Electronic Colloquium on Computational Complexity, Report No. 5 (2004)

# On Graph Complexity

Stasys Jukna *†
Universität Frankfurt, Institut für Informatik
Robert-Mayer-Str. 11-15, D-60054 Frankfurt, Germany
&
Institute of Mathematics and Informatics
Akademijos str. 4, LT-2600 Vilnius, Lithuania

**Abstract**

A boolean circuit $f(x_1, \ldots, x_n)$ *represents* a graph $G$ on $n$ vertices if for every input vector $a \in \{0,1\}^n$ with precisely two 1's in, say, positions $i$ and $j$, $f(a) = 1$ precisely when $i$ and $j$ are adjacent in $G$; on inputs with more or less than two 1's the circuit can output arbitrary values.

We consider several types of boolean circuits (depth-3 circuits and boolean formulas) and show that some explicit graphs cannot be represented by small circuits. As a consequence we obtain that an explicit boolean function in $2m$ variables cannot be computed as an OR of fewer than $2^{\Omega(m)}$ products of linear forms over $GF(2)$. Lower bounds for this model obtainable by previously known (algebraic) arguments do not exceed $2^{O(\sqrt{m})}$.

We conclude with a graph-theoretic problem whose solution would have some intriguing consequences in computational complexity.

*Keywords*: Graph complexity, depth-3 circuits, $C_4$-free graphs, clique covering number

*AMS subject classification*: 05C62, 05C35, 05C99, 68Q17, 68Q05

## 1 Introduction

A major challenge in computational complexity is to exhibit an *explicit* boolean function $f : \{0,1\}^m \to \{0,1\}$ which has high combinational complexity, i.e. cannot be computed using a small number of basic boolean operations such as OR $x \vee y$, AND $x \wedge y$ or Parity $x \oplus y = x + y \pmod 2$; inputs for such a circuit are literals, i.e.

*Email: jukna@thi.informatik.uni-frankfurt.de
†Research supported in part by a DFG grant SCHN 503/2-1.



ISSN 1433-8092

variables $x_i$ and their negations $\overline{x}_i$. Though this problem is intensively studied for more than fifty years there is no proof of a lower bound nonlinear in the number of variables $m$. The main difficulty here is that we want the function $f$ be *explicitely constructed*—easy counting shows that almost all functions require circuits of size $2^{\Omega(m)}$.

The problem of proving super-linear lower bounds is widely open even if we assume the additional restriction of circuit depth be $O(\log m)$. As shown by Valiant [25] this problem could be solved by proving a $2^{\omega(m/\log\log m)}$ lower bound for depth-3 circuits with unbounded fanin AND and OR gates; such circuits are also called $\Sigma_3$-*circuits*. In the meanwhile we have exponential lower bounds for such circuits [1, 7, 26, 9, 11, 15], but these bounds do not exceed $2^{O(\sqrt{m})}$.

In this paper we use a graph-theoretic approach to make some further steps in this last direction—proving high lower bounds for depth-3 circuits. In particular, we prove that an explicit boolean function $\mathsf{f}_m$ in $2m$ variables cannot be computed as an OR of fewer than $2^{\Omega(m)}$ products of linear forms over $GF(2)$ (Theorem 3.2). That is, we show that $\mathsf{f}_m$ cannot be represented in the form

$$\mathsf{f}_m(x_1,\ldots,x_{2m}) = \bigvee_{i=1}^{s} \bigwedge_{j=1}^{r} \bigoplus_{k\in K_{ij}} x_k \oplus \lambda_{ij}$$

with $\lambda_{ij} \in \{0,1\}$ and $K_{ij} \subseteq \{1,\ldots,2m\}$, unless $s = 2^{\Omega(m)}$. This does not imply super-linear lower bound for log-depth circuits, because we cannot carry out Valiant's reduction with Parity gates on the bottom (next to the inputs) level: here we need OR gates. Still, the result may be interesting because previously known arguments for depth-3 circuits with AND and OR gates [1, 7, 26, 9, 11, 15] do not seem to work for this model at all, and known algebraic arguments for depth-3 circuits with AND and Parity gates [21, 24, 8] seem to be incapable of proving lower bounds higher than $2^{\Omega(\sqrt{m})}$ (see Remark 3.1 below).

Our proof uses a relatively simple graph-theoretic argument, and one of the aims of this paper is to draw once more readers attention to *graph complexity*. This concept has already led to interesting results [3, 23, 20, 22, 17, 14], and its potential seems to be far from being exhausted.

# 2 Graph complexity

All graphs considered here are finite, simple and undirected. A *non-edge* in a graph $G = (V, E)$ is a pair $uv$ of non-adjacent vertices; if the graph is bipartite, then we additionally require that $u$ and $v$ belong to different parts.

A boolean function $g(X)$ *represents* the graph $G$ if it accepts all edges and rejects all non-edges of $G$. That is, $g(X)$ *represents* the graph $G$ if for every input vector $a \in \{0,1\}^X$ with precisely two 1's in, say, positions $u$ and $v$, $f(a) = 1$ precisely when

$u$ and $v$ are adjacent in $G$; on inputs with more or less than two 1's the circuit can output arbitrary values.

For example, the OR $g(X) = \bigvee_{v \in S} x_v$ with $S \subseteq V$ represents the complement of a clique (complete graph) on $\overline{S} = V \setminus S$, whereas the Parity $g(X) = \bigoplus_{v \in S} x_v$ represents the graph $S \times \overline{S} \cup \overline{S} \times S$. In the case of bipartite graphs (when a bipartition of $V$ is fixed) an OR of variables represents a (bipartite) complement of a bipartite complete graph, whereas a Parity represents a union of two vertex disjoint bipartite complete graphs. To give a less trivial example, let us consider the *Kneser graph* $K(r,t)$. This graph has all $t$-element subsets $v$ of $\{1,\ldots,r\}$ as vertices, and two vertices are adjacent if the corresponding $t$-subsets are disjoint. It is easy to see that $K(r,t)$ can be represented by the following depth-2 formula:

$$g(X) = \bigwedge_{i=1}^{r} \bigvee_{v \in S_i} x_v \qquad \text{where} \qquad S_i = \{v \,:\, i \notin v\}.$$

Indeed, $u \neq v$ are non-adjacent in $K(r,t)$ iff $u \cap v \neq \emptyset$ iff $\exists i \in u \cap v$ iff $\{u,v\} \cap S_i = \emptyset$ for some $i$ iff $uv$ is rejected by some OR $\bigvee_{v \in S_i} x_v$. Note that with respect to the total number $n = \binom{r}{t}$ of vertices the representation is quite compact: the formula has only $1 + r = O(tn^{1/t})$ gates.

The idea of the graph-theoretic approach is that a lower bound on the size of circuits representing a given bipartite $n \times n$ graph $G \subseteq U \times V$ with $n = 2^m$ can be translated to a lower bound on the size of circuits computing the *characteristic function* $f_G$ of $G$: this is a boolean function in $2m$ variables such that $f_G(u,v) = 1$ if and only if $(u,v) \in G$ (here and throughout we assume that the vertices are encoded by binary strings of length $m$). The translation is based on a simple but quite interesting observation made by Pudlák, Rödl and Savický in [20]. In a slightly different setting this observation—which we call the *Magnification Lemma*—can be stated as follows (for completeness, we include its proof in Appendix):

**Magnification Lemma.** *Given a circuit computing the characteristic function $f_G$ of a bipartite graph $G$, it is possible to replace its input literals by ORs of variables so that the obtained positive circuit (no negated inputs) represents the graph $G$. The same holds when Parity gates are used instead of OR gates.*

This fact may be particularly useful in such circuit models where computing an OR (or a Parity) of input literals is "cheap." For example, if the circuit $\Phi$ computing $f_G$ has unbounded fanin OR (or Parity) gates on the bottom (next to the inputs) level, then the obtained circuit $\Phi_+$ represents $G$ and has the same number of gates! Hence, if we could prove that $G$ cannot be represented using, say, fewer than $n^\epsilon$ gates, this would immediately imply that the function $f_G$ requires at least $n^\epsilon = 2^{\epsilon m}$ gates, which is *exponential* in the number $2m$ of variables of $f_G$ (this is where the term "magnification" comes from). That is, even moderate lower bounds on the combinational complexity of graphs would yield high lower bounds on the combinational complexity

of boolean functions. Thus, proving lower bounds for graphs is even harder than for boolean functions. However, studying the graph-theoretic structure of boolean functions may provide new insights into their complexity—unlike for boolean functions, the structure of graphs is much better understood.

Such a graph-theoretic frame of proving lower bounds on the circuit size of boolean functions was first investigated by Pudlák, Rödl and Savický [20], and by Razborov [23]. Their results discovered an interesting (and somewhat unexpected) fact that there is a big discrepancy between the combinatorial and combinational complexity of graphs: some "combinatorially complicated" graphs, like graphs with good Ramsey properties (no large cliques or independent sets), *can* be represented by very small boolean circuits of depth-3 with unbounded fanin AND and Parity gates. On the other hand, using the graph-theoretic frame, Razborov [22], and Pudlák and Rödl [17, 18] have found interesting measures of graphs—their affine and projective dimensions—forcing large formula size and branching program size of their characteristic functions.

In this paper we consider the combinational complexity of graphs in the model of depth-3 circuits and in the model of boolean formulas.

# 3 $\Sigma_3$ circuits

A $\Sigma_3$ *circuit* consist of unbounded fanin OR and AND gates arranged in three levels: an OR gate on the top, AND gates on the middle level, and OR gates on the bottom (next to inputs) level. Inputs are variables and their negations; if there are no negated inputs, the circuit is *monotone*. Hence, such a circuit has the form:

$$\Phi(x_1,\ldots,x_m)=\bigvee_{i=1}^{s}\bigwedge_{j=1}^{r}\bigvee_{k\in K_{ij}} z_k$$

where $z_k \in \{x_k, \overline{x}_k\}$ and $K_{ij} \subseteq \{1,\ldots,m\}$; $s$ is the *top fanin*, $r$ the *middle fanin* and $\max_{i,j}|K_{ij}|$ the *bottom fanin*; by the *size* of a circuit we will mean the maximum $\max\{s,r\}$ of its top and middle fanins.

Our main motivation to study such circuits comes from the result of Valiant [25]: if a boolean function $f_m$ in $m$ variables can be computed by a circuit of depth $O(\log m)$ using only $O(m)$ constant-fanin gates, then $f_m$ can be computed by a $\Sigma_3$ circuit of top fanin $s \leq 2^{O(m/\log\log m)}$ and middle fanin $r \leq 2^{m^\epsilon}$ for arbitrarily small constant $\epsilon > 0$. Thus, strongly exponential lower bounds on the size of $\Sigma_3$ circuits would imply nonlinear lower bounds on the size of logarithmic-depth combinational circuit, thus solving a well known and more than twenty-five years old problem in computational complexity. It is, therefore, not surprising that proving strongly exponential lower bounds on $\Sigma_3$ circuits is a rather difficult task. Although there was a considerable progress in this direction ([1, 7, 26, 9, 11, 15]), the obtained lower bounds do not exceed $2^{O(\sqrt{m})}$. The only known strongly exponential lower bounds were obtained in [16] under the restriction that the bottom OR gates have fanin 2, that is, when the

circuit is just an OR of 2-CNFs. However, Valiant's reduction requires bottom fanin $m^\epsilon$ and, as noted in [16], their argument fails already when bottom fanin is 4.

Our first result concerns $\Sigma_3$ circuits under a different restriction: instead of bounding the fanin of the bottom gates we require these gates be Parity gates; we call these circuits $\Sigma_3^\oplus$ *circuits*. Such a circuit computes an OR of products of linear forms over $GF(2)$:

$$\Phi(x_1,\ldots,x_m) = \bigvee_{i=1}^{s} \bigwedge_{j=1}^{r} \bigoplus_{k\in K_{ij}} x_k \oplus \lambda_{ij}$$

where $\lambda_{ij} \in \{0,1\}$ and $K_{ij} \subseteq \{1,\ldots,m\}$; $s$ is the top fanin of the circuit.

**Remark 3.1.** If we would require that the top gate of a circuit must also be a Parity gate (not an OR gate), then truly exponential lower bounds $2^{\Omega(m)}$ for such circuits could be obtained using the algebraic (approximation by low-degree polynomials) techniques of [21, 24, 8]. However, these techniques seem incapable of proving such high lower bounds for $\Sigma_3^\oplus$ circuits because, in this case, we would be forced to approximate the top OR gate as well, which would invariably result in the square root $2^{\Omega(\sqrt{m})}$ in the final bound. [1]

We use a graph-theoretic argument to prove a *strongly* exponential lower bound on the top fanin of $\Sigma_3^\oplus$ circuits computing the boolean function $\mathsf{f}_m$ in $2m$ variables, which is defined as follows. We take the desarguesian projective plane $PG(2,q)$ where $q$ is a prime or a prime power; this plane has $n = q^2+q+1$ points and $n = q^2+q+1$ lines. We then fix an (arbitrary) encoding of points and lines of $PG(2,q)$ by binary strings of length $m = \lceil \log(n+1) \rceil$. The function $\mathsf{f}_m$ is then defined by: $\mathsf{f}_m(a,b) = 1$ if and only if the point encoded by $a$ lies on the line encoded by $b$. According to the well-known construction of $PG(2,q)$ (which can be found in any textbook on finite geometries), $\mathsf{f}_m$ is just the boolean version of the function $f : GF(q)^6 \to \{0,1\}$ defined by:

$$f(x,y,z,a,b,c) = 1 \quad \Longleftrightarrow \quad ax+by+cz = 0 \pmod q.$$

**Theorem 3.2.** *Any $\Sigma_3^\oplus$ circuit computing $\mathsf{f}_m$ has top fanin $\Omega(2^{m/2})$.*

The function $\mathsf{f}_m$ is the characteristic function of the incidence graph $\mathsf{PG}_{n,q}$ of $PG(2,q)$. The graph $\mathsf{PG}_{n,q}$ has $n = q^2+q+1$ vertices on each part. The vertices on the left part correspond to points and the vertices on the right part correspond to lines of $PG(2,q)$, and $(i,j)$ is an edge if and only if the $i$-th point lies on the $j$-th line. The graph is $(q+1)$-regular and contains no 4-cycles (because any two lines intersect in precisely one point, and every two points lie on a unique line).

Since the graph $\mathsf{PG}_{n,q}$ has $M = n(q+1) = \Omega(n^{3/2})$ edges and contains no 4-cycles, Theorem 3.2 follows directly from the Magnification Lemma and the following general lower bound.

[1] **Note added in proof:** Using different arguments, Pudlák and Rödl [19] have recently proved a lower bound of the form $2^{m/2}/(m-2)$ for $\Sigma_3^\oplus$ circuits with a threshold gate on the top. Their function $f_m$ is more complicated and is constructed using the properties of pseudorandom sets.

**Theorem 3.3.** *Let $G \subseteq U \times V$ be a bipartite $n \times n$ graph without 4-cycles. Then any $\Sigma_3^{\oplus}$ circuit representing $G$ has top fanin at least $|G|/(2n)$.*

*Proof.* A *fat matching* is a union of vertex-disjoint bipartite cliques. Let $\mathrm{fat}(G)$ denote the smallest number of fat matchings whose union coincides with $G$. This measure was already considered by several authors, [4, 6, 2] among others (here fat matchings are called "equivalence graphs"). An upper bound $\mathrm{fat}(G) = O(n/\log n)$ is proved in [18].

**Claim 3.4.** *For every bipartite graph $G$, $\mathrm{fat}(G)$ is the smallest top fanin of a $\Sigma_3^{\oplus}$ circuit representing $G$.*

*Proof.* A *double-clique* in $U \times V$ is a union of two bipartite cliques $A \times B$ and $\overline{A} \times \overline{B}$ where $A \subseteq U$, $B \subseteq V$, $\overline{A} = U \setminus A$ and $\overline{B} = V \setminus B$.

Let $\Phi$ be a $\Sigma_3^{\oplus}$ circuit of top fanin $s$ representing a bipartite graph $G \subseteq U \times V$. Let $g = \bigoplus_{v \in T} x_v \oplus \lambda$ with $\lambda \in \{0,1\}$ be a gate on the bottom level of $\Phi$. Set $A = U \cap T$ and $B = V \cap T$. Then $g$ represents a double-clique $(A \times \overline{B}) \cup (\overline{A} \times B)$, if $\lambda = 0$, or a double-clique $(A \times B) \cup (\overline{A} \times \overline{B})$, if $\lambda = 1$. Since the intersection of any number of double-cliques (as well as fat matchings) is a fat matching, each AND gate on the middle level represents a fat matching. Hence, the OR gate on the top represents a union of these $s$ fat matchings, implying that $s \geq \mathrm{fat}(G)$.

To show that $G$ can be represented by a $\Sigma_3^{\oplus}$ circuit of top fanin $\mathrm{fat}(G)$, assume that $G$ is a union of $s$ fat matchings $M = A_1 \times B_1 \cup \cdots \cup A_r \times B_r$. Observe that every such fat matching $M$ can be obtained as an intersection of $r$ double-cliques $A_i \times B_i \cup (A \setminus A_i) \times (B \setminus B_i)$ in $A \times B$ where $A$ ($B$) is the union of all $A_j$'s ($B_j$'s). Since each double-clique $A \times B \cup \overline{A} \times \overline{B}$ can be represented by the Parity gate $g(X) = \bigoplus_{v \in A \cup \overline{B}} x_v$, we are done. □

**Claim 3.5.** *Let $G$ be an $n \times n$ bipartite graph. If $G$ has no 4-cycles, then $\mathrm{fat}(G) \geq |G|/(2n)$.*

*Proof.* Let $G$ be a bipartite graph without 4-cycles, $H = \bigcup_{i=1}^{t} A_i \times B_i$ be a fat matching, and suppose that $H \subseteq G$. By the definition of a fat matching, the sets $A_1, \ldots, A_t$, as well as the sets $B_1, \ldots, B_t$ are mutually disjoint. Moreover, since $H$ has no 4-cycles, we have that in every clique $A_i \times B_i$ at least one of its sides $A_i$ or $B_i$ must have cardinality 1. Hence, if we set $I = \{i : |A_i| = 1\}$, then

$$|H| = \sum_{i=1}^{t} |A_i \times B_i| = \sum_{i=1}^{t} |A_i| \cdot |B_i| = \sum_{i \in I} |B_i| + \sum_{i \notin I} |A_i| \leq 2n.$$

Thus, no fat matching $H \subseteq G$ can cover more than $2n$ edges of $G$, implying that we need at least $|G|/(2n)$ fat matchings to cover all edges of $G$.

This completes the proof of Claim 3.5, and thus, the proof of Theorem 3.3. □

When applied to $\Sigma_3$ circuits, the argument used in the proof of Theorem 3.2 yields the following trade-off between top and middle fanins.

**Theorem 3.6.** *Let $\Phi$ be a $\Sigma_3$ circuit with top fanin $s$ and middle fanin $r$. If $\Phi$ computes $\mathsf{f}_m$, then $r + \log s = \Omega(m)$. If $\Phi$ computes $\neg\mathsf{f}_m$, then $s \log r = \Omega(m)$.*

A trade-off $sr = \Omega\left(m^3/(\log m)^5\right)$ between these parameters was recently proved by Lokam [14] (for boolean functions arising from Hadamard matrices). The trade-off in Theorem 3.6 is better only if one of the parameters $r$ or $s$ is at most $m^\epsilon$: then the second parameter must be at least $2^{m^{1-\epsilon}}$.

Theorem 3.6 follows directly from Claim 3.5 and the following claim. A *bipartite complement* of a bipartite graph $G \subseteq U \times V$ is the graph $\overline{G} = (U \times V) \setminus A \times B$. The *clique covering number* of a bipartite graph $G$, denoted by $\mathrm{cc}(G)$, is the minimum number of complete bipartite subgraphs of $G$ covering all edges of $G$. The non-bipartite version of this measure was first studied in [5], and now is the subject of extensive literature.

**Claim 3.7.** *If a bipartite graph $G$ can be represented by a monotone $\Sigma_3$ circuit of middle fanin at most $r$ and top fanin $s$, then $\mathrm{fat}(G) \le s2^r$ and $\mathrm{cc}\left(\overline{G}\right) \le r^s$.*

*Proof.* Let $\Phi$ be a monotone $\Sigma_3$ circuit of middle fanin at most $r$ and top fanin $s$ representing a bipartite graph $G \subseteq U \times V$. Each gate $g = \bigvee_{j \in T} x_j$ on the bottom level represents a bipartite complement of a bipartite clique $A \times B$, where $A = U \setminus T$ and $B = V \setminus T$. Each such complement is a union of two fat matchings $\overline{A} \times \overline{B}$ and $\overline{A} \times B \cup A \times \overline{B}$. Hence, each AND gate on the middle level represents a union of at most $2^r$ fat matchings. Since $G$ is a union of $s$ such graphs, we have $\mathrm{fat}(G) \le s2^r$.

To prove $\mathrm{cc}\left(\overline{G}\right) \le r^s$, observe that $\overline{G}$ is an intersection of $s$ graphs $H_1, \ldots, H_s$, each of which is a union of $r$ bipartite cliques. Since the intersection of any number of bipartite cliques is a bipartite clique, we have that $\mathrm{cc}\left(\overline{G}\right) \le \prod_{i=1}^{s} \mathrm{cc}\left(H_i\right) \le r^s$. $\square$

Note that in the context of boolean functions, $\Sigma_3^\oplus$ circuits *cannot* be efficiently simulated by $\Sigma_3$ circuits: the Parity function $x_1 \oplus x_2 \oplus \cdots \oplus x_m$ has an obvious $\Sigma_3^\oplus$ circuit of size 1, whereas (as shown in [9]) this function requires $\Sigma_3$ circuits of size $2^{\Omega(\sqrt{m})}$. It may be, therefore, interesting that, in the context of graphs, $\Sigma_3^\oplus$ circuits *can* be simulated by monotone $\Sigma_3$ circuits of almost the same size.

**Proposition 3.8.** *If a bipartite graph $G$ can be represented by a $\Sigma_3^\oplus$ circuit of top fanin $s$ and middle fanin $r$, then $G$ can be represented by a monotone $\Sigma_3$ circuit of top fanin $s$ and middle fanin $2r$*

*Proof.* Every double-clique $(A \times B) \cup (\overline{A} \times \overline{B})$ represented by a parity gate on the bottom level is the intersection of bipartite complements of two graphs $\overline{A} \times B$ and $A \times \overline{B}$, and each such intersection is represented by

$$g = \left( \bigvee_{u \in A \cup \overline{B}} x_u \right) \wedge \left( \bigvee_{v \in \overline{A} \cup B} x_v \right).$$

□

We conclude this section with a combinatorial characterization of graphs represented by small monotone $\Sigma_3$ circuits.

**Definition 3.9.** For a graph $G$ let $\mu(G)$ be the smallest number $t$ for which there exist at most $t$ graphs $H_1, \ldots, H_t$ such that $G = H_1 \cup \ldots \cup H_t$ and $\mathrm{cc}\left(\overline{H_i}\right) \leq t$ for all $i = 1, \ldots, t$. Hence, $\mu(G)$ is the smallest number $t$ such that the complement $\overline{G}$ of $G$ can be represented as an intersection of at most $t$ graphs with clique covering number at most $t$.

In same situations, especially when trying to give an *upper* bound on $\mu(G)$, the following equivalent reformulation may be more convenient: $\mu(G)$ is the minimum number $t$ for which it is possible to associate with every vertex a 0-1 matrix of dimension $t \times t$ so that $(u, v)$ is an edge precisely when, for some $i$ $(1 \leq i \leq t)$, the $i$-th rows of the corresponding matrices are orthogonal (i.e. their scalar product over reals is zero).

**Proposition 3.10.** *A graph $G$ can be represented by a monotone $\Sigma_3$ circuit of size $t$ if and only if $\mu(G) \leq t$.*

*Proof.* As already noted in the introduction, an OR of variables represents a complement of a clique. Hence, each gate in the middle level of a monotone $\Sigma_3$ circuit represents an intersection $H$ of such complements. But then $\overline{H}$ is a union of the corresponding cliques, implying that $\mathrm{cc}\left(\overline{H}\right)$ is at most the middle fanin of the circuit. Since the top OR gate is just a union of graphs, represented at the middle level, we are done. □

**Remark 3.11.** Alon [2] has proved that $\mathrm{cc}\left(\overline{H}\right) = O(d^2 \log n)$ for every $n$-vertex graph of maximal degree $d$. This, in particular, gives an upper bound $\mu(G) = O(D^{2/3} \log n)$ for all $n$-vertex graphs of maximal degree $D$: simply break $G$ into $D^{2/3}$ subgraphs of maximal degree $D^{1/3}$ each. In particular, $\mu(G) = O(n^{2/3} \log n)$ for every graph $G$ with $n$ vertices.

Together with Proposition 3.10, Alon's result implies the following

**Corollary 3.12.** *Every $n$-vertex graph of maximum degree $D$ can be represented by a monotone $\Sigma_3$ circuit of size $O(D^{2/3} \log n)$.*

# 4 $\Sigma_3$ versus $\Pi_3$ circuits

So far, no explicit graphs requiring large monotone $\Sigma_3$ circuits are known. But what about monotone $\Pi_3$ circuits? These circuits have the form

$$\Phi(X) = \bigwedge_{i=1}^{s} \bigvee_{j=1}^{r} \bigwedge_{v \in S_{ij}} x_v.$$

It is worth to mention that, in the context of boolean functions, proving lower bounds for $\Sigma_3$ circuits is the same as proving lower bounds for the dual model of $\Pi_3$ circuits: if a function is hard in the former model then its negation is hard in the later. However, the following theorem shows that in the context of graphs the situation is quite different: if a graph is hard for (monotone) $\Pi_3$ circuits, then we cannot conclude that its complement must be also hard for (monotone) $\Sigma_3$ circuits.

**Theorem 4.1.** *Let $M_n$ be an $n$ to $n$ matching. Then both the graph $M_n$ and its complement $\overline{M}_n$ can be represented by monotone $\Sigma_3$ circuits of size $O(\log n)$, but every monotone $\Pi_3$ circuit representing $\overline{M}_n$ must have size at least $\Omega(\sqrt{n})$.*

A larger lower bound on the size of monotone $\Pi_3$ circuits can be obtained for Hadamard graphs. A Hadamard matrix of oder $n$ is an $n \times n$ matrix with entries $\pm 1$ and with row vectors mutually orthogonal. A graph associated with a Hadamard matrix $M$ (or just a Hadamard graph) of oder $n$ is a bipartite $n \times n$ graph where two vertices $u$ and $v$ are adjacent if and only if $M(u,v) = +1$.

**Theorem 4.2.** *Every monotone $\Pi_3$ circuit representing a Hadamard graph of oder $n$ must have size at least $\Omega(n^{2/3})$.*

We derive both theorems from the following property of graphs represented by monotone $\Pi_3$ circuits.

**Lemma 4.3.** *Suppose that a graph $G$ can be represented by a monotone $\Pi_3$ circuit of size $t$. Then it is possible to add to $\overline{G}$ a set $H$ of $|H| \leq t^2$ edges so that $\mathrm{cc}\left(\overline{G} \cup H\right) \leq t$.*

*Proof.* Let $\Phi$ be a monotone $\Pi_3$ circuit of size $t$ representing a bipartite graph $G \subseteq U \times V$. Our goal is to show that then there is a graph $H$ with $|H| \leq t^2$ edges such that $\mathrm{cc}\left(\overline{G} \cup H\right) \leq t$. The circuit $\Phi$ is an AND of at most $t$ monotone DNFs

$$D_i = \bigvee_{j=1}^{t} \bigwedge_{v \in T_{ij}} x_v \qquad i = 1, \ldots, t$$

each containing (at most) $t$ monomials (ANDs of variables). Since we are interested in the behavior of the circuit only on arcs (edges and non-edges), we may assume that none of these monomials contains more than two variables, i.e. $|T_{ij}| \leq 2$ for all $i, j$. Each DNF $D_i$ accepts some set $S_i \subseteq U \cup V$ of vertices, some subset $H_i \subseteq G$ of edges, and (apparently) some set of non-edges. Let $H = \bigcup_{i=1}^{t} H_i$ and call the edges in $H$ *marked*. Since each of the DNFs $D_1, \ldots, D_t$ has at most $t$ monomials of length 2, the number $|H|$ of marked edges does not exceed $t^2$. Let $E := G \setminus H$ be the set of remaining (non-marked) edges. We may assume that $E \neq \emptyset$, since otherwise we would have $H = G$, meaning that $\overline{G} \cup H$ is just a complete graph.

Let us remove from the DNFs $D_1, \ldots, D_t$ all monomials of length 2 corresponding to marked edges. Every non-marked edge must be accepted by *all* resulting DNFs

$D'_1, \ldots, D'_t$. Hence, it cannot be that some $D'_i$ contains only length-2 monomials, because these monomials can accept only non-edges (length-2 monomials accepting edges are removed), implying that the DNF $D'_i$ (and hence, the whole circuit $\Phi$) would accept none of the edges from $E$. This means that $S_i \neq \emptyset$ for all $i = 1, \ldots, t$. Thus, the CNF

$$\Psi = \left( \bigvee_{u \in S_1} x_u \right) \wedge \left( \bigvee_{u \in S_2} x_u \right) \wedge \cdots \wedge \left( \bigvee_{u \in S_t} x_u \right)$$

must accept all edges from $E$ and do not accept any of the non-edges of $G$ (since otherwise such a non-edge would be also accepted by the original circuit $\Phi$). That is, every edge from $E$ must intersect all of the sets $S_1, \ldots, S_t$, and every non-edge of $G$ must avoid at least one of these sets. Hence, if we consider the cliques $R_i = A_i \times B_i$ with $A_i = U \setminus S_i$ and $B_i = V \setminus S_i$, then: (i) $E \cap R_i = \emptyset$ for all $i = 1, \ldots, t$, and (ii) $\overline{G} \subseteq R_1 \cup \cdots \cup R_t$. In other words, the cliques $R_1, \ldots, R_t$ cover all edges of $\overline{G}$, and do not cover any of the non-edges of $\overline{G}$ lying in $E = G \setminus H$. Hence, up to at most $|H| \leq t^2$ errors, the clique cover number of $\overline{G}$ does not exceed $t$, as claimed. □

*Proof of Theorem 4.1.* Let $M_n$ be an $n$ to $n$ matching, and $\overline{M}_n$ its complement. Our first goal is to show that both $M_n$ and $\overline{M}_n$ can be represented by monotone $\Sigma_3$ circuits of size $O(\log n)$. This follows from Proposition 3.10 and the following two observations. First, $\mu(M_n) = O(\log n)$ because we can associate with each vertex on the left part its *own* binary code and assign to the unique matched vertex on the right side the complement of this code. Second, $\mu(\overline{M}_n) = O(\log n)$ because we can associate with each pair of matched (in $M_n$) vertices their *own* $s \times 2$ matrix with $s = O(\log n)$ rows and precisely one 1 in each row.

Let now $t$ be the minimum size of a monotone $\Pi_3$ circuit representing $\overline{M}_n$. Then, by Lemma 4.3, it must be possible to add a set $H$ of $|H| \leq t^2$ edges to the matching $M_n$ so that the resulting graph $M_n \cup H$ can be covered by at most $t$ cliques. At least one of these cliques, say $R = A \times B$, must contain at least $|M_n|/t = n/t$ edges of the matching $M_n$. But this means that $|H \cap (A \times B)| \geq (n/t)^2 - (n/t)$. Together with $|H| \leq t^2$ this implies that $t$ must satisfy the inequality $(n/t)^2 - (n/t) \leq t^2$, that is, $t^4 \geq n^2 - tn$, which implies $t = \Omega(\sqrt{n})$. □

*Proof of Theorem 4.2.* Let $\Phi$ be a monotone $\Pi_3$ circuit of size $t$ representing a bipartite $n \times n$ Hadamard graph $H \subseteq U \times V$. We may assume that $t \leq n/16$, for otherwise there is nothing to prove. We will use the known fact that any Hadamard graph contains about the same number of edges and non-edges; in particular, both $|H|, |\overline{H}| \geq n^2/4$.

By Lemma 4.3, there is a set $E$ of $|E| \leq t^2$ arcs such that the graph $\overline{H} \cup E$ can be covered by at most $t$ cliques $R_1, \ldots, R_t$, that is, (i) $H \cap R_i \subseteq E$ for all $i = 1, \ldots, t$, and (ii) $\overline{H} \subseteq R_1 \cup \cdots \cup R_t$.

Let $N = |\overline{H}|$ be the total number of non-edges in $H$ (hence, $N \geq n^2/4$) and take a clique $R \in \{R_1, \ldots, R_t\}$ containing the largest number of non-edges. By (ii),

$N_0 := |R \cap \overline{H}| \geq N/t$. Let $N_1 := |R \cap H|$ be the number of edges of $H$ lying in $R$. Since, by (i), $R$ can contain only edges from $E$, we have that $N_1 \leq |E| \leq t^2$. On the other hand, by Lindsey's Lemma (see, e.g. [12, Sect. 15.1.3]), $|N_1 - N_0| \leq \sqrt{|R| \cdot n}$, implying that

$$N_1 \geq N_0 - \sqrt{|R| \cdot n}.$$

Remembering that

$$N_1 + N_0 = |R| \geq \frac{N}{t} \geq \frac{n^2}{4t} \geq 4n,$$

we obtain

$$2N_1 \geq |R| - \sqrt{|R| \cdot n} = |R|\left(1 - \sqrt{\frac{n}{|R|}}\right) \geq \frac{N}{2t},$$

that is, $N_1 \geq N/(4t)$. Together with $N_1 \leq t^2$, this implies that $t^3 \geq N/4$. Thus, $t$ must be at least $(N/4)^{1/3} \geq (n^2/16)^{1/3} = \Omega(n^{2/3})$. □

# 5 Boolean formulas

Our last result concerns boolean formulas of *arbitrary* depth with AND and OR gates. As in the case of general circuits, inputs here are literals (variables and their negations). The only restriction is that the fanout of each gate is 1. The *size* of a formula is the number of input literals. Given a boolean function $f$ and a graph $G$, let $L(f)$ be the minimum size of a formula computing $f$, and $L_+(G)$ the minimum size of a monotone formula representing $G$.

If $\Phi$ is a formula computing the characteristic function $f_G$ (in $2m$ variables) of a bipartite $n \times n$ graph $G$ (with $n = 2^m$) then, by the Magnification Lemma, we can replace each input literal in $\Phi$ by a monotone formula of size at most $2n$ (computing the corresponding OR of variables) so that the resulting monotone formula $\Phi_+$ recognizes $G$. Thus,

$$L(f_G) \geq L_+(G)/(2n).$$

Easy counting shows that $L_+(G) = \Omega(n^2/\log n)$ for most $n \times n$ graphs $G$. But, so far, no *explicit* graph even with $L_+(G) = \Omega(n \log^3 n)$ is known. Such a graph would improve the strongest currently known lower bound $\Omega(m^{3-o(1)})$ on the (non-monotone) formula size of an explicit boolean function in $m$ variables [10].

The reason, why it is difficult to show that a given graph cannot be represented by a small (monotone!) formula, is that we only know that the formula must behave correctly on the 2-*element* subsets of vertices: it must reject such a subset precisely when it is a non-edge of (= independent set of size 2 in) $G$. On larger sets the formula may output arbitrary values. In particular, it can accept independent sets of size $k \geq 3$.

In this section we look what happens if we require that the formula must reject all independent sets up to some size $k \geq 2$. Namely, say that a boolean function

*k-represents* the graph $G$ if it accepts all edges of $G$ and rejects all independent sets $S$ in $G$ of size $2 \leq |S| \leq k$. (Hence, a function represents $G$ in a sense considered above precisely when it 2-represents $G$.) If the graph $G = (V, E)$ has $n$ vertices then it can be $n$-represented by a trivial monotone formula

$$\Phi(X) = \bigvee_{uv \in E} x_u x_v$$

of size $2|E|$. This formula accepts all edges and rejects *all* independent sets in $G$. Can we essentially decrease the formula size by requiring that it must reject only independent sets up to some size $k < n$? Using a rank-argument it can be shown that, for some graphs, this is *not* possible unless $k$ is smaller than two times the maximum degree of $G$.

**Theorem 5.1.** *Let $G = (V, E)$ be a graph with maximum degree $d \geq 2$. If $G$ has no triangles and no 4-cycles, then any monotone formula $(2d-2)$-representing $G$ must have size at least $|E|/2$.*

*Proof.* Let $k = 2d - 2$ and let $\Phi$ be a monotone formula $k$-representing the graph $G$. That is, the formula must accept all edges of $G$ and reject all independent sets of size up to $k$. For a vertex $u \in V$, let $S_u$ be the set of its neighbors. For an edge $e \in E$, let $S_e$ be the set of all its *proper* neighbors; that is, $v \in S_e$ precisely when $v \notin e$ and $v$ is adjacent with an endpoint of $e$. Each set $S_y$ with $y \in V \cup E$ has size at most $2d - 2$. Moreover, since $G$ has no triangles and no 4-cycles, the sets $S_y$ are independent and the formula $\Phi$ must reject them; we will concentrate only on these independent sets.

Let $M = E \times (E \cup V)$ be an empty matrix whose rows are labeled by edges whereas columns are labeled by edges and by vertices of $G$. A *rectangle* in $M$ is a submatrix $A \times B \subseteq M$ with the property that there is a vertex $v$ such that

$$v \in x - S_y \text{ for all } x \in A \text{ and } y \in B;$$

we call $v$ a common element of the rectangle (we consider vertices as one element and edges as two element sets). It is well known and can be easily shown by induction on the size of $\Phi$ (see, e.g. [13, 22] or [12, Sect. 15.2.2]) that the size of the formula $\Phi$ must be at least the minimum number of mutually disjoint rectangles covering the whole matrix $M$. So, let $\mathcal{R}$ be such a covering. Fill the entries of $M$ with constants 0 and 1 by the following rule:

$$M_{x,y} = 1 \text{ if and only if } x \cap y \neq \emptyset \tag{1}$$

Let $R = A \times B$ be a rectangle in $\mathcal{R}$, and let $v$ be its common element. Then $v \in x$ for all edges $x \in A$. Hence, for each $y \in B$, the corresponding column in $R$ is either the all-1 column (if $v \in y$) or the all-0 column (if $v \notin y$) because in this last case the second endpoint of $x$ cannot belong to $y$ (for otherwise, the first endpoint $v$ would

belong to $S_y$). Thus, either the rectangle $R$ is monochromatic or we can split it into two monochromatic rectangles. This way we obtain a covering $\mathcal{R}'$ of $M$ by at most $2|\mathcal{R}|$ mutually disjoint monochromatic rectangles. To estimate their number we use the rank argument. Let $\mathrm{rk}(M)$ stand for the row-rank of $M$ over $GF(2)$. Since the rectangles in $\mathcal{R}'$ are mutually disjoint and have rank 1, it follows that $|\mathcal{R}'| \geq \mathrm{rk}(M)$. Hence, it remains to prove that $M$ has full row-rank over $GF(2)$.

Take an arbitrary subset $\emptyset \neq F \subseteq E$ of edges. We have to show that the rows of the submatrix $M_F$ of $M$ corresponding to the edges in $F$ cannot sum up to the all-0 row over $GF(2)$. If $F$ is not an even factor, that is, if the number of edges in $F$ containing some vertex $v$ is odd, then the column of $v$ in $M_F$ has an odd number of 1's, and we are done. Hence, we may assume that $F$ *is* an even factor. Take an arbitrary edge $e = uv \in F$, and let $H \subseteq F$ be the set of edges in $F$ incident to at least one endpoint of $e$. Since both vertices $u$ and $v$ have even degree (in $F$), the edge $e$ has a nonempty intersection with an *odd* number of edges in $F$: one intersection with itself and an even number of intersections with the edges in $H \setminus \{e\}$. Hence, the colum of $e$ in $M_F$ contains an odd number of 1's, as desired.

Thus, $size(\Phi) \geq |\mathcal{R}| \geq |\mathcal{R}'|/2 \geq \mathrm{rk}(M)/2 \geq |E|/2$. □

**Remark 5.2.** Note that if we would only know that the formula 2-represents the graph $G$ (the case interesting in the context of boolean functions), then the same rank argument with the matrix $M$ defined by the rule (1) would not work. In this case we would have that $M_{x,y} = 1$ if and only if $|x \cap y| = 1$ (edge and non-edge can share at most one vertex). That is, $M$ would be just a matrix of scalar products (over the reals) of the characteristic vectors of edges $x$ and non-edges $y$, and (even over the reals) the rank of $M$ would not exceed $n$.

# 6 Conclusion and open problem

We have proved that some explicit graphs cannot be recognized by $\Sigma_3^{\oplus}$ circuits of small top fanin (Theorem 3.2). This gives the first truly exponential lower bound on the size of $\Sigma_3^{\oplus}$ circuits computing an explicit boolean function. Using the same argument we have proved an exponential tradeoff between the top and middle fanins in $\Sigma_3$ circuits (Theorem 3.6). We have also observed (Corollary 3.12) that the upper bound on the clique covering number, given by Alon in [2], implies that any $n$-vertex graph can be represented by a monotone $\Sigma_3$ circuit of size $O(n^{2/3}\log n)$, which is much better than the trivial upper bound $n$. Then, in Theorem 4.1, we have established an exponential trade-off between the size of monotone $\Pi_3$ and $\Sigma_3$ circuits: there are explicit graphs $G$ on $n$ vertices such that *both* the graph $G$ and its complement $\overline{G}$ have monotone $\Sigma_3$ circuits of size $O(\log n)$, but every monotone $\Pi_3$ circuit for $G$ must have size at least $\Omega(\sqrt{n})$. This contrasts with the case of boolean functions, where no such (exponential) trade-off is possible because any $\Sigma_3$ circuit for a boolean function $f$ is at the same time a $\Pi_3$ circuit for its complement $\neg f$. Finally, we have also

shown that the main difficulty in proving that a given graph requires large monotone formulas is that the formula is required to reject only independent sets of size 2 (i.e. non-edges): if the formula is required to reject larger independent sets, then lower bounds are relatively easy to prove (Theorem 5.1).

In the context of this paper the most interesting problem remains to prove that $\mu(G)$ is large for some *explicit* $n$-vertex graphs $G$:

**Problem 6.1.** Exhibit a bipartite $n \times n$ graph $G \subseteq U \times V$ which cannot be represented as an intersection of a small number of graphs, whose clique covering number is small. That is, find a graph which cannot be represented in the form

$$G = \bigcap_{i=1}^{t} \bigcup_{j=1}^{t} A_{ij} \times B_{ij} \quad \text{or in the form} \quad G = \bigcup_{i=1}^{t} \bigcap_{j=1}^{t} \overline{A_{ij} \times B_{ij}}$$

unless $t$ is large.

Graphs $G$ with $t = \Omega(\log n)$ are easy to find: such is, for example, the $n$ to $n$ matching. On the other hand, easy counting shows that $t = \Omega(\sqrt{n})$ for almost all $n$-vertex graphs $G$. However, to obtain some important consequences in computational complexity, we need a lower bound of the form $t \geq n^{\epsilon}$ for *explicit* graphs $G$. If proved with $\epsilon = \omega(1/\sqrt{\log n})$, this would give the first explicit boolean function in $m$ variables requiring (non-monotone) $\Sigma_3$ circuit of size $2^{\omega(\sqrt{m})}$. If proved with $\epsilon = \omega(1/\log\log n)$, this would give a nonlinear lower bound for log-depth circuits, thus solving an old problem in computational complexity.

## Acknowledgments

I would like to thank Noga Alon for interesting conversations concerning the measure $\mu(G)$ of graphs (Remark 3.11), and Alexander Razborov for useful remarks concerning the impossibility to obtain truly exponential lower bounds for $\Sigma_3^{\oplus}$ circuits using previously known techniques for depth-3 circuits (Remark 3.1).

# References

[1] Ajtai, M. (1983): $\Sigma_1^1$-formulae on finite structures, *Ann. Pure and Appl. Logic* **24**, 1–48.

[2] Alon, N. (1986): Covering graphs by the minimum number of equivalence relations, *Combinatorica* **6**, 201–206.

[3] Bublitz, S. (1986): Decomposition of graphs and monotone size of homogeneous functions, *Acta Informatica* **23**, 689–696.

[4] Duchet, P. (1979): *Représentations, noyaux en théorie des graphes et hypergraphes.* Thése de doctoral d'Etat, Université Paris VI.

[5] Erdős, P., Goodman, A. W. and Pósa, L. (1966): The representation of a graph by set intersections, *Can. J. Math.* **18**, 106–112.

[6] Frankl, P. (1982): Covering graphs by equivalence relations, *Annals of Discrete Math.* **12**, 125–127.

[7] Furst, M., Saxe, J. and Sipser, M. (1984): Parity, circuits and the polynomial time hierarchy, *Math. Systems Theory* **17**, 13–27.

[8] Grigoriev, D. and Razborov, A. (2000): Exponential lower bounds for depth 3 arithmetic circuits in algebras of functions over finite fields, *Applicable Algebra in Engineering, Communication and Computing* **10**:6, 465–487.

[9] Hastad, J. (1989): *Almost Optimal Lower Bounds for Small Depth Circuits.* Advances in Computing Research, ed. S. Micali, Vol 5, 143–170.

[10] Hastad, J. (1998): The shrinkage exponent of de Morgan formulas is 2, *SIAM J. Comput.* **27**:1, 48–64.

[11] Hastad, J., Jukna, S. and Pudlák, P. (1995): Top-down lower bounds for depth 3 circuits, *Computational Complexity* **5**, 99–112.

[12] Jukna, S. (2001): *Extremal Combinatorics: With Applications in Computer Science*, Springer-Verlag.

[13] Karchmer, M. and Wigderson, A. (1988): Monotone circuits for connectivity require super-logarithmic depth. In: *Proc. 20th ACM STOC,* 539–550.

[14] Lokam, S. V. (2003): Graph complexity and slice functions, *Theory of Computing Systems* **36**:1, 71–88.

[15] Paturi, R., Pudlák, P., Zane, F. (1997): Satisfiability coding lemma. In: *Proc. of* 39*-th IEEE FOCS*, pp. 566–574.

[16] Paturi, R., Saks, M., Zane, F. (2001): Exponential lower bounds for depth three boolean circuits, *Computational Complexity* **9**:1, 1–15.

[17] Pudlák, P. and Rödl, V. (1992): A combinatorial approach to complexity, *Combinatorica* **14**, 221–226.

[18] Pudlák, P. and Rödl, V. (1994): Some combinatorial-algebraic problems from complexity theory, *Discrete Mathematics* **136**, 253–279.

[19] Pudlák, P. and Rödl, V. (2004): Pseudorandom sets and explicit constructions of Ramsey graphs. Manuscript.

[20] Pudlák, P., Rödl, V., Savický, P. (1988): Graph complexity, *Acta Informatica* **25**, 515–535.

[21] Razborov, A. A. (1987): Lower bounds for the size of circuits of bounded depth with basis $\{\wedge, \oplus\}$, *Math. Notes of the Academy of Sciences of the USSR* **41**:4, 333–338.

[22] Razborov, A. A. (1990): Applications of matrix methods to the theory of lower bounds in computational complexity, *Combinatorica,* **10**:1, 81–93.

[23] Razborov, A. A. (1988): Bounded-depth formulae over the basis $\{\&, \oplus\}$ and some combinatorial problem. In *Problems of Cybernetics. Complexity Theory and Applied Mathematical Logic*, S.I. Adian (ed.), VINITI, Moscow, pp. 149–166. (Russian)

[24] Smolensky, R. (1987): Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In: *Proc. of 19-th Ann. ACM Symp. Theor. Comput.*, 77–82.

[25] Valiant, L. (1977): Graph-theoretic methods in low-level complexity. In: *Proc. of 6-th Conf. on Mathematical Foundations of Computer Science*, Springer Lect. Notes in Comput. Sci., vol. 53, 162–176.

[26] Yao, A. C. (1985): Separating the polynomial time hierarchy by oracles. In: *Proc. 26-th Ann. IEEE Symp. Found. Comput. Sci.*, pp. 1–10.

# Appendix: Proof of the Magnification Lemma

In the lemma below, by a *circuit* we will mean an arbitrary computational model whose inputs are literals, i.e. variables $x_i^1 = x_i$ and their negations $x_i^0 = \overline{x}_i$. A boolean function $g$ is *isolating* if $g(a) = 0$ for the all-0 string $a = (0, \ldots, 0)$, and $g(b) = 1$ for all strings $b$ contains precisely one 1; on other input strings the function can take arbitrary values. Since OR and Parity functions are isolating, the Magnification Lemma is a special case of Lemma 6.2 below.

Let $G \subseteq U \times V$ be a bipartite graph with $|U| = |V| = n = 2^m$, and

$$f_G(y_1, \ldots, y_m, z_1, \ldots, z_m)$$

be its characteristic function; that is, $f_G(\vec{u}, \vec{v}) = 1$ iff $(u, v) \in G$ (remember that vertices $u$ are encoded by binary strings $\vec{u}$ of length $m$). Suppose we have a circuit $\Phi$ computing $f_G$. A *positive extension* of $\Phi$ has $2^{m+1}$ variables $x_u$ with $u \in U$ and $x_v$ with $v \in V$, and is obtained from $\Phi$ by replacing input literals $y_i^\sigma$ and $z_i^\sigma$ by functions

$$Y_i^\sigma = g\left(\{x_u : u \in U;\, \vec{u}(i) = \sigma\}\right) \quad \text{and} \quad Z_i^\sigma = h\left(\{x_v : v \in V;\, \vec{v}(i) = \sigma\}\right)$$

where $g$ and $h$ are arbitrary isolating functions, and $\vec{u}(i)$ is the $i$-th bit in the binary code $\vec{u}$ of the vertex $u$.

**Lemma 6.2.** *Let $G \subseteq U \times V$ be a bipartite $n \times n$ graph. If a circuit $\Phi$ computes the characteristic function $f_G$ of $G$, then every its positive extension $\Phi^+$ represents the graph $G$.*

*Proof.* For an arc $(u,v) \in U \times V$, let $\vec{a}_{u,v}$ be the vector in $\{0,1\}^{U \cup V}$ with precisely two 1's in positions $u$ and $v$. Suppose now that the original circuit $\Phi$ computes the characteristic function $f_G$ of $G$. Then $(u,v) \in G$ iff $\Phi(\vec{u},\vec{v}) = 1$. Hence, it remains to show that $\Phi^+(\vec{a}_{u,v}) = 1$ iff $\Phi(\vec{u},\vec{v}) = 1$. The only difference of the circuit $\Phi^+$ from $\Phi$ is that instead of input literals it takes the corresponding isolating functions as inputs. Hence, it is enough to show that on input strings $\vec{a}_{u,v}$ these isolating functions output the same values as the corresponding literals do on input strings $(\vec{u},\vec{v})$. We show this only for $y$-variables (for $z$-variables the argument is the same).

Let $y_i^\sigma$ be some input literal of $\Phi$. On every input $(\vec{u},\vec{v}) \in \{0,1\}^{2m}$, $y_i^\sigma(\vec{u},\vec{v}) = 1$ iff $\vec{u}(i) = \sigma$. By the definition, the function $Y_i^\sigma$ depends only on the variables $x_u$ corresponding to the left part $U$ of the bipartition such that $\vec{u}(i) = \sigma$. Each input of the form $\vec{a}_{u,v}$ assigns precisely one 1 to these variables, and this 1 is in the position $x_u$. Hence, $Y_i^\sigma(\vec{a}_{u,v}) = 1$ iff $\vec{u}(i) = \sigma$, which happens precisely when $y_i^\sigma(\vec{u},\vec{v}) = 1$. □



ECCC ISSN 1433-8092
http://www.eccc.uni-trier.de/eccc
ftp://ftp.eccc.uni-trier.de/pub/eccc
ftpmail@ftp.eccc.uni-trier.de, subject 'help eccc'