Definability of Summation Problems for Abelian Groups and Semigroups.

Anuj Dawar

University of Cambridge

joint work with Farid Abu-Zaid, Erich Grädel and Wied Pakusa

LICS 2017

Logical Structures in Computation Reunion
Simons Institute, 12 December 2017

Logics for Polynomial Time

Long-standing open question in *descriptive complexity theory*:

> *Is there a logic in which we can express exactly the polynomial-time properties of finite relational structures?*

Some logics studied in this context:

- FP—fixed-point logic;
- FPC—fixed-point logic *with counting*;
- FPrk—fixed-point logic with *rank* operators;
- CPT—choiceless polynomial-time;
- CPT^-—choiceless polynomial-time *without counting*.

Map

A map of the logics:

$$
\begin{tikzcd}
\mathsf{FP} \arrow[r] \arrow[dr] & \mathsf{FPC} \arrow[r] \arrow[dr] & \mathsf{FPrk} \arrow[dr] & \\
& \mathsf{CPT}^- \arrow[r] & \mathsf{CPT} \arrow[r] & \mathrm{P}
\end{tikzcd}
$$

All inclusions shown except the rightmost two are known to be proper.

Fixed-Point Logic

FP is an extension of first-order logic with *inductive definitions*

FP captures P on *ordered* finite structures. (**Immerman; Vardi**)

On general finite structures, the expressive power of FP is weak.
Indeed, it obeys a 0–1 law. (**Blass-Gurevich-Kozen**)

A proof by **Kolaitis-Vardi** based on *pebble games* and *extension axioms* extends this to $L^{\omega}_{\infty\omega}$—infinitary logic with finitely many variables.

In particular, it follows that FP cannot express *counting* properties.

Asymptotic Probabilities

Let P be a class (or *property*) of τ-structures.

Let $\mathcal{S}_n$ consist of τ-structures on the universe $[n] = \{1, \ldots, n\}$.

$$\mu_n(P) = \frac{|P \cap \mathcal{S}_n|}{|\mathcal{S}_n|}$$

is the proportion of n element structures with property P.

$$\mu(P) = \lim_{n \to \infty} \mu_n(P)$$

if defined, is the *asymptotic probability* of P.

If P is definable by a sentence of FP, then $\mu(P)$ is defined and in $\{0, 1\}$.

Fixed-Point Logic with Counting

FPC is an extension of FP with a mechanism for *counting*

- variables ranging over *numbers* in addition to element variables;
- $\#x\varphi$ is a *term* denoting the *number* of elements that satisfy φ;
- quantification over number variables is *bounded*: $(\exists \mu < t)\,\varphi$.

Highly expressive: captures P over all *proper minor-closed* classes.

(Grohe).

There are classes of graphs in P that cannot be defined in FPC.

(Cai-Fürer-Immerman)

Extensions of FPC

Key examples of properties in P that we know are *not* definable in FPC include solving systems of linear equations over

- *finite fields*;
- *finite rings*;
- *finite Abelian groups*. **(Atserias-Bulatov-D.)**

Extensions of FPC that have been studied include

- FPrk–fixed point logic with operators for the *rank of a matrix* over a *finite field*. **(D.-Grohe-Holm-Laubner; Grädel-Pakusa)**.
- CPT–choiceless polynomial-time with counting. The polynomial-time restriction of **Blass-Gurevich-Shelah** *abstract state machines*.

For both of these it remains open to establish a separation from P.

Choiceless Polynomial Time

CPT can be understood as an extension of FPC with *higher-order objects*.

A CPT formula φ can be translated to an FPC formula $\varphi^\star$ so that the evaluation of φ on a finite structure $\mathbb{A}$ is equivalent to the evaluation of $\varphi^\star$ on a finite extension of $\mathbb{A}$ with higher-order objects which is:

- *polynomial* in the size of $\mathbb{A}$;
- closed under *automorphisms* of $\mathbb{A}$.

CPT$^-$ is a similar extension of FP.

NB: CPT$^-$ obeys a 0-1 law **(Shelah)**.

Challenge: Separating CPT from PTime

Establishing a separation of CPT from P is a major research goal.

In 2002, **Blass, Gurevich, Shelah** listed *six* open problems, of which the first four are:

1. Can *CFI* graphs be distinguished in CPT?
2. Can *multipedes* be ordered in CPT?
3. Can *perfect matching* on graphs be decided in CPT?
4. Can the *determinant* of a matrix over a finite field be defined in CPT?

CFI graphs

The construction of **Cai, Fürer and Immerman** gives for each *ordered graph* G, a pair of graphs $\mathcal{G}_0$ and $\mathcal{G}_1$ which are *not isomorphic* but, for sufficiently richly connected G, *indistinguishable* in FPC

1. *Can a* CPT *program distinguish between the (unpadded) Cai, Fürer, Immerman graphs* $\mathcal{G}_0$ *and* $\mathcal{G}_1$*?*

They were shown to be distinguished in CPT^- in **(D., Richerby, Rossman 2008)**.

Multipedes

Multipedes were defined by **Gurevich and Shelah** to give a class of finite structures that was *first-order definable*, *rigid* but in which no order is definable in FPC.

> *2. Can isomorphism of multipedes with shoes be decided by a* CPT *program?*

It is a consequence of results of **(Abu Zaid, Grädel, Grohe, Pakusa 2014)** that it can.

Matching

A *perfect matching* in a graph G is a subset M of its edges such that every vertex of G is incident on *exactly one* vertex of M.

Blass, Gurevich and Shelah showed that deciding the existence of perfect matchings for *bipartite* graphs is in FPC but not in CPT^-.

> *3. Can a* CPT *program decide whether a given graph (not necessarily bipartite) admits a complete matching?*

It is shown in **(Anderson, D., Holm 2015)** that the existence of perfect matchings in general graphs is in FPC.

Determinants

4. Can a CPT *program compute, up to sign, the determinant of an* $I \times J$ *matrix over a finite field (where* $|I| = |J|$*)?*

Rossman showed that determinants could be computed in CPT by implementing a version of Csanky's algorithm.

Holm improved this to FPC.

Abelian Subset Sum

Blass, Gurevich 2005 introduce a new challenge problem for CPT.

> *Given a commutative semigroup S in the form of the multiplication table and given $X \subseteq S$ and an element $y \in S$, is y the sum of all elements of X?*

This is attributed to **Rossman** with the quote:

> *"This is the most basic problem I can think of that appears difficult for* CPT *but is obviously polynomial time. I don't even know the answer when S is an abelian group, or even a direct product of cyclic groups $\mathbb{Z}_2$"*

Results

ASS: Given a *commutative semigroup* S in the form of the multiplication table and given $X \subseteq S$ and an element $y \in S$, is y the sum of all elements of X?

1. ASS on finite commutative semigroups is in FPC.
2. ASS, on *abelian groups* or even direct products of cyclic groups $\mathbb{Z}_2$ is *not* in FP or CPT^-.
3. A *first-order reduction* from ASS on *abelian groups* to solvability of linear equation systems over *finite rings*.

ASS for semigroups in FPC

- *Abelian semigroup* $(S, +)$, $X \subseteq S$

$$\Sigma^k(g) = \Big\{(x_1, \ldots, x_k) \in X^k \,:\, x_i \neq x_j \,(i \neq j), \sum_i x_i = g\Big\}$$

- $\Sigma^k(g) \neq \emptyset \quad \iff \quad g$ is a k-sum of elements from X
- $\sum X = g \quad \iff \quad \Sigma^n(g) \neq \emptyset \qquad$ (where $n = |X|$)

Idea: Inductively ($1 \leq k \leq n$) define the sets $\Sigma^k(g)$; *however:*

- Constructing the sets $\Sigma^k(g)$ explicitly *not possible*; and
- Maintaining "$\Sigma^k(g) \neq \emptyset$" *not sufficient*

Solution: Use *counting mechanism* of FPC to maintain $|\Sigma^k(g)|$.

ASS for semigroups not in CPT^-

CPT^- cannot express *modular counting* **(Blass, Gurevich, Shelah' 99)**

Given a set T and some $n \geq 2$.

- Fix some $\star \notin T$
- Define the *commutative semigroup* $S[T]$ over $T \cup \{\star\}$, by setting

$$x + y = \star$$

- Consider $G = S[T] \times \mathbb{Z}_n$ with subset $X = T \times \{1\}$
- Then $\sum X = (\star, i) \iff |T| \equiv i \mod n$

Question: What happens if we restrict to Abelian *groups*?

Not Even for Groups

Consider expansions of n-fold product of $\mathbb{Z}_p$ by set X (for some fixed *prime* p)

$$S(n) = \{(\mathbb{Z}_p^n, +, X) : 0 \in X\}$$

$\mu_n(\psi)$— the probability that a *randomly chosen* $G \in S(n)$ satisfies ψ

Theorem
For every sentence ψ of FP: $\lim_{n\to\infty} \mu_n(\psi) \in \{0, 1\}$
This can be shown by defining suitable *extension axioms* for this class of structures.

ASS is not FP-definable, as *modular counting* reduces to it.

Remark: This can be generalized to prove *undefinability* in CPT^- using Shelah's techniques for the 0-1 law

New Challenge Problems

In ASS, the semigroup is given *explicitly* by its multiplication table.

Such problems can be more challenging if the algebraic structure is given *succinctly*.

An interesting such problem (though not a subset sum problem) is given by *permutation group membership*.

Permutation Group Membership

Given a collection $\rho_1, \ldots, \rho_m \in \mathsf{Sym}(n)$ of permutations of the set $[n]$.

> *(say, as a structure with universe $[n] \uplus [m]$, and a ternary relation $\rho_i(j) = k$ for $i \in [m]$ and $j, k \in [n]$)*

and a permutation $\sigma \in \mathsf{Sym}(n)$.

> *Is σ in $\langle \rho_1, \ldots, \rho_m \rangle$?*

This problem is in P (by the *Schreier-Sims* algorithm) and known to be *not* in FPC.

Is it in CPT?
Either answer would have interesting consequences.