

Logical Refinements of Church's Problem

GAMES and CSL, Lausanne, September 2007

Alexander Rabinovich Wolfgang Thomas

Tel Aviv University

RWTH Aachen

Introductory Remark

In the terminology used today in the games community, Church's Problem asks for the solution of regular infinite games, i.e. infinite games with a winning condition formalizable in monadic second-order logic over the ordering of the natural numbers.

It is a nice coincidence that the first (however preliminary) formulation of Church's Problem appeared precisely 50 years ago, in summer 1957.

Church's Problem

Alonzo Church

at the “Summer Institute of Symbolic Logic”

Cornell University, 1957:

“Given a requirement which a circuit is to satisfy, we may suppose the requirement expressed in some suitable logistic system which is an extension of restricted recursive arithmetic. The *synthesis problem* is then to find recursion equivalences representing a circuit that satisfies the given requirement (or alternatively, to determine that there is no such circuit).”

(By “circuits”, Church means finite automata with output.)

APPLICATION OF RECURSIVE ARITHMETIC TO THE PROBLEM OF CIRCUIT SYNTHESIS

Alonzo Church

RESTRICTED RECURSIVE ARITHMETIC

Primitive symbols are individual (i.e., numerical) variables x, y, z, t, \dots , singular functional constants i_1, i_2, \dots, i_μ , the individual constant 0, the accent ' as a notation for successor (of a number), the notation () for application of a singular function to its argument, connectives of the propositional calculus, and brackets [].

Axioms are all tautologous wffs. Rules are modus ponens; substitution for individual variables; mathematical induction,

from $P \supset S_a^a P$ and $S_0^a P$ to infer P ;

and any one of several alternative recursion schemata or sets of recursion schemata.

$$\chi_1(x_1 + M + 1, 0, \dots, 0, 0) \equiv \text{falsehood}$$

.....

$$\chi_N(x_1 + M + 1, M, \dots, M, g) \equiv \text{falsehood}$$

$$\chi_1(x_1 + M + 1, x_2 + M + 1, \dots, 0, 0) \equiv \text{falsehood}$$

.....

$$\chi_1(x_1 + M + 1, x_2 + M + 1, \dots, x_m + M + 1, 0) \equiv \text{falsehood}$$

$$\chi_2(x_1 + M + 1, x_2 + M + 1, \dots, x_m + M + 1, 0) \equiv \text{falsehood}$$

.....

$$\chi_N(x_1 + M + 1, x_2 + M + 1, \dots, x_m + M + 1, 0) \equiv \text{falsehood}$$

$$\chi_1(x_1 + M + 1, x_2 + M + 1, \dots, x_m + M + 1, 1) \equiv \text{falsehood}$$

.....

$$\chi_N(x_1 + M + 1, x_2 + M + 1, \dots, x_m + M + 1, g) \equiv \text{falsehood}$$

$$\chi_1(0, 0, \dots, 0, t + g + 1) \equiv \chi_1(0, 0, \dots, 0, t + g) \vee$$

$$Q_{100\dots 0}[\chi_1(0, 0, \dots, 0, t), \dots, \chi_N(0, 0, \dots, 0, t), \chi_1(0, 0, \dots, 1, t), \dots, \chi_N(M+1, M+1, \dots, M+1, t)]$$

$$\chi_2(0, 0, \dots, 0, t + g + 1) \equiv \chi_2(0, 0, \dots, 0, t + g) \vee$$

$$\bar{\chi}_1(0, 0, \dots, 0, t + g) Q_{200\dots 0}[\chi_1(0, 0, \dots, 0, t), \dots,$$

$$\chi_N(0, 0, \dots, 0, t), \chi_1(0, 0, \dots, 1, t), \dots, \dots,$$

$$\chi_N(M + 1, M + 1, \dots, M + 1, t)]$$

.....

$$\chi_N(M, M, \dots, M, t + g + 1) \equiv \chi_N(M, M, \dots, M, t + g) \vee$$

$$\bar{\chi}_1(M, M, \dots, M, t + g) \bar{\chi}_2(M, M, \dots, M, t + g) \dots$$

$$\bar{\chi}_{N-1}(M, M, \dots, M, t + g) Q_{NM\dots M}[\chi_1(0, 0, \dots,$$

$$0, t), \dots, \chi_N(0, 0, \dots, 0, t), \chi_1(0, 0, \dots, 1, t),$$

$$\dots, \dots, \chi_N(2M + 1, 2M + 1, \dots, 2M + 1, t)]$$

$$\chi_1(x_1 + M + 1, 0, \dots, 0, t + g + 1) \equiv \chi_1(x_1 + M + 1, 0,$$

$$\dots, 0, t + g) \vee Q_{10\dots 0}[\chi_1(x_1, 0, \dots, 0, t), \dots, \chi_N(x_1, 0, \dots, 0, t), \chi_1(x_1, 0, \dots, 1, t), \dots, \dots, \chi_N(x_1 + 2M + 2, M + 1, \dots, M + 1, t)]$$

$$\chi_2(x_1 + M + 1, 0, \dots, 0, t + g + 1) \equiv \chi_2(x_1 + M + 1, 0, \dots, 0,$$

$$t + g) \vee \bar{\chi}_1(x_1 + M + 1, 0, \dots, 0, t + g) Q_{20\dots 0}[\chi_1(x_1, 0, \dots, 0, t), \dots, \chi_N(x_1, 0, \dots, 0, t), \chi_1(x_1, 0, \dots, 1, t), \dots, \dots, \chi_N(x_1 + 2M + 2, M + 1, \dots, M + 1, t)]$$

.....

$$\chi_1(x_1 + M + 1, x_2 + M + 1, \dots, x_m + M + 1, t + g + 1) \equiv$$

$$\chi_1(x_1 + M + 1, x_2 + M + 1, \dots, x_m + M + 1, t + g) \vee$$

$$Q_1[\chi_1(x_1, x_2, \dots, x_m, t), \dots, \chi_N(x_1, x_2,$$

$$\dots, x_m, t), \chi_1(x_1, x_2, \dots, x_m + 1, t), \dots,$$

$$\dots, \chi_N(x_1 + 2M + 2, x_2 + 2M + 2, \dots,$$

$$x_m + 2M + 2, t)]$$

$$\chi_2(x_1 + M + 1, x_2 + M + 1, \dots, x_m + M + 1, t + g + 1) \equiv$$

$$\chi_2(x_1 + M + 1, x_2 + M + 1, \dots, x_m + M + 1, t + g) \vee$$

$$\bar{\chi}_1(x_1 + M + 1, x_2 + M + 1, \dots, x_m + M + 1, t + g) Q_2[\chi_1(x_1,$$

$$x_2, \dots, x_m, t), \dots, \chi_N(x_1, x_2, \dots, x_m, t),$$

$$\chi_1(x_1, x_2, \dots, x_m + 1, t), \dots, \dots,$$

$$\chi_N(x_1 + 2M + 2, x_2 + 2M + 2, \dots, x_m + 2M + 2, t)]$$

$$\dots$$

$$\chi_N(x_1 + M + 1, x_2 + M + 1, \dots, x_m + M + 1, t + g + 1) \equiv$$

$$\chi_N(x_1 + M + 1, x_2 + M + 1, \dots, x_m + M + 1, t + g) \vee$$

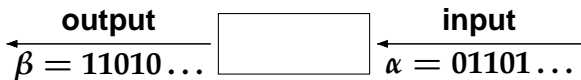
$$\bar{\chi}_1(x_1 + M + 1, x_2 + M + 1, \dots, x_m + M + 1, t + g) \bar{\chi}_2(x_1 + M + 1,$$

$$x_2 + M + 1, \dots, x_m + M + 1, t + g) \dots \bar{\chi}_{N-1}(x_1 + M + 1, x_2 + M + 1,$$

$$\dots, x_m + M + 1, t + g) Q_N[\chi_1(x_1, x_2, \dots, x_m, t), \dots,$$

$$\chi_N(x_1, x_2, \dots, x_m, t), \chi_1(x_1, x_2, \dots, x_m + 1, t), \dots,$$

Requirements as Winning Conditions



Bitstreams α, β are represented by subsets P_α, P_β of \mathbb{N} .

Use variables X, Y for subsets of \mathbb{N} .

Requirement $\varphi(X, Y)$ is considered as winning condition in an infinite two-person game.

Players 1 and 2 choose bits $P(i), Q(i)$ ($i = 0, 1, \dots$) in alternation.

Play $\begin{pmatrix} P(0) \\ Q(0) \end{pmatrix} \begin{pmatrix} P(1) \\ Q(1) \end{pmatrix} \begin{pmatrix} P(2) \\ Q(2) \end{pmatrix} \dots$ is won by 2 if $(\mathbb{N}, \dots) \models \varphi(P, Q)$

Strategies

A strategy for Player 1 is a map

$$\binom{P(0)}{Q(0)} \binom{P(1)}{Q(1)} \cdots \binom{P(k)}{Q(k)} \mapsto 0/1$$

A strategy for player 2 is a map

$$\binom{P(0)}{Q(0)} \binom{P(1)}{Q(1)} \cdots \binom{P(k)}{*} \mapsto 0/1$$

Finite-state strategy: computable by a finite automaton over

$$\Sigma = \left\{ \binom{0}{0}, \binom{0}{1}, \binom{1}{0}, \binom{1}{1}, \binom{0}{*}, \binom{1}{*} \right\}$$

with output function.

Solution of Church's Problem

MSO = monadic second-order logic over $(\mathbb{N}, <)$

Büchi-Landweber Theorem (1969)

For each MSO-requirement $\varphi(X, Y)$ either Player 1 or Player 2 has a finite-state winning strategy.

It is decidable who wins, and a finite-state winning strategy for the respective winner is computable.

Definability of Strategies

A strategy $f : \binom{P(0)}{Q(0)} \binom{P(1)}{Q(1)} \cdots \binom{P(k-1)}{Q(k-1)} \binom{P(k)}{P(k)_*} \mapsto 0/1$

is **MSO-definable** iff there is an MSO-formula $\psi(X, Y, z)$ such that

$$([0, k], <) \models \psi(P \cap [0, k], (Q \cap [0, k - 1]), k)$$

iff

$$f\left(\binom{P(0)}{Q(0)} \cdots \binom{P(k-1)}{Q(k-1)} \binom{P(k)}{P(k)_*}\right) = 1$$

Büchi, Elgot, Trakhtenbrot (abstracts 1957):
Finite-state strategies are MSO-definable.

Some Logics

1. **MSO, monadic second-order logic over $(\mathbb{N}, <)$**
(with free set variables, similarly for the FO-logics below),
2. **FO($<$), first-order logic over $(\mathbb{N}, <)$**
3. **FO($<$)+MOD, the extension of FO($<$) by modular counting quantifiers,**
4. **FO(S), first-order logic over (\mathbb{N}, S) with successor relation S ,**
5. **strictly bounded logic, which is quantifier-free logic over $(\mathbb{N}, 0, +1)$.**
6. **Presburger arithmetic, first-order logic over $(\mathbb{N}, +)$**

$\mathcal{L}, \mathcal{L}', \dots$ will stand for any of these logics.

\mathcal{L} -Definable Games and Strategies

An \mathcal{L} -defined game is **determined with \mathcal{L}' -definable strategies** if

for each \mathcal{L} -formula $\varphi(X, Y)$, there is either an \mathcal{L}' -definable winning strategy of Player 1 or an \mathcal{L}' -definable winning strategy for Player 2.

Büchi-Landweber:

MSO-defined games are determined with MSO-definable strategies.

Main Results

Main Theorem

Let \mathcal{L} be any of the logics MSO, FO($<$), FO($<$)+MOD, FO(S), or strictly bounded logic. Then each \mathcal{L} -definable game is determined with \mathcal{L} -definable winning strategies.

Theorem

If \mathcal{L} is FO+ $\exists^\omega(S)$ or FO(S)+MOD or Presburger arithmetic, then there are \mathcal{L} -definable games that are not determined with \mathcal{L} -definable winning strategies.

Presburger Arithmetic

A winning condition $\varphi(X, (Y, Z))$ can fix that $Z = \text{Squares}$:

$$0 \in Z \wedge \forall x_1, x_2, x_3 (x_1 < x_2 < x_3 \text{ successive in } Z \\ \rightarrow x_3 - x_2 = (x_2 - x_1) + 2)$$

Putnam 1957: In $\text{FO}(+, \text{Squ})$ multiplication is definable.

Proof: $2xy = (x + y)^2 - x^2 - y^2$

$$x^2 = y \Leftrightarrow$$

$$y \in \text{Squ} \wedge y - (2x - 1) \text{ is the greatest square } < y$$

Consequence: Each winning condition $\exists^\omega x R(X, (Y, \text{Squ}), x)$ with recursive R can be expressed.

Even hyperarithmetical winning strategies do not suffice (but the winning conditions are all arithmetical).

Proof of Main Theorem

Let \mathcal{L} be any of MSO, FO($<$), FO($<$)+MOD.

Essential steps:

1. Recall k -types
2. Recall Composition Theorem
3. Transform given \mathcal{L} -formula $\varphi(X, Y)$ into a “bounded normal form”, say of quantifier depth k
4. Use k -types as vertices of finite game graph, with Muller winning condition
5. Transform into parity game over k' -types (for some $k' > k$)
6. Use \mathcal{L} -definability of k' -types and positional determinacy of parity games
 - to decide the winner
 - to obtain \mathcal{L} -definable winning strategies

k -Types

M, M' are models $(\mathbb{N}, \dots, P, Q)$ or $([m, n], \dots, P, Q)$

A **k -type** is an equivalence class of $\equiv_k^{\mathcal{L}}$:

- $M \equiv_k^{\mathcal{L}} M'$
iff $M \models \varphi \Leftrightarrow M' \models \varphi$ for every \mathcal{L} -formula $\varphi(X, Y)$ of quantifier depth k .

$H_k :=$ set of k -types (finite!)

k -type t is \mathcal{L} -definable by a formula φ_t of quantifier-depth k .

For each \mathcal{L} -formula φ of quantifier-depth k and any model M :

$$M \models \varphi \leftrightarrow \bigvee_{\varphi_t \models \varphi} \varphi_t$$

Composition Theorem

Let \mathcal{L} be any of the logics MSO, FO($<$), FO($<$)+MOD.

- (a) The k -types of M_0, M_1 for \mathcal{L} determine the k -type of the ordered sum $M_0 + M_1$ for \mathcal{L} , which moreover can be computed from the k -types of M_0, M_1 .
- (b) If M_0, M_1, \dots all have the same k -type for \mathcal{L} , then this k -type determines the k -type of the ordered sum $\Sigma_{i \in \mathbb{N}} M_i$, which moreover can be computed from the k -type of M_0 .

“Bounded Normal Form”

An \mathcal{L} -formula $\varphi(X, Y)$ is equivalent to a formula in **bounded normal form** (W.T. 1981):

$$\bigvee_{i=1}^n (\exists^\omega z \psi_i(X, Y, z) \wedge \neg \exists^\omega z \psi'_i(X, Y, z))$$

where the ψ_i, ψ'_i are bounded in z .

Let k be the quantifier depth of the ψ_i, ψ'_i .

Construct a game graph over the set H_k of k -types.

After a play prefix $(\begin{smallmatrix} P^{(0)} \\ Q^{(0)} \end{smallmatrix}) \dots (\begin{smallmatrix} P^{(n)} \\ Q^{(n)} \end{smallmatrix})$, the vertex $T_k([0, n], \dots P \cap [0, n], Q \cap [0, n])$ is reached.

Derived Muller Game

Take as game graph $G_\varphi = (V, V_1, V_2, E)$ with

- $V_1 = H_k \cup \{\varepsilon\}$, $V_2 = V_1 \times \{0, 1\}$, $V = V_1 \cup V_2$
- an edge from $t \in V_1$ to (t, a) for each $t \in V_1$, $a \in \{0, 1\}$,
- an edge from (t, a) to “ $t + (a, b)$ ” for each $b \in \{0, 1\}$.

Winning condition:

For some i and some pair (t, t')

where t implies ψ_i and t' implies ψ'_i :

t is visited infinitely often but t' only finitely often

Call these pairs “good” (for φ)

LAR (Latest Appearance Record)

Let $\rho = t_0 t_1 \dots t_j \dots$ be a play over V .

We consider the associated play ρ' of LAR's.

LAR at time point j : $(t_j, t_{i_1}, \dots, t_{i_m})$ where

$(t_{i_1}, t_{i_2}, \dots, t_{i_m})$ is the list of types visited before j in the order of last visits (most recent noted first).

[McNaughton 1965: “order-vector”,

Gurevich-Harrington 1982: “LAR”]

Assume t_j occurs in t_{i_1}, \dots, t_{i_m} at place h .

$\text{Color}(t_j, t_{i_1}, \dots, t_{i_m}) = 2h$ or $2h - 1$ depending on whether

\exists good pair (t, t') s.t. t but not t' occurs in $\{t_{i_1}, \dots, t_{i_m}\}$ or not

Fact: ρ satisfies the Muller condition iff ρ' satisfies the parity condition.

Expanding the Game Graph

Extend the k -types t by LAR-information:

Example of LAR-information on a play prefix:

t_1, t_2, t_3 occur at $x_1 < x_2 < x_3 \wedge \bigwedge_i \neg \exists y > x_i : t_i$ occurs at y

Proceed from k -types to $(k + |H_k| + 1)$ -types of same logic.

Let $k' = k + |H_k| + 1$.

Apply memoryless determinacy of parity games.

Fix a winning strategy by choosing, for each (t, a) in $H_{k'} \times \{0, 1\}$, a bit $b(t, a)$.

Define the winning strategy by $\psi(X, Y, x) :=$

$$\bigvee_{(t,a)} (T_{k'}([0, x-1], X \cap [0, x], Y \cap [0, x]) = t \wedge X(x) = a \wedge b(t, a))$$

Proof Sketch for FO(S)

Apply Hanf's Theorem:

$\varphi(X, Y)$ can only express the existence of segment words in a play (if multiple existence, then only up to a fixed threshold).

$\varphi(X, Y)$ specifies a **weak Muller game** (in which only occurrence and non-occurrence of states is relevant).

Reduction to weak parity games only uses the **appearance record AR**.

Again use positional determinacy, and note that AR is FO(S)-definable.

On $FO+\exists^\omega(S)$

The idea :

Winning condition may use \exists^ω .

But models for strategies are finite prefixes of plays – where \exists^ω is irrelevant.

Example (derived from Dziembowski, Jurdzinski, Walukiewicz, LICS 1997)

Player 1 picks from $\{a, b, c\}$

Player 2 picks from $\{0, 1, 2\}$

Winning condition:

“maximal number occurring infinitely often (0 or 1 or 2) says how many elements of $\{a, b\}$ occur infinitely often”

Perspectives I

Winning conditions given by MSO-formulas $\varphi(X, Y, \mathbb{P})$ with fixed set $\mathbb{P} \subseteq \mathbb{N}$.

A.R. (CSL 2006):

- Determinacy holds with operators $P \mapsto Q$ which are definable by MSO-formulas $\psi(X, Z, x)$:
Given P, n , choose $Q(n) = 1$ iff $(\mathbb{N}, <) \models \psi(P, \mathbb{P}, n)$
[Since ψ is not bounded, this does not necessarily define a strategy.]
- Recursive strategies suffice if $\text{MSO-Th}(\mathbb{N}, <, \mathbb{P})$ is decidable.

Perspectives II

- **How essential is the Composition Theorem?**

Are there serious extensions of MSO where the main result still holds?

- **General perspective:**

Develop a precise understanding of the relation between requirements and winning strategies.

Language theoretical view: Relate classes of ω -languages (specifications) to classes of $*$ -languages (winning strategies).