Games and Symmetric Circuits

Anuj Dawar

Department of Computer Science and Technology, University of Cambridge

FAMT, Les Houches, 27 May 2025

Finite Model Theory: Early Promise

The field of *descriptive complexity* started with the hope that we would:

- characterize complexity classes by means of *logic*
- use logical methods to prove *lower bounds*
- methods largely based on versions of *Ehrenfeucht-Fraïssé* games

Fagin:

- $\exists$SO captures NP; and so $\forall$SO captures coNP.
- Use games to separate $\exists$MSO and $\forall$MSO

Immerman:

- FP captures P and TC captures NL on *ordered structures*.
- Use games to separate FP from TC on *unordered* structures.

Game Arguments

Development of techniques using *games* gave us increasingly sophisticated arguments.

Two examples:

separation of $\exists MSO$ and $\forall MSO$ on ordered graphs **(Schwentick 1994)**

separation of $\exists MSO$ and $\forall MSO$ on graphs with built-in relations that exclude a minor. **(Kreidler, Seese 1998)**

a precursor to later work on tame classes of finite structures.

separation of FPC from P **(Cai, Fürer, Immerman 1992)**

highly influential construction, much used in combination with bijection games of **(Hella 1996)**.

Games and Circuits

Sometimes we can obtain *inexpressibility* results in logic from *lower bounds* in complexity.

FO *does not collapse to its* k*-variable fragment for any fixed* k*.*

(Rossman 2008)

At the same time, we can see game-based techniques from finite model theory as giving us *lower bounds* on *restricted models of computation*. particularly, *symmetric models*.

FPC defines exactly the properties decidable by *P-uniform* families of *symmetric circuits*.

(Anderson, D. 2017)

Boolean Functions

Any language $L \subseteq \{0,1\}^*$ can be seen as a family of *Boolean functions*

$$L_n : \{0,1\}^n \to \{0,1\}.$$

For a group $\Gamma \leq \mathsf{Sym}_n$, we say that L_n is Γ-*invariant* if for all $\pi \in \Gamma$:

$$L_n(\pi \mathbf{x}) = L_n(x)$$

where $\pi\mathbf{x}$ is the string $x_{\pi(1)} \cdots x_{\pi(n)}$.

Invariant Functions

A function $f : \{0,1\}^n \to \{0,1\}$ is *fully symmetric* if it is *Sym$_n$-invariant*.

This means that $f(\mathbf{x})$ is completely determined by the number of 0s and 1s in $\mathbf{x}$.

Say that a function $f : \{0,1\}^{n \times n} \to \{0,1\}$ is *square symmetric* if it is *Sym$_n$-invariant*. Here, Sym$_n$ is seen as a subgroup of Sym$_{n \times n}$.

$\pi \in \mathsf{Sym}_n$ acts on strings $\mathbf{x} \in \{0,1\}^{n \times n}$ by

$$\pi(\mathbf{x}_{ij}) = \mathbf{x}_{\pi(i)\pi(j)}.$$

The square symmetric functions include, *for example*, any function deciding a property of graphs, given the *adjacency matrix*.

Matrix Symmetric Functions

Say that a function $f : \{0,1\}^{m \times n} \to \{0,1\}$ is *matrix symmetric* if it is $(Sym_m \times Sym_n)$*-invariant*.
Here, $\mathsf{Sym}_m \times \mathsf{Sym}_n$ is seen as a subgroup of $\mathsf{Sym}_{m \times n}$.
$(\pi, \sigma) \in \mathsf{Sym}_m \times \mathsf{Sym}_n$ acts on strings $\mathbf{x} \in \{0,1\}^{m \times n}$ by

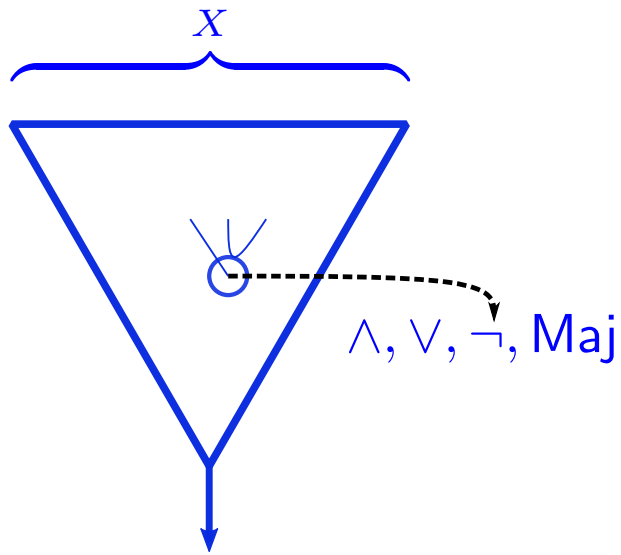
$$(\pi, \sigma)(\mathbf{x}_{ij}) = \mathbf{x}_{\pi(i)\sigma(j)}.$$

The matrix symmetric functions are those properties of an $m \times n$ matrix that are invariant under *independent* permutations of the rows and columns.

Circuits

Each L_n may be computed by a *circuit* C_n made up of

- Gates labeled by Boolean operators: $\wedge, \vee, \neg$,
- Boolean inputs: $x_1, \ldots, x_n$, and
- A distinguished gate determining the output.

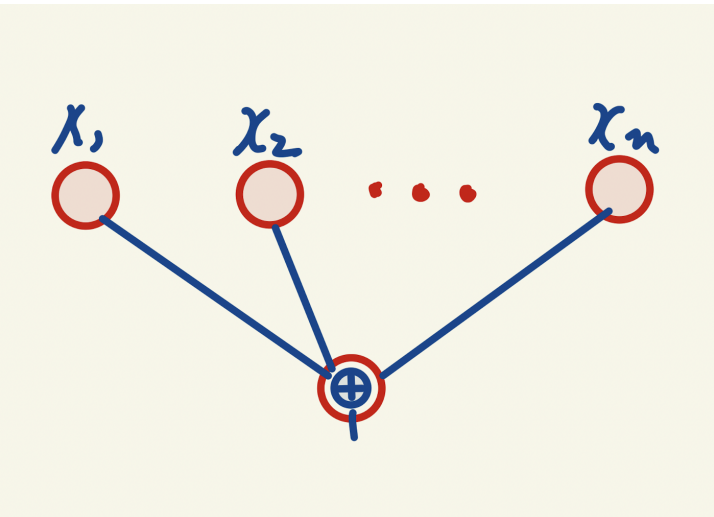


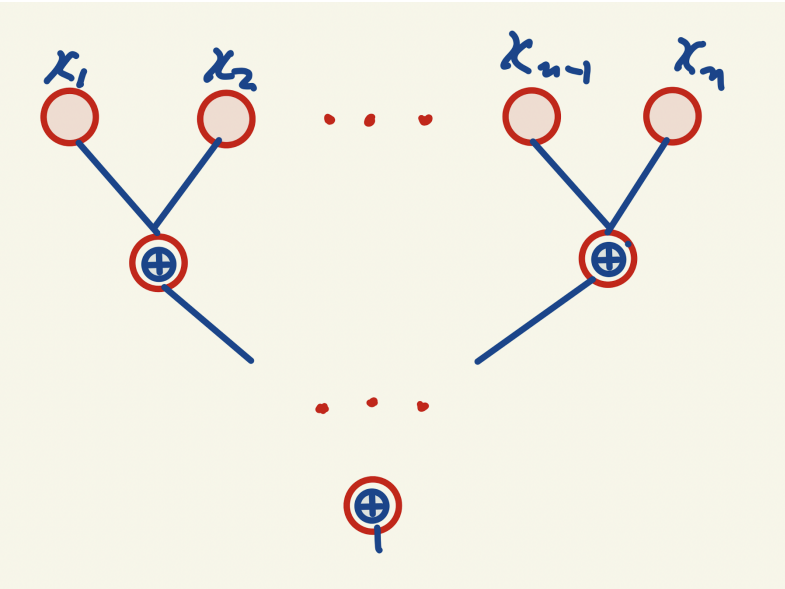
We always assume that the Boolean functions labelling individual gates are *fully symmetric*.

Symmetric Circuits

For a group $\Gamma \leq \mathsf{Sym}_n$, a circuit C_n is Γ-*symmetric* if every permutation $\pi \in \Gamma$ acting on the *inputs* of C_n extends to an *automorphism* of C_n.

Example: $\bigoplus_{1 \leq i \leq n} x_i$.





FPC

A graph property is in *fixed-point logic with counting* (FPC) *if, and only if,* it is decided by a P-uniform family of *square symmetric* circuits using *AND*, *OR*, *NOT* and *MAJ* gates.

Excluding *MAJ* gates gives us something *strictly weaker*.

A graph property is in FPC *if, and only if,* it is decided by a P-uniform family of *square symmetric* circuits using *fully symmetric gates*.

Similar characterizations work with other structured inputs: *matrices*; *Boolean formulas*; *systems of equations*.

FPC gives a natural notion of *polynomial-time, symmetric* computation.

This means *bijection games* give us a method for proving *circuit lower bounds*.

Counting Quantifiers

C^k is the logic obtained from *first-order logic* by allowing:

- *counting quantifiers*: $\exists^i x\, \varphi$; and
- only the variables $x_1, \ldots . x_k$.

Every formula of C^k is equivalent to a formula of first-order logic, albeit one with more variables.

For every sentence φ of FPC, there is a k such that if $\mathbb{A} \equiv^{C^k} \mathbb{B}$, then

$$\mathbb{A} \models \varphi \quad \text{if, and only if,} \quad \mathbb{B} \models \varphi.$$

Bijection Games

$\equiv^{C^k}$ is characterized by a k-pebble *bijection game*. **(Hella 96)**.

The game is played on structures $\mathbb{A}$ and $\mathbb{B}$ with pebbles $a_1, \ldots, a_k$ on $\mathbb{A}$ and $b_1, \ldots, b_k$ on $\mathbb{B}$.

- *Spoiler* chooses a pair of pebbles a_i and b_i;
- *Duplicator* chooses a bijection $h : A \to B$ such that for pebbles a_j and $b_j (j \neq i)$, $h(a_j) = b_j$;
- *Spoiler* chooses $a \in A$ and places a_i on a and b_i on $h(a)$.

Duplicator loses if the partial map $a_i \mapsto b_i$ is not a partial isomorphism.
Duplicator has a strategy to play forever if, and only if, $\mathbb{A} \equiv^{C^k} \mathbb{B}$.

Bijection Games and Symmetric Circuits

The aim now is to use the *bijection game* as a method for proving lower bounds on the size of *symmetric circuits*.

The key parameter of a circuit that links to the *number of pebbles* in the game is the *support size*.

> *Every gate in a Sym_n or Alt_n symmetric circuit of polynomial size has a stabilizer group with small support.*

Stabilizers

For a gate g in a Γ-symmetric circuit C_n, $\mathrm{Stab}(g)$ denotes the *stabilizer group of* g, i.e. the *subgroup* of Γ:

$$\mathrm{Stab}(g) = \{\pi \in \mathsf{Sym}_n \mid \pi(g) = g\}.$$

The *orbit* of g is the set of gates $\{h \mid \pi(g) = h \text{ for some } \pi \in \Gamma\}$

By the *orbit-stabilizer* theorem, there is one gate in the orbit of g for each *co-set* of $\mathrm{Stab}(g)$ in Γ.
Thus the size of the *orbit* of g in C_n is $[\Gamma : \mathrm{Stab}(g)] = \frac{|\Gamma|}{|\mathrm{Stab}(g)|}$.

So, an upper bound on $\mathrm{Stab}(g)$ gives us a lower bound on the orbit of g.

Supports

For a group $\Delta \subseteq \Gamma$, we say that a set $X \subseteq [n]$ is a *support* of Δ if

For every $\pi \in \Gamma$, if $\pi(x) = x$ for all $x \in X$, then $\pi \in G$.

In other words, Δ contains all permutations of Γ that pointwise fix X.

So, in the case when $\Gamma = \mathsf{Sym}_n$, if $|X| = k$, $[\Gamma : \Delta]$ is at most $\frac{n!}{(n-k)!} \leq n^k$.

Groups with small support are *big*.

The converse is clearly false since $[\mathsf{Sym}_n : \mathsf{Alt}_n] = 2$, but Alt_n has no support of size less than $n - 1$.

Γ-restricted Bijection Game

We are given structures $\mathbb{A}, \mathbb{B}$ and a group $\Gamma \leq \mathsf{Sym}_B$.

Spoiler chooses an initial bijection $h : A \to B$ and then at each move

- *Spoiler* chooses a pair of pebbles a_i and b_i;
- *Duplicator* chooses a *permutation* $\pi \in \Gamma$ such that for pebbles a_j and $b_j (j \neq i)$, $\pi \circ h(a_j) = b_j$;
- *Spoiler* chooses $a \in A$ and places a_i on a and b_i on $\pi \circ h(a)$.

The winning conditions are the same as before.

Note that this is the standard bijection game when $\Gamma = \mathsf{Sym}_B$.

Circuits and Pebble Games

If C is a Γ-symmetric circuit on n-element structures such that every gate of C has a support of size at most k, and $\mathbb{A}$ and $\mathbb{B}$ are inputs such that Duplicator wins the $2k$-pebble Γ-bijection game on $\mathbb{A}$ and $\mathbb{B}$:

C accepts $\mathbb{A}$ if, and only if, C accepts $\mathbb{B}$.

This can be proved by showing that if C distinguishes $\mathbb{A}$ from $\mathbb{B}$, then it provides a *winning strategy* for *Spoiler* in the $2k$-pebble bijection game.

Proof Sketch

Show that if

- C accepts $\mathbb{A}$ when it is mapped to the inputs by bijection $\alpha : A \to [n]$; and
- C rejects $\mathbb{B}$ when it is mapped to the inputs by bijection $\beta : B \to [n]$.

then, *Spoiler* has a winning strategy in the $2k$-pebble bijection game played on $\mathbb{A}$ and $\mathbb{B}$.

Show by induction that, while playing the *bijection game Spoiler* can maintain a pointer to a gate g of C and the following invariants for the game position $(\overline{u}, \overline{v})$:

- $\alpha(\overline{u})$ includes the support of g.
- For any bijection $\pi \in \Gamma$ such that $\alpha(\overline{u}) = \beta\pi(\overline{v})$:

$$C_g(\alpha(\mathbb{A})) \neq C_g(\beta\pi(\mathbb{B})).$$

Proof Sketch – 2

Base Case:
Initially, *Spoiler* plays $\beta^{-1}\alpha$.
By assumption, for g the *output gate* $C_g(\alpha(\mathbb{A})) = 1$ and $C_g(\beta(\mathbb{B})) = 0$ and so $C_g(\pi\beta(\mathbb{B})) = 0$ by Γ-invariance.

Induction Step:
While keeping pebbles on the support of g, *Spoiler* moves the other k pebbles to the support of a *child* h of g.
At each move, *Duplicator* plays a bijection $\pi : B \to B$ such that $\alpha(\overline{u}) = \beta\pi(\overline{v})$.
Thus, $C_g(\alpha(\mathbb{A})) \neq C_g(\beta\pi(\mathbb{B}))$, and there is an h for which

$$C_h(\alpha(\mathbb{A})) \neq C_h(\beta\pi(\mathbb{B}))$$

Alternating Supports

Groups with small support are *big*.

The converse is clearly false since $[\mathsf{Sym}_n : \mathsf{Alt}_n] = 2$, but Alt_n has no support of size less than $n - 1$.

In a sense, the alternating group is the *only* exception, due to a standard result from permutation group theory.

Theorem

If $n > 8$, $1 \leq k \leq n/4$, and G is a subgroup of Sym_n with $[\mathsf{Sym}_n : G] < \binom{n}{k}$, then there is a set $X \subseteq [n]$ with $|X| < k$ such that $\mathsf{Alt}_{(X)} \leq G$.

where $\mathsf{Alt}_{(X)}$ denotes group $\{\pi \in \mathsf{Alt}_n : \pi(i) = i \text{ for all } i \in X\}$

Support Theorems

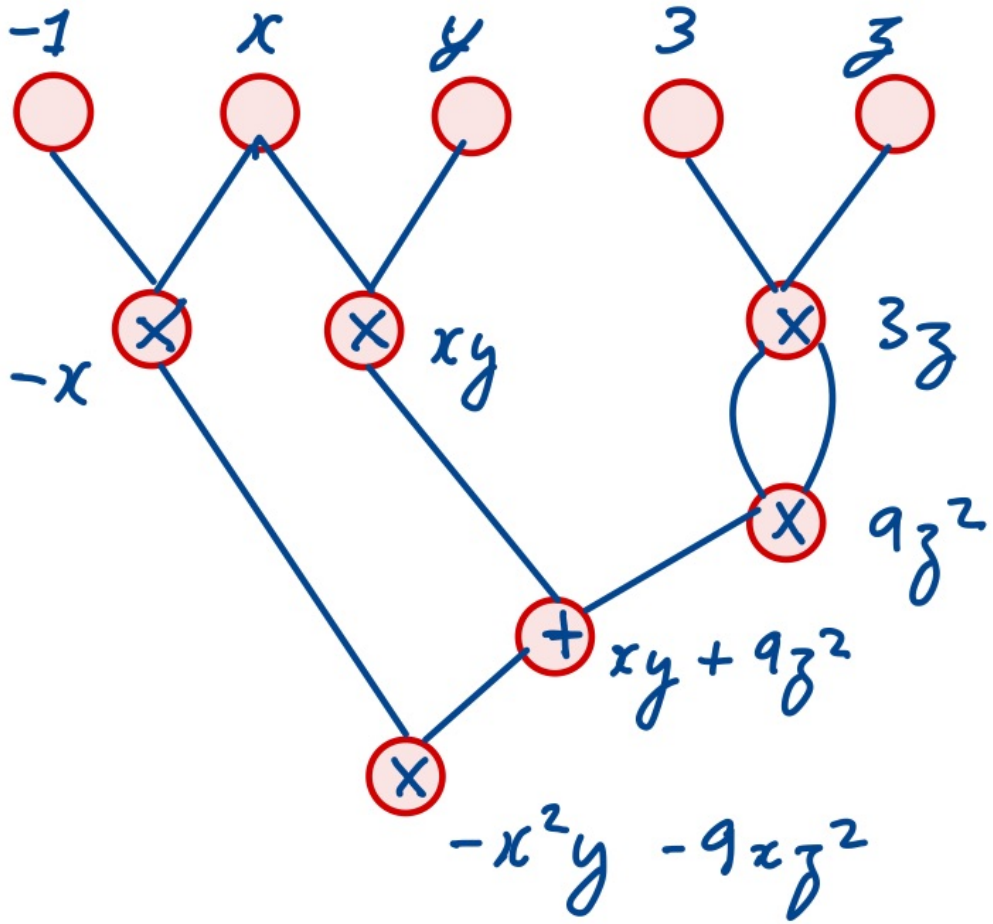
If $(C_n)_{n\in\omega}$ is a family of *symmetric* circuits of size n^k, then for all sufficiently large n and gates g in C_n, there is a set $X \subseteq [n]$ with $|X| \leq k$ such that $\mathsf{Alt}_{(X)} \leq \mathrm{Stab}(g)$.

In polynomial-size Alt_n-symmetric circuits, all gates have small support.

The same can be shown for Sym_n-symmetric circuits by an *induction* on the structure of the circuit, showing that the alternating group does not appear as the stabilizer of any gate

We can also establish *support theorems* for *matrix symmetric* circuits with symmetry groups of the form $\mathsf{Sym}_m \times \mathsf{Sym}_n$ and $\mathsf{Alt}_m \times \mathsf{Alt}_n$.

Algebraic Circuits



Algebraic Circuits

Algebraic Circuits over a field K are given by:

- A *directed acyclic graph*.
- Inputs labelled by a *variable* $x \in X$, or constant $c \in K$.
- Internal gates labelled by $+$ or $\times$.
- A designated *output*.

Each circuit computes (or represents) a *polynomial* in $K[X]$.

Valiant's conjecture VP $\neq$ VNP is the *algebraic analogue* of P $\neq$ NP.

Matrix Inputs

We are often interested in inputs which are entries of *a matrix*.

$$X = \{x_{ij} \mid 1 \leq i \leq m; 1 \leq j \leq n\}$$

Especially, when the input is a *square matrix*, so $m = n$.

$$\mathrm{tr}(X) = \sum_i x_{ii}$$

$$\mathrm{Det}(X) = \sum_{\sigma \in \mathsf{Sym}_n} \mathsf{sgn}(\sigma) \prod_{i \in [n]} x_{i\sigma(i)}$$

$$\mathrm{Per}(X) = \sum_{\sigma \in \mathsf{Sym}_n} \prod_{i \in [n]} x_{i\sigma(i)}$$

Valiant's Conjecture

$\mathrm{Det}(X)$ is in VP—it can be expressed by polynomial size circuits, for example by implementing a *Gaussian elimination* algorithm.

$\mathrm{Per}(X)$ is VNP-complete.

Valiant's conjecture is that $\mathrm{Per}(X)$ *cannot* be expressed by circuits of polynomial size.

Symmetric Algebraic Circuits

Suppose C is a circuit computing a polynomal $p \in K[X]$.

Sym_X—the group of *permutations* of X.

For $\Gamma \leq \mathsf{Sym}_X$, p is Γ-*symmetric* if for all $\pi \in \Gamma$, $p^\pi = p$.

C is Γ-*symmetric* if the action of Γ on the inputs X extends to an *automorphism* of C.

Symmetric Polynomials

The matrix polynomials $\mathrm{tr}(X)$, $\mathrm{Det}(X)$ and $\mathrm{Per}(X)$ are all *square symmetric*, i.e. invariant under the action of Sym_n given by

$$x_{ij}^{\pi} = x_{\pi(i)\pi(j)}.$$

i.e., *simultaneous row and column permutations*.

$\mathrm{Per}(X)$ is also *matrix symmetric*, i.e. invariant under *independent row and column permutations*:
the action of $\mathsf{Sym}_n \times \mathsf{Sym}_n$ given by

$$x_{ij}^{(\sigma,\pi)} = x_{\sigma(i)\pi(j)}.$$

$\mathrm{tr}(X)$ and $\mathrm{Det}(X)$ are not matrix symmetric.

Determinant

The invariance group of

$$\mathrm{Det}(X) = \sum_{\sigma \in \mathsf{Sym}_n} \mathsf{sgn}(\sigma) \prod_{i \in [n]} x_{i\sigma(i)}$$

includes

$$D = \{(\sigma, \pi) \in \mathsf{Sym}_n \times \mathsf{Sym}_n \mid \mathsf{sgn}(\sigma) = \mathsf{sgn}(\pi)\} \ltimes \mathbb{Z}_2.$$

In particular, it is $\mathsf{Alt}_n \times \mathsf{Alt}_n$-symmetric.

The defining expression yields a circuit with these symmetries, but of $\Omega(n!)$ size.

Results

Γ	$\{\mathsf{id}\}$	$\mathsf{Sym}_{[n]}$	$\mathsf{Alt}_{[n]} \times \mathsf{Alt}_{[n]}$	$\mathsf{Sym}_{[n]} \times \mathsf{Sym}_{[n]}$
Det	$O(n^\omega)$	$O(n^3)$ *(char 0)*	$2^{\Omega(n)}$ *(char 0)*	N/A
Perm	$O(n^2 2^n)$ VP $=$ VNP?	$2^{\Omega(n)}$ *(char 0)*	$2^{\Omega(n)}$ *(char $\neq 2$)*	$2^{\Omega(n)}$ *(char $\neq 2$)*

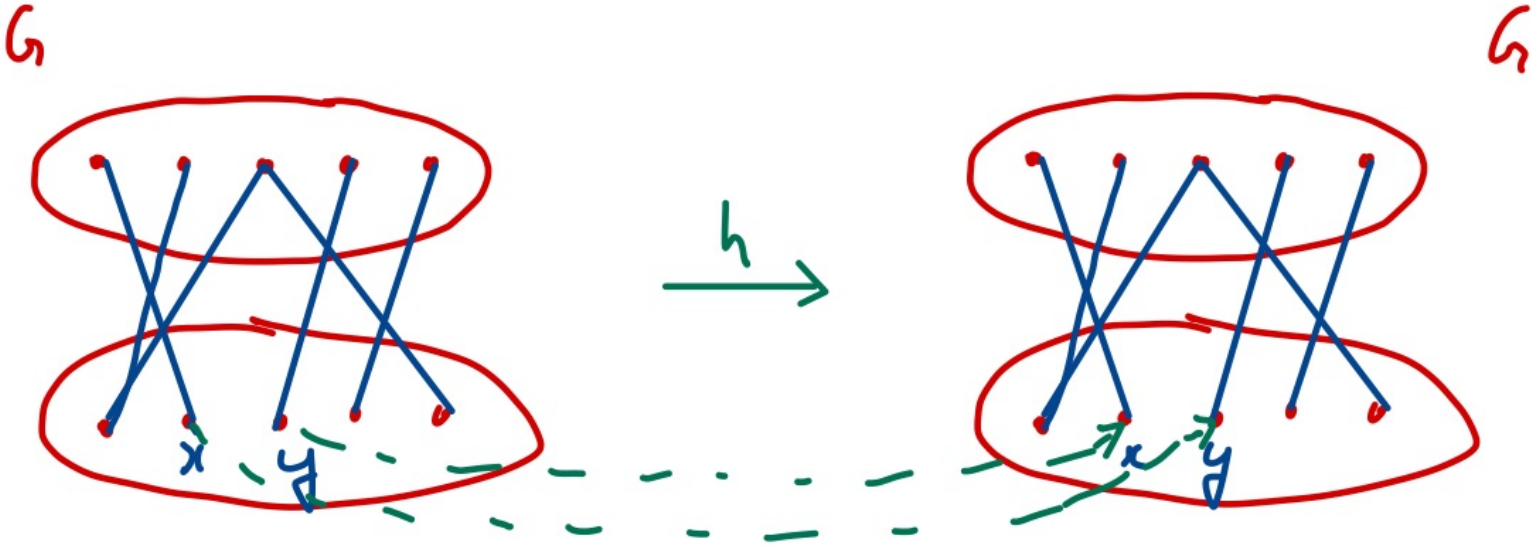
Results from **(D., Wilsenach, 2020/2022)**

Determinant Lower Bound

We construct a bipartite graph $G = (A, B, E)$ with

- $|A| = |B| = O(k)$
- the bi-adjacency matrix has *non-zero* determinant
- *Duplicator* wins the k-pebble, $\mathsf{Alt}_A \times \mathsf{Alt}_B$ bijection game on two copies of G starting with any bijection swapping two elements of B.

Alternating Game



Characterizing Families of Symmetric Polynommials

Given a family $(p_{m,n})_{m,n\in\mathbb{N}}$ of polynomials where

- $p_{m,n} \in \mathbb{Q}[X]$ with $X = \{x_{ij} \mid i \in [m], j \in [n]\}$;
- $p_{m,n}$ is $\mathsf{Sym}_m \times \mathsf{Sym}_n$-symmetric;

when can this be computed by a family of $\mathsf{Sym}_m \times \mathsf{Sym}_n$-symmetric circuits of *polynomial-size* (or *orbit size*)?

We have a fairly complete answer. **(D,Pago, Seppelt 2025)**