Topics in Logic and Complexity

Handout 3

Anuj Dawar

http://www.cl.cam.ac.uk/teaching/2223/L15

Expressive Power of First-Order Logic

We noted that there are computationally easy properties that are not definable in first-order logic.

- There is no sentence ϕ of first-order logic such that $\mathbb{A} \models \phi$ if, and only if, $|A|$ is even.
- There is no sentence ϕ that defines exactly the *connected* graphs.

How do we *prove* these facts?

Our next aim is to develop the tools that enable such proofs.

Quantifier Rank

The *quantifier rank* of a formula ϕ, written $\mathrm{qr}(\phi)$ is defined inductively as follows:

1. if ϕ is atomic then $\mathrm{qr}(\phi) = 0$,
2. if $\phi = \neg\psi$ then $\mathrm{qr}(\phi) = \mathrm{qr}(\psi)$,
3. if $\phi = \psi_1 \vee \psi_2$ or $\phi = \psi_1 \wedge \psi_2$ then $\mathrm{qr}(\phi) = \max(\mathrm{qr}(\psi_1), \mathrm{qr}(\psi_2))$.
4. if $\phi = \exists x\psi$ or $\phi = \forall x\psi$ then $\mathrm{qr}(\phi) = \mathrm{qr}(\psi) + 1$

More informally, $\mathrm{qr}(\phi)$ is the *maximum depth of nesting of quantifiers* inside ϕ.

Formulas of Bounded Quantifier Rank

Note: For the rest of this lecture, we assume that our signature consists only of relation and constant symbols. That is, there are *no function symbols of non-zero arity*.

With this proviso, it is easily proved that in a finite vocabulary, for each q, there are (up to logical equivalence) only finitely many sentences ϕ with $\mathrm{qr}(\phi) \leq q$.

To be precise, we prove by induction on q that for all m, there are only finitely many formulas of quantifier rank q with at most m free variables.

Formulas of Bounded Quantifier Rank

If $\mathrm{qr}(\phi) = 0$ then ϕ is a Boolean combination of atomic formulas. If it is has m variables, it is equivalent to a formula using the variables $x_1, \ldots, x_m$. There are finitely many formulas, *up to logical equivalence*.

Suppose $\mathrm{qr}(\phi) = q + 1$ and the *free variables* of ϕ are among $x_1, \ldots, x_m$. Then ϕ is a Boolean combination of formulas of the form

$$\exists x_{m+1} \psi$$

where ψ is a formula with $\mathrm{qr}(\psi) = q$ and free variables $x_1, \ldots, x_m, x_{m+1}$. By induction hypothesis, there are only finitely many such formulas, and therefore finitely many Boolean combinations.

Equivalence Relation

For two structures $\mathbb{A}$ and $\mathbb{B}$, we say $\mathbb{A} \equiv_q \mathbb{B}$ if for any sentence ϕ with $\mathrm{qr}(\phi) \leq q$,

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

More generally, if a and b are m-tuples of elements from $\mathbb{A}$ and $\mathbb{B}$ respectively, then we write $(\mathbb{A}, \mathsf{a}) \equiv_q (\mathbb{B}, \mathsf{b})$ if for any formula ϕ with m free variables $\mathrm{qr}(\phi) \leq q$,

$$\mathbb{A} \models \phi[\mathsf{a}] \text{ if, and only if, } \mathbb{B} \models \phi[\mathsf{b}].$$

Partial Isomorphisms

A map f is a partial isomorphism between structures $\mathbb{A}$ and $\mathbb{B}$, if

- the domain of $f = \{a_1, \ldots, a_l\} \subseteq A$,
- the range of $f = \{b_1, \ldots, b_l\} \subseteq B$,
- f is an isomorphism between the substructures generated by its domain and its range.

Note that, in the absence of function symbols, the substructure generated by $\{a_1, \ldots, a_l\} \subseteq A$ is the structure induced by $\{a_1, \ldots, a_l\} \cup \{c^{\mathbb{A}} \mid c \text{ a constant}\}$.

Note that if f is a partial isomorphism taking a tuple a to a tuple b, then for any *quantifier-free* formula θ

$$\mathbb{A} \models \theta[\mathrm{a}] \text{ if, and only if, } \mathbb{B} \models \theta[\mathrm{b}].$$

Ehrenfeucht-Fraïssé Games

The q-round Ehrenfeucht game on structures $\mathbb{A}$ and $\mathbb{B}$ proceeds as follows:

- There are two players called *Spoiler* and *Duplicator*.
- At the ith round, *Spoiler* chooses one of the structures (say $\mathbb{B}$) and one of the elements of that structure (say b_i).
- *Duplicator* must respond with an element of the other structure (say a_i).
- If, after q rounds, the map $a_i \mapsto b_i$ is a partial isomorphism, then *Duplicator* has won the game, otherwise *Spoiler* has won.

Equivalence and Games

Write $\mathbb{A} \sim_q \mathbb{B}$ to denote the fact that *Duplicator* has a *winning strategy* in the q-round Ehrenfeucht game on $\mathbb{A}$ and $\mathbb{B}$.
The relation $\sim_q$ is, in fact, an *equivalence relation*.

Theorem (Fraïssé 1954; Ehrenfeucht 1961)
$\mathbb{A} \sim_q \mathbb{B}$ if, and only if, $\mathbb{A} \equiv_q \mathbb{B}$

While one direction $\mathbb{A} \sim_q \mathbb{B} \Rightarrow \mathbb{A} \equiv_q \mathbb{B}$ is true for an arbitrary vocabulary, the other direction assumes that the vocabulary is *finite* and has *no function symbols*.

Proof

To prove $\mathbb{A} \sim_q \mathbb{B} \Rightarrow \mathbb{A} \equiv_q \mathbb{B}$, it suffices to show that if there is a sentence ϕ with $\mathrm{qr}(\phi) \leq q$ such that

$$\mathbb{A} \models \phi \quad \text{and} \quad \mathbb{B} \not\models \phi$$

then *Spoiler* has a winning strategy in the q-round Ehrenfeucht game on $\mathbb{A}$ and $\mathbb{B}$.

Assume that ϕ is in *negation normal form*, i.e. all negations are in front of atomic formulas.

Proof

We prove by induction on q the stronger statement that if ϕ is a formula with $\mathrm{qr}(\phi) \leq q$ and $\mathsf{a} = (a_1, \ldots, a_m)$ and $\mathsf{b} = (b_1, \ldots, b_m)$ are tuples of elements from $\mathbb{A}$ and $\mathbb{B}$ respectively such that

$$\mathbb{A} \models \phi[\mathsf{a}] \quad \text{and} \quad \mathbb{B} \not\models \phi[\mathsf{b}]$$

then *Spoiler* has a winning strategy in the q-round Ehrenfeucht game which starts from a position in which $a_1, \ldots, a_m$ and $b_1, \ldots, b_m$ have *already been selected*.

Proof

When $q = 0$, ϕ is a quantifier-free formula. Thus, if

$$\mathbb{A} \models \phi[\mathrm{a}] \quad \text{and} \quad \mathbb{B} \not\models \phi[\mathrm{b}]$$

there is an *atomic* formula θ that distinguishes the two tuples and therefore the map taking a to b is not a *partial isomorphism*.

When $q = p + 1$, there is a subformula θ of ϕ of the form $\exists x\psi$ or $\forall x\psi$ such that $\mathrm{qr}(\psi) \leq p$ and

$$\mathbb{A} \models \theta[\mathrm{a}] \quad \text{and} \quad \mathbb{B} \not\models \theta[\mathrm{b}]$$

If $\theta = \exists x\psi$, *Spoiler* chooses a witness for x in $\mathbb{A}$.
If $\theta = \forall x\psi$, $\mathbb{B} \models \exists x\neg\psi$ and *Spoiler* chooses a witness for x in $\mathbb{B}$.

Using Games

To show that a class of structures S is not definable in FO, we find, for every q, a pair of structures $\mathbb{A}_q$ and $\mathbb{B}_q$ such that

- $\mathbb{A}_q \in S$, $\mathbb{B}_q \in \overline{S}$; and
- *Duplicator* wins a q-round game on $\mathbb{A}_q$ and $\mathbb{B}_q$.

This shows that S is not closed under the relation $\equiv_q$ for *any* q.

Fact:

> *S is definable by a first order sentence if, and only if, S is closed under the relation $\equiv_q$ for some q.*

The direction from right to left requires a *finite, function-free* vocabulary.

Evenness

Let $\mathbb{A}$ be a structure in the *empty vocabulary* with q elements and $\mathbb{B}$ be a structure with $q+1$ elements.
Then, it is easy to see that $\mathbb{A} \sim_q \mathbb{B}$.

It follows that there is no first-order sentence that defines the structures with an even number of elements.

If $S \subseteq \mathbb{N}$ is a set such that

$$\{\mathbb{A} \mid |\mathbb{A}| \in S\}$$

is definable by a first-order sentence then S is finite or co-finite.

Linear Orders

Let L_n denote the structure in one binary relation $\leq$ which is a linear order of n elements. Then $L_6 \not\equiv_3 L_7$ but $L_7 \equiv_3 L_8$.

In general, for $m, n \geq 2^p - 1$,

$$L_m \equiv_p L_n$$

Duplicator's strategy is to maintain the following condition after r rounds of the game:
for $1 \leq i < j \leq r$,

- *either* $\mathrm{length}(a_i, a_j) = \mathrm{length}(b_i, b_j)$
- *or* $\mathrm{length}(a_i, a_j), \mathrm{length}(b_i, b_j) \geq 2^{p-r} - 1$

Evenness is not first order definable, even on linear orders.

Connectivity

Consider the signature $(E, <)$.

Consider structures $G = (V, E, <)$ in which E is a graph relation and $<$ is a linear order.

There is no first order sentence γ in this signature such that

$$G \models \gamma \text{ if, and only if, } (V, E) \text{ is connected.}$$

Proof

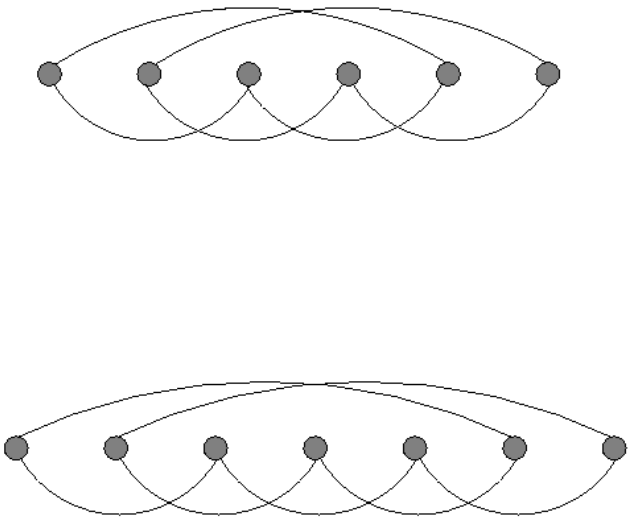
Suppose there was such a formula γ.

Let γ' be the formula obtained by replacing every occurrence of $E(x, y)$ in γ by the following formula

$$\begin{array}{l} y = x + 2 \vee \\ (x = \max \wedge y = \min + 1) \vee \\ (y = \min \wedge x = \max - 1). \end{array}$$

Then, $\neg\gamma'$ defines evenness on linear orders!

Proof



We obtain two *disjoint* cycles on linear orders of even length, and a *single* cycle on linear orders of odd length.

Reduction

The above is, in fact, a *first-order definable reduction* from the problem of evenness of linear orders to the problem of connectivity of ordered graphs.

It follows from the above that there is no first order formula that can express the *transitive closure* query on graphs.

Any such formula would also work on ordered graphs.

Gaifman Graphs and Neighbourhoods

On a structure $\mathbb{A}$, define the binary relation:

> $E(a_1, a_2)$ *if, and only if, there is some relation* R *and some tuple* a *containing both* a_1 *and* a_2 *with* $R(\mathrm{a})$.

The graph $G\mathbb{A} = (A, E)$ is called the *Gaifman graph* of $\mathbb{A}$.

$dist(a, b)$ — the distance between a and b in the graph (A, E).

$\mathrm{Nbd}_r^{\mathbb{A}}(a)$ — the substructure of $\mathbb{A}$ given by the set:

$$\{b \mid dist(a, b) \leq r\}$$

Hanf Locality Theorem

We say $\mathbb{A}$ and $\mathbb{B}$ are *Hanf equivalent* with radius r ($\mathbb{A} \simeq_r \mathbb{B}$) if, there is a bijection $f : A \to B$ such that:

$$\text{for all } a \in A : \mathrm{Nbd}_r^{\mathbb{A}}(a) \cong \mathrm{Nbd}_r^{\mathbb{B}}(f(a))$$

by an isomorphism that takes a to $f(a)$.

Theorem (Hanf)
For every vocabulary σ and every p there is $r \leq 3^p$ such that for any σ-structures $\mathbb{A}$ and $\mathbb{B}$: if $\mathbb{A} \simeq_r \mathbb{B}$ then $\mathbb{A} \equiv_p \mathbb{B}$.

In other words, if $r \geq 3^p$, the equivalence relation $\simeq_r$ is a refinement of $\equiv_p$.

Hanf Locality

Duplicator's strategy is to maintain the following condition:
After k moves, if $a_1, \ldots, a_k$ and $b_1, \ldots, b_k$ have been selected, then

$$\bigcup_i \mathrm{Nbd}^{\mathbb{A}}_{3^{p-k}}(a_i) \cong \bigcup_i \mathrm{Nbd}^{\mathbb{B}}_{3^{p-k}}(b_i)$$

by an isomorphism that takes a_i to b_i.
If *Spoiler* plays on a within distance $2 \cdot 3^{p-k-1}$ of a previously chosen point, play according to the isomorphism, otherwise, find b such that

$$\mathrm{Nbd}_{3^{p-k-1}}(a) \cong \mathrm{Nbd}_{3^{p-k-1}}(b)$$

and b is not within distance $2 \cdot 3^{p-k-1}$ of a previously chosen point.
Such a b is guaranteed by $\simeq_r$.

Uses of Hanf locality

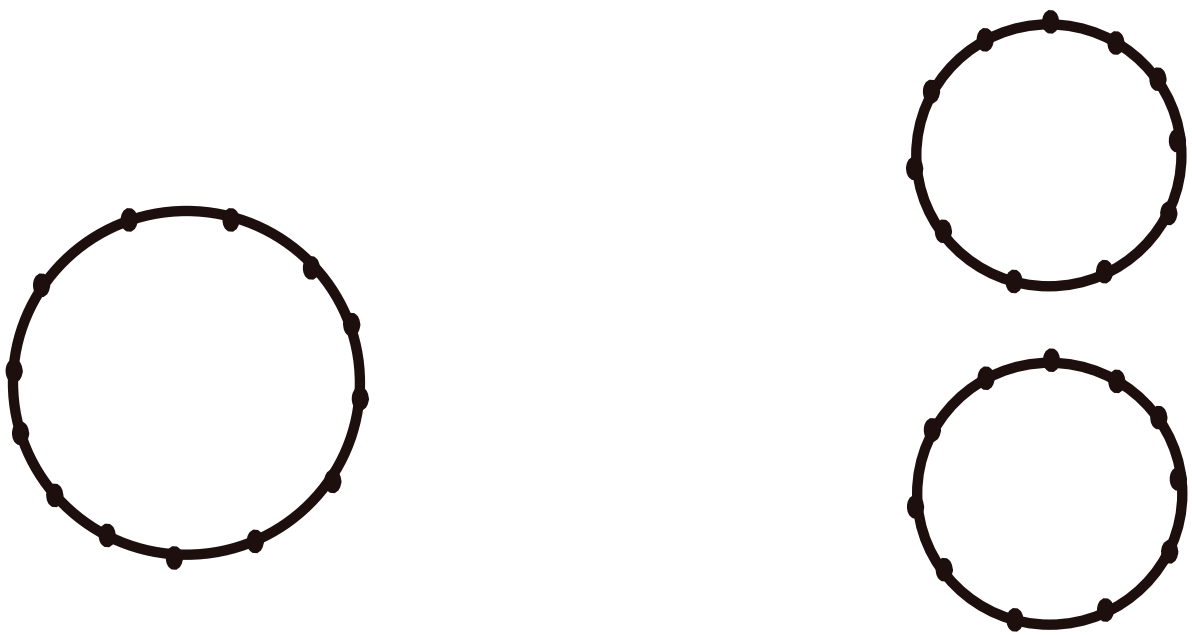
The Hanf locality theorem immediately yields, as special cases, the proofs of undefinability of:

- *connectivity*;
- *2-colourability*
- *acyclicity*
- *planarity*

A simple illustration can suffice.

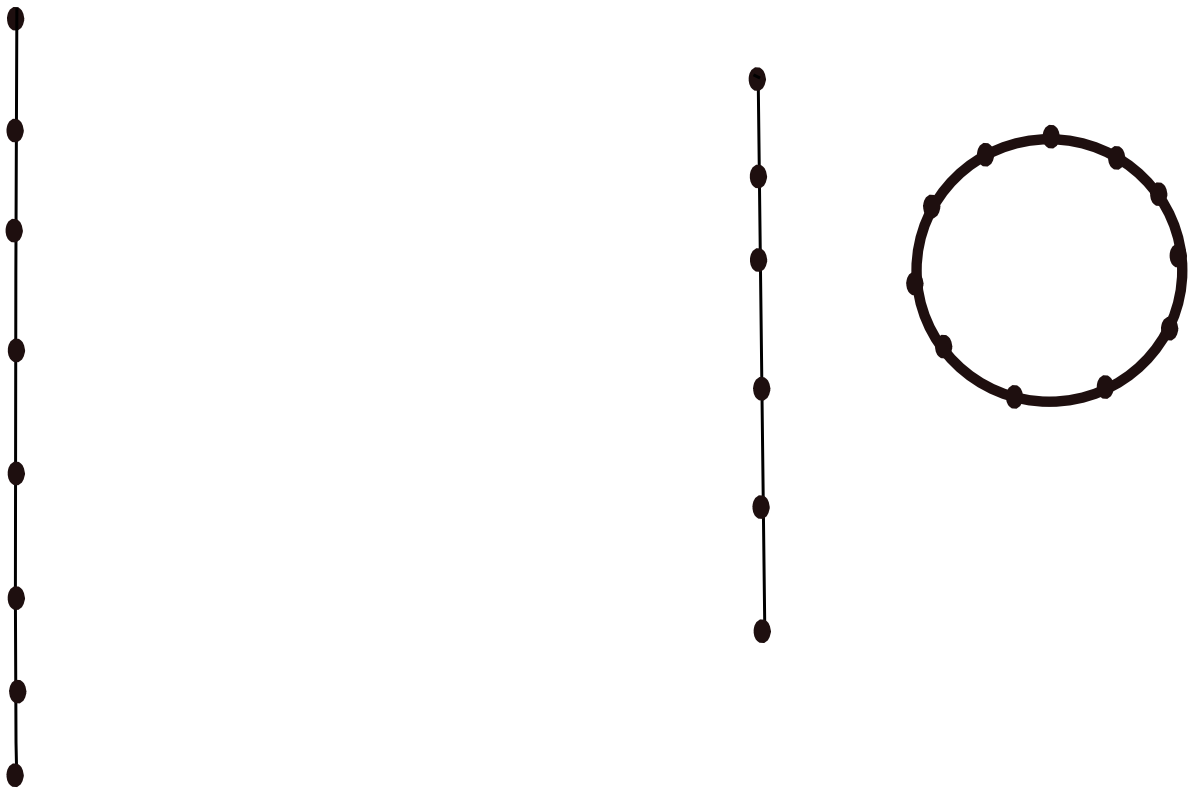
Connectivity

To illustrate the undefinability of *connectivity* and *2-colourability*, consider on the one hand the graph consisting of a single cycle of length $4r + 6$ and, on the other hand, a graph consisting of two disjoint cycles of length $2r + 3$.



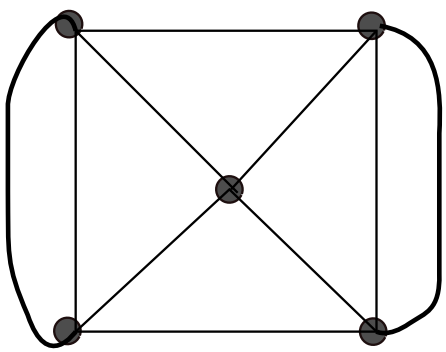
Acyclicity

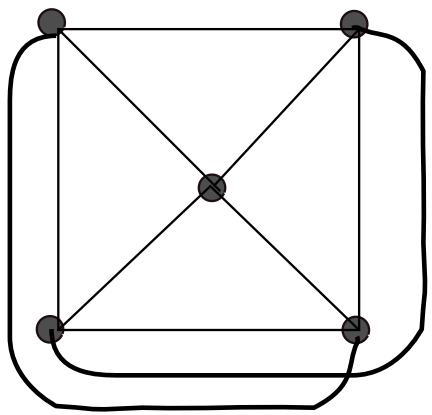
A figure illustrating that *acyclicity* is not first-order definable.



Planarity

A figure illustrating that *planarity* is not first-order definable.





Monadic Second Order Logic

MSO consists of those second order formulas in which all relational variables are *unary*.

> *That is, we allow quantification over sets of elements, but not other relations.*

Any MSO formula can be put in prenex normal form with second-order quantifiers preceding first order ones.

Mon.Σ^1_1 — MSO formulas with only *existential* second-order quantifiers in prenex normal form.

Mon.Π^1_1 — MSO formulas with only *universal* second-order quantifiers in prenex normal form.

Undefinability in MSO

The method of games and *locality* can also be used to show *inexpressibility* results in MSO.

In particular,
There is a Mon.Σ^1_1 query that is not definable in Mon.Π^1_1

(Fagin 1974)

Note: A similar result without the *monadic* restriction would imply that NP $\neq$ co-NP and therefore that P $\neq$ NP.

Connectivity

Recall that *connectivity* of graphs can be defined by a Mon.Π^1_1 sentence.

$$\forall S(\exists x\, Sx \wedge (\forall x \forall y\, (Sx \wedge Exy) \rightarrow Sy)) \rightarrow \forall x\, Sx$$

and by a Σ^1_1 sentence (simply because it is in NP).

We now aim to show that *connectivity* is not definable by a Mon.Σ^1_1 sentence.

MSO Game

The m-round monadic Ehrenfeucht game on structures $\mathbb{A}$ and $\mathbb{B}$ proceeds as follows:

- At the ith round, *Spoiler* chooses one of the structures (say $\mathbb{B}$) and plays either a point move or a set move.

  In a point move, it chooses one of the elements of the chosen structure (say b_i) – Duplicator must respond with an element of the other structure (say a_i).

  In a set move, it chooses a subset of the universe of the chosen structure (say S_i) – Duplicator must respond with a subset of the other structure (say R_i).

MSO Game

- If, after m rounds, the map

$$a_i \mapsto b_i$$

is a partial isomorphism between

$$(\mathbb{A}, R_1, \ldots, R_q) \text{ and } (\mathbb{B}, S_1, \ldots, S_q)$$

then *Duplicator* has won the game, otherwise *Spoiler* has won.

MSO Game

If we define the *quantifier rank* of an MSO formula by adding the following inductive rule to those for a formula of FO:

if $\phi = \exists S\psi$ *or* $\phi = \forall S\psi$ *then* $\mathrm{qr}(\phi) = \mathrm{qr}(\psi) + 1$

then, we have

Duplicator has a winning strategy in the m*-round monadic Ehrenfeucht game on structures* $\mathbb{A}$ *and* $\mathbb{B}$ *if, and only if, for every sentence* ϕ *of MSO with* $\mathrm{qr}(\phi) \leq m$

$$\mathbb{A} \models \phi \quad \textit{if, and only if,} \quad \mathbb{B} \models \phi$$

Existential Game

The m, p-move existential game on ($\mathbb{A}$,$\mathbb{B}$):

- First *Spoiler* makes m set moves on $\mathbb{A}$, and *Duplicator* replies on $\mathbb{B}$.
- This is followed by an Ehrenfeucht game with p point moves.

If *Duplicator* has a winning strategy, then for every Mon.Σ^1_1 sentence:

$$\phi \equiv \exists R_1 \ldots \exists R_m \, \psi$$

with $\mathrm{qr}(\psi) = p$,

$$\text{if } \mathbb{A} \models \phi \text{ then } \mathbb{B} \models \phi$$

Variation

To show that a Boolean query Q is not $Mon.\Sigma^1_1$ definable, find for each m and p

- $\mathbb{A} \in Q$; and
- $\mathbb{B} \notin Q$; such that
- *Duplicator* wins the m, p move game on $(\mathbb{A}, \mathbb{B})$.

Or,

- *Duplicator* chooses $\mathbb{A}$.
- *Spoiler* colours $\mathbb{A}$ (with 2^m colours).
- *Duplicator* chooses $\mathbb{B}$ and colours it.
- They play a p-round Ehrenfeucht game.

Application

Write C_n for the graph that is a simple *cycle* of length n.

For n sufficiently large, and any *colouring* of C_n, we can find an $n' < n$ and a colouring of

> $C_{n'} \oplus C_{n-n'}$ *the disjoint union of two cycles—one of length* n', *the other of length* $n - n'$

So that the graphs C_n and $C_{n'} \oplus C_{n-n'}$ are $\simeq_r$ equivalent.

Taking $n > (4r + 2)(2^m)^{2r+1}$ suffices.