 2012

P.Oliva, T.Powell. A constructive Interpretation of Ramsey's Theorem via the Product of Selection Functions. Math. Struct. in Comp. Science, 2012

S. Berardi, S. Steila. Ramsey Theorem for pairs as a classical principle in Intuitionistic Arithmetic. Types Post-proceedings, 2013

S. Berardi, S. Steila. Ramsey Theorem as an intuitionistic property of well founded relations. RTA-TLCA, 2014