2488

Logical characterization of the counting hierarchy

Juha Kontinen

Outline

- Preliminaries
- PP and the counting hierarchy (CH)
- Second-order generalized quantifiers
- The characterization of CH in terms of majority quantifiers
- General proportional quantifiers
- Monadic CH

Preliminaries

PP: $L \in PP$ iff there is a polynomial time-bounded nondeterministic Turing machine M such that $x \in L$ iff more than half of the computations of M with input x halt with "yes".

Properties

- $NP \cup (co - NP) \subseteq PP \subseteq PSPACE$.
- PP closed under intersection and union.
- $PH \subseteq P^{PP}$ (Toda's theorem).

The counting hierarchy (CH):

- $C_oP = P$,
- $C_{k+1}P = PP^{C_kP}$,
- $CH = \cup_{k \in N} C_kP$.

Note that $PH \subseteq CH \subseteq PSPACE$.

Definition of CH in terms of the polynomial counting quantifier $\mathcal{C}$

Pairing function String (x, y) is defined by doubling the bits of x followed by the string $01y$.

Definition Let K be a class of languages. Then $L \in \mathcal{C}K$ if there is $L' \in K$ and polynomial p s.t. $x \in L$ iff

$$|\{y : \ |y| = p(|x|) \text{ and } (x, y) \in L'\}| > 2^{p(|x|)-1}.$$

Definition of CH in terms of $\mathcal{C}$:

- $C_0 P = P$,
- $C_{k+1} P = \mathcal{C} C_k P$,
- $CH = \cup_{k \in N} C_k P$.

J. Torán showed that $\mathcal{C}K = PP^K$ for all classes K in CH.

Second-order generalized quantifiers

Relevant quantifiers

- The k-ary second-order existential quantifier $\exists^2_k$.
- The k-ary second-order majority quantifier $Most^k$:

$$\mathbf{M} \models Most^k X\, \psi(X) \Leftrightarrow |\psi^{\mathbf{M}}| > 2^{|M|^k - 1},$$

where $\psi^{\mathbf{M}} = \{A \subseteq M^k \mid \mathbf{M} \models \psi(A)\}$.

- The relativized k-ary majority quantifier $Most^k_r$:

$$\mathbf{M} \models Most^k_r X, Y\, (\psi, \phi) \Leftrightarrow |\psi^{\mathbf{M}} \cap \phi^{\mathbf{M}}| > 1/2 |\psi^{\mathbf{M}}|.$$

- The k-ary second-order Rescher quantifier R^k:

$$\mathbf{M} \models R^k X, Y\, (\psi, \phi) \Leftrightarrow |\psi^{\mathbf{M}}| > |\phi^{\mathbf{M}}|.$$

Definability results

Note that $Most^k \leq Most_r^k \leq R^k$, since

$$\models Most^k Y\, \psi(Y) \Leftrightarrow Most_r^k X, Y\, (X = X, \psi(Y)),$$
$$\models Most_r^k X, Y\, (\psi, \phi) \Leftrightarrow R^k X, Y\, (\psi \wedge \phi, \psi \wedge \neg\phi).$$

Proposition The quantifier $\exists_k^2$ is definable in $FO(Most^k)$.

Proof Given $\psi(X)$, we can express $\mathbf{M} \models \exists_k^2 X\, \psi(X)$ using $Most^k$ as follows:

- The case $\mathbf{M} \models \psi(M^k)$ can be expressed in FO.
- If $\mathbf{M} \models \psi(A)$ and there is $\overline{a} \in M^k$ s.t. $\overline{a} \notin A$, then

  $$|\{B \subseteq M^k \mid \overline{a} \in B\} \cup \psi^{\mathbf{M}}| > 2^{|M|^k - 1},$$

  which can be expressed as

  $$\exists x_1 \ldots \exists x_k (Most^k Y\, (Y(\overline{x}) \vee \psi(Y))).$$

Proposition R^k is definable in $FO(Most^{k+1})$.

Proof Given $\psi(X)$ and $\phi(Y)$, where X, Y k-ary, we express $|\psi^{\mathbf{M}}| > |\phi^{\mathbf{M}}|$ using $Most^{k+1}$ as follows:

1. Let $\overline{a} \in M^{k+1}$ and $G = \{A \subseteq M^{k+1} \mid \overline{a} \in A\}$.

2. Now $|\psi^{\mathbf{M}}| > |\phi^{\mathbf{M}}|$ is equivalent with

$$|(G \setminus \phi^{*\mathbf{M}}) \cup \psi^{*\mathbf{M}}| > 2^{|M|^{k+1}-1}.$$

Proposition Let $k \geq 2$. Then the quantifier R^k is definable in $FO(Most^k)$.

The characterization of CH in terms of majority quantifiers

Definition $FO(Most)$ is FO extended by $Most^k$ for all $k \in N^*$. L_φ is the language determined by φ, assuming a fixed encoding of structures $\mathbf{M}$ to strings $bin(\mathbf{M})$.

Definition A language L_1 is reducible to L_2 via a *Polynomial time disjunctive truth-table reduction* if there is a f, computable in P, mapping an input x to $y_1, \ldots, y_j$ s.t.

$$x \in L_1 \text{ iff } y_i \in L_2 \text{ for some } 1 \leq i \leq j.$$

Lemma Let $k \in N$. Then

- $C_k P$ is closed under intersection,
- $C_k P$ is closed under complement,
- $C_k P$ is closed under disjunctive truth-table reductions.

Theorem The logic $FO(Most)$ strongly captures CH.

Proof "$FO(Most) \subseteq CH$" using induction on φ.

By Lemma above, if $L_\varphi, L_\psi \in C_kP$, then

- $L_{\varphi\wedge\psi} \in C_kP$,
- $L_{\neg\varphi} \in C_kP$,
- $L_{\exists x\varphi} \in C_kP$.

Finally, $L_{Most^k X\,\varphi} \in PP^{L_\varphi} \subseteq C_{k+1}P$.

"$C_kP \subseteq FO(Most)$", using induction on k. We restrict attention to binary strings and assume built-in predicates for $+$ and $\times$.

Case $k = 1$ and $C_1P = PP$. Let N be a nondeterministic machine using time n^k for inputs of length n.

Then, for all $\mathbf{M}$:

$$N \text{ accepts } bin(\mathbf{M}) \text{ iff } \mathbf{M} \models Most_r^l X, Y\,(\phi, \psi),$$

where

- $\phi(X)$ says "Relation X codes an n^k time-bounded run of N",
- $\psi(Y)$ says "Relation Y codes an n^k time-bounded run which accepts".

Suppose $L \in C_{k+1}P = \mathcal{C}C_kP$. Then there is $L' \in C_kP$ s.t. $x \in L$ iff

$$|\{y \;:\; |y| = |x|^r \text{ and } (x, y) \in L'\}| > 2^{|x|^r - 1}.$$

By the assumption, there is $\phi \in FO(Most)$ s.t. $L_\phi = L'$.

Let $\phi^*(R) \in FO(Most)$ s.t. for all x and y, where $|y| = |x|^r$:

$$x \models \phi^*(y) \Leftrightarrow (x, y) \models \phi.$$

Then $L = L_\chi$, where $\chi = Most^r R\, \phi^*(R)$.

Definition Let $qr(\varphi)$ be the maximal nesting depth of the quantifiers $Most^k$ in $\varphi \in FO(Most)$.

Proposition On binary strings equipped with $+$ and $\times$:

1. $PP = \{L_\varphi \mid \varphi \in FO(Most),\ qr(\varphi) \leq 1\}$,
2. $C_kP = \{L_\varphi \mid \varphi \in FO(Most),\ qr(\varphi) \leq k\}$,
3. $PH \subseteq \{L_\varphi \mid \varphi \in FO(Most),\ qr(\varphi) \leq 2\}$.

Proposition On arbitrary τ structures,

$$C_kP[\tau] = \{L_\varphi \mid \varphi \in FO(Most)[\tau],\ qr(\varphi) \leq k+3\}.$$

General Proportional quantifiers

Fact For any rational $0 < \delta < 1$, $PP_\delta = PP$, where PP_δ is defined by the input acceptance condition "more than an δ-fraction of accepting computations".

Definition Let $0 < \delta < 1$ be a real number. The k-ary proportional quantifier $\mathcal{Q}_\delta^k$ is defined by

$$\mathbf{M} \models \mathcal{Q}_\delta^k X \, \psi(X) \Leftrightarrow |\psi^{\mathbf{M}}| > \delta 2^{|M|^k}.$$

$FO(\mathcal{Q}_\delta)$ is FO extended by $\mathcal{Q}_\delta^k$ for $k \in N^*$.

Theorem Let $0 < \delta < 1$. Then

1. If $\delta = s/2^m$ for some $s, m \in N^*$, then $FO(\mathcal{Q}_\delta)$ strongly captures the counting hierarchy.
2. If δ is not of the form $s/2^m$, then $FO(\mathcal{Q}_\delta)$ satisfies the 0-1 law, i.e., every sentence $\varphi \in FO(\mathcal{Q}_\delta)[\tau]$, over relational τ, has asymptotic probability 0 or 1.

Idea of the Proof

1. Definability results of $\exists_k^2$ and R^k generalize, thus, it follows that $FO(\mathcal{Q}_\delta) \geq FO(Most)$. On the other hand, since $PP_\delta = PP$, we have $FO(\mathcal{Q}_\delta) \subseteq CH$.

2. The logic $FO(\mathcal{Q}_\delta)$ has almost sure elimination of quantifiers.

Remark In case 2, e.g., $EVEN \in P = C_0P$ cannot be expressed in $FO(\mathcal{Q}_\delta)$.

Corollary Every sentence of the form

$$Most^{k_1} X_1 Most^{k_2} X_2 \dots Most^{k_j} X_j \, \varphi,$$

where φ is a FO sentence, has asymptotic probability 0 or 1.

Monadic CH

MSO is monadic second-order logic.

Proposition $FO(Most^1) \geq MSO$.

Definition First-order Rescher quantifier R:

$$\mathbf{M} \models R^k x, y\,(\psi(x), \phi(y)) \Leftrightarrow |\psi^{\mathbf{M}}| > |\phi^{\mathbf{M}}|.$$

Proposition The logic $FO(Most^1)$ defines R.

Corollary $FO(Most^1) > MSO$.

Paper (Preprint 435) available at:

http://mathstat.helsinki.fi/reports/

Thank you!