Descriptive Complexity

Albert Atserias
UPC Barcelona

Île d'Oléron, June 2023.

Introduction

Descriptive Complexity:

the complexity theory of logic.
vs. the complexity theory of algorithms

Motivation 1: machine-independent model.
Quest of logic for iso-invariant P.
An approach to P vs. NP.

Motivation 2: algorithmic meta-theorems.

Syllabus

Lecture 1: FO and SO logic, Fagin's Theorem,
Ehrenfeucht-Fraïssé games, Hanf locality,
Two applications, Open.

Lecture 2: IFP and PFP logic, Immerman-Vardi
Weakness + strength: Abiteboul-Vianu,
Invariants, Ordering the invariants, Open.

Lecture 3: Add counting, Expressivity,
Weisfeiler-Lehman, Cai-Fürer-Immerman,
Definable ellipsoid, Application, Open.

First-Order Logic: Examples.

TRIANGLE: $\exists u \exists v \exists w \, (E(u,v) \wedge E(v,w) \wedge E(u,w))$

size $= O(1)$
quantifier rank $= 3$
width $=$ number of vars $= 3$

$PATH_n(x,y) =$ "there is a walk from x to y of length n"

$$PATH_1(x,y) = E(x,y)$$

$$PATH_n(x,y) = \exists z \; \overbrace{\big(E(x,z) \wedge PATH_{n-1}(z,y)\big)}^{x,\,y,\,z}$$

$$PATH_n(x,y) = \exists z \; \big(\underbrace{PATH_{\frac{n}{2}}(x,z)} \wedge \underbrace{PATH_{\frac{n}{2}}(z,y)}\big)$$

$qr = n$ size $= O(n)$ width $= 3$

$qr = \log n$ size $= O(n)$ width $= 3$

$$PATH_n(x,y) = \exists z \; \forall u \; \forall v \left(\left(\begin{array}{c} (u = x \,\&\, v = z) \\ \vee \\ (u = z \,\&\, v = y) \end{array} \right) \rightarrow PATH_{\frac{n}{2}}(u,v) \right)$$

$qr = 3 \log n$ size $= O(\log n)$ width $= O(1)$

First-Order Logic : Syntax & Semantics.

vars: $x, y, z, u, v, \ldots$ (range over some domain)

atomic formulas: $x = y$, $E(x,y)$, $\underbrace{P_1(x), \ldots, P_r(x)}_{2^r \text{ colors}}$

connectives:

$\neg, \wedge, \vee.$ $\qquad \wedge \equiv \neg \vee \neg$

quantifiers:

$\exists x \quad \forall x$ $\qquad \forall x \equiv \neg \exists x \neg$

$\varphi(x_1, \dots, x_k)$

$G = (V, E, P_1, \dots, P_r)$

$\bar{c} = (c_1, \dots, c_k) \in V^k$

$G, \bar{c} \models \varphi$

$G, \bar{c} \models x_i = x_j$ if $c_i = c_j$

$G, \bar{c} \models E(x_i, x_j)$ if $(c_i, c_j) \in E$

$G, \bar{c} \models P_i(x_j)$ if $c_j \in P_i$

$G, \bar{c} \models \psi \wedge \theta$ if $G, c \models \psi$ & $G, c \models \theta$

$G, \bar{c} \models \neg\psi$ if $G, c \not\models \psi$

$G, \bar{c} \models \exists x_j\ \psi$ if there is $c \in V$ $G, \bar{c}[j/c] \models \psi$

Second Order Logic:

$(a \to b) \equiv (\neg a \vee b)$

2nd order vars: $X_1, X_2, Y, Z, \ldots$

of some arity r

2nd order quant: $\exists X, \forall Y$

$X(x_1, \ldots, x_r)$

Example: 3-colorability

$$\exists X_1 \exists X_2 \exists X_3 \Big(\forall x \, (X_1(x) \vee X_2(x) \vee X_3(x))$$
$$\forall x \, (\neg X_1(x) \vee \neg X_2(x))$$
$$(\neg X_1(x) \vee \neg X_3(x))$$
$$(\neg X_2(x) \vee \neg X_3(x))$$
$$\forall x \forall y \, (E(x,y) \to \neg X_1(x) \vee \neg X_1(y)$$

Semantics

$$\begin{cases} G = (V, E, P_1, \dots, P_r) \\ \varphi(\mathcal{X}_1, \dots, \mathcal{X}_k, x_1, \dots, x_k) \quad \text{formula} \\ \overline{C} = (C_1, \dots, C_k), \ \overline{c} = (c_1, \dots, c_k) \end{cases}$$

$$G, \overline{C}, \overline{c} \models \varphi$$

$$\begin{cases} G, \overline{C}, \overline{c} \models X_j(x_{i_1}, \dots x_{i_r}) & \text{if } (c_{i_1}, \dots, c_{i_r}) \in C_j \\ G, \overline{C}, \overline{c} \models \exists \mathcal{X}_j \ \psi & \text{if there is } C \subseteq V^r \text{ s.t. } G, \overline{C}[j/C], \overline{c} \models \psi \end{cases}$$

Fagin's Theorem

1974 ?

Theorem: $NP = \exists SO$

existential second-order logic

$\exists X_1 \cdots \exists X_k \ \psi$

first-order.

NP : $L \in NP$ iff $\exists$ Verifier $\boxed{V \in P}$ $\exists$ poly $p(n)$
s.t. $\forall x \in \{0,1\}^*$
$x \in L \Leftrightarrow \exists y, |y| \leq p(|x|)$
$V(x,y) = acc$

$NP \subseteq \exists SO$
$\boxed{\exists SO} \subseteq NP$
3-COL $\in NP$

s.t. for all graph G
$\langle G \rangle \in L \Leftrightarrow \exists y, |y| \leq p(|x|)$
$V(x,y) = acc$

$n = |V|$

$y_1 \dots y_2$

n^2 positions

$\underbrace{0101101}_{1\text{'st}}\underbrace{11000}_{2\text{nd}} \cdots \underbrace{011}_{n\text{-th vertex}}$

$(\{1, \dots, n^2\}, \leq, P)$
bits of the adjacency matrix

FO

$\circledast \quad \boxed{G, \bar{c}, \bar{c} \models \psi}$

$\boxed{\exists x \exists y \exists z (\sim -)}$

for $x = 1, \dots |V|$
  for $y = 1, \dots |V|$
    for $z = 1, \dots |V|$
      $\vdots$

Given $\underline{G, \bar{c}, \bar{c}}$
we can check $\circledast$
in time

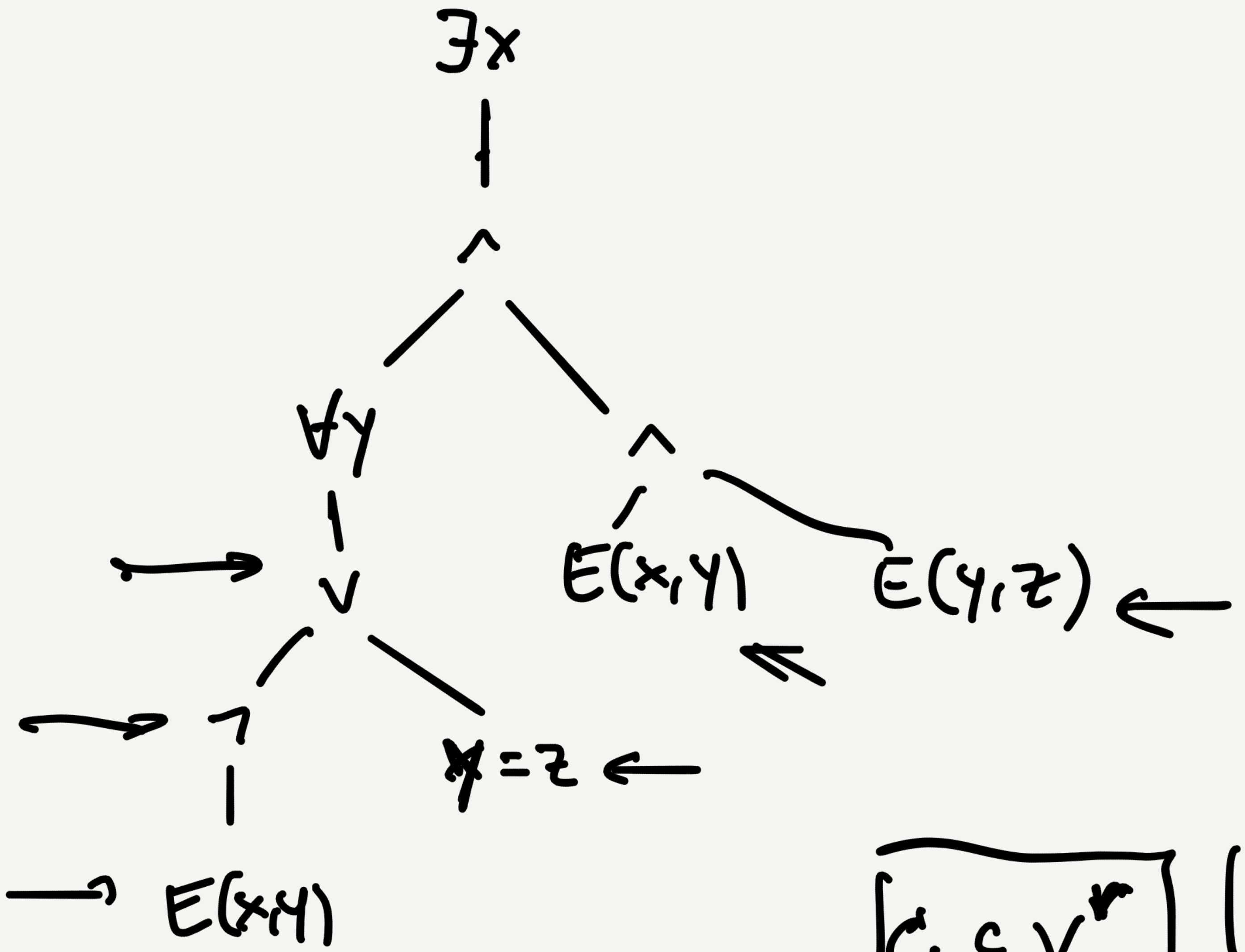
$$O(\mathrm{size}(\psi)) \cdot \left|\frac{G}{\bar{c}}\right|^{\mathrm{width}(\psi)}$$

for
  for

NP

$\exists \cancel{X} \; \psi$

G, z



$\boxed{G \subseteq V^r}$ $\boxed{n^r \text{ bits}}$

$G \subseteq V^2$ n^2 bits

Corollary:

If $\exists SO \neq \forall SO$ then $NP \neq co\text{-}NP$ and $P \neq NP$

(1) Ehrenfeucht - Fraïssé Games

(2) Locality theorems

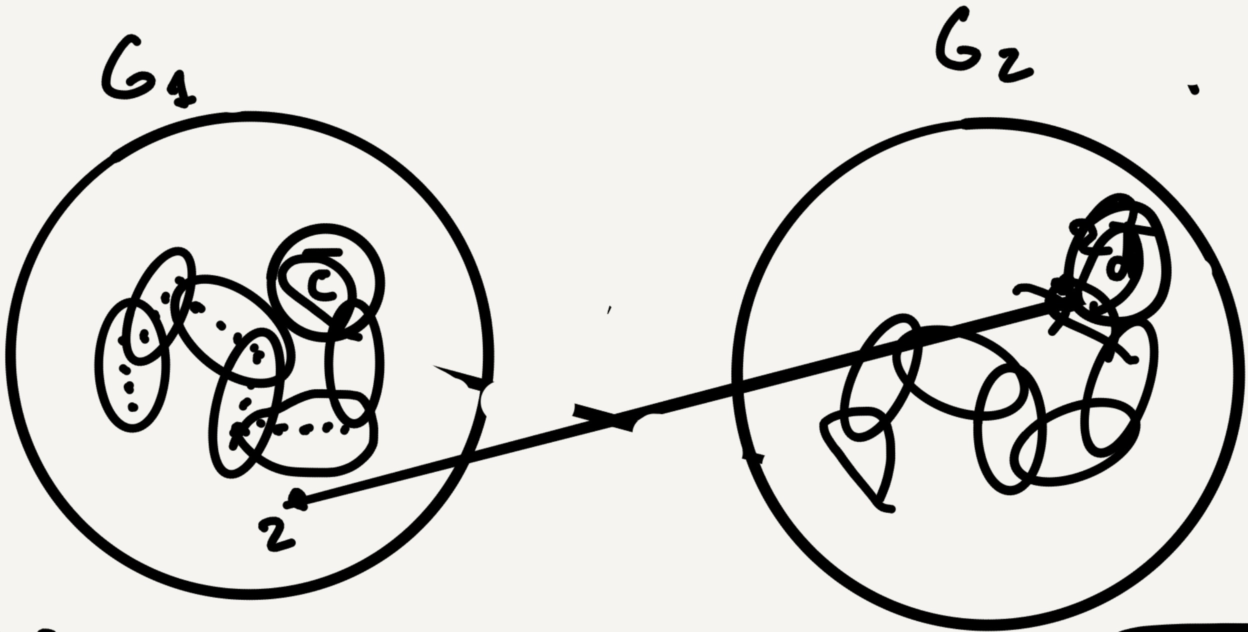
(3) Converting to Boolean circuits

$\exists x \leftrightarrow \bigvee_{u=1}^{n}$

$\forall x \leftrightarrow \bigwedge_{u=1}^{n}$

EF-Games

$m \in \mathbb{N}$



2 graphs

2 players

number of rounds: $m \in \mathbb{N} \cup \{\omega\}$

~~number of pebbles: $k \le \mathbb{N}$~~

objective: Spoiler: exhibit non-isomorphism

Duplicator: maintain local isomorphism

$\boxed{\bar{c} \mapsto \bar{d}}$

$c_1 \mapsto d_1$
$c_2 \mapsto d_2$
$\vdots$
$c_k \mapsto d_k$
is an local iso.

Theorem: TFAE, $m \in \mathbb{N} \cup \{\omega\}$, $k \in \mathbb{N}$, $\bar{c} \in V^k$, $\bar{d} \in V^k$

(1) $G, \bar{c}$ and $H, \bar{d}$ satisfy the same formulas of $qr \leq m$ and width $\leq k$

(2) Duplicator has a winning strategy on $G, \bar{c}$ and $H, \bar{d}$ with m rounds and k pebbles

initial position

the m-round k-pebble game.

$\underbrace{\neg(1)} \Rightarrow \neg(2)$

initial position

$G, \bar{c} \models \varphi$ & $H, \bar{d} \not\models \varphi$ for some

or $G, \bar{c} \not\models \varphi$ & $H, \bar{d} \models \varphi$

φ of $qr \leq m$ and width $\leq k$.

$\varphi = E(x_i, y_j)$ atomic

$\underbrace{(c_i, c_j) \in E(G)}$ & $\underbrace{(d_i, d_j) \notin E(H)}$

$\hookrightarrow$ 0-rounds win for spoiler.

$\varphi = \psi \wedge \Theta$

$\varphi = \exists x_j \, \psi$

$\hookrightarrow$ select this witness ~~with~~ pebble j

$\max(qr(\psi), qr(\Theta))$ win for spoiler

(1) $\Rightarrow$ (2)

Hintikka / Scott sentences.

$G, \bar{c} \equiv_m^k H, \bar{d}$: indistinguishability with $qr \leq m$ and width $\leq k$.

$\varphi_{m,G,\bar{c}}^k$ = defines the equivalence class of $G, \bar{c}$.

$$\varphi_{0,G,\bar{c}}^k = \bigwedge_{\substack{\psi \text{ atomic} \\ \text{width}(\psi) \leq k \\ G, \bar{c} \models \psi}} \psi \wedge \bigwedge_{\substack{\psi \text{ atomic} \\ \text{width}(\psi) \leq k \\ G, \bar{c} \not\models \psi}} \neg\psi$$

$$\boxed{\begin{aligned}\varphi^k_{m+1,G,\bar c} = {} & \varphi^k_{0,G,\bar c} \wedge \\ & \bigwedge_{i=1}^{k} \bigwedge_{u \in V(G)} \exists x_i \, \varphi^k_{m,G,\bar c[i/u]} \wedge \\ & \bigwedge_{i=1}^{k} \forall x_i \bigvee_{u \in V(G)} \varphi^k_{m,G,\bar c[i/u]}\end{aligned}}$$

<u>Fact</u>: Duplicator wins the m-round k-pebble game on $G,\bar c$ and $H,\bar d$ iff $H,\bar d \models \varphi^k_{m,G,\bar c}$

Pf: Induction on m. $\square$

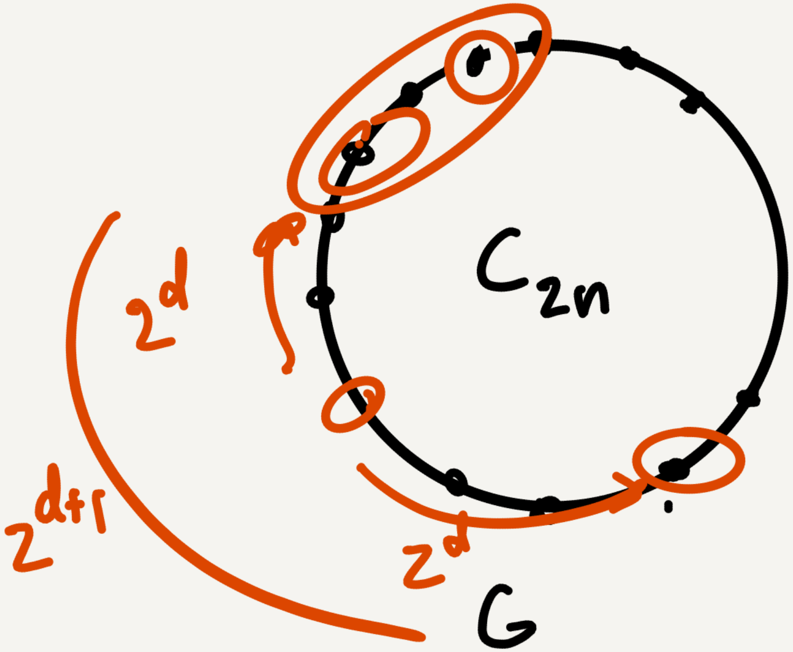
$$\boxed{G,\bar c \models \varphi^k_{m,G,\bar c}} \leftarrow$$

Application: Connectivity requires qr $= \Omega(\log n)$

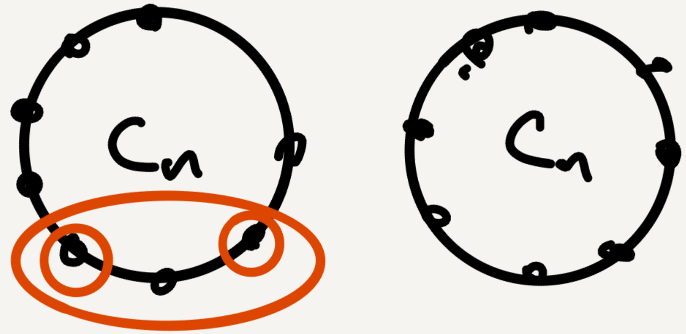
$$\forall x \forall y \bigvee_{t=0}^{n} \mathrm{PATH}_t(x,y)$$

qr $= \log t$

$O(\log n)$.



$\equiv_{\frac{1}{2}\log n}$



Strategy for Duplicator
preserve distances
up to 2^{m-i} after i rounds.

Hanf's Locality

<u>Thm:</u> Let A and B be two colored finite digraphs, let $m \in \mathbb{N}$ and let $e \in \mathbb{N}$ be bigger that the # of elements in any 3^m-neighborhood
3^m-ball
of a vertex in A or B.

If for each 3^m-ball type T

either A and B have the same # of vertices with 3^m-ball type T

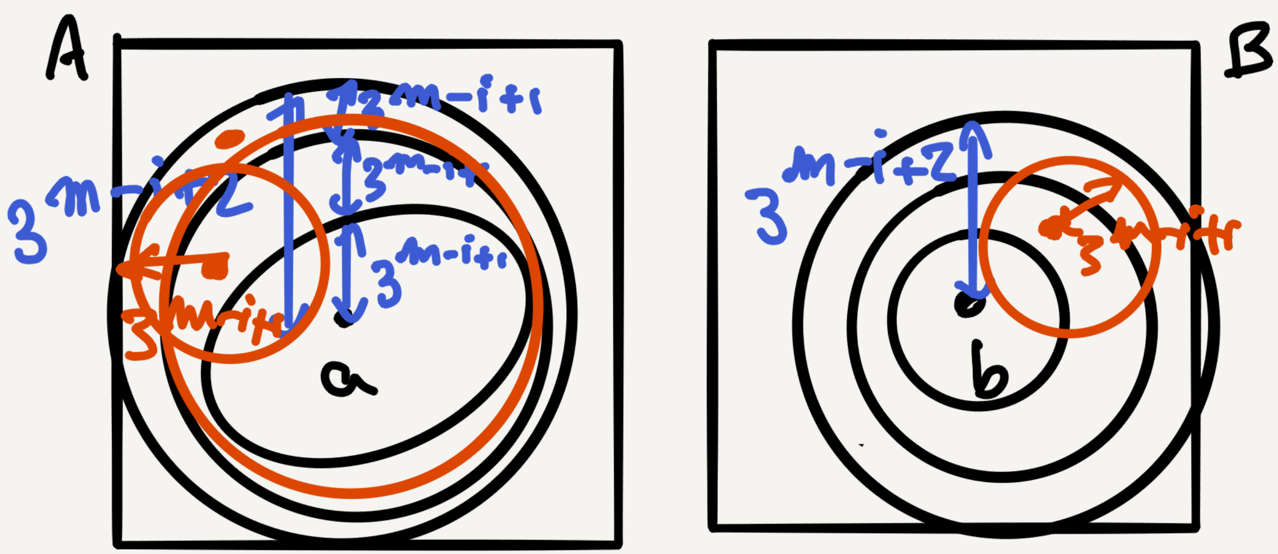
or both A and B have more than $m \cdot e$ vertices with 3^m-ball type T

then $A \equiv_m B$.

Pf: We want $A \equiv_m B$, we design a strategy for Duplicator in the m-round game.

At the end of round i:

Inv: $$S_A(3^{m-i+1}, \bar{a}) \cong S_B(3^{m-i+1}, \bar{b})$$



Round 1:

Round $i > 1$:

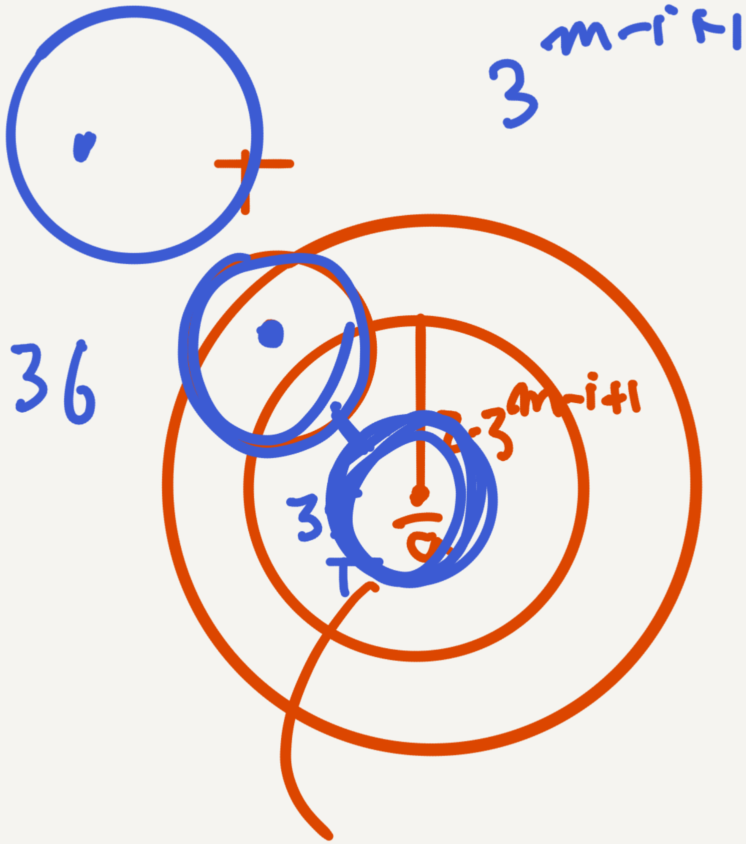
new element

Case 1_a: $c \in S_A(2\cdot 3^{m-i+1}, \bar{a})$

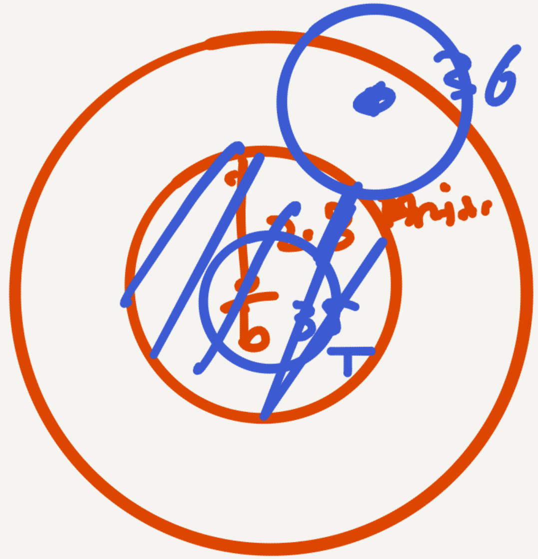
choose $d \in B$ s.t. $S_A(3^{m-i+1}, \bar{a}c) \cong S_B(3^{m-i+1}, \bar{b}d)$

case 2_a: $c \notin S_A(2\cdot 3^{m-i+1}, \bar{a})$

$S_A(3^{m-i+1}, c) \cap S_A(3^{m-i+1}, \bar{a}) = \emptyset$



element $e \cdot m$



element $e \cdot m$

Application 1: model checking.

Given a graph G and first-order sentence φ decide if $G \models \varphi$.

straightforward: $O(\mathrm{size}(\varphi) \cdot |G|^{\mathrm{width}(\varphi)})$

<u>Thm</u>: For every $d > 0$ there is an algorithm that solves MC for graphs of degree $\leq d$ in time $\boxed{\exp(\mathrm{size}(\varphi)) \cdot \mathrm{poly}(|G|)}$

universal constant in the exponent.

Given G and φ: $\boxed{\text{Seese}}$

exp(size(φ))

Preprocessing depends only on φ and d:

- Let N be the # of 3^m-ball types on graphs of degree $\leq d$
- Let e be the bound on # element of 3^m-ball types of graphs of degree $\leq d$
- S

Checking:

set $a_i := 0$ for $i = 1, \dots, N$

for $u \in V$:

Compute the 3^m-ball H_i around u

a_i++ truncated at $m \cdot e$

check if $(a_1, \dots, a_N) \in S$

if yes accept else reject

Let S be the set of all profiles of graphs of deg $\leq d$ such that

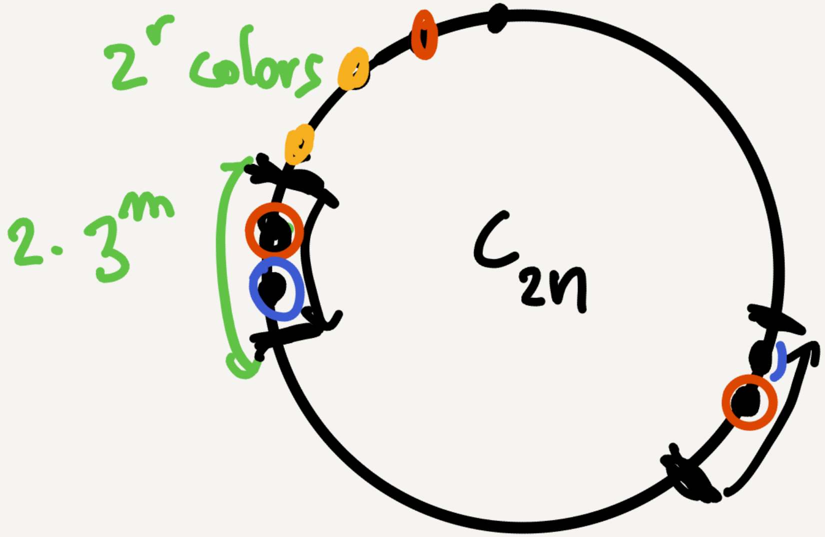
if G has profile in S then $G \models \varphi$

if G has profile outside S then $G \not\models \varphi$

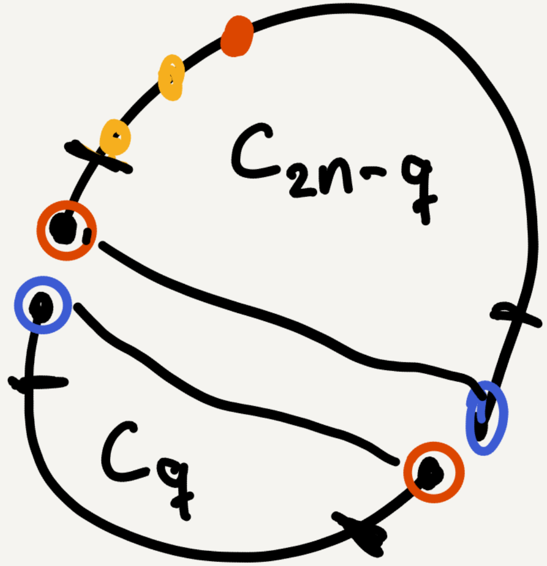
Application 2: Connectivity is not in Monadic $\exists SO$ (aka Monadic NP)

¿ Binary $\exists SO$?

$$\varphi = \exists \underbrace{X_1} \cdots \exists \underbrace{X_r}\ \psi$$



$\equiv_m$

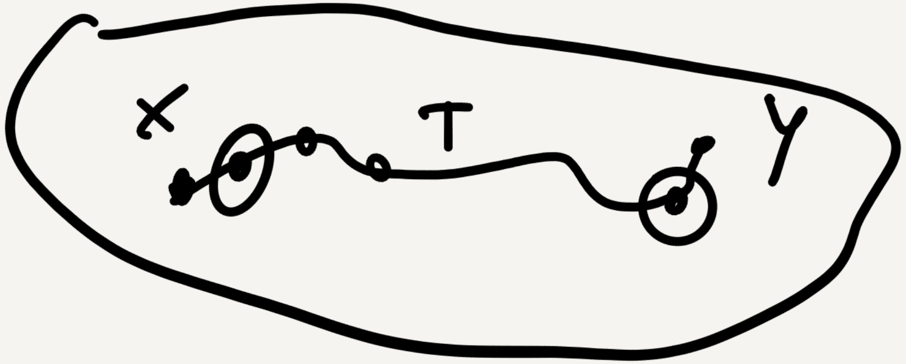


$C_{2n} \models \varphi$

$C_{2n}, X_1, \ldots, X_r \models \psi$

$C_q \oplus C_{2n-q} \models \varphi$

contradiction.



$$\forall x \forall y \ \exists T$$

$$T(x) \wedge T(y) \wedge$$

$$\exists! z\, (T(z) \wedge E(x,z)) \wedge$$

$$\exists! z\, (T(z) \wedge E(z,y)) \wedge$$

$$\forall z\, (T(z) \wedge z \neq x \wedge z \neq y \rightarrow \exists z_1 \exists z_2$$

$$(z_1 \neq z_2 \,\&\, T(z_1) \wedge T(z_2) \wedge E(z_1,z) \wedge E(z,z_2) \wedge$$

$$\forall z' (T(z') \wedge E(z',z) \longrightarrow z' = z_1))$$

$$\forall z' = z_2$$

OPEN: LB for closed Monadic NP:

FO closed under $\exists X$ monadic

$\forall y$ first-order

$$\forall y_1 \exists X_1 \forall y_2 \exists X_2 \cdots \ \text{FO}$$

Fagin's Thm:

NP = $\exists$SO on all graphs

Stockmeyer

PH = SO.

$$\boxed{\text{Is there a "logic" whose definable properties are precisely the iso-invariant polynomial decidable properties of graphs?}}$$

Thm: [Immerman-Vardi]

P = **LFP** on ordered graphs (or strings)

P = **IFP**

IFP : Inflationary Fixed-Point Logic.

$$\begin{cases} PATH_1(x,y) = E(x,y) \\ PATH_n(x,y) = PATH_{n-1}(x,y) \vee \boxed{\exists z\,(E(x,z) \wedge PATH_{n-1}(z,y))} \end{cases}$$

Syntax

New formula formation rule:

$$\frac{\varphi(X, \bar{x})}{(IFP_{X,\bar{x}}\, \varphi(X,\bar{x}))(\bar{x})} \quad \text{with } arity(X) = |\bar{x}|$$

$$PATH(x,y) \equiv \boxed{IFP_{X,xy}\ \exists z\,(E(x,z) \wedge X(z,y))}$$

Semantics:

$$\Theta_\varphi(\bar{x}, \bar{x})^G = R \longmapsto \{\bar{c} \in V(G)^r : G, R, \bar{c} \models \varphi\}$$

$$S_0 = \emptyset$$

$$S_{t+1} = S_t \cup \Theta_\varphi(S_t)$$

relations of arity r

$$S_0 \subseteq S_1 \subseteq S_2 \subseteq \dots$$

converges to a fixed-point in $\leq |V|^r$

$S_\infty = S_{t^*}$ where $t^* = \min$ s.t. $S_{t^*} = S_{t^*+1}$.

$\leq$: a guess in Fagin's Thm.

$$V = \{0, \dots, n-1\}$$
$$\leq$$

$X_q(\underbrace{t_1, \dots, t_r}_{})$: "at time t state is q"

$\approx$ a number t in $\{0, \dots, n^r - 1\}$

$X_a(\underbrace{t_1, \dots, t_r}_{t}, \underbrace{p_1, \dots, p_r}_{p})$: "at time t position p of the tape contains symbol a"

$X(t_1, \dots, t_r, p_1, \dots, p_r)$

$X_0 / X_1(t_1, \dots, t_r)$: at time t the 0/1 branch of non-det is taken

Logics with Counting

$\boxed{FOC}$

Add counting quantifiers: for $t \in \mathbb{N}$

$\exists^{\geq t} x \quad \psi$: "there at least t elements that satisfy ψ."

$$\underbrace{\exists x_1 \exists x_2 \cdots \exists x_t}\left(\bigwedge_{i \neq j} x_i \neq x_j \wedge \bigwedge_{i=1}^{t} \psi(\cancel{x}/x_j) \right)$$

$G = \{a_1, \dots, a_n\} \models \quad \exists x \exists y \exists z \quad \cdots$

Logics with Counting Constructs:

FO+C
IFP+C

structures are 2-sorted
- domain sort (vertices as an ex.)
- number sort.

3-ary relations

$$G = \Big((V, E, P_1, \dots, P_r) \, , \, (\{0, \dots, |V|\}, \le, +, \times, 0, 1, \max) \Big)$$

graph sort

$p + q = r$

$p \times q = r$

Syntax:

$\#x.\,\psi(x)$: gives the number in $\{0, \dots, |V|\}$ of elements in V that satisfy ψ.

G is 3-regular

$$\exists p \, (p = 3 \wedge \forall x \, (\# y . E(x,y) = p))$$

quantification over number sort

domain sort

domain vars $x, y, u, v, \ldots$

number vars $p, q, r, \ldots$

$$\exists q \, \exists q' \, \exists q'' \, (q = 0+1 \wedge q' = q+1 \wedge q'' = q'+1)$$

$\# x,y : \psi$: (p,q) s.t. $p\overbrace{(n+1)}^{|V|+1}+q$ is the number of pairs (x,y) that satisfy ψ

$(\# x,y : \psi)_1$

$(\# x,y : \psi)_2$

$\exists p\,(p+p = \max \wedge \forall x\ \# y.\, E(x,y) = p)$

3-regular

$\frac{n}{2}$-regular

EVEN

ODD

$Ex\ \psi$ = "there is an even number of x ...

$Ox\ \psi$ = "there ~ ~ odd ... "

$A \in GF(2)^{V \times V}$ $\qquad$ $A \subseteq V \times V$

"A is non-singular over GF(2)".

← Gaussian elimination : NO GOOD.

$$A^{N_n} = Id \iff \forall x \forall y \left(\text{power}(A, \underline{N_n})(x,y) \leftrightarrow x = y \right)$$

the order of the group of non-singular matrices in ~~of~~ $GF(2)^{n \times n}$

$$N_n = (2^n - 1)(2^n - 2)(2^n - 2^2) \cdots$$
$$\cdots (2^n - 2^i) \cdots (2^n - 2^{n-1})$$
$$\cong 2^{n^2} \qquad \sim n^2 \text{ bits.}$$

There is a formula $\psi(x,y)$ of IFP that, on the number sort, describes the bits N_n.

$A \subseteq V \times V$ $\qquad$ $R \subseteq [n] \times [n]$ (a number of n^2 bits)

$\text{power}(A, R)(x,y)$

$$\text{power}(A, N_n)(x,y) := \text{power}(A, \psi)(x,y)$$

$$\underbrace{A^2}_{\text{square}(A)}(x,y) = \sum_z A(x,z)\,A(z,y) \bmod 2$$

$$= \bigoplus_z \big(A(x,z) \wedge A(z,y) \big).$$

$$\underbrace{(A \cdot B)}_{\text{prod}(A,B)}(x,y) = \bigoplus_z \big(A(x,z) \wedge B(z,y) \big).$$

$$\text{power}(A, 0)(x,y) := x = y$$

$$\text{power}(A, k)(x,y) :=$$

$$\quad \text{prod}(A, \text{square}(\text{power}(A, \lfloor k/2 \rfloor))) \text{ if } k \text{ odd}$$

$$\quad \text{prod}(I, \text{square}(\text{power}(A, \lfloor k/2 \rfloor))) \text{ if } k \text{ even}$$

$I(x,y) := x = y$

IFP+C can do non-singularity $GF(q)^{n \times n}$

[Grohe '98] IFP+C = P on planar graphs

↳ IFP+C has definable cannonization for planar graphs.

[Grohe '08] IFP+C = P on any minor-closed class of graphs (non-trivial).

$\boxed{\text{[Anderson Dawar Holm] IFP+C can do LINEAR PROG. FEASIBILITY}}$

$\boxed{\text{[A. Ochremiak] } C^{\omega}_{\infty\omega} \text{ can do SDP FEASIBILITY}}$

Infinitary Logics

- add infinite $\bigvee$ and infinite $\bigwedge$

$L_{\infty\omega}$ $\quad \varphi(x,y) = \bigvee_{n\geq 1} \mathrm{PATH}_n(x,y)$

$C_{\infty\omega}$: same as $L_{\infty\omega}$ with counting quantifiers $\exists^{\geq t} x\, \psi$

$L^{k}_{\infty\omega}$ $\quad L^{\omega}_{\infty\omega}$: same $L_{\infty\omega}$ but of bdd width

$C^{k}_{\infty\omega}$ $\quad C^{\omega}_{\infty\omega}$: — $C_{\infty\omega}$ —

$$\mathrm{IFP} \subseteq L^{\omega}_{\infty\omega}$$

$\#x.\psi$

$$\mathrm{IFP{+}C} \subseteq C^{\omega}_{\infty\omega} \qquad \exists^{\geq t}_{x}\, \psi$$

Why? $\psi(X, \bar{x})$

$(\mathrm{IFP}_{X,\bar{x}}\ \psi)$ means

$$\equiv \bigvee_{t\geq 0} \psi^{(t)}(x,y)$$

$S_0 = \emptyset$

$S_{t+1} = S_t \cup \psi(S_t)$

$S_\infty = S_{t^*} = \bigcup_{t\geq 0} S_t$

$\emptyset$

$\psi^{(0)}(x,y) = \text{false}$

$\psi^{(t+1)}(x,y) = \psi(\psi^{(t)}, x, y) \vee \psi^{(t)}$

$\leq 2k$ vars where $k = \mathrm{width}(\psi)$

Ehrenfeucht-Fraïssé Games for $C^{\omega}_{\infty\omega}$ $L^{\omega}_{\infty\omega}$

For $L^{k}_{\infty\omega}$, the game is $\equiv^{k}_{\omega}$

For $C^{k}_{\infty\omega}$, the game is:

2 players
k pebbles
ω rounds

Thm: TFAE

(1) A and B satisfy the same sentences of $C^k_{\infty\omega}$

(2) Duplicator has a winning strategy on A and B with k pebbles in the counting game.

Notation $A \overset{C}{\equiv}{}^{k} B$

Weisfeiler - Lehman Algorithm

~~Color~~ Vertex refinement algorithm:

0. color each vertex by its degree.
1. color each vertex by the multi-set of colors of its neighbors
2. rename the colors to $1, \dots, c$ lexicographically
   \# of colors.
3. Go back to 1 until color class stabilize.

Given G, H:

compute refinement

compare

if $\neq$, say non-iso, else maybe iso

k-dimensional refinement

ordered

Let $A_1, \dots, A_n$ be the isomorphism types (atomic type) of k-tuples (all of them).

Given G:

$c(\bar{v}) = i$

ordered

0. Color each k-tuple by iso-type A_i

1. Color each k-tuple $\bar{v} = (v_1, \dots, v_k)$ with

$$\{\{ (\underbrace{c(\bar{v}[1/u]), \dots, c(\bar{v}[k/u])}_{k\text{-tuple of colors}}) : u \in V \}\}$$

2. Rename colors to $1, \dots, c$ ← # colors
   lexicographically.

3. Go back to 1 until stabilizes

Thm [Cai-Fürer-Immerman 1992]

TFAE

(1) A and B are $C^{k+1}_{\infty\omega}$-equivalent

(2) $A \equiv^{C}_{k+1} B$ (Duplicator wins)

(3) k-DiM-WL(A) = k-DiM-WL(B)

$\boxed{\text{CFI- constructions}}$ $\simeq$ Tseitin Construction

Thm:

There is a family of pairs of bdd-degree graphs (G_n, H_n) s.t.

(1) $G_n \not\cong H_n$ $\longleftrightarrow$ $(G_n, G_n) \overset{C}{\equiv}_{\Omega(n)} (G_n, H_n)$

(2) $G_n \overset{C}{\equiv}_{\Omega(n)} H_n$

(3) $|V(G_n)| = |V(H_n)| = \Theta(n)$.

Cor: IFP+C $\neq$ P on bdd graphs.

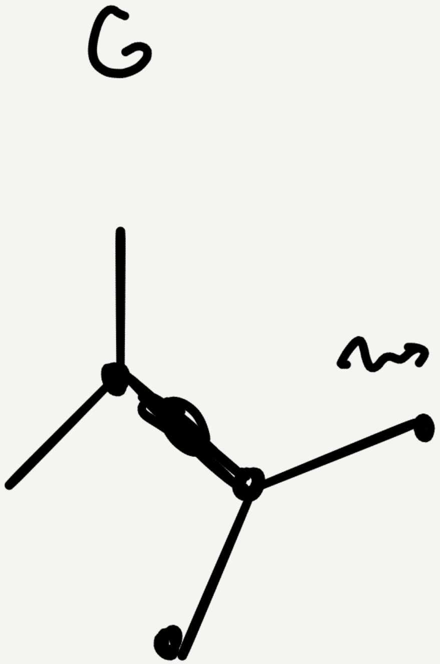
3-regular n-vertex connected εn

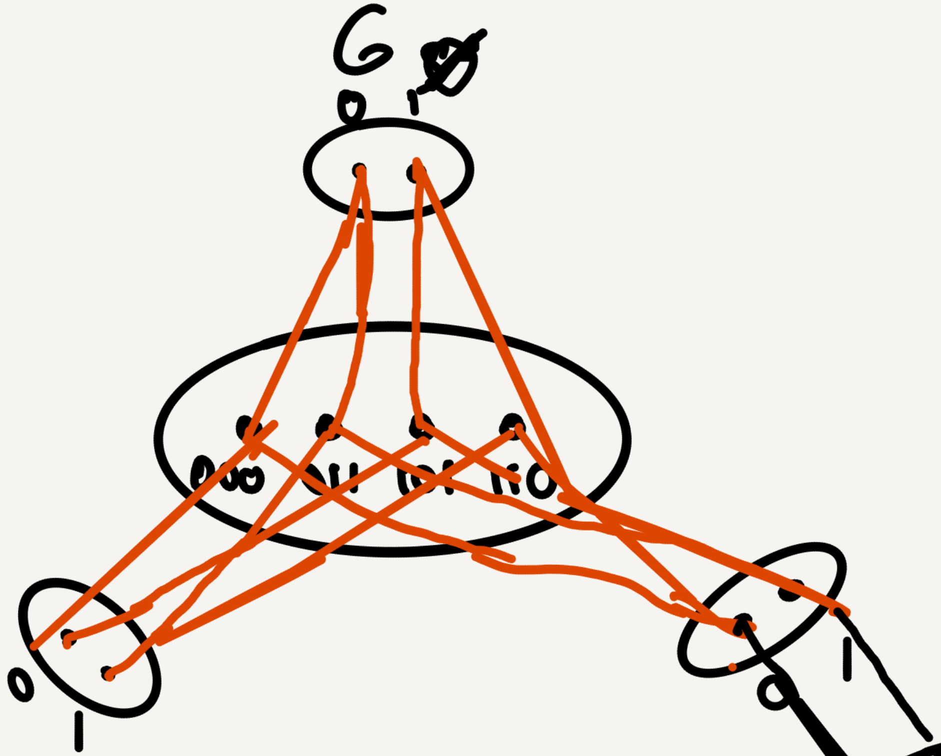
Let G be a 3-regular n-vertex connected graph without $o(n)$-separators:

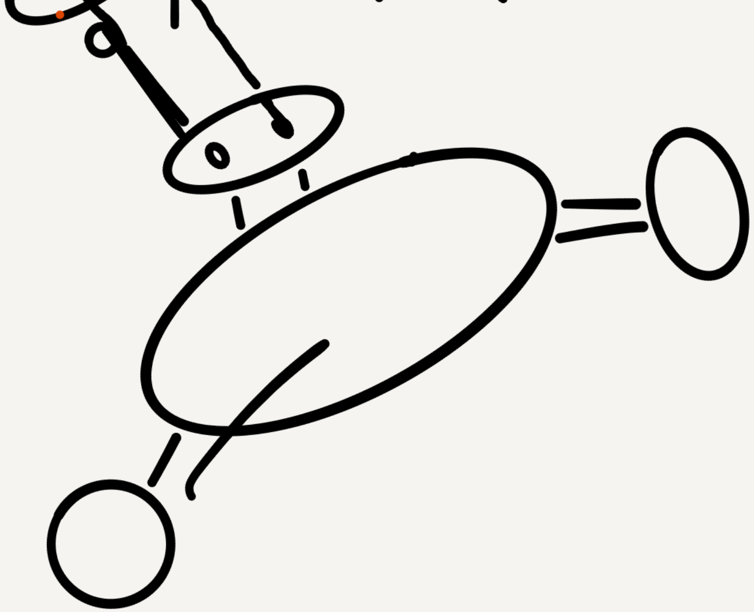
removing any εn set of vertices leaves a connected component with more than half the vertices.

$$
\begin{tikzcd}
 & G \arrow[dl] \arrow[d] \arrow[dr] & \\
G_n & & H_n \\
 & \boxed{G_S} &
\end{tikzcd}
$$

where $S \subseteq V(G)$.





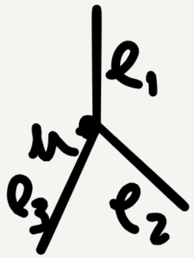


G_S
$=$
$G_\emptyset$ with the gadgets of $v \in S$ flipped: odd/even

Thm: If $|S| \equiv |T| \bmod 2$, then $G_S \cong G_T$

If $|S| \not\equiv |T| \bmod 2$, then $G_S \ncong G_T$.

$x_{u,e}$: a variable for every $u \in V(G)$
and incident edge e



eq 1 : $x_{u,e_1} + x_{u,e_2} + x_{u,e_3} = I[u \in S] \bmod 2$

eq 2 : $x_{u,e} + x_{v,e} = 0 \bmod 2$

$|S|$ even $\Rightarrow$ $0 = 0$ $\quad e = \{u, v\}$

$|S|$ odd $\Rightarrow$ $0 = 1 \bmod 2$

Corollary : XOR-SAT $\notin C^{\omega}_{inv}$

$\notin$ IFP+C

non-singularity GF(2) $\in$ IFP+C