Decidability of S1S in Constructive Type Theory

Master's Thesis Talk

Moritz Lichter

SAARLAND UNIVERSITY
COMPUTER SCIENCE

Advisor: Prof. Dr. Gert Smolka

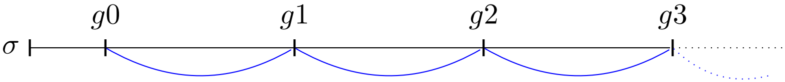
August 23, 2017

Ramseyan Factorizations

ω-**Sequence** over Γ: function $\mathbb{N} \to \Gamma$
Finite Semigroup $(\Gamma, +)$: Γ finite type, $+$ associative

RF

A sequence over a finite semigroup $(\Gamma, +)$ admits a Ramseyan factorization.



$$\sum \sigma[g0..g1) = \sum \sigma[g1..g2) = \sum \sigma[g2..g3) = \cdots$$

RF := $\forall \sigma.\ \exists$ strictly montone g.

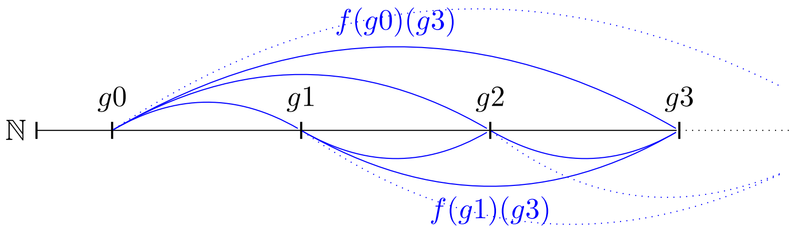
$$\forall i.\ \sum \sigma[g0..g1) = \sum \sigma[gi..g(i+1))$$

Additive Ramsey

Coloring $f : \mathbb{N} \to \mathbb{N} \to \Gamma$ **additive** $:= (fij) + (fjk) = fik$ for $i < j < k$

AR

For an additive coloring there is a strictly monotone and monochromatic function.



AR $:= \forall$ additive f. $\exists$ strictly monotone g.

$$\forall i < j.\ f(g0)(g1) = f(gi)(gj)$$

Independence of RF

Excluded Middle

↓

$P_1 \vee \mathrm{DM}(\neg P_1)$,
$P_2 \vee \mathrm{DM}(\neg P_2)$

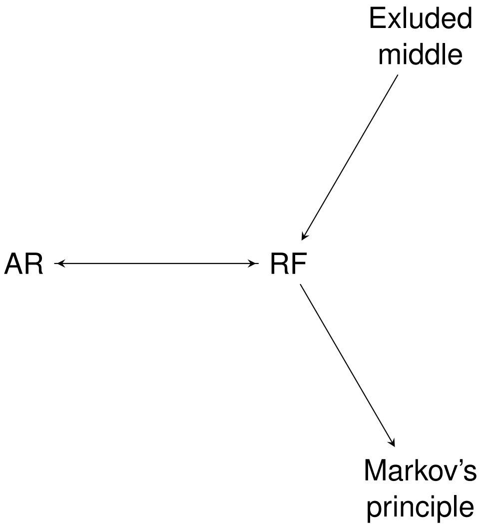
↓

RF

↓

Markov's Principle

Summary



Büchi Automata

Büchi Acceptance

Büchi automaton: NFA $\mathcal{A} = (Q, I, F, \rightarrow)$ over finite Γ with Büchi acceptance
An infinite run ϱ is final if

$$\forall n.\ \exists m \geq n.\ \varrho m \in F.$$

$$\mathscr{L}_B(\mathcal{A}) := \{\sigma | \exists \varrho.\ \varrho \text{ is accepting for } \sigma\}$$

Facts

- Closure operations implementing closure under
  - image
  - preimage
  - union
  - intersection
- Decidability of language emptiness: $\mathscr{L}_B(\mathcal{A}) \equiv \emptyset$ or $\exists xy^\omega \in \mathscr{L}_B(\mathcal{A})$

Complementation of Büchi Automata

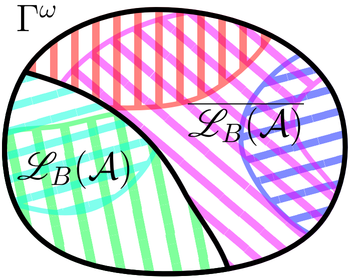
BC

Büchi automata are closed under complement and the word problem is logically decidable.

$$\begin{aligned} \mathsf{BC} := \forall \mathcal{A}.\ & (\exists \overline{\mathcal{A}}.\ \mathscr{L}_B(\overline{\mathcal{A}}) \equiv \overline{\mathscr{L}_B(\mathcal{A})}) \wedge \\ & (\forall \sigma.\ \sigma \in \mathscr{L}_B(\mathcal{A}) \vee \sigma \notin \mathscr{L}_B(\mathcal{A})) \end{aligned}$$

Complementation by Büchi

For Büchi automaton $\mathcal{A}$, there are finitely many languages L_i:



1. L_i are accepted by Büchi automata:

$$\mathscr{L}_B(\mathcal{A}_i) \equiv L_i$$

2. Compatibility:

$$\sigma \in (L_i \cap \mathscr{L}_B(\mathcal{A})) \rightarrow L_i \subseteq \mathscr{L}_B(\mathcal{A})$$

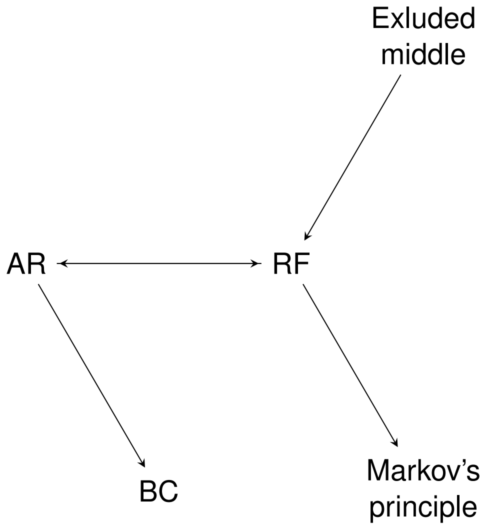
3. Totality (only under AR):

$$\forall \sigma.\ \exists L_i.\ \sigma \in L_i$$

$$\mathcal{A}^C := \bigcup_{\{L_i | L_i \cap \mathscr{L}_B(\mathcal{A}) \equiv \emptyset\}} \mathcal{A}_i$$

Corollary: AR implies BC.

Summary



Sequence Structures

Abstraction from Representation of Sequences

- $\mathscr{A}$: finite Type $\to$ Type
- $\mathsf{C}_{\mathscr{A}} : \forall \Gamma.\ \mathscr{A}(\Gamma) \to \Gamma^\omega$
- $\circ_{\mathscr{A}} : \forall \Gamma \Sigma.\ \mathscr{A}(\Gamma) \to (\Gamma \to \Sigma) \to \mathscr{A}(\Sigma)$
- $\otimes_{\mathscr{A}} : \forall \Gamma \Sigma.\ \mathscr{A}(\Gamma) \to \mathscr{A}(\Sigma) \to \mathscr{A}(\Gamma \times \Sigma)$
- $@_{\mathscr{A}} : \forall \Gamma.\ \Gamma \to \mathbb{N} \to \Gamma \to \mathscr{A}(\Gamma)$

Compatibility with ω-Sequences

$$\mathsf{C}_{\mathscr{A}}(\sigma \circ_{\mathscr{A}} f) \equiv \mathsf{C}_{\mathscr{A}}\sigma \circ f \qquad \sigma \circ f := \lambda n. f(\sigma n)$$

$$\mathsf{C}_{\mathscr{A}}(\sigma \otimes_{\mathscr{A}} \tau) \equiv \mathsf{C}_{\mathscr{A}}\sigma \otimes \mathsf{C}_{\mathscr{A}}\tau \qquad \sigma \otimes \tau := \lambda n.(\sigma n, \tau n)$$

$$\mathsf{C}_{\mathscr{A}}(a @^m_{\mathscr{A}} b) \equiv a @^m b \qquad a @^m b := \lambda n. \text{if } (m = n) \text{ then } b \text{ else } a$$

Admissible Sequence Structures

A sequence structure is **admissible** if

1. $\mathscr{L}_{\mathscr{A}}(\mathcal{A}) \equiv \emptyset$ or $\exists \sigma . \sigma \in \mathscr{L}_{\mathscr{A}}(\mathcal{A})$ is decidable, where

$$\mathscr{L}_{\mathscr{A}}(\mathcal{A}) := \{\sigma : \mathscr{A}(\Gamma) | \mathsf{C}_{\mathscr{A}} \sigma \in \mathscr{L}_B(\mathcal{A})\},$$

2. Image construction for Büchi automata is correct, and
3. Totality holds: $\forall \mathcal{A}.\ \forall \sigma : \mathscr{A}(\Gamma).\ \exists L_i(\mathcal{A}).\ \sigma \in L_i(\mathcal{A})$.

Theorem: For all admissible sequence structures

- All closure operations on Büchi Automata are correct and
- The word problem is logically decidable.

Instantiations

1. *Given AR:* ω-sequences $\mathbb{N} \to \Gamma$
2. *Constructively:* Ultimately periodic sequences $\Gamma^* \times \Gamma^+$

Monadic Second Order Logic of $(\mathbb{N}, <)$ (S1S)

Full and Minimal System

$$\mathsf{MSO}\ \varphi, \psi ::= x < y \mid x \in X \mid X \subseteq Y \mid \varphi \wedge \psi \mid \neg\varphi \mid \exists x.\, \varphi \mid \exists X.\, \psi$$

$$\mathsf{MSO}_0\ \varphi, \psi ::= X \lessdot Y \mid X \subseteq Y \mid \varphi \wedge \psi \mid \neg\varphi \mid \exists X.\, \varphi$$

Satisfaction is defined with admissible sequence structures:
$\mathscr{A}(\mathbb{B})$ for second order variables

$$J \vDash_0 X \lessdot Y := \exists n \in JX.\, \exists m \in JY.\, n < m$$

Reduction of MSO to MSO_0

MSO can be reduced to MSO_0 using singleton sets for first order variables: $\{n\} := \mathsf{false} @^n_{\mathscr{A}} \mathsf{true}$

Translation of MSO_0 to Büchi Automata

Theorem: An MSO_0 formula φ can be translated to a Büchi automaton $\mathcal{A}_\varphi$ such that:

$$J \vDash_0 \varphi \to fJ \in \mathscr{L}_{\mathscr{A}}(\mathcal{A}_\varphi)$$
$$\sigma \in \mathscr{L}_{\mathscr{A}}(\mathcal{A}_\varphi) \to f'\sigma \vDash_0 \varphi$$

Corollary: For all admissible sequence structures

1. Satisfiability is decidable and
2. Satisfaction is logically decidable.

S1S with UP and ω-Sequences

Corollary: For MSO_0 and MSO

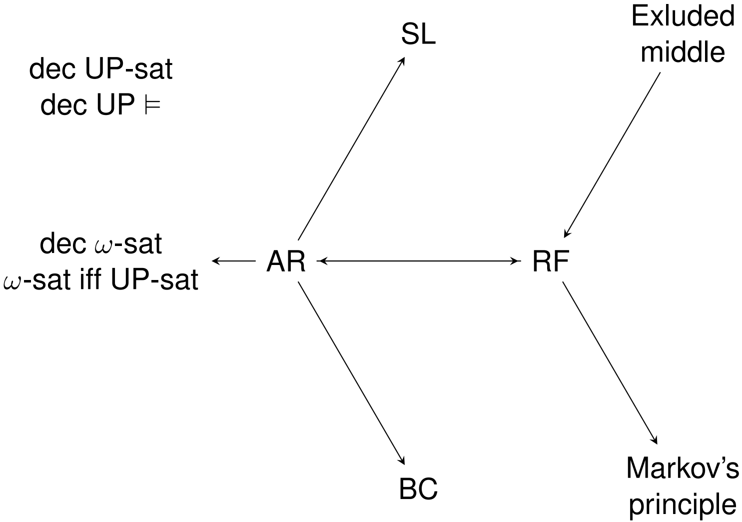
1. Satisfiability for UP sequences is decidable
2. Satisfaction for UP sequences is decidable
3. Given AR:
   - Satisfiability for ω-sequences is decidable
   - Satisfaction for ω-sequences is logically decidable
   - A formula is UP satisfiable if and only if it is ω-satisfiable

Corollary: AR implies SL.

$$\mathsf{SL} := \forall \varphi I J.\ I, J \vDash \varphi \vee I, J \nvDash \varphi$$

Satisfaction in MSO for ω-sequences is logically decidable.

Summary


SL
Exluded
middle
dec UP-sat
dec UP ⊨
dec ω-sat
ω-sat iff UP-sat
AR
RF
BC
Markov's
principle

BC implies RF

Let $(\Gamma, +)$ be a finite semigroup and σ a sequence over Γ.

There is an $\mathcal{A}$ with

$$\mathscr{L}_B(\mathcal{A}) \equiv \{\sigma | \sigma \text{ admits a Ramseyan factorization}\}.$$

By BC $\sigma \in \mathscr{L}_B(\mathcal{A}) \vee \sigma \notin \mathscr{L}_B(\mathcal{A})$.

If $\sigma \notin \mathscr{L}_B(\mathcal{A})$ then $\sigma \in \mathscr{L}_B(\overline{\mathcal{A}})$ and there is a $xy^\omega \in \mathscr{L}_B(\overline{\mathcal{A}})$.
Every xy^ω admits a Ramseyan factorization: $xy^\omega \in \mathscr{L}_B(\mathcal{A})$.

SL implies RF

Let $(\Gamma, +)$ be a finite semigroup and σ a sequence over Γ.

Recall: $P_1 \vee \mathrm{DM}(\neg P_1)$ and $P_2 \vee \mathrm{DM}(\neg P_2)$ imply RF.

Infinite Pigeonhole Principle:

$$P_1 := \exists a.\ \forall i.\ \exists j \geq i.\ \sigma j = a$$

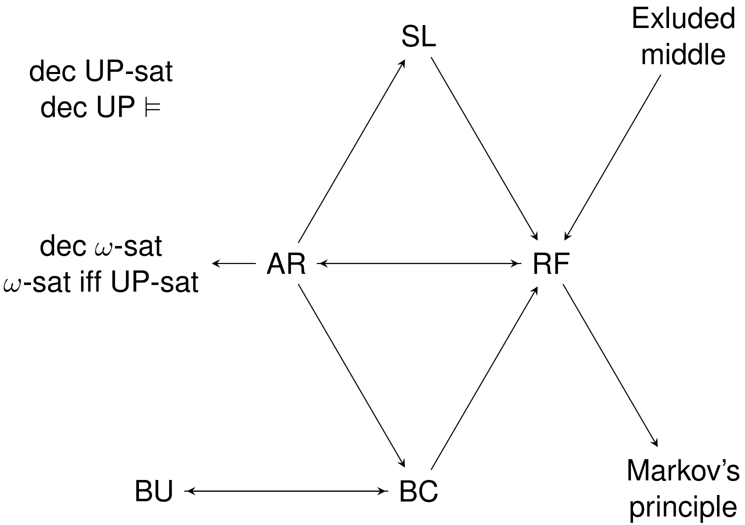
Encoding into MSO:

$$P_1 \leftrightarrow I, J_\sigma \vDash \bigvee_{a \in \Gamma} \forall x.\ \exists y.\ x < y \wedge y \in X_a$$

SL implies $P_1 \vee \mathrm{DM}(\neg P_1)$.

P_2: more specific proposition and more complicated encoding

Summary


SL
Exluded middle
dec UP-sat
dec UP ⊨
dec ω-sat
ω-sat iff UP-sat
AR
RF
BU
BC
Markov's principle

Coq Development

	Specification	Proof
Preliminaries	520	1160
Ramseyan Properties	150	430
NFAs	240	490
Basic Operation on Büchi Automata	230	460
Büchi Complementation	180	550
Admissible Sequence Structures	160	450
S1S	490	940
Necessity of AR	170	470
Total	**2120**	**4950**