A Dichotomy Theorem for Homomorphism Polynomials

N. de Rugy-Altherre

Univ Paris Diderot, Sorbonne Paris Cité, Institut de Mathématiques de Jussieu,
UMR 7586 CNRS,
F-75205 Paris, France

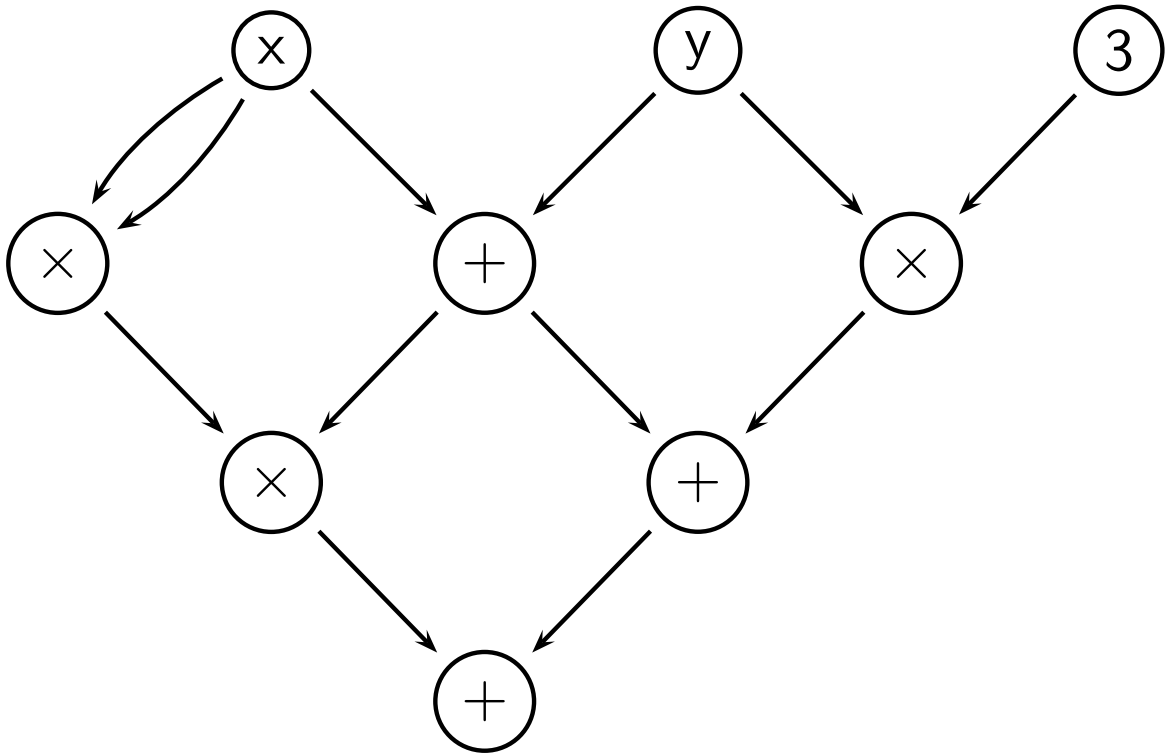
September 18, 2012

Algebraic Complexity

Definition

An *arithmetic circuit* is an acyclic directed graph with indegree at maximum 2. The nodes with indegree 0 are labeled with constants of a field $\mathbb{K}$ or variables; the one with indegree 2 are labeled with $+$ and $\times$.

Algebraic Complexity



$$f(x, y) = x^3 + x^2y + 3xy + 3y^2$$

Algebraic Complexity

Definition

- The *size* of an arithmetic circuit is the number of operational gates.

Algebraic Complexity

Definition

- The *size* of an arithmetic circuit is the number of operational gates.
- A p-family (f_n) is a sequence of polynomials such that the number of variables as well as the degree of f_n are polynomially bounded in n.

Algebraic Complexity

Definition

- The *size* of an arithmetic circuit is the number of operational gates.
- A p-family (f_n) is a sequence of polynomials such that the number of variables as well as the degree of f_n are polynomially bounded in n.
- A p-family (f_n) of polynomials is in VP if it can be computed by a family of arithmetic circuits of polynomial size in n.

Algebraic Complexity

Definition

- The *size* of an arithmetic circuit is the number of operational gates.
- A p-family (f_n) is a sequence of polynomials such that the number of variables as well as the degree of f_n are polynomially bounded in n.
- A p-family (f_n) of polynomials is in VP if it can be computed by a family of arithmetic circuits of polynomial size in n.
- A p-family (f_n) is in VNP if there is a family (g_n) in VP such that

$$f_n(\bar{x}) = \sum_{\bar{\epsilon} \in \{0,1\}^n} g_n(\bar{\epsilon}, \bar{x})$$

Algebraic Complexity

Definition

- A p-family (g_n) is a *p-reduction* of (f_n), write $(g_n) \leq_p (f_n)$, is there is a polynomial p and $a_1, \ldots, a_{p(n)}$ variables or constants such that

$$g_n(\bar{x}) = f_{p(n)}(\bar{a})$$

Algebraic Complexity

Definition

- A p-family (g_n) is a *p-reduction* of (f_n), write $(g_n) \leq_p (f_n)$, is there is a polynomial p and $a_1, \ldots, a_{p(n)}$ variables or constants such that
$$g_n(\bar{x}) = f_{p(n)}(\bar{a})$$

- A p-family (g_n) is a *c-reduction* of (f_n), write $(g_n) \leq_c (f_n)$, is there is a polynomial p an arithmetic circuit of polynomial size with oracle $f_{p(n)}$ that compute g_n.

Algebraic Complexity

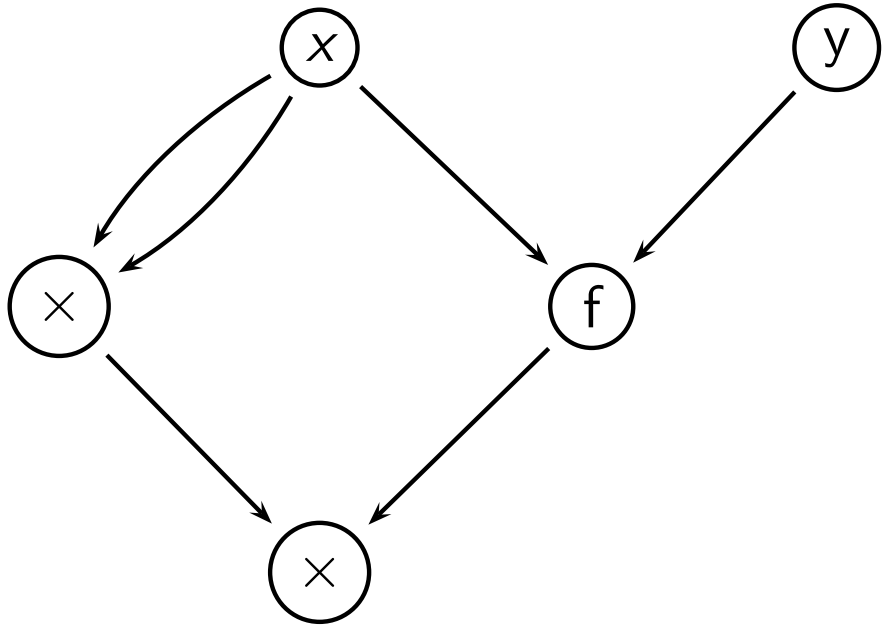
Definition

- A p-family (g_n) is a *p-reduction* of (f_n), write $(g_n) \leq_p (f_n)$, is there is a polynomial p and $a_1, \ldots, a_{p(n)}$ variables or constants such that
$$g_n(\bar{x}) = f_{p(n)}(\bar{a})$$

- A p-family (g_n) is a *c-reduction* of (f_n), write $(g_n) \leq_c (f_n)$, is there is a polynomial p an arithmetic circuit of polynomial size with oracle $f_{p(n)}$ that compute g_n.
- A p-family (f_n) is VNP*-complete* for c-reductions is for any family $(g_n) \in \mathrm{VNP}$,
$$(g_n) \leq_c (f_n)$$

Algebraic Complexity

$$g(x, y) = x^2(x^3 + x^2y + 3xy + 3y^2)$$



If $f(x, y) = x^3 + x^2y + 3xy + 3y^2$, then $g \leq_c f$.

Algebraic Complexity

- Let (f_n) be a p-family. Let us write $\mathbf{HC}_k(f_n)$ for the homogeneous component of degree k of f_n.
- There is some constants $w_{i,k} \in \mathbb{R}$ such that

$$\mathbf{HC}_k(f_n)(\bar{x}) = \sum_{i=0}^{d_n} w_{i,k} f^n(2^i \bar{x})$$

- Then for any sequence of integers (k_n),

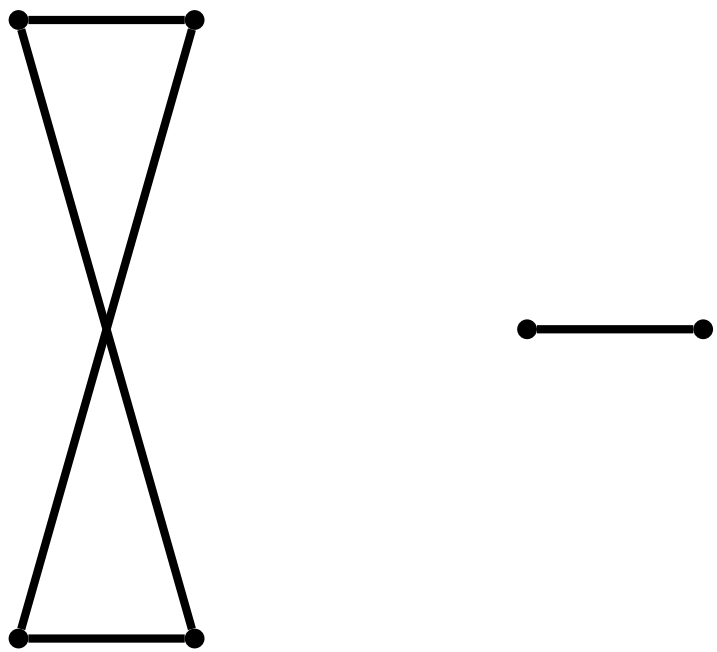
$$(\mathbf{HC}_{k_n}(f_n)) \leq_c (f_n)$$

Graph homomorphisms

Definition

Let G and H be two graphs and let ϕ an application from $V(G)$ to $V(H)$. It is an homomorphism if:

$$\forall u, v \in V(G), (u, v) \in E(G) \Rightarrow (\phi(u), \phi(v)) \in E(F)$$

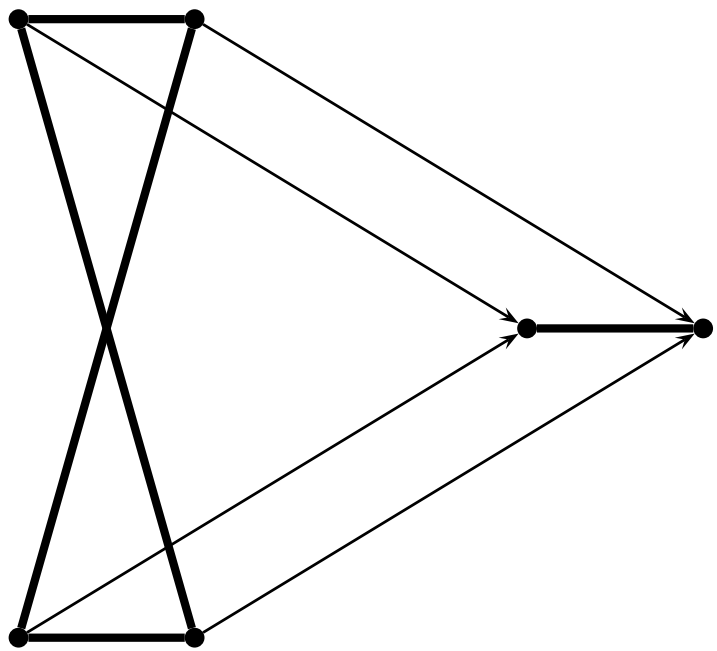


Graph homomorphisms

Definition

Let G and H be two graphs and let ϕ an application from $V(G)$ to $V(H)$. It is an homomorphism if:

$$\forall u, v \in V(G), (u, v) \in E(G) \Rightarrow (\phi(u), \phi(v)) \in E(F)$$



Homomorphism polynomials

Definition

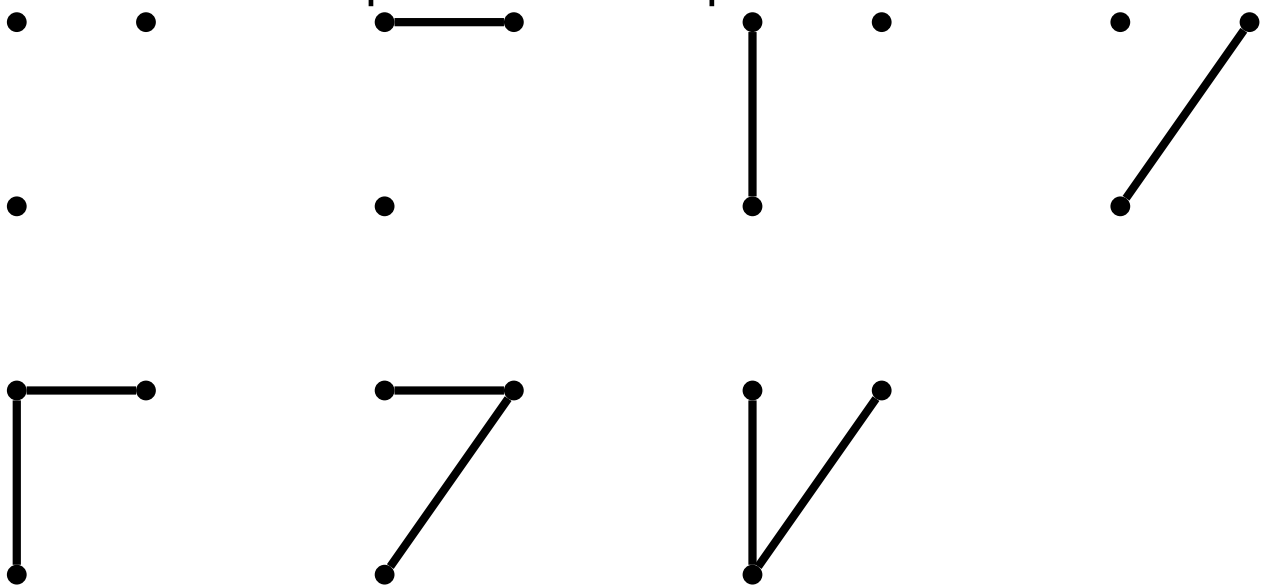
Let H be a graph. The polynomial enumerating all graphs G with n vertices which are homomorphic to H is:

$$f_n^H((x_e)_{e\in E(K_n)}) := \sum_{\bar{\epsilon}\in\{0,1\}^{|E(K_n)|}} \Phi_n^H(\bar{\epsilon}) \prod_{e\in E(K_n)} x_e^{\epsilon_e}$$

Where $\Phi_n^H(\bar{\epsilon})$ is equal to 1 if the graph G such that $V(G) = [n]$ and $E(G) = \{e \in E(K_n) | \epsilon_e = 1\}$ is homomorphic to H, 0 otherwise.

Homomorphism polynomials

Graphs homomorphic to  .



$$f_{\bullet\!-\!\bullet}(\bar{x}) = 1 + x_{1,2} + x_{1,3} + x_{2,3} + x_{1,2}x_{1,3} + x_{1,2}x_{2,3} + x_{1,3}x_{2,3}$$

Homomorphism polynomials

Theorem

Let H be a graph. Then, over $\mathbb{Q}$

- *If H has a loop or no edges, (f_n^H) is in VP.*
- *Else (f_n^H) is VNP-complete under c-reductions.*

The first step of the proof

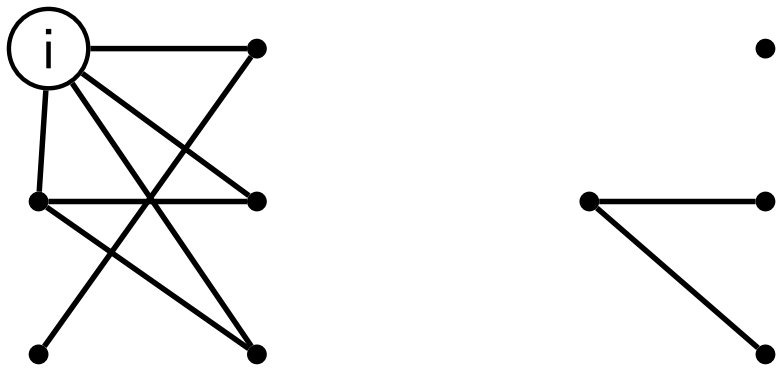
Proposition

For any graph H with no loops and at least one edge,

$$(f_n^{\bullet\!-\!\bullet}) \leq_c \left(f_n^H\right)$$

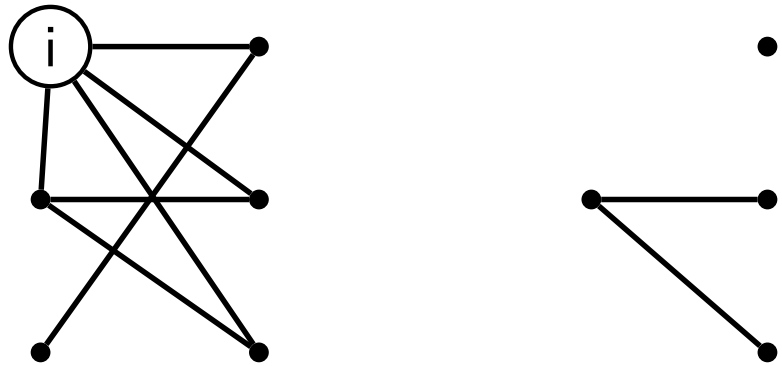
The first step of the proof

- Let H_i be the subgraph of H built by the neighbour of i and $\tilde{H} = \cup_{i \in V(H)} H_i$.

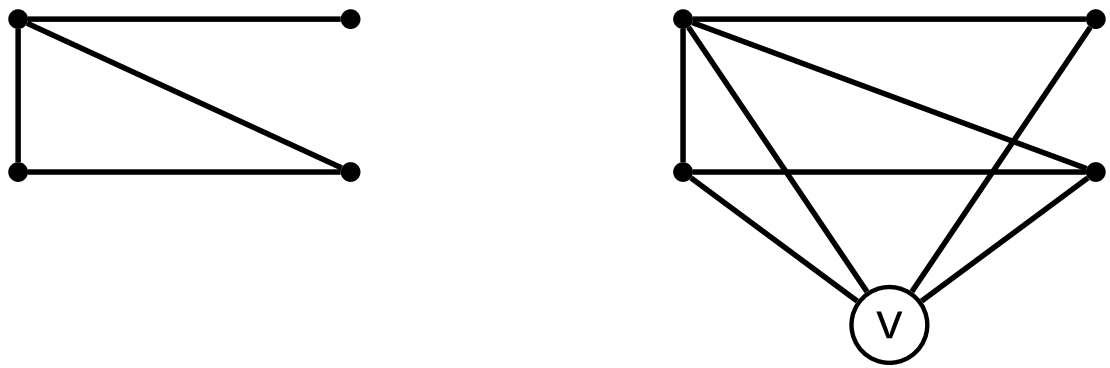


The first step of the proof

- Let H_i be the subgraph of H built by the neighbour of i and $\tilde{H} = \cup_{i \in V(H)} H_i$.

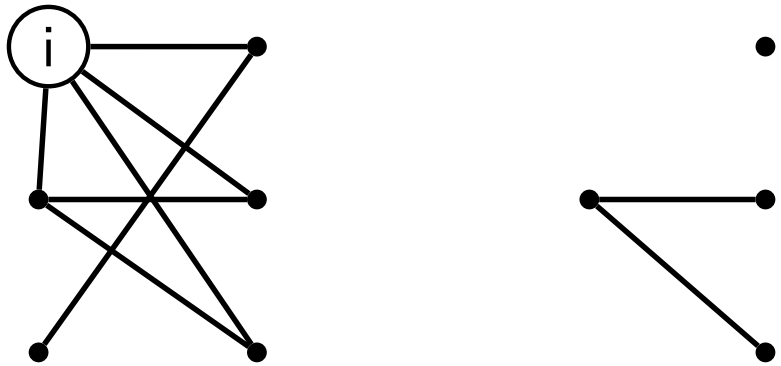


- Let us write G' the graph G with a new vertex v linked to every others.

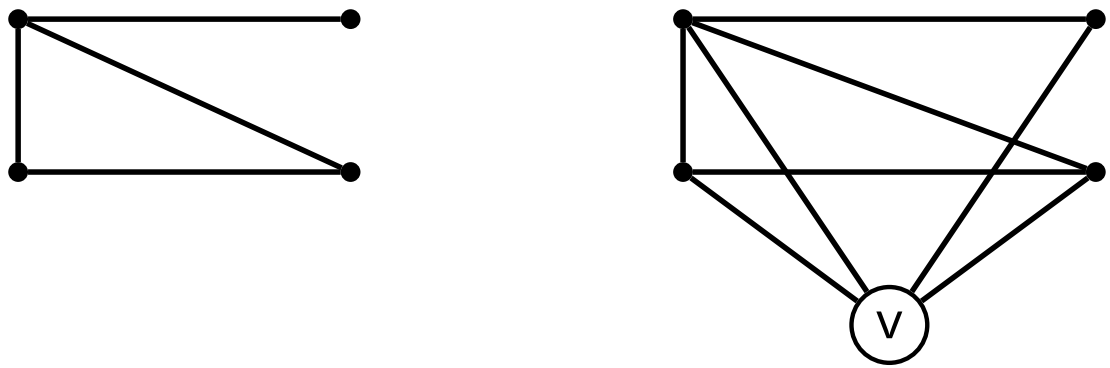


The first step of the proof

- Let H_i be the subgraph of H built by the neighbour of i and $\tilde{H} = \cup_{i \in V(H)} H_i$.



- Let us write G' the graph G with a new vertex v linked to every others.



- G' is homomorphic to H iff G is to $\tilde{H}$.

The first step of the proof

$$f_{n+1}^{H}(\bar{x}, x_{1,n+1}, \ldots, x_{n,n+1}) = \sum_{G \text{ homomorphic to } H} \bar{x}^{G}$$

$$f_{n+1}^{H}(\bar{x}, y, \ldots, y) = \sum_{G \text{ homomorphic to } H} \bar{x}^{G} y^{m(G)}$$

Where $m(G)$ is the number of edges from $n+1$ to an other vertex.

$$\begin{aligned}
\mathbf{HC}_{n}^{y}\left(f_{n+1}^{H}\right)(\bar{x}, 1, \ldots, 1) &= \sum_{G' \text{ homomorphic to } H} \bar{x}^{G} \\
&= \sum_{G \text{ homomorphic to } \tilde{H}} \bar{x}^{G} \\
&= f_{n}^{\tilde{H}}(\bar{x})
\end{aligned}$$

Therefore, $(f_n^{\tilde{H}}) \leq_c (f_n^{H})$

The first step of the proof

Definition

The *maximal degree* of a graph is the maximal number of edge coming from a single vertex.

The maximal degree of $\tilde{H}$ is strictly lower than the maximal degree of H.

The first step of the proof

Definition

The *maximal degree* of a graph is the maximal number of edge coming from a single vertex.

The maximal degree of $\tilde{H}$ is strictly lower than the maximal degree of H.

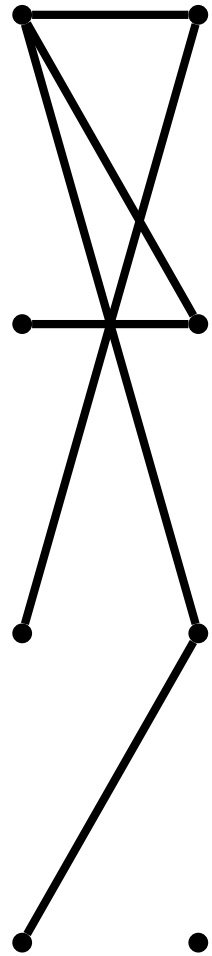
Proposition

For any graph H with no loops and at least one edge,

$$(f_n^{\bullet\!-\!\bullet}) \leq_c \left(f_n^H\right)$$

Proof that $(f_n^{\bullet-\bullet})$ is VNP-complete

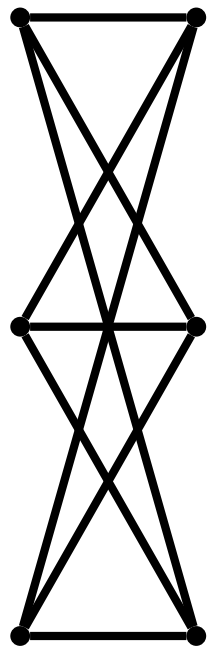
$f_n^{\bullet-\bullet}$ enumerates every bipartite graphs on n vertices.



Proof that $(f_n^{\bullet-\bullet})$ is VNP-complete

G_n enumerates every complete bipartite graphs on $2n$ vertices.

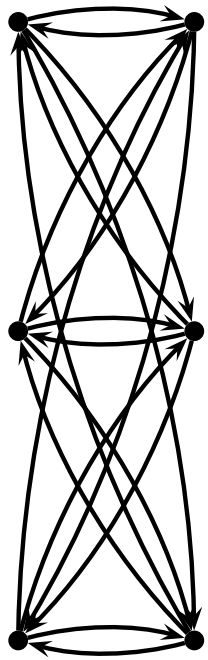
G_n



Proof that $(f_n^{\bullet\text{—}\bullet})$ is VNP-complete

Cut_n^2 enumerates every oriented complete bipartite graphs on $2n$ vertices.

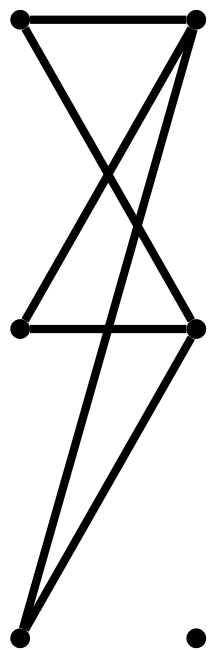
$\mathbf{Cut}_n^2$



Proof that $(f_n^{\bullet-\bullet})$ is VNP-complete

F_n enumerates every complete bipartite graphs on a subset of $2n$ vertices.

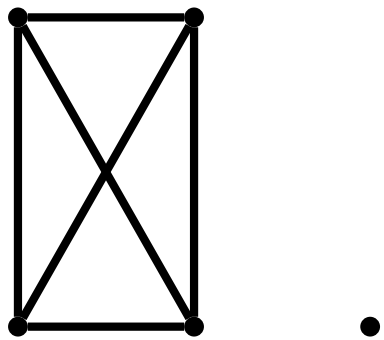
F_n



Proof that $(f_n^{\bullet\!-\!\bullet})$ is VNP-complete

GF(K_n, clique) enumerates every cliques on n vertices.

G_n



Conclusion

$$(\mathrm{GF}(K_n, \mathrm{clique})) \leq_c (F_n) \leq_p (\mathrm{Cut}_n^2) \leq_c (G_n) \leq_c (f_n^{\bullet\!-\!\bullet}) \leq_c (f_n^H)$$

Conclusion

$$(\mathrm{GF}(K_n, \mathrm{clique})) \leq_c (F_n) \leq_p (\mathrm{Cut}_n^2) \leq_c (G_n) \leq_c (f_n^{\bullet\!-\!\bullet}) \leq_c (f_n^H)$$

Theorem (Bürgisser, 5.22)

Let q be a power of the prime p. The family of cut enumerators (Cut^q) over $\mathbb{F}_q$ is neither VP nor VNP-complete with respect to c-reductions, provided $Mod_p\mathrm{NP} \not\subseteq \mathrm{P}/poly$.

Conclusion

$$(\mathrm{GF}(K_n, \mathrm{clique})) \leq_c (F_n) \leq_p (\mathrm{Cut}_n^2) \leq_c (G_n) \leq_c (f_n^{\bullet\!-\!\bullet}) \leq_c (f_n^H)$$

Theorem (Bürgisser, 5.22)

Let q be a power of the prime p. The family of cut enumerators (Cut^q) over $\mathbb{F}_q$ is neither VP nor VNP-complete with respect to c-reductions, provided $Mod_p\mathrm{NP} \not\subseteq \mathrm{P}/poly$.

Problem (Bürgisser, 5.2)

Is Cut^2, interpreted as family over the rationals, VNP-complete?

Conclusion

$$(\mathrm{GF}(K_n, \mathrm{clique})) \leq_c (F_n) \leq_p (\mathrm{Cut}_n^2) \leq_c (G_n) \leq_c (f_n^{\bullet\!-\!\bullet}) \leq_c (f_n^H)$$

Theorem (Bürgisser, 5.22)

Let q be a power of the prime p. The family of cut enumerators (Cut^q) over $\mathbb{F}_q$ is neither VP nor VNP-complete with respect to c-reductions, provided $Mod_p\mathrm{NP} \not\subseteq \mathrm{P}/poly$.

Problem (Bürgisser, 5.2)

Is Cut^2, interpreted as family over the rationals, VNP-complete?

This answer is yes.

Conclusion

$$(\mathrm{GF}(K_n, \mathrm{clique})) \leq_c (F_n) \leq_p (\mathrm{Cut}_n^2) \leq_c (G_n) \leq_c (f_n^{\bullet\!-\!\bullet}) \leq_c (f_n^H)$$

Theorem (Bürgisser, 5.22)

Let q be a power of the prime p. The family of cut enumerators (Cut^q) over $\mathbb{F}_q$ is neither VP nor VNP-complete with respect to c-reductions, provided $Mod_p\mathrm{NP} \not\subseteq \mathrm{P}/poly$.

Problem (Bürgisser, 5.2)

Is Cut^2, interpreted as family over the rationals, VNP-complete?

This answer is yes.
Thank you!