An intuitionistic version of Ramsey Theorem and its use in Program Termination

DOI:10.1016/j.apal.2015.08.002

Ramsey Theorem as an Intuitionistic Property of Well Founded Relations

Stefano Berardi and Silvia Steila

Dipartimento di Informatica, Università di Torino
{stefano,steila}@di.unito.it

Abstract. Ramsey Theorem for pairs is a combinatorial result that cannot be intuitionistically proved. In this paper we present a new form of Ramsey Theorem for pairs we call H-closure Theorem. H-closure is a property of well-founded relations, intuitionistically provable, informative, and simple to use in intuitionistic proofs. Using our intuitionistic version of Ramsey Theorem we intuitionistically prove the Termination Theorem by Poldenski and Rybalchenko. This theorem concerns an algorithm inferring termination for while-programs, and was originally proved from the classical Ramsey Theorem, then intuitionistically, but using an intuitionistic version of Ramsey Theorem different from our one. Our long-term goal is to extract effective bounds for the while-programs from the proof of Termination Theorem, and our new intuitionistic version of Ramsey Theorem is designed for this goal.

Keywords: Intuitionism, Ramsey Theorem, inductive definitions, termination of while-programs.

1 Introduction

Podelski and Rybalchenko [1] defined an algorithm taking in input an imperative program made with the instructions **while**, **if** and assignment, and able to decide in some case whether the program is terminating or not, and in some other cases leaving the question open. The authors prove a result they call the Termination Theorem, stating the correctness of their algorithm. The authors use in their proof Ramsey Theorem for pairs [2], from now on called just "Ramsey" for short. Ramsey is a classical result that cannot be intuitionistically proved: we refer to [3] for a detailed analysis of the minimal classical principle required to prove Ramsey. According to the Π^0_2-conservativity of Classical Analysis w.r.t. Intuitionistic Analysis [4], the proof of Termination Theorem hides some effective bounds for the while program which the theorem shows to terminate. Our long-term goal is to find them, by first turning the proof of Termination Theorem into an intuitionistic proof.

Our first step is to formulate a version of Ramsey which has a purely intuitionistic proof, that is, a proof which does not use Excluded Middle, nor Brouwer Thesis nor Choice. Our version of Ramsey is informative, in the sense that it has no negation, while it has a disjunction. We say that a relation R

G. Dowek (ed.): RTA-TLCA 2014, LNCS 8560, pp. 93–107, 2014.

is H-well-founded if the tree of all R-decreasing transitive sequences is well-founded. We express Ramsey as a property of well-founded relations, saying that H-well-founded relations are closed under finite unions. For short we will call this statement the *H-closure Theorem*. Thus, we are able to split the proof of Ramsey into two parts: the intuitionistic proof of the H-closure Theorem, followed by an easy classical proof of the equivalence between Ramsey and the H-closure Theorem.

The result closest to H-closure we could find is by Coquand [5]. Coquand, as Veldman and Bezem did before him [6], considers *almost full relations* and proves that they are closed under finite *intersections*. Veldman and Bezem use Choice Axiom of type 0 (if $\forall x \in \mathbb{N}.\exists y \in \mathbb{N}.C(x, y)$, then $\exists f : \mathbb{N} \to \mathbb{N}.\forall x \in \mathbb{N}.C(x, f(x)))$ and Brouwer's thesis. Coquand's proof, instead, is purely intuitionistic, and it may be used to give a purely intuitionistic proof of the Termination Theorem [7]. However, it is not evident what are the effective bounds hidden in Coquand's proof of Termination Theorem. If we compare H-closure with the Almost Full Theorem, in the most recent version by Coquand [5], we find no easy way to intuitionistically deduce one from the other, due to the use of de' Morgan laws to move from the definition of almost full to the definition of H-closure. H-closure is in a sense more similar to the original Ramsey Theorem, because it was obtained from it with just one classical step, a contrapositive (see §2), while almost fullness requires one application of de' Morgan Law, followed by a contrapositive. We expect that H-closure, hiding one application less of de' Morgan laws, should be a version of Ramsey simpler to use in intuitionistic proofs and for extracting bounds.

Our motivation for producing a new intuitionistic version of Ramsey is to provide a new intuitionistic proof of the Termination Theorem. We expect that, by analysing this new proof, we will be able to extract effective bounds from the Termination Theorem, and possibly, from other concrete applications of Ramsey.

This is the plan of the paper. In section 2 we present Ramsey Theorem for pairs and we informally introduce H-closure. In section 3 we formally define inductive well-foundedness and H-well-foundedness, whose main properties are stated in section 4. The goal of section 5 is to present what we call Nested Fan Theorem, which is a part of the proof of the H-closure Theorem, as shown in section 6. In section 7 we intuitionistically prove the Termination Theorem. In section 8 we compare our result with the previous works along the same line and we draw some conclusions. Unless explicitly stated, our proofs use intuitionistic second order arithmetic, without Choice Axiom, Brouwer Thesis, Bar-Induction.

2 Ramsey Theorem and a Variant of It, *H*-Closure

We first recall the statement of Ramsey Theorem for pairs, just Ramsey for short. Assume G is a countable non-oriented graph which is complete, i.e., between any two different elements of G there is exactly one edge in G. Assume we "colored" the edges of G with $n > 0$ different colors, that is, we partioned the edges of G into n sets. Then there is an infinite set $X \subseteq G$ such that all the edges between any two different $x, y \in X$ have the same color: for some $k = 1, \ldots, n$, all the edges of X fall in the k-th subset of the partition. We call X an *homogenous* set of color k.

Assume $\sigma = x_0, x_1, \ldots, x_n, \ldots$ is an injective enumeration of the elements of G, that is: $G = \mathtt{range}(\sigma)$. We represent a non-oriented edge, between two points x_i, x_j in G with $j < i$, by the pair (i, j), arbitrarily oriented from i to j. The opposite edge from x_j to x_i is the same edge of G, and it is again represented with (i, j). Thus, a partition of edges in n sets $S_1, \ldots, S_n$ may be represented by a partition of the set $\{(x_i, x_j) : j < i\}$ into n binary relations $S_1, \ldots, S_n$. Therefore one possible formalization of Ramsey is the following.

Theorem 1 (Ramsey for pairs [2]). *Assume I is a set having some injective enumeration $\sigma = x_0, x_1, \ldots, x_i, \ldots$. Assume $S_1, \ldots, S_n$ are binary relations on I which are a partition of $\{(x_i, x_j) \in I \times I : j < i\}$, that is:*

1. $S_1 \cup \cdots \cup S_n = \{(x_i, x_j) \in I \times I : j < i\}$
2. *for all* $1 \leq k < h \leq n$: $S_k \cap S_h = \emptyset$.

Then for some $k = 1, \ldots, n$ there exists some infinite $X \subseteq \mathbb{N}$ such that: $\forall i, j \in X.(j < i \implies x_i S_k x_j)$.

In the statement above three assumptions may be dropped.

1. First of all, we may drop the assumption that $S_1, \ldots, S_n$ are pairwise disjoint. Suppose we do. Then, if we set $S'_1 = S_1$, $S'_2 = S_2 \backslash S'_1$, $S'_3 = S_3 \backslash (S'_1 \cup S'_2)$, $\ldots$, we obtain a partition $S'_1, \ldots, S'_n$ of $\{(x_i, x_j) : j < i\}$. Therefore there exists a $k = 1, \ldots, n$ and some infinite $X \subseteq \mathbb{N}$, such that $\forall i, j \in X.(j < i \implies x_i S'_k x_j)$, and with more reason, $\forall i, j \in X.(j < i \implies x_i S_k x_j)$.
2. Second, we may drop the assumption "σ is injective" (in this case, $\mathtt{range}(\sigma)$ may be a finite set). Assume we do. Then, if we set $S'_k = \{(i, j) : x_i S_k x_j\}$ for all $k = 1, \ldots, n$, we obtain n relations $S'_1, \ldots, S'_k$ on $\mathbb{N}$, whose union is the set $\{(i, j) \in \mathbb{N} \times \mathbb{N} : j < i\}$. Therefore there exists a $k = 1, \ldots, n$ and some infinite $X \subseteq \mathbb{N}$, such that $\forall i, j \in X.(j < i \implies i S'_k j)$, and with more reason, $\forall i, j \in X.(j < i \implies x_i S_k x_j)$.
3. Third, we may drop the assumption that σ is an enumeration of I. Suppose we do. Then, if we restrict $S_1, \ldots, S_n$ to $I_0 = \mathtt{range}(\sigma)$, we obtain some binary relations $S'_1, \ldots, S'_n$ on I_0 such that $S'_1 \cup \ldots \cup S'_n = \{(x_i, x_j) \in I_0 \times I_0 : j < i\}$. Again, we conclude that there exists some $k = 1, \ldots, n$ and some infinite $X \subseteq \mathbb{N}$, such that $\forall x_i, x_j \in X.(j < i \implies x_i S'_k x_j)$, and with more reason, $\forall i, j \in X.(j < i \implies x_i S_k x_j)$.

Summing up, we showed that, classically, we may restate Ramsey Theorem as follows:

For all sequences $\sigma = x_0, x_1, x_2, \ldots$ on I, if $\forall i, j \in \mathbb{N}.(j < i \implies x_i(S_1 \cup \ldots \cup S_n)x_j)$, then for some k there is some infinite $X \subseteq \mathbb{N}$, such that $\forall i, j \in X.(j < i \implies x_i S_k x_j)$.

It is likely that even this statement cannot be intuitionistically proved, because the sequence τ is akin to an homogeneous set, and there is no effective way to produce homogeneous sets (see for instance [3]). By taking the contrapositive, we obtain the following corollary:

If for all $k = 1, \dots, n$, all sequences $\tau = y_0, \dots, y_n, \dots$ such that $\forall i, j \in \mathbb{N}.(j < i \implies y_i S_k y_j)$ are finite, then all sequences $\sigma = x_0, \dots, x_n, \dots$ such that $\forall i, j \in \mathbb{N}.(j < i \implies x_i(S_1 \cup \ldots \cup S_n)x_j)$ are finite.

It is immediate to check that, classically, this is yet another version of Ramsey. We call this property *classical H-closure*.

Let us call $H(S)$ the set of all lists such that $1 \leq j < i \leq n$ implies $x_i S x_j$. Then classical H-closure may be restated as follows: if $S_1, \dots, S_n$ are binary relations over some set I, and $H(S_1), \dots, H(S_k)$ are sets of lists well-founded by extension, then $H(S_1 \cup \ldots \cup S_k)$ is a set of list well-founded by extension. Thus, classical H-closure is a property classically equivalent to Ramsey Theorem, but which is about well-founded relations. In Proof Theory, there is plenty of examples of classical proofs of well-foundedness which are turned into intuitionistic proofs, and indeed from H-closure we will obtain an intuitionistic version of Ramsey.

There is a last step to be done. We call *intuitionistic H-closure*, or just H-closure for short, the statement obtained by replacing, in classical H-closure, the classical definition of well-foundedness (all decreasing sequences are finite) with the inductive definition of well-foundedness, which is customary in intuitionistic logic. We will recall the inductive definition of well-foundedness in §3.1: thus, for the formal definition of H-well-foundedness we have to wait until §3.2.

3 Well-Founded Relations

In this section we introduce the main objects we will deal with in this paper: well-founded relations.

We will use $I,\ J,\ \dots$ to denote sets, $R,\ S,\ T,\ U$ will denote binary relations, $X,\ Y,\ Z$ will be subsets, and $x,\ y,\ z,\ t,\ \dots$ elements. We identify the properties $P(\cdot)$ of elements of I with their extensions $X = \{x \in I : P(x)\} \subseteq I$.

Let R be a binary relation on I. Classically $x \in I$ is R-well-founded if there is no infinite decreasing R-chain $\dots x_n R x_{n-1} R \dots x_1 R x_0 = x$ from x in I. Classically R is well-founded if and only if every $x \in I$ is R-well-founded.

The inductive definition of well-founded relations is more suitable than the classical one in the intuitionistic proofs. In the first subsection we introduce this definition; in the last subsection we present the definition of H-well-foundedness, which is fundamental to state the new intuitionistic form of Ramsey Theorem.

3.1 Intuitionistic Well-Founded Relations

The intuitionistic definition of well-founded relation uses the definition of inductive property. For short we will say that a relation is "well-founded" to say that it is intuitionistically well-founded.

Let R be a binary relation on I. A property is R-inductive if whenever it is true for all R-predecessors of a point it is true for the point. $x \in I$ is

R-well-founded if and only if it belongs to every R-inductive property; R is well-founded if every x in I is R-well-founded. Formally:

Definition 1. *Let R be a binary relation on I.*

- *A property $X \subseteq I$ is* R-inductive *if and only if* IND_X^R*; where* $\mathrm{IND}_X^R := \forall y.\,(\forall z.\,(zRy \implies z \in X) \implies y \in X)$.
- *An element $x \in I$* is R-well-founded *if and only if* $\mathrm{WF}^R(x)$*; where* $\mathrm{WF}^R(x) := \forall X.\,\big(\mathrm{IND}_X^R \implies x \in X\big)$.
- R is well-founded *if and only if* $\mathrm{WF}(R)$*; where* $\mathrm{WF}(R) := \forall x.\,\mathrm{WF}^R(x)$.

A binary structure, just a *structure* for short, is a pair (I, R), where R is a binary relation on I. We say that (I, R) is well-founded if R is well-founded.

We need to introduce also the notion of co-inductivity. A property X is R-co-inductive in $y \in I$ if it satisfies the inverse property of R-inductive: if the property X holds for a point, then it holds also for all its R-predecessors. Formally:

Definition 2. *Let R be a binary relation on I.*

- *A property X is* R-co-inductive in $y \in I$ *if and only if* $\mathrm{CoIND}_X^R(y)$*; where*
$$\mathrm{CoIND}_X^R(y) := \forall z.\,(zRy \implies z \in X)\,.$$
- *A property X is* R-co-inductive *if and only if* CoIND_X^R*; where*
$$\mathrm{CoIND}_X^R := \forall y.(y \in X \implies \forall z.\,(zRy \implies z \in X)).$$

In general we will intuitionistically prove that if there exists an infinite decreasing R-chain from x then x is not R-well-founded. Classically, and by using the Axiom of Choice, x is R-well-founded if and only if there are no infinite decreasing R-chains from x, and R is well-founded if and only if there are no infinite decreasing R-chains in I.

3.2 *H*-Well-Founded Relations

In order to define H-well-foundedness we need to introduce some notations. We denote a list on I with $\langle x_1, \dots, x_n\rangle$; $\langle\rangle$ is the empty list. We define the operation of concatenation of two lists on I in the natural way as follows: $\langle x_1, \dots, x_n\rangle * \langle y_1, \dots, y_m\rangle = \langle x_1, \dots, x_n, y_1, \dots, y_m\rangle$. We define the relation of one-step expansion $\succ$ between two lists $(L,\ M)$ on the same I, as $L \succ M \iff L = M*\langle y\rangle$, for some y.

Definition 3. *Let R be a binary relation on I.*

- *$H(R)$ is the set of the R-decreasing transitive finite sequences on I:*
$$\langle x_1, \dots, x_n\rangle \in H(R) \iff \forall i, j \in [1, n].i < j \implies x_j R x_i.$$
- *R is H-well-founded if $H(R)$ is $\succ$-well-founded.*

H-well-founded relations are more common than well-founded relations.

Proposition 1. *1. R well-founded implies that R H-well-founded.*
2. R H-well-founded and R transitive imply that R well-founded

4 Basic Properties of Well-Founded Relations

There are several methods to intuitionistically prove that a binary relation R is well-founded by using the well-foundedness of another binary relation S.

The goal of this section is to prove these results. In §4.1 we are going to define simulation relations, in §4.2 we introduce some operations which preserve well-foundedness, while in §4.3 we will show the main properties of well-foundedness.

4.1 Simulation Relations

A simulation relation is a binary relation which correlates two other binary relations.

Definition 4. *Let R be a binary relation on I and S be a binary relation on J. Let T be a binary relation on $I \times J$.*

- *Domain of T.* $\mathrm{dom}(T) = \{x \in I : \exists y \in J.xTy\}$.
- *Morphism. $f : (I, R) \to (I, S)$ is a morphism if f is a function such that $\forall x, y \in I.xRy \implies f(x)Sf(y)$.*
- *Simulation. T is a simulation of R in S if and only if it is a relation and*

$$\forall x, z \in I.\forall y \in J. ((xTy \wedge zRx) \implies \exists t \in J. (tSy \wedge zTt))$$

- *Total simulation. A simulation relation T of R in S is total if* $\mathrm{dom}(T) = I$.
- *Simulable. R is simulable in S if there exists a* total *simulation relation T of R in S.*

If we have a simulation T of R in S and xTy holds, we can transform each finite decreasing R-chain in I from x in a finite decreasing S-chain in J from y. By using the Axiom of Choice this result holds also for infinite decreasing R-chains from a point in $\mathrm{dom}(T)$. Then if there are no infinite decreasing S-chains in J there are no infinite decreasing R-chains in $\mathrm{dom}(T)$. If, furthermore, the simulation is total there are no infinite decreasing R-chains in I. By using classical logic and the Axiom of Choice we may conclude that if S is well-founded and T is a total simulation relation of R in S then R is well-founded. In the last subsection of this section we will present an intuitionistic proof of this result that does not use the Axiom of Choice.

We may see binary relations as abstract reduction relations. Recall that an abstract reduction relation is a simply binary relation (for example rewriting relations). A reduction relation is said to be terminating or strongly normalizing if and only if there are no infinite chains [8]. Observe that we use simulation to prove well foundedness and this is the same method used for labelled state transition systems [9]; for us all the set of labels is a singleton.

4.2 Some Operations on Binary Structures

In this subsection we introduce some operations mapping binary structures into binary structures. In §4.3 we prove that these operations preserves well-foundedness.

The first operation is the successor operation (adding a top element).

Definition 5. *Let R be a relation on I and let $\top$ be an element not in I. We define the relation $R+1 = R \cup \{(x, \top) : x \in I\}$ on $I+1 = I \cup \{\top\}$. We define the successor structure of (I, R) as $(I, R) + 1 = (I+1, R+1)$.*

Another operation on binary structures is the relation defined by components, inspired by the order by components.

Definition 6. *Let R be a binary relation on I, and let S be a binary relation on J. The relation $R \otimes S$ of components R, S is defined as below:*

$$R \otimes S := (R \times \mathrm{Diag}(J)) \cup (\mathrm{Diag}(I) \times S) \cup (R \times S),$$

where $\mathrm{Diag}(X) = \{(x, x) : x \in X\}$.

Equivalently $R \otimes S$ is defined for all $x, x' \in I$ and for all $y, y' \in J$ by:

$$(x, y) R \otimes S (x', y') \iff$$
$$((xRx') \wedge (y = y')) \vee ((x = x') \wedge (ySy')) \vee ((xRx') \wedge (ySy')) .$$

If R, S are orderings then $R \otimes S$ is the componentwise ordering, also called the product ordering. In this case $R \otimes S = R \times S$, while in general $R \otimes S \supseteq R \times S$.

4.3 Properties of Well-Foundedness

Now we may list the main intuitionistic properties of well-founded relations.

Proposition 2. *Let R be a binary relation on I, and let S be a binary relation on J.*

1. *Well-foundedness is both an inductive and a co-inductive property:*

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

2. *If R, S are well-founded, then $R \otimes S$ is well-founded.*
3. *If T is a simulation of R in S and if xTy and y is S-well-founded, then x is R-well-founded.*
4. *If T is a simulation of R in S and S is well-founded, then $\mathrm{dom}(T)$ is R-well-founded.*
5. *If R is simulable in S and S is well-founded, then R is well-founded.*
6. *If $f : (I, R) \to (J, S)$ is a morphism and if S is well-founded, then R is well-founded.*
7. *If R is included in S and S is well-founded then R is well-founded.*

Corollary 1. *Let R be a binary relation on I. (I, R) well-founded implies that $(I, R) + 1$ well-founded.*

Corollary 2. *Let R be a binary relation on I and $x \in I$. If there exists an infinite decreasing R-chain from x, then x is not R-well-founded.*

So the intuitionistic definition of well-founded intuitionistically implies the classical definition; while the other implication is purely classical.

When I and R are finite, we may characterize the well-foundedness and the H-well-foundedness in an elementary way.

Definition 7. *Let R be a binary relation on I and $x \in I$. A finite sequence $\langle x_0, \dots, x_n \rangle$ is an R-cycle from x if $n > 0$ and*

$$x = x_n R x_{n-1} R x_{n-2} R \dots R x_0 = x.$$

If $n = 1$ (that is, if xRx), we call the R-cycle an R-loop.

Proposition 3. *Assume $I = \{x_1, \dots, x_k\}$ for some $k \in \mathbb{N}$. Let R be any binary relation on I.*

1. *R is well-founded if and only if there are no R-cycles.*
2. *R is H-well-founded if and only if there are no R-loops.*

Thanks to Proposition 3 we may prove H-closure Theorem if $R_1, \dots, R_n$ are relations over a finite set I. In fact $R = (R_1 \cup R_2 \cup \dots \cup R_n)$ is H-well-founded if and only if there are no R-loops. This is equivalent to: there are no R_i-loops for any $i \in [1, n]$. Hence R is H-well-founded if and only if for each $i \in [1, n]$, R_i is H-well-founded.

Now we want to prove H-closure Theorem for any set I.

5 An Intuitionistic Version of König's Lemma

In this section we deal with binary trees. In the first part we introduce binary trees with some equivalent definitions, while in the second part we use binary trees to prove an intuitionistic version of König Lemma for nested binary trees (binary trees whose nodes are themselves binary trees), which we call Nested Fan Theorem. As in the classical case [3], there is a strong link between intuitionistic Ramsey Theorem and Nested Fan Theorem.

5.1 Binary Trees

Let R be a binary relation. Then we can define the set of all binary trees where each child node is in relation R with its father node. If R is well-founded, this set will be well-founded with respect to the relation "one-step extension" between trees.

A finite binary tree may be defined in many ways, the most common runs as follows.

Definition 8. *A finite binary tree on I is defined inductively as an empty tree, called* Nil*, or a triple composed by one element of I and two trees, called immediate subtrees: so we have* $\mathrm{Tr} = \mathrm{Nil}$ *or* $\mathrm{Tr} = \langle x, \mathrm{Tr}_1, \mathrm{Tr}_2 \rangle$.

$$\mathrm{BinTr} = \{\mathrm{Tr} : \mathrm{Tr} \ \textit{is a binary tree}\ \}$$

Let $\mathrm{Tr} = \langle x, \mathrm{Tr}_1, \mathrm{Tr}_2 \rangle$, then

- Tr is a tree with root x;
- if $\mathrm{Tr}_1 = \mathrm{Tr}_2 = \mathrm{Nil}$, we will say that Tr is a leaf-tree;
- if $\mathrm{Tr}_1 \neq \mathrm{Nil}$ and $\mathrm{Tr}_2 = \mathrm{Nil}$, we will say that Tr has exactly one left child;
- if $\mathrm{Tr}_1 = \mathrm{Nil}$ and $\mathrm{Tr}_2 \neq \mathrm{Nil}$, we will say that Tr has exactly one right child;
- if $\mathrm{Tr}_1 \neq \mathrm{Nil}$ and $\mathrm{Tr}_2 \neq \mathrm{Nil}$, we will say that Tr has two children: one right child and one left child.

A binary tree may be also define as a labelled oriented graph on I, empty (if $\mathrm{Tr} = \mathrm{Nil}$) or with a special element, called root, which has exactly one path from the root to any node. Each edge is labelled with a color $c \in C = \{1, 2\}$ in such a way that from each node there is at most one edge in each color.

Equivalently we may define firstly colored lists and then the binary tree as a set of some colored lists.

Definition 9. *A colored list (L, f) is a pair, where $L = \langle x_1, \ldots, x_n \rangle$ is a list on I equipped with a list $f = \langle c_1, \ldots, c_{n-1} \rangle$ on $C = \{1, 2\}$.* nil $= (\langle\rangle, \langle\rangle)$ *is the empty colored list and* $\mathrm{ColList}(C)$ *is the set of the colored lists with colors in C.*

We should imagine that the list L is drawn as a sequence of its elements and that for each $i \in [1, n-1]$ the segment (x_i, x_{i+1}) has color c_i. Observe that if $L = \langle\rangle$ or if $L = \langle x \rangle$, then $f = \langle\rangle$: if there are no edges in L, then there are no colors (L, f).

We use $\lambda, \mu, \ldots$ to denote colored lists in $\mathrm{ColList}(C)$. Let $c \in C$. We define the composition of color c of two colored lists by connecting the last element of the first list (if any) with the first of the second list (if any) with an edge of color c. Formally we set $\mathrm{nil} *_c \lambda = \lambda *_c \mathrm{nil} = \lambda$, and $(L, f) *_c (M, g) = (L*M, f*\langle c \rangle *g)$ whenever $L, M \neq \mathrm{nil}$.

We can define the relation one-step extension on colored lists: $\succ_c$ is the one-step extension of color c and $\succ_{\mathrm{col}}$ is the one-step extension of any color. Assume $C = \{1, 2\}$ and $x \in I$ and $\lambda, \mu \in \mathrm{ColList}(C)$. Then we set:

- $\lambda *_c (\langle x \rangle, \langle\rangle) \succ_c \lambda$.
- $\lambda \succ_{\mathrm{col}} \mu$ if $\lambda \succ_c \mu$ for some $c \in C$.

Now we can equivalently define a binary tree on I as a particular set of some colored lists.

Definition 10. *A binary tree* Tr *is a set of colored lists on I, such that:*

1. nil *is in* Tr*;*
2. *If $\lambda \in \mathrm{Tr}$ and $\lambda \succ_{col} \mu$, then $\mu \in \mathrm{Tr}$;*
3. *Each list in* Tr *has at most one one-step extension for each color $c \in C$: if $\lambda_1, \lambda_2, \lambda \in \mathrm{Tr}$ and $\lambda_1, \lambda_2 \succ_c \lambda$, then $\lambda_1 = \lambda_2$.*

For all sets $\mathcal{L} \subseteq \mathrm{ColList}(C)$ of colored lists, $\mathrm{BinTr}(\mathcal{L})$ *is the set of binary trees whose branches are all in $\mathcal{L}$.*

For instance the empty tree is the set $\mathrm{Nil} = \{\mathrm{nil}\}$. From $(\langle x \rangle, \langle\rangle) \succ_c \mathrm{nil}$ we deduce that there is at most one $(\langle x \rangle, \langle\rangle) \in \mathrm{Tr}$: x is root of Tr. The leaf-tree of root x is equal to $\{(\langle x \rangle, \langle\rangle), \mathrm{nil}\}$. The tree with only one root x and two children y, z is equal to

$$\{(\langle x, y \rangle, \langle 1 \rangle), (\langle x, z \rangle, \langle 2 \rangle), (\langle x \rangle, \langle\rangle), \mathrm{nil}\}\,.$$

The last definition we need is the one-step extension $\succ_T$ between binary trees; $\mathrm{Tr}' \succ_T \mathrm{Tr}$ if Tr' has one leaf more than Tr.

Definition 11 (One-step extension for binary trees). *If* Tr *is a binary tree and* $\lambda \in \mathrm{Tr}$ *and* $\mu \succ_c \lambda$ *and* $\lambda' \succ_c \lambda$ *for no* $\lambda' \in \mathrm{Tr}$*, then*

$$\mathrm{Tr} \cup \{\mu\} \succ_T \mathrm{Tr}$$

5.2 Nested Fan Theorem

König Lemma is a result of classical logic which guarantees that if every branch of a binary tree is finite then the tree is finite.

There exists a corresponding intuitionistic result, intuitionistically weaker than the original one that we may state as follows.

Lemma 1 (Fan Theorem). *Each inductively well-founded binary tree is finite.*

Here we are interested to an intuitionistic version of Fan Theorem for nested trees (trees whose nodes are trees), that we will call Nested Fan Theorem.

Let consider a tree Tr whose nodes are finite binary trees, and whose father/child relation between nodes is the one-step extension $\succ_T$. Classically we may say: if for each branch of Tr the union of the nodes in this branch is a binary tree with only finite branches, then each branch of Tr is finite.

In the intuitionistic proof of the intuitionistic Ramsey Theorem we will use an intuitionistic version of this statement, in which the finitess of the branches is replaced by inductive well-foundedness of branches. Intuitionistic Nested Fan Theorem states that if a set of colored lists $\mathcal{L}$ is well-founded then the set $\mathrm{BinTr}(\mathcal{L})$, of all binary trees whose branches are all in $\mathcal{L}$, is well-founded.

Lemma 2 (Intuitionistic Nested Fan Theorem). *Let* $C = \{1, 2\}$ *be a set of colors and let* $\mathcal{L} \subseteq \mathrm{ColList}(C)$ *be any set of colored lists with all colors in* C*. Then*

$$(\mathcal{L}, \succ_{col}) \text{ is well-founded} \implies (\mathrm{BinTr}(\mathcal{L}), \succ_T) \text{ is well-founded.}$$

Proof (sketch). Let $c \in C$, $\lambda \in \mathrm{ColList}(C)$. We define $\mathrm{BinTr}(\mathcal{L}, \lambda, c)$ as the set of binary trees $\{\mathrm{Tr} \in \mathrm{BinTr}(\mathcal{L}) : \lambda *_c \mathrm{Tr} \subseteq \mathcal{L}\}$. $\mathrm{BinTr}(\mathcal{L}, \lambda, c)$ is the set of trees occurring in some tree of $\mathrm{BinTr}(\mathcal{L})$, as immediate subtree number c of the last node of the branch λ. For instance, $\mathrm{BinTr}(\mathcal{L}, \mathrm{nil}, c) = \mathrm{BinTr}(\mathcal{L})$.

Since $\mathcal{L}$ is well-founded, it can be proved that $(\mathrm{BinTr}(\mathcal{L}, \lambda, c), \succ_T)$ is well-founded for all $\lambda \in \mathcal{L}$ by induction over λ. The thesis will follow if we set $\lambda = \mathrm{nil}$, $c = 1$ (a dummy value).

6 An Intuitionistic Form of Ramsey Theorem

In this section we present a new intuitionistic version of Ramsey Theorem, the H-closure Theorem. In the first part of the section we state it and we prove the easy classical equivalence between it and Ramsey Theorem, in the second part we prove the H-closure Theorem.

6.1 Stating an Intuitionistic Form of Ramsey Theorem

In [3] we proved that the first order fragment of Ramsey Theorem is equivalent to the purely classical principle Σ^0_3- LLPO [10], so it is not an intuitionistic result. The H-closure Theorem is a version of Ramsey Theorem intuitionistically valid.

Theorem 2. *[H-closure Theorem] The H-well-founded relations are closed under finite unions:*

$$(R_1, \ldots, R_n \ H\text{-well-founded}) \implies ((R_1 \cup \cdots \cup R_n) \ H\text{-well-founded}).$$

H-closure Theorem is classically true, because there exists a simple classical proof of the equivalence between Ramsey Theorem and H-closure Theorem. This is one reason for finding an intuitionistic proof of H-closure Theorem: it splits the proof of Ramsey Theorem into two parts, one intuitionistic and the other classical but simple (it could be proved using the sub-classical principle LLPO-3 [3]). We claim we may derive Ramsey for recursive colorings in Heyting Arithmetic plus the following sub-classical schema:

Assume T is an infinite r.e. k-branching tree. There is an arithmetical formula defining a branch r of T and some $i \leq k$ such that r includes infinitely many "i-children".

6.2 Proving the Intuitionistic Form Ramsey Theorem

We introduce a particular set of colored lists: the (R_1, R_2)-colored lists. This set will be well-founded if R_1, R_2 are H-well-founded. Let (L, f) be a colored list. We say that (L, f) is a (R_1, R_2)-colored list if for every segment (x_i, x_{i+1}) of (L, f), if it has color $k \in \{1, 2\}$ then x_i is R_k-greater than all the elements of L that follows it. Informally, a sequence is a (R_1, R_2)-colored list if whenever the sequence decreases w.r.t. R_i, then it remains smaller w.r.t. to R_i. Formally:

Definition 12. $(L, f) \in \mathrm{ColList}(C)$ *is a R_1, R_2-colored list if either $L = \langle\rangle$ and $f = \langle\rangle$ or $L = \langle x_1, \ldots, x_n\rangle$, $f = \langle c_1, \ldots, c_{n-1}\rangle$, and*

$$\forall i \in [1, n-1].(c_i = k \implies (\forall j \in [1, n].i < j \implies (x_j R_k x_i))).$$

$\mathrm{ColList}(R_1, R_2) \subseteq \mathrm{ColList}(C)$ *is the set of (R_1, R_2)-colored lists.*

We may think of a (R_1, R_2)-colored list as a simultaneous construction of one R_1-decreasing transitive list and one R_2-decreasing transitive list. We call an *Erdős-tree over* R_1, R_2, a (R_1, R_2)-tree for short, any binary tree whose branches are all in $\mathrm{ColList}(R_1, R_2)$. Erdős-trees are inspired by the trees used first by Erdős then by Jockusch in their proofs of Ramsey [11], hence the name. We may think of a (R_1, R_2)-tree as a simultaneous construction of many R_1-decreasing transitive lists and many R_2-decreasing transitive lists.

$\mathrm{BinTr}(\mathrm{ColList}(R_1, R_2))$ is the set of all (R_1, R_2)-trees. We will considering the one-step extension $\succ_{\mathrm{col}}$ on colored lists in $\mathrm{ColList}(R_1, R_2)$, and the one-step extension $\succ_T$ on binary trees in $\mathrm{BinTr}(\mathrm{ColList}(R_1, R_2))$.

Now we note that each one-step step extension in a $R_1 \cup R_2$-decreasing transitive list may be simulated as an one-step step extension of some Erdős-tree on (R_1, R_2), that is, as an one-step extension either of one R_1-decreasing transitive list or of one R_2-decreasing transitive list, among those associated to the branches of the (R_1, R_2)-tree. From the well-foundedness of the set $\mathrm{BinTr}(\mathrm{ColList}(R_1, R_2))$ of Erdős-trees we will derive our intuitionistic version of Ramsey Theorem.

Lemma 3. *(Simulation) Let R_1, R_2 be binary relations on a set I.*

1. $(\mathrm{ColList}(R_1, R_2), \succ_{col})$ *is simulable in* $(H(R_1) \times H(R_2), \succ \otimes \succ) + 1$.
2. $H(R_1 \cup R_2, \succ)$ *is simulable in* $(\mathrm{BinTr}(\mathrm{ColList}(R_1, R_2)), \succ_T)$.

Corollary 3. *Let R_1, R_2 be binary relations H-well-founded on a set I.*

1. *The set* $(\mathrm{ColList}(R_1, R_2), \succ_{col})$ *of R_1, R_2-colored lists is well-founded.*
2. *The set* $(\mathrm{BinTr}(\mathrm{ColList}(R_1, R_2)), \succ_T)$ *is well-founded.*

Proof. 1. $(H(R_1) \times H(R_2), \succ \otimes \succ)$ is well-founded by Proposition 2.2, since its components are. By Corollary 1, $(H(R_1) \times H(R_2), \succ \otimes \succ) + 1$ is well-founded. Since $(\mathrm{ColList}(R_1, R_2), \succ_{\mathrm{col}})$ is simulable in $(H(R_1) \times H(R_2), \succ \otimes \succ) + 1$ by Lemma 3, then it is well-founded by Proposition 2.5.

2. Since $(\mathrm{ColList}(R_1, R_2), \succ_{\mathrm{col}})$ is well-founded thanks to the previous point, $(\mathrm{BinTr}(\mathrm{ColList}(R_1, R_2)), \succ_T)$ is well-founded by Lemma 2.

Let $\emptyset$ be the empty binary relation on I. Then $H(\emptyset)$ does not contain lists of length greater or equal than 2. Hence $H(\emptyset) = \{\langle x \rangle : x \in I\} \cup \{\langle\rangle\}$. $H(V)$ is $\succ$-well-founded since each $\langle x \rangle$ is $\succ$-minimal, and $\langle\rangle$ has height less or equal than 1. Thus, the empty relation is H-well-founded.

Theorem 3. *Let $n \in \mathbb{N}$. If $R_1, \ldots, R_n$ H-well-founded then $(R_1 \cup \cdots \cup R_n)$ is H-well-founded.*

Proof. We may prove it by induction on $n \in \omega$. If $n = 0$ then $(R_1 \cup \cdots \cup R_n) = \emptyset$: we already considered this case. Assume that $n > 0$, and that the thesis holds for any $m < n$. Then $R_1 \cup \cdots \cup R_{n-1}$ is H-well-founded. Thus, in order to prove that $(R_1 \cup \cdots \cup R_n)$ is H-well-founded, it is enough to consider the case $n = 2$.

Assume R_1, R_2 are H-well-founded relations: then by applying Corollary 3.2, $(\mathrm{BinTr}(\mathrm{ColList}(R_1, R_2)), \succ_T)$ is well-founded. By Lemma 3, $(H(R_1 \cup R_2), \succ)$ is simulable in $(\mathrm{BinTr}(\mathrm{ColList}(R_1, R_2)), \succ_T)$, well-founded, therefore it is itself well-founded by Proposition 2.5.

Corollary 4. *Let $n \in \mathbb{N}$. $R_1, \ldots, R_n$ are H-well-founded if and only if $(R_1 \cup \cdots \cup R_n)$ is H-well-founded.*

Proof. $\Rightarrow$ Theorem 3.

$\Leftarrow$ If R and S are binary relations such that $R \subseteq S$, then S is H-well-founded implies that R is H-well-founded. In fact we have $H(R) \subseteq H(S)$; so by Proposition 2.7, if $(H(S), \succ)$ is well-founded then $(H(R), \succ)$ is well-founded. Since $\forall i \in [1, n].R_i \subseteq R_1 \cup \cdots \cup R_n$, then R_i is H-well-founded.

7 Podelski and Rybalchenko's Termination Theorem

In this last section we prove that the Termination Theorem [1, Theorem 1] is intuitionistically valid. For all details we refer to this paper: here we only include the definitions of program, computation, transition invariant and disjunctively well-founded relations that Podelski and Rybalchenko used.

Definition 13 (Transition Invariants). *As in [1]:*

- *A program $P = (W, I, R)$ consists of:*
  - *W: a set of states,*
  - *I: a set of starting states, such that $I \subseteq W$,*
  - *R: a transition relation, such that $R \subseteq W \times W$.*
- *A computation is a maximal sequence of states $s_1, s_2, \ldots$ such that*
  - *$s_1 \in I$,*
  - *$(s_i, s_{i+1}) \in R$ for all $i \geq 1$.*
- *The set* Acc *of accessible states consists of all states that appear in some computation.*
- *A transition invariant T is a superset of the transitive closure of the transition relation R restricted to the accessible states* Acc*. Formally,*

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

- *The program P is terminating if and only if $R \cap (Acc \times Acc)$ is well-founded.*
- *A relation T is disjunctively well-founded if it is a finite union $T = T_1 \cup \cdots \cup T_n$ of well-founded relations.*

Lemma 4. *If $T = R \cap (\mathrm{Acc} \times \mathrm{Acc})$ is well-founded then $U = R^+ \cap (\mathrm{Acc} \times \mathrm{Acc})$ is well-founded.*

Theorem 4 (Termination). *The program P is terminating if and only if there exists a disjunctively well-founded transition invariant for P.*

Proof. $\Leftarrow$ Let $T = T_1 \cup \cdots \cup T_n$ with $T_1, \ldots, T_n$ well-founded and T transitive, then by H-closure Theorem 3 and thanks to the Proposition 1 we obtain T is well-founded, so P is terminating.

$\Rightarrow$ Let P be terminating then $R \cap (\mathrm{Acc} \times \mathrm{Acc})$ is well-founded. By Lemma 4 $R^+ \cap (\mathrm{Acc} \times \mathrm{Acc})$ is well-founded. Then we are done.

8 Related Works and Conclusions

In [3] we studied how much Excluded Middle is needed to prove Ramsey Theorem. The answer was that the first order fragment of Ramsey Theorem is equivalent in HA to Σ_3^0-LLPO, a classical principle strictly between Excluded Middle for 3-quantifiers arithmetical formulas and Excluded Middle for 2-quantifiers arithmetical formulas [10]. Σ_3^0-LLPO may be interpreted as König's Lemma restricted to trees definable by some Δ_3^0-predicate (see again [10]).

However, Ramsey Theorem in the proof of the Termination Theorem [1] may be replaced by H-closure, obtaining a fully intuitionistic proof. It is worth noticing that we obtained the result of H-closure by analyzing the proof of Termination Theorem, not by building over any existing intuitionistic interpretation.

We could not find any evident connection with the intuitionistic interpretations by Bellin, Oliva and Powell. Bellin [12] applied the no-counterexample interpretation to Ramsey theorem, while Oliva and Powell [13] used the dialectica interpretation. They approximated the homogeneous set by a set which may stand any test for some initial segment (a segment dependent by the try itself). Instead we proved a well-foundedness result.

Instead, we found interesting connections with the intuitionistic interpretations expressing Ramsey Theorem as a property of well-founded relations. This research line started in 1974: the very first intuitionistic proof used Bar Induction. We refer to §10 of [6] for an account of this earlier stage of the research. Until 1990, all intuitionistic versions of Ramsey were negated formulas, hence non-informative. In 1990 [6] Veldman and Bezem proved, using Choice Axiom and Brouwer thesis, the first intuitionistic negation-free version of Ramsey: *almost full relations are closed under finite intersections*, from now on the *Almost-Full Theorem*.

We explain the Almost-full theorem. *Brouwer thesis* says: a relation R is inductively well-founded if and only if all R-decreasing sequences are finite. Brouwer thesis is classically true, yet it is not provable using the rules of intuitionistic natural deduction. In [5] (first published in 1994, updated in 2011) Coquand showed that we may bypass the need of Choice Axiom and Brouwer thesis in the Almost Full Theorem, provided we take as definition of well-founded directly the inductive definition of well-founded (as we do in this paper).

In [6], a binary relation R over a set is *almost full* if for all infinite sequences $x_0, x_1, x_2, \ldots, x_n, \ldots$ on I there are *some* $i < j$ such that $x_i R x_j$. We claim that, 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. Indeed, let $\neg R^{-1}$ be the complement of the inverse of R: then, classically, $\neg R^{-1}$ almost full means that in all infinite sequences we have $x_i \neg R^{-1} x_j$ for some $i < j$, that is, $x_j \neg R x_i$ for some $i < j$, that is, all sequences such that $x_j R x_i$ for all $i < j$ are finite. Classically, this is equivalent to H-well-foundedness of R. The fact that the relationship between H-well-founded and almost full requires a complement explains why we prove closure under finite unions, while Veldman, Bezem and Coquand proved the closure under finite *intersections*.

For the future, we plan to use our proof to extract some effective bounds for the Termination Theorem. Another challenge is to extract the bounds implicit in the intuitionistic proof [7], which, as we said, uses Ramsey Theorem in the form: "almost full relations are closed under intersection", and to compare the two bounds.

References

1. Podelski, A., Rybalchenko, A.: Transition invariants. In: LICS, pp. 32–41 (2004)
2. Ramsey, F.P.: On a problem in formal logic. Proc. London Math. Soc. 30, 264–286 (1930)
3. Berardi, S., Steila, S.: Ramsey Theorem for pairs as a classical principle in Intuitionistic Arithmetic. Accepted in Types 2013 Postproceedings (2013)
4. Friedman, H.: Classically and intuitionistically provably recursive functions, vol. 699 (1978)
5. Coquand, T.: A direct proof of Ramsey's Theorem. Author's website (1994) (revised in 2011)
6. Veldman, W., Bezem, M.: Ramsey's theorem and the pigeonhole principle in intuitionistic mathematics. Journal of the London Mathematical Society s2-47(2), 193–211 (1993)
7. Vytiniotis, D., Coquand, T., Wahlstedt, D.: Stop when you are almost-full - adventures in constructive termination. In: Beringer, L., Felty, A. (eds.) ITP 2012. LNCS, vol. 7406, pp. 250–265. Springer, Heidelberg (2012)
8. Harrison, J.: Handbook of Practical Logic and Automated Reasoning, 1st edn. Cambridge University Press (2009)
9. Park, D.: Concurrency and automata on infinite sequences. In: Deussen, P. (ed.) Proceedings of the 5th GI-Conference on Theoretical Computer Science. LNCS, vol. 104, pp. 167–183. Springer, Heidelberg (1981)
10. Akama, Y., Berardi, S., Hayashi, S., Kohlenbach, U.: An Arithmetical Hierarchy of the Law of Excluded Middle and Related Principles. In: LICS, pp. 192–201. IEEE Computer Society (2004)
11. Jockusch, C.: Ramsey's Theorem and Recursion Theory. J. Symb. Log. 37(2), 268–280 (1972)
12. Bellin, G.: Ramsey interpreted: a parametric version of Ramsey's Theorem. In: AMS (ed.) Logic and Computation: Proceedings of a Symposium held at Carnegie-Mellon University, vol. 106, pp. 17–37 (1990)
13. Oliva, P., Powell, T.: A Constructive Interpretation of Ramsey's Theorem via the Product of Selection Functions. CoRR abs/1204.5631 (2012)