Finite Model Theory and Graph Isomorphism. IV.

Anuj Dawar

University of Cambridge Computer Laboratory
visiting RWTH Aachen

Beroun, 14 December 2013

Recapitulation

Finite Model Theory gives rise to notions of *indistinguishability* on finite structures, such as graphs. These are used to prove inexpressibility results for various logics.

These *equivalences* are often characterised by games.

When the relations of indistinguishability are computable in *polynomial time*, they give rise to *tractable approximations* of graph isomorphism.

In many cases, they give a *structural explanation* of when certain *graph classes* admit polynomial time isomorphism tests.

Recapitulation. II

The equivalences $\equiv^{C^k}$ correspond (as a family) to the k-dimensional *Weisfeiler-Lehman* ismorphism test.

This family of equivalences has a number of different *characterisations* in combinatorics, logic and linear programming.

It captures isomorphism in many significant *graph classes* including, most generally, any graph class excluding a minor.

There are graphs (of *degree* bounded by 3 and *colour-class size* bounded by 4) in which $\equiv^{C^k}$ fails to capture isomorphism.

This can be used to show that FPC does not express *all* polynomial-time properties of graphs.

Solvability of Linear Equations

It has been shown by similar methods that the problem of solving linear equations over the two element field $\mathbb{Z}_2$ is not definable in FPC.
(Atserias, Bulatov, D. 09)

The question arose in the context of definability of *Constraint Satisfaction Problems*.

The problem is clearly solvable in polynomial time by means of Gaussian elimination.

Undefinability in FPC

Take G a 3-regular, connected graph with treewidth $> k$.
Define equations $\mathbf{E}_{\mathcal{G}}$ with two variables x_0^e, x_1^e for each edge e.
For each vertex v with edges e_1, e_2, e_3 incident on it, we have eight equations:

$$E_v : \qquad x_a^{e_1} + x_b^{e_2} + x_c^{e_3} \equiv a + b + c \pmod 2$$

$\tilde{\mathbf{E}}_{\mathcal{G}}$ is obtained from $\mathbf{E}_{\mathcal{G}}$ by replacing, for exactly one vertex v, E_v by:

$$E'_v : \qquad x_a^{e_1} + x_b^{e_2} + x_c^{e_3} \equiv a + b + c + 1 \pmod 2$$

We can show: $\mathbf{E}_{\mathcal{G}}$ is satisfiable; $\tilde{\mathbf{E}}_{\mathcal{G}}$ is unsatisfiable;
$\mathbf{E}_{\mathcal{G}} \equiv^{C^k} \tilde{\mathbf{E}}_{\mathcal{G}}$ follows by the same proof as for **Cai, Fürer, Immerman** graphs.

Satisfiability

$\mathbf{E}_G$ is satisfiable.

by setting the variables x_i^e *to* i.

$\tilde{\mathbf{E}}_G$ is unsatisfiable.

Consider the subsystem consisting of equations involving only the variables x_0^e.
The sum of all left-hand sides is

$$2\sum_e x_0^e \equiv 0 \pmod 2$$

However, the sum of right-hand sides is 1.

Rank Operators

This motivates the introduction of an operator for *matrix rank* into the logic.

We have, as with FPC, terms of *element sort* and *numeric sort*.

> *We interpret $\eta(x, y)$—a term of numeric sort—in G as defining a matrix with rows and columns indexed by elements of G with entries $\eta[a, b]$.*
>
> *$\mathrm{rk}_{x,y}\eta$ is a term denoting the number that is the rank of the matrix defined by $\eta(x, y)$.*

To be precise, we have, for each finite field $\mathbb{GF}(q)$ (q prime), an operator rk^q which defines the rank of the matrix with entries $\eta[a, b] (\bmod q)$.

(D., Grohe, Holm, Laubner, 2009)

FPrk vs. FPC

Adding rank operators to FP, we obtain a proper extension of FPC.

$$\#x\varphi \quad = \quad \mathrm{rk}_{x,y}[x = y \land \varphi(x)]$$

In FPrk we can express the solvability of linear systems of equations, as well as the Cai-Fürer-Immerman graphs.

FOrk

More generally, for each prime p and each arity m, we have an operator rk^p_m which binds $2m$ variables and defines the rank of the $n^m \times n^m$ matrix defined by a formula $\varphi(\mathbf{x}, \mathbf{y})$.

FOrk, the extension of first-order logic with the rank operators is already quite powerful.

- it can express *deterministic transitive closure*;
- it can express *symmetric transitive closure*;
- it can express solvability of linear equations.

Games for Logics with Rank

Define the equivalence relation $G \equiv^{R^k_{\Omega,m}} H$ to mean that G and H are not distinguished by any formula of FOrk using operators rk^p_m (for $p \in \Omega$) and with at most k variables.

This equivalence relation has a characterisation in terms of *games*.

(**D., Holm 2012**)

What can we say about the approximations of isomorphism given by $\equiv^{R^k_{\Omega,m}}$?

Partition Games

We formulate a general framework of *partition games*, played with k pebbles.

First consider a simple version.

- *Spoiler* picks a pebble from G and the corresponding pebble from H.
- *Duplicator* reponds with
  - a partition $\mathbf{P}$ of $V(G)$
  - a partition $\mathbf{Q}$ of $V(H)$
  - a bijection $f : \mathbf{P} \to \mathbf{Q}$ such that a condition *(*)* holds.
- *Spoiler* chooses a part $A \in \mathbf{P}$ and places the chosen pebbles on an element in A and the matching pebble on an element in $f(A)$.

With no restriction *(*)*, we have a game for $\equiv^k$.

If we require A and $f(A)$ to have the same size for all $A \in \mathbf{P}$, we have a game for $\equiv^{C^k}$.

Stable Partitions

The equivalence defined by the game is the *stable partition* of k-tuples reached by refining equivalences:

$$\equiv_0^k \supseteq \equiv_1^k \supseteq \cdots \supseteq \equiv_i^k \quad \cdots$$

Each tuple $\mathbf{a}$ and each $\equiv_p^k$ induce a partition of V where u and v are in the same part if any way of substituting them into $\mathbf{a}$ gives $\equiv_p^k$-tuples.

Two tuples are $\equiv_{p+1}^k$-equivalent iff they induce *similar* partitions.

Games for Rank Quantifiers

Since the rank quantifier rk_1^p binds *two* variables, we have the following variation.

- *Spoiler* picks 2 pebbles from G and the corresponding pebbles from H and $p \in \Omega$.
- *Duplicator* reponds with
  - a partition $\mathbf{P}$ of $V(G) \times V(G)$
  - a partition $\mathbf{Q}$ of $V(H) \times V(H)$
  - a bijection $f : \mathbf{P} \to \mathbf{Q}$ such that for all labellings $\gamma : \mathbf{P} \to \mathbb{GF}(p)$

$$\mathrm{rank}(\sum_{A \in \mathbf{P}} \gamma(A) M_A) = \mathrm{rank}(\sum_{A \in \mathbf{P}} \gamma(A) M_{f(A)})$$

- *Spoiler* chooses a part $A \in \mathbf{P}$ and places the chosen pebbles on a pair in A and the matching pebbles on a pair in $f(A)$.

This characterises the equivalence $\equiv^R_{k,\Omega,1}$.

Games for Logics with Rank

The *arity hierarchy* does not collapse for rank logics, so the general game is defines as follows.

- *Spoiler* picks $2m$ pebbles from $V(G)$ and from $V(H)$ and $p \in \Omega$.
- *Duplicator* reponds with
  - a partition $\mathbf{P}$ of $V(G)^m \times V(G)^m$
  - a partition $\mathbf{Q}$ of $V(H)^m \times V(H)^m$
  - a bijection $f : \mathbf{P} \to \mathbf{Q}$ such that for all labellings $\gamma : \mathbf{P} \to \mathbb{GF}(p)$

$$\mathrm{rank}(\sum_{A \in \mathbf{P}} \gamma(A) M_A) = \mathrm{rank}(\sum_{A \in \mathbf{P}} \gamma(A) M_{f(A)})$$

- *Spoiler* chooses a part $A \in \mathbf{P}$ and places the chosen pebbles on an m-tuple in A and the matching pebbles on an m-tuple in $f(A)$.

This characterises the equivalence $\equiv^R_{k,\Omega,m}$.

Limitations of the Game

The arbitrary arity *m* and the *matrix-equivalence* condition make the game unwieldy. It's difficult to prove inexpressibility results with it.

- the relation $\equiv^k$ can itself be defined in FP; and
- the relation $\equiv^{C^k}$ can itself be defined in FPC.

Both of these follow by an inductive definition of the game winning positions.

Is $\equiv^R_{k,\Omega,m}$ definable in FPrk?
Is it even decidable in *polynomial time*?

Stable Rank Partitions

In the stepwise refinement of equivalences converging to $\equiv^R_{k,\Omega,m}$

$$\equiv_0 \supseteq \equiv_1 \supseteq \cdots \supseteq \equiv_i \quad \cdots$$

to decide if $\mathbf{a}$ and $\mathbf{a}'$ are equivalent at stage $p+1$, we can compute the partitions of $V^m \times V^m$ induced using the equivalence $\equiv_p$ by $\mathbf{a}$ and $\mathbf{a}'$ respectively.

We then need to compute the rank of the matrices formed by taking *all linear combinations* of parts of the partitions.
There are potentially *exponentially* many of these.

Invertible Map Game

We define a variant parition game with a *stronger* condition:

> *There is an invertible matrix S such that for all labellings* $\gamma : \mathbf{P} \to \mathbb{GF}(p)$, $\sum_{A \in \mathbf{P}} \gamma(A) M_A = S(\sum_{A \in \mathbf{P}} \gamma(A) M_{f(A)}) S^{-1}$

Since this (unlike the rank function) is *linear* on the space of matrices, it is sufficient to check it on a basis, which is given by the individual parts of $\mathbf{P}$.

That is, it suffices to check, for each $A \in \mathbf{P}$ that $M_A = S M_{f(A)} S^{-1}$.

A result of **(Chistov, Karpinsky, Ivanyov 1997)** guarantees that *simultaneous similarity* of a collection of matrices is decidable in polynomial time.

Approximations of Isomorphism

This gives us a family of polynomial-time isomorphism tests $\equiv^{\mathrm{IM}}_{k,\Omega,m}$.

- $\equiv^{\mathrm{IM}}_{k,\Omega,m}$ refines $\equiv^{R}_{k,\Omega,m}$
- $\equiv^{\mathrm{IM}}_{k,\Omega,m}$ gets finer as we increase any of k, m or Ω.
- The *CFI* graphs are distinguished by $\equiv^{\mathrm{IM}}_{4,\{2\},1}$

(D., Holm 2012)

Coherent Algebras

Weisfeiler and Lehman presented their algorithm in terms of *cellular algebras*.

These are algebras of matrices on the *complex numbers* defined in terms of *Schur multiplication*:

$$(A \circ B)(i,j) = A(i,j)B(i,j)$$

They are also called *coherent configurations* in the work of **Higman**.

Definition:
A *coherent algebra* with index V is an algebra $\mathcal{A}$ of $V \times V$ matrices over $\mathbb{C}$ that is:

> *closed under Hermitian adjoints; closed under Schur multiplication; contains the identity I and the all 1's matrix J.*

Coherent Algebras

One can show that a coherent algebra has a *unique basis* $A_1, \ldots, A_m$ (i.e. every matrix in the algebra can be expressed as a linear combination of these) of *0-1* matrices which is closed under *adjoints* and such that

$$\sum_i A_i = J.$$

One can then derive *structure constants* p_{ij}^k such that

$$A_i A_j = \sum_k p_{ij}^k A_k.$$

Associate with any graph G, its *coherent invariant*, defined as the smallest coherent algebra $\mathcal{A}_G$ containing the adjacency matrix of G.

Weisfeiler-Lehman method

Say that two graphs G and H are *WL*-equivalent if there is an isomorphism between their *coherent invariants* $\mathcal{A}_G$ and $\mathcal{A}_H$.

G and H are *WL*-equivalent if, and only if, $G \equiv^{C^3} H$.

Friedland (1989) has shown that two coherent algebras with standard bases $A_1, \ldots, A_m$ and $B_1, \ldots, B_m$ are isomorphic if, and only if, there is an invertible matrix S such that

$$SA_iS^{-1} = B_i \quad \text{for all } 1 \leq i \leq m.$$

Complex Invertible Map Game

Define the k-pebble *complex invertible map game*.

- *Spoiler* picks 2 pebbles from G and the corresponding pebbles from H.
- *Duplicator* reponds with
  - a partition $\mathbf{P}$ of $V(G) \times V(G)$
  - a partition $\mathbf{Q}$ of $V(H) \times V(H)$
  - a bijection $f : \mathbf{P} \to \mathbf{Q}$ and an invertible matrix S over $\mathbb{C}$ such that for all $A \in \mathbf{P}$: $\quad M_A = SM_{f(A)}S^{-1}$.
- *Spoiler* chooses a part $A \in \mathbf{P}$ and places the chosen pebbles on a pair in A and the matching pebbles on a pair in $f(A)$.

The game defines an equivalence $\equiv^{\mathrm{IM}}_{\mathbb{C},k}$ over graphs.

We can show $\equiv^{\mathrm{IM}}_{\mathbb{C},k+1} \;\subseteq\; \equiv^{C^k} \;\subseteq\; \equiv^{\mathrm{IM}}_{\mathbb{C},k-1}$.

Invertible Map Games

The *complex invertible map game* gives us essentially the same family of approximations of isomorphism as the *Weisfeiler-Lehman* method and the *bijection games*.

The *invertible map game* we defined in connection with rank logics can then be seen as the tightening of these approximations to a game where *Duplicator* is required to choose the invertible map S not over $\mathbb{C}$ but over a *finite field* whose *characteristic* has been chosen by *Spoiler*.

> *Proviso: we defined the latter game with partitions of higher arity. These seem to be unnecessary in the complex invertible map game.*

Colour Class Size 4

Isomorphism for graphs of colour class size 3 is captured by $\equiv^{C^3}$.

Isomorphism for graphs of colour class size 4 is captured by $\equiv^{\mathrm{IM}}_{4,\{2\},1}$.
This is proved by a reduction to the solvability of a system of equations over $\mathbb{GF}(2)$.

(D., Holm 2014)

Inexpressibility

Similarly to the **Cai, Fürer and Immerman** construction, we can construct a sequence of graphs to show that there is no fixed k and no finite set of primes Ω for which $\equiv^{\mathrm{IM}}_{k,\Omega,1}$ is the same as isomorphism.

(D., Holm 2014)

Doing this for $\equiv^{\mathrm{IM}}_{k,\Omega,m}$ for $m > 1$ remains a challenge as the games become very unwieldy.

Research Questions

Is the *arity hierarchy* really strict on graphs? Could it be that $\equiv^{\mathrm{IM}}_{k,\Omega,m}$ is subsumed by $\equiv^{\mathrm{IM}}_{k',\Omega,1}$ for sufficiently large k'?

Show that no fixed $\equiv^{\mathrm{IM}}_{k,\Omega,m}$ is the same as isomorphism on graphs.

Are the relations $\equiv^{\mathrm{IM}}_{k,\Omega,m}$ definable in FPrk?

Does some $\equiv^{\mathrm{IM}}_{k,\Omega,m}$ capture isomorphism on graphs of *bounded colour class size*?

What about graphs of *bounded degree*?