Games and Isomorphism in Finite Model Theory

Part 2

Anuj Dawar
University of Cambridge

Games Winter School, Champéry, 6 February 2013

Review

Games are used to establish *inexpressibility* results for first-order logic and its extensions.

The equivalence relations defined by the games define stratifications of the relation of isomorphism, based on limiting resources.

- *quantifier rank* $\equiv_q$
- *number of variables* $\equiv^k$
- *number of variables* in the presence of *counting quantifiers* $\equiv^{C^k}$.

Stratifications of Isomorphism

$\equiv_q$ has finitely many equivalence classes for each q.

$\equiv^k$ has infinitely many classes for $k \geq 2$, but for each k, there is a *monster class* that includes *almost all* graphs.

$\equiv^{C^k}$, already for $k = 2$ distinguishes between *most* graphs.

For two randomly chosen graphs G_1 and G_2 of the same size, with *high probability* $G_1 \not\equiv^{C^2} G_2$.

Linear Algebra in IFPC

The limitations on the expressive power of IFPC, and of $\equiv^{C^k}$ as an approximation of graph isomorphism, are based on coding *linear algebra over finite fields*.

A considerable amount of linear algebra can be expressed in IFPC.

Over the *rational numbers*, we can

- define the *determinant*, *characteristic polynomial*; *inverse* and *rank* of a matrix;
- test a system of linear equations for *solvability*; and **(Holm 2010)**
- test feasibility of linear programs by the *ellipsoid method*.

(Anderson, D., Holm 2013)

Over *finite* fields, we can define the *determinant* and *characteristic polynomial*, but not the *rank*.

We cannot determine *solvability* of systems of equations.

Rank Operators

The limitations of IFPC identify a source of new operators.

We can introduce an operator for *matrix rank* into the logic.

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

> We interpret $\eta(x, y)$—a *term* of numeric sort—in $\mathbb{A}$ as defining a *matrix* with rows and columns indexed by elements of A with entries $\eta[a, b]$.
>
> $\mathsf{rk}_{x,y}\eta$ 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 $\mathbf{GF}(q)$ (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)

IFPrk vs. IFPC

Adding rank operators to IFP, we obtain a proper extension of IFPC.

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

Rank operators are a generalized form of counting, as they count the *dimension of a vector space* rather than the *cardinality* of a set.

In IFPrk we can express the solvability of linear systems of equations, as well as the Cai-Fürer-Immerman graphs and the order on multipedes.

FO(rk)

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 $\varphi(\mathbf{x}, \mathbf{y})$.

FO(rk), 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.

Symmetric Transitive Closure

Let $G = (V, E)$ be an *undirected graph* and let s and t be vertices in V.

Define the system of equations $\mathbf{E}_{G,s,t}$ over $\mathbf{GF}(2)$ with variables x_v for each $v \in V$, and equations

- for each edge $e = u, v \in E$: $\quad x_u + x_v = 0$;
- $x_s = 1 \quad x_t = 0$.

$\mathbf{E}_{G,s,t}$ is solvable if, and only if, there is no path from s to t in G.

Arity Hierarchy

In the case of IFPC, adding counting operators of arities higher than 1 does not increase expressive power. These can all already be defined in IFPC with *unary* counting.

This is not the case with IFPrk:

> For each m, there is a property definable in FO(rk^2_{m+1}) that is not definable in IFP(rk_m).

The proof is based on a construction due to Hella, and requires vocabularies of increasing arity.

It is conceivable that *over graphs*, the arity hierarchy collapses.

Games for Logics with Rank

Define the equivalence relation $\mathbb{A} \equiv^{R}_{k,\Omega,m} \mathbb{B}$ to mean that $\mathbb{A}$ and $\mathbb{B}$ are not distinguished by any formula of FO(rk) with at most k variables using operators rk^p_m for p in the finite set of primes Ω.

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

(**D., Holm 2012**)

This game can been used to show that for *distinct* primes p, q, solvability of linear equations $\mod q$ cannot be defined in IFP with operators rk^p_1.

Partition Games

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

First consider a simple version.

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

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

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

Games for Rank Quantifiers

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

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

$$\mathsf{rank}(M^{\gamma}) = \mathsf{rank}(M^{\gamma \circ f^{-1}})$$

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

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

Games for Logics with Rank

Since the *arity hierarchy* does not collapse for rank logics, the general game we define is as follows.

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

$$\text{rank}(M^\gamma) = \text{rank}(M^{\gamma \circ f^{-1}})$$

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

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

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

Is $\equiv^R_{k,\Omega,m}$ definable in IFPrk?

Is it even decidable in *polynomial time*?

Invertible Map Game

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

> There is an invertible matrix S such that for all labellings $\gamma : \mathbf{P} \rightarrow \mathbf{GF}(p)$, $M^{\gamma} = S(M^{\gamma \circ f^{-1}})S^{-1}$

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 $P \in \mathbf{P}$ that $M^{P} = SM^{f(P)}S^{-1}$.

A result of **(Chistov, Karpinsky, Ivanyov 1997)** guarantees that *simultaneous similarity* of a collection of matrices is decidable in polynomial time to get a family of polynomial-time equivalence relations $\equiv^{\text{IM}}_{k,\Omega,m}$.

Approximations of Isomorphism

This gives us a family of polynomial-time isomorphism tests.

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

(D., Holm 2012)

Could the relation $\equiv^{\mathsf{IM}}_{k,\Omega,m}$ be definable in IFPrk?

Colour Refinement

Define, on a graph $G = (V, E)$, a series of equivalence relations:

$$\sim_0 \;\supseteq\; \sim_1 \;\supseteq \cdots \supseteq\; \sim_i \quad \cdots$$

where $u \sim_{i+1} v$ if they have the same number of neighbours in each $\sim_i$-equivalence class.

For a pair of graphs, G_1 and G_2, we take the maximally refined such relation on $G_1 \uplus G_2$ and say $G_1 \sim G_2$ if there are vertices $v_1 \in G_1$ and $v_2 \in G_2$ such that $v_1 \sim v_2$.

It is not hard to see that $G_1 \sim G_2$ if, and only if, $G_1 \equiv^{C^2} G_2$.

Some adjustment is needed if the graphs are not connected.

Weisfeiler-Lehman method

The *k-dimensional Weisfeiler-Lehman* test for isomorphism (as described by **Babai**), generalises colour refinement to k-tuples.

Define a series of refining equivalence relations on k-tuples by, $\mathbf{u} \sim_0 \mathbf{v}$ if they are *partially isomorphic* and $\mathbf{u} \sim_{i+1} \mathbf{v}$ if, and only if, for each $\sim_i$-class α and each $j \leq k$,

$$|\{u \mid \mathbf{u}[u/u_j] \in \alpha\}| = |\{v \mid \mathbf{v}[v/v_j] \in \alpha\}|$$

$G_1 \equiv^{C^{k+1}} G_2$ if, and only if, there are $\mathbf{u} \in G_1$ and $\mathbf{v} \in G_2$ such that:

for all i, $\mathbf{u} \sim_i \mathbf{v}$ in $G_1 \uplus G_2$.

Graph Isomorphism Integer Program

Yet another way of approximating the *graph isomorphism relation* is obtained by considering it as a *0/1 linear program*.

If A_1 and A_2 are adjacency matrices of graphs G_1 and G_2, then $G_1 \cong G_2$ if, and only if, there is a *permutation matrix* P such that:

$$PA_1P^{-1} = A_2 \quad \text{or, equivalently} \quad PA_1 = A_2P$$

Introducing a variable x_{ij} for each entry of P and adding the constraints:

$$\sum_i x_{ij} = 1 \quad \text{and} \quad \sum_j x_{ij} = 1$$

we get a system of equations that has a *0-1 solution* if, and only if, G_1 and G_2 are isomorphic.

Fractional Isomorphism

To the system of equations:

$$PA_1 = A_2P; \quad \sum_i x_{ij} = 1 \quad \text{and} \quad \sum_j x_{ij} = 1$$

add the inequalities

$$0 \leq x_{ij} \leq 1.$$

Say that G_1 and G_2 are *fractionally isomorphic* ($G_1 \cong^f G_2$) if the resulting system has *any real solution*.

$G_1 \cong^f G_2$ if, and only if, $G_1 \equiv^{C^2} G_2$.

(Ramana, Scheiermann, Ullman 1994)

Sherali-Adams Hierarchy

If we have any *linear program* for which we seek a *0-1 solution*, we can relax the constraint and admit *fractional solutions*.

The resulting linear program can be solved in *polynomial time*, but admits solutions which are not solutions to the original problem.

Sherali and Adams (1990) define a way of *tightening* the linear program by adding a number of *lift and project* constraints.

Sherali-Adams Hierarchy

The kth *lift-and-project* of a linear program is defined as follows:

For each constraint $\mathbf{a}^T\mathbf{x} = b$ in the linear program, and each set I of variables with $|I| < k$ and $J \subseteq I$, multiply the constraint by

$$\prod_{i \in I \setminus J} x_i \prod_{j \in J} (1 - x_j)$$

and then *linearize* by replacing x_i^2 by x_i and $\prod_{j \in K} x_j$ by a new variable y_K for each set K.

Say that $G_1 \cong^{f,k} G_2$ if the kth lift-and-project of the *isomorphism program* on G_1 and G_2 admits a solution.

Sherali-Adams Isomorphism

For each k

$$\equiv^{C^{k+1}} \subseteq \ \simeq^{f,k} \ \subseteq \equiv^{C^k}$$

(Atserias, Maneva 2012)

For $k > 2$, the inclusions are strict. **(Grohe, Otto 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 algebras* 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 also 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_1 and G_2 are *WL*-equivalent if there is an isomorphism between their *coherent invariants* $\mathcal{A}_{G_1}$ and $\mathcal{A}_{G_2}$.

G_1 and G_2 are *WL*-equivalent if, and only if, $G_1 \equiv^{C^3} G_2$.

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

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.

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 IFPrk?

Use the games to prove undefinability results for *rank logics*.

- Separate FO(rk) from IFPrk
- Show for some concrete problem that it is not definable in IFPrk.