Probabilistic Algorithms and Ramsey-Type Principles in Reverse Mathematics

Laurent Bienvenu Ludovic Patey Paul Shafer

LIAFA

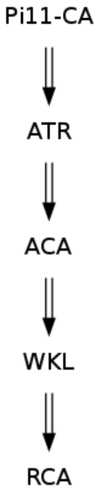
February 25, 2013

Summary

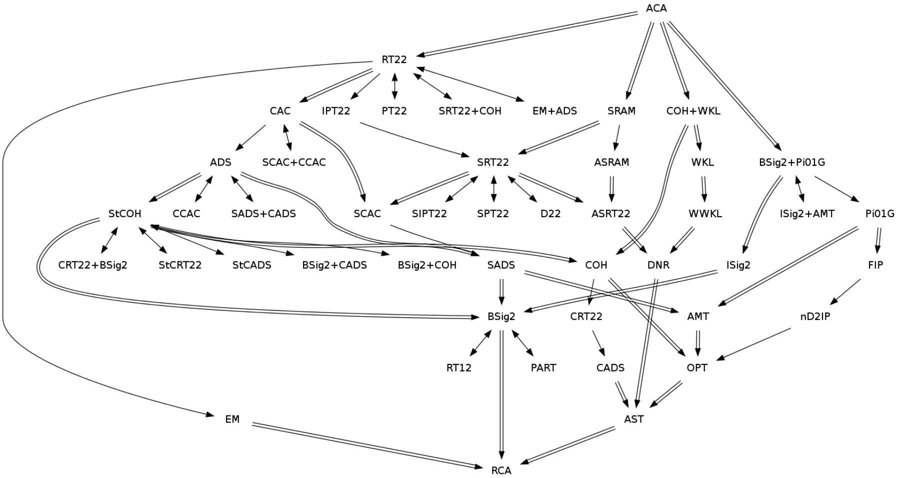
Plan

1. Introduction
2. Probabilistic Algorithms
3. Ramsey's Theorems
4. Ramsey-Type Weak König's Lemmas
5. Conclusion

The "big five" subsystems



The reverse mathematics zoo



Plan

Why probabilistic algorithms ?

- Faster algorithms using randomness.
  - Primality testing
  - Cryptographic
  - Sorting
- Crucial questions in Complexity Theory
  - **BPP** vs **P**
- Which computational power ?

Weak Weak König's Lemma

Definition (Tree)

A tree T is a set closed under prefixes:

$$\forall \sigma \in T, \tau \prec \sigma \Rightarrow \tau \in T$$

Definition (Measure of a tree)

$$\mu(T) \stackrel{def}{=} \lim_{n \to \infty} \frac{\texttt{card}\{\sigma \in T \ : \ |\sigma| = n\}}{2^n}$$

Definition ($\mathbf{WWKL_0}$)

$\mathbf{RCA_0}$ + Every subtree of $2^{<\omega}$ of positive measure has a path.

Why does $\mathbf{WWKL_0}$ captures randomness ?

Properties of Martin-Löf randoms

Theorem (A. Kucera, 1985)

A Martin-Löf random is a path (up to prefix) in a tree iff the tree has positive measure.

Theorem

There is a tree capturing only Martin-Löf randoms.

Power of $\mathbf{WWKL_0}$

Theorem (Simpson et al.)

$$\mathbf{WKL_0} \Rightarrow \mathbf{WWKL_0} \Rightarrow \mathbf{RCA_0}$$

And Ramsey version ?...

What about knowing only an infinity of random digits ?

Plan

Ramsey's Theorems

Notation

$[\mathbb{N}]^n$ is the collection of subsets of ω of size n

Definition (System RT)

$\mathbf{RCA_0}$ + "given n and $k \in \omega$, for every function (called a coloring) $f \in \{0, \ldots, k-1\}^{[\mathbb{N}]^n}$, there is an infinite set $H \subseteq \omega$ which is given one color by f".

Definition (System $\mathbf{RT^n_k}$)

Restriction of **RT** to a fixed n and k.

Difficulty of Ramsey theorems

Difficulty of predicting power of a Ramsey principle.

Example

- Peano completion: complete for $\mathbf{WKL_0}$.
- Infinite subset of a Peano completion: computable.

Ramsey's Theorems

Theorem (Simpson)

(i) *For each* $n \geq 3$ *and* $k \geq 2$, $\mathbf{RCA_0} \vdash \mathbf{RT^n_k} = \mathbf{ACA_0}$.

(ii) $\mathbf{RT}$ *is not provable in* $\mathbf{ACA_0}$.

Theorem

- $\mathbf{RCA_0} \vdash \mathbf{RT^2_1}$
- $\mathbf{RCA_0} \vdash \mathbf{ACA_0} \Rightarrow \mathbf{RT^2_2}$ *(1995)*
- $\mathbf{RT^2_2} \not\leftarrow \mathbf{WKL_0}$ *(2001)*
- $\mathbf{RT^2_2} \not\rightarrow \mathbf{WKL_0}$ *(2011)*

Plan

Ramsey-Type Weak König's Lemmas

Definition (Homogeneous set)

A set H is *homogeneous for* $\sigma \in 2^{<\omega}$ *with color* $c \in \{0,1\}$ if $\sigma(x) = c$ for each $x \in H$ s.t. $x < |\sigma|$. H is *homogeneous for a path trough* T if $\exists c \in \{0,1\}$ s.t. H is homogeneous for σ with color c for arbitrarily long $c \in T$.

Definition ($\mathbf{RWKL_0}$)

$\mathbf{RCA_0}$ + "each binary tree T has an infinite set which is homogeneous for a path through T."

Ramsey-Type Weak König's Lemmas

Theorem (Flood)

(i) $\mathbf{RT^2_2} \Rightarrow \mathbf{RWKL}$

(ii) $\mathbf{WKL_0} \Rightarrow \mathbf{RWKL}$

(iii) $\mathbf{RWKL} \to \mathbf{DNC}$

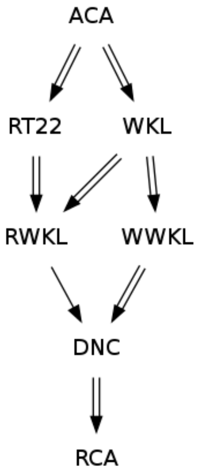
Definition ($\mathbf{RWWKL_0}$)

$\mathbf{RWWKL_0}$ is obtained from $\mathbf{RWKL_0}$ by considering only trees of positive measure.

Power of $\mathbf{RWWKL_0}$

What is the expressive power of $\mathbf{RWWKL_0}$?

Local zoo : version 1



Diagonally Non-Computable functions

X is a set, f a function and e a Turing index.

DNC

$\forall X, \exists f \in \omega^\omega$ such that $\forall e, f(e) \neq \Phi_e^X(e)$.

FPF

$\forall X, \exists f \in \omega^\omega$ such that $\forall e, \Phi_{f(e)}^X \neq \Phi_e^X$.

Theorem (Jockusch, Lerman, Soare & Solovay)

$\mathbf{RCA_0} \vdash \mathbf{DNC} = \mathbf{FPF}$

The system $\mathbf{RWWKL_0}$

Theorem (Bienvenu, Patey, Shafer)

$\mathbf{RCA_0} \vdash \mathbf{DNC} = \mathbf{RWWKL_0}$

Intuition

- $\mathbf{WWKL_0}$ $\Leftrightarrow$ existence of a Martin-Löf Random
- $\mathbf{RWWKL_0}$ $\Leftrightarrow$ existence of an infinite subset of a Martin-Löf Random

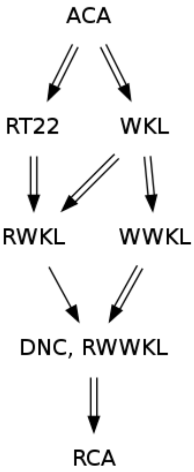
Theorem (Kjos-Hanssen, Greenberg & Miller)

The following are equivalent:

(i) *A computes a DNC function.*

(ii) *A computes an infinite subset of a Martin Löf random.*

Local zoo : version 2



Graph Colorability

Definition ($\mathbf{RCOLOR_k}$)

$\mathbf{RCOLOR_k} = \mathbf{RCA_0}$ + "for every infinite graph $G = (V, E)$, if every finite $V_0 \subseteq V$ induces a k-colorable subgraph, then there is an infinite $H \subseteq V$ such that every finite $V_0 \subseteq V$ induces a subgraph that is k-colorable by a coloring that colors every $v \in V_0 \cap H$ by color 0."

Definition ($\mathbf{LRCOLOR_k}$)

$\mathbf{LRCOLOR_k} = \mathbf{RCA_0}$ + "for every infinite graph $G = (V, E)$ and every infinite $X \subseteq V$, if every finite $V_0 \subseteq V$ induces a k-colorable subgraph, then there is an infinite $H \subseteq X$ such that every finite $V_0 \subseteq V$ induces a subgraph that is k-colorable by a coloring that colors every $v \in V_0 \cap H$ color 0."

Some results

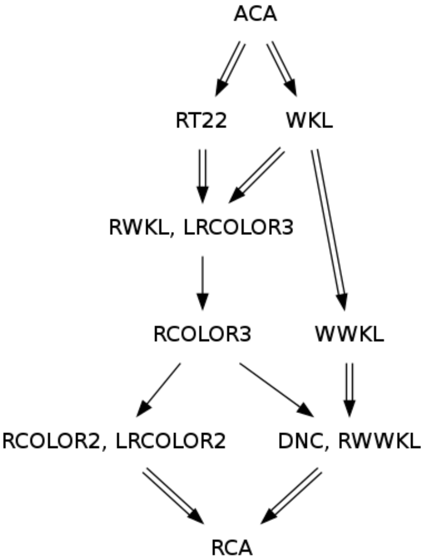
Theorem (Bienvenu, Patey, Shafer)

$\mathbf{RCA_0} \vdash \mathbf{LRCOLOR_3} = \mathbf{RWKL_0} \rightarrow \mathbf{RCOLOR_3} \rightarrow \mathbf{DNC}$

Theorem (Bienvenu, Patey, Shafer)

$\mathbf{RCA_0} \vdash \mathbf{RCOLOR_3} \rightarrow \mathbf{LRCOLOR_2} = \mathbf{RCOLOR_2}$

Local zoo : version 3



$\mathbf{WWKL_0}$ and $\mathbf{RWKL_0}$ are incomparable

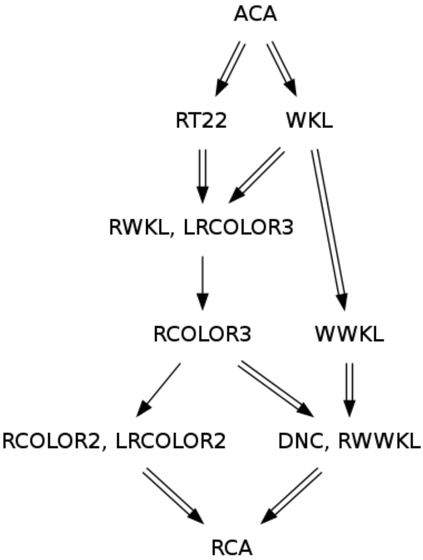
Theorem (Jiayi Liu, 2011)

$\mathbf{RCA_0} \nvdash \mathbf{RT^2_2} \rightarrow \mathbf{WWKL_0}$

Theorem (Bienvenu, Patey, Shafer)

$\mathbf{RCA_0} \nvdash \mathbf{WWKL_0} \Rightarrow \mathbf{RCOLOR_2}$

Local zoo : version 4



Plan

References

Stephen Flood.
Reverse mathematics and a ramsey-type könig's lemma.
2011.

S.G. Simpson, Association for Symbolic Logic, and Inc ebrary.
Subsystems of second order arithmetic, volume 42.
Springer Berlin, 1999.

Thank you for listening !