Resolution complexity of perfect matching principles for sparse graphs*

Dmitry Itsykson[†1], Mikhail Slabodkin[‡2], and Dmitry Sokolov[§1]

[1]Steklov Institute of Mathematics at St.Petersburg
[2]St. Petersburg Academic University

July 23, 2014

Abstract

The resolution complexity of the perfect matching principle was studied by Razborov [Raz04], who developed a technique for proving its lower bounds for dense graphs. We construct a a constant degree bipartite graph G_n such that the resolution complexity of the perfect matching principle for G_n is $2^{\Omega(n)}$, where n is the number of vertices in G_n. This lower bound matches with the upper bound $2^{O(n)}$ up to an application of a polynomial. Our result implies the $2^{\Omega(n)}$ lower bounds for the complete graph K_n and the complete bipartite graph $K_{n,O(n)}$ that improve the lower bounds followed from [Raz04]. Our results also implies the well-known exponential lower bounds on the resolution complexity of the pigeonhole principle, the functional pigeonhole principle and the pigeonhole principle over a graph.

We also prove the following corollary. For every natural number d, for every n large enough, for every function $h : \{1, 2, \dots, n\} \to \{1, 2, \dots, d\}$, we construct a graph with n vertices that has the following properties. There exists a constant D such that the degree of the i-th vertex is at least $h(i)$ and at most D, and it is impossible to make all degrees equal to $h(i)$ by removing the graph's edges. Moreover, any proof of this statement in the resolution proof system has size $2^{\Omega(n)}$. This result implies well-known exponential lower bounds on the Tseitin formulas as well as new results: for example, the same property of a complete graph.

1 Introduction

The resolution proof system is one of the simplest and well-studied proof systems. There are well known methods of proving lower and upper bounds on the complexity of several

*The research is partially supported by the RFBR grant 14-01-00545, by the President's grant MK-2813.2014.1 and by the Government of the Russia (grant 14.Z50.31.0030).

†dmitrits@pdmi.ras.ru
‡slabodkinm@gmail.com
§sokolov.dmt@gmail.com

types of formulas. However, there are no known universal methods to determine an asymptotic resolution complexity of a given family of formulas. We say that a family of unsatisfiable CNF formulas F_n is weaker than a family of unsatisfiable formulas H_n if every clause of H_n is an implication of a constant number of clauses of F_n. Since the resolution proof system is implication complete, the size of any resolution proof of H_n is at least the size of the minimal resolution proof of F_n. Thus it is interesting to prove lower bounds for for fomulas as weak as possible.

CNF formulas PHP_n^m encode the pigeonhole principle; PHP_n^m states that it is possible to put m pigeons into n holes in such a way that every pigeon is contained in at least one hole and every hole contains at most one pigeon. PHP_n^m depends on variables $p_{i,j}$ for $i \in [m]$ and $j \in [n]$ and $p_{i,j} = 1$ iff the i-th pigeon is in the j-th hole. PHP_n^m is unsatisfiable iff $m > n$. Haken [Hak85] proved the lower bound $2^{\Omega(n)}$ on the resolution complexity of PHP_n^{n+1}. Raz [Raz01a] proved the lower bound 2^{n^ϵ} on the resolution complexity of PHP_n^m for some positive constant ϵ and arbitrary $m > n$. This lower bound was simplified and improved to $2^{\Omega(n^{1/3})}$ by Razborov [Raz01b].

Urquhart [Urq03] and Ben-Sasson, and Wigderson [BSW01] consider formulas $G-\mathrm{PHP}_m^n$ that are defined by a bipartite graph G; the first part of G corresponds to pigeons and consists of m vertices, and the second part corresponds to holes and consists of n vertices. Every pigeon must be contained in one of adjacent holes. Formulas $G-\mathrm{PHP}_n^m$ may be obtained from PHP_n^m by substituting variables which do not have corresponding edges in G with zeroes. The paper [BSW01] presents the lower bound $2^{\Omega(n)}$ for formulas $G-\mathrm{PHP}_n^m$ where $m = O(n)$ and G is a bipartite constant degree expander.

Razborov [Raz03] considers a so called functional pigeonhole principle FPHP_n^m that is a weakening of PHP_n^m; the formula FPHP_n^m is the conjunction of PHP_n^m and additional conditions stating that every pigeon is contained in at most one hole. Razborov proved a lower bound $2^{\Omega\left(\frac{n}{(\log m)^2}\right)}$ for FPHP_n^m that implies a lower bound $2^{\Omega\left(n^{1/3}\right)}$ depending only on n.

Let for every graph G a formula PMP_G (from the Perfect Matching Principle) encode that G has a perfect matching. Variables of PMP_G correspond to edges, and for every vertex of G exactly one incident edge has value 1. Razborov [Raz04] proved that if G has no perfect matchings, then the resolution complexity of PMP_G is at least $2^{\frac{\delta(G)}{\log^2 n}}$, where $\delta(G)$ is the minimal degree of the graph and n is the number of vertices.

Alekhnovich [Ale04] and Dantchev and Riis [DR01] consider the graphs of the chessboard $2n \times 2n$ with two opposite corners removed. The perfect matching principle for such graphs is equivalent to the possibility to tile such chessboards with domino. The strongest lower bound $2^{\Omega(n)}$ was proved in [DR01] and this lower bound is polynomially connected with the upper bound $2^{O(n)}$. We note that the number of variables is $\Theta(n^2)$.

Our results For all n and all $m \in [n+1, O(n)]$ we give an example of a bipartite graph $G_{m,n}$ with m and n vertices in its parts such that all degrees are bounded by a constant and the resolution complexity of $\mathrm{PMP}_{G_{m,n}}$ is $2^{\Omega(n)}$. The number of variables in such formulas is $O(n)$, therefore the lower bound matches (up to an application of a polynomial) the trivial upper bound $2^{O(n)}$ that holds for every formula with $O(n)$ variables. This is the first lower bound for perfect matching principle that is exponential in the number of variables. In particular, our results imply that the resolution complexity of $\mathrm{PMP}_{K_{m,n}}$ is $2^{\Omega(n)}$, where $K_{m,n}$ is the complete bipartite graph and $m = O(n)$. And this lower bound improves the lower bound $2^{\Omega(n/\log^2 n)}$ that follows from [Raz04] and matches (up to a polynomial application) the upper bound $n2^n$ that follows from the upper bound for PHP_n^{n+1} [SB97]. Our result implies the lower bound $2^{\Omega(n)}$ on the resolution complexity of PMP_{K_n}, where K_n is a complete graph on n vertices, and it is also better than the lower bound $2^{\Omega(n/\log^2 n)}$ that follows from [Raz04]. We note that $PMP_{G_{m,n}}$ is weaker than $G_{m,n} - \mathrm{PHP}_n^m$, PHP_n^m and FPHP_n^m, therefore our lower bound implies the same lower bound for $G_{m,n} - \mathrm{PHP}_n^m$, PHP_n^m and FPHP_n^m. To put it more precisely, we we prove the following theorem:

Theorem 1.1. Let G be a bipartite graph with parts X and Y such that the folowing holds:

1. G is a (r, c)-boundary expander; i.e. for all $A \subseteq X$, if $|A| \leq r$ then $|\delta(A)| \geq c|A|$, where $\delta(A)$ is the set of all vertices in Y that are connected with exactly one vertex in A;

2. There is a matching in G that covers all vertices from Y.

Then the width of all resolution proofs of PMP_G is at least $cr/2$. If additionally degrees of all vertices are at most D, then (using [BSW01] we get that) the size of any resolution proof of PHP_G is at least $2^{\Omega\left(\frac{(cr/2-D)^2}{n}\right)}$, where n is the number of edges in G.

The condition that G has a matching covering all vertices from Y cannot be removed for free since for every (r, c)-boundary expander it is possible to add one vertex to X and $\lceil c \rceil$ vertices to Y such that the new vertex in X is connected with all new vertices in Y. The resulting graph is also (r, c)-boundary expander but the resulting formula will contain unsatisfiable subformula that depends on $\lceil c \rceil$ variables, hence it can be refuted with width $\lceil c \rceil$. We do not know whether it is possible to replace the second condition in the theorem by a weaker condition.

To estimate the width we use the method introduced by Ben-Sasson and Wigderson in [BSW01]. However, we use a non-standard notion of a semantic implication and a non-standard measure on the set of clauses.

An example of a graph that suits the conditions of Theorem 1.1 can be constructed from every lossless expander by removing vertices of high degrees as it was shown in [IS11], and by adding a matching that covers all vertices from Y. For example, we can use the explicit construction of lossless expanders from [MCW02] (or the randomized construction [HLW06]).

Theorem 1.1 implies a more general theorem:

Theorem 1.2. For graph $G(V, E)$ and function $h : V \to \{1, 2, \dots, d\}$ we define a formula $\Psi_G^{(h)}$, that code that G has a subgraph H such that for all v in H the degree of v equals $h(v)$. For any $d \in \mathbb{N}$, there exists $D \in \mathbb{N}$ that for all n large enough and every function $h : V \to \{1, 2, \dots, d\}$, where $|V| = n$, there exists graph $G(V, E)$ with degrees of vertices at most D such that the formula $\Psi_G^{(h)}$ is unsatisfiable and the size of any resolution proof of $\Psi_G^{(h)}$ is at least $2^{\Omega(n)}$.

If h maps V to $\{1, 2\}$, then $\Psi_G^{(h)}$ is weaker than Tseitin formulas based on graph G. Thus our result implies the lower bound $2^{\Omega(n)}$ on the resolution complexity of Tseitin formulas that was proved in [Urq87].

2 Preliminaries

We consider simple graphs without loops and multiple edges. The graph G is called bipartite if its vertices can be divided into two disjoint parts X and Y in such a way that any edge is incident to one vertex from X and one vertex from Y. We denote $G(X, Y, E)$ a bipartite graph with parts X and Y and set of edges E. A matching in a graph $G(V, E)$ is such a set of edges $E' \subseteq E$ that any vertex $v \in V$ has at most one incident edge from E'. A matching E' covers a vertex v if there exists $e \in E'$ that is incident to v. A perfect matching is a matching that covers all vertices of G. For a bipartite graph $G(X, Y, E)$ and a set $A \subseteq X$ we denote $\Gamma(A)$ a set of all neighbors of vertices from A.

Lemma 2.1 (Hall)**.** Consider such a bipartite graph $G(X, Y, E)$ that for some $A \subseteq X$ for all $B \subseteq A$ the following inequality holds: $\Gamma(B) \geq |B|$. Then there is a matching that covers all vertices from A.

For a CNF formula φ a proof of its unsatisfiability in the resolution proof system is a sequence of clauses with the following properties: the last clause is an empty clause (we denote it by $\square$); any other clause is either a clause of initial formula φ or can be obtained from previous ones by the resolution rule. The resolution rule admits to infer a clause $(B \vee C)$ from clauses $(x \vee B)$ and $\neg x \vee C$. The size of a resolutional proof is the number of clauses in it.

In [BSW01] E. Ben-Sasson and A. Wigderson introduced a notion of formula width. A width of a clause is a number of literals contained it it. For a k-CNF formula φ a width of φ is a maximum width of clauses of φ. A width of a resolution proof is a width of the largest clause used in it.

Theorem 2.1 ([BSW01])**.** For any k-CNF unsatisfiable formula φ the size of resolution proof is at least $2^{\Omega\left(\frac{(w-k)^2}{n}\right)}$, where w is a minimal width of a resolutional proof and n is a number of variables used in φ.

Lemma 2.2. Let ϕ be a formula that is obtained from unsatisfiable formula ψ by a substitution of several variables. Then ϕ is unsatisfiable and the size of the minimal resolution proof of ψ is at least the size of the minimal resolution proof of ϕ.

3 Subgraph extraction

3.1 Existence of a perfect matching

For an undirected graph $G(V, E)$ we construct a formula PMP_G that encodes that G has a perfect matching. We assign a binary variable x_e for all $e \in E$. PMP_G is the conjunction of the following conditions: for all $v \in V$ exactly one edge that incident to v has value 1. Such conditions can be written as the conjunction of the statement that at least one edge takes value 1: $\bigvee_{(v,u)\in E} x_{(v,u)}$ and the statement that for any pair of edges e_1, e_2 incident to v at most one of them takes value 1: $\neg x_{e_1} \vee \neg x_{e_2}$.

Note that if degrees of all vertices are at most D, then PMP_G is a D-CNF formula.

In this section we prove the following theorem:

Theorem 3.1. There exists a constant D such that for all C that for all n large enough and for all $m \in [n+1, Cn]$ it is possible to construct in polynomial in n time such bipartite graph $G(V, E)$ with m and n vertices in parts that all degrees are at most D and the formula PMP_G is unsatisfiable and the size of any resolution proof of PMP_G is at least $2^{\Omega(n)}$.

Definition 3.1. A bipartite graph $G(X, Y, E)$ is (r, c)-boundary expander if for any set $A \subseteq X$ such that $|A| \le r$ the following inequality holds $|\delta(A)| \ge c|A|$, where $\delta(A)$ denotes the set of all such vertices in Y that are connected with the set A by the unique edge.

Lemma 3.1. Let bipartite graph $G(X, Y, E)$ have two matchings, the first one covers all vertices from Y and the second covers all vertices from $A \subseteq X$. Then there exists a matching in G that covers A and Y simultaneously.

Proof. Let L denote the matching that covers all vertices from the set A and let F be a matching that covers all vertices from Y. We prove that if F does not cover all vertices from A, then one may construct a matching F' that covers more vertices of A than F and also covers all vertices from Y. Therefore there is such a matching that covers A and Y.

Consider some vertex $v_1 \in A$ that is not covered by F and such path $v_1, u_1, v_2, u_2, \ldots, u_{k-1}, v_k$ that $(v_i, u_i) \in L$, $(u_i, v_{i+1}) \in F$ and $v_1, v_2, \ldots, v_{k-1} \in A$ and $v_k \notin A$.

For any fixed $v_1 \in A$ such a path can be constructed deterministically: starting at vertex v_1 the edges of the path belong to alternating matchings L and F. For every vertex from X at most one of outgoing edges belongs to L. For every vertex from Y exactly one of outgoing edges belongs to F. The path can't become a cycle because v_1 has no incident edges from F, therefore the constructed path will lead to some vertex $v_k \notin A$.

Let matching F' be constructed from F by removing all edges (v_i, v_{i+1}) and adding edges (u_i, v_i) for $1 \le i < k$. Now F' covers all Y and covers one additional vertex of A in comparison with F. □

Lemma 3.2. Let $G(X, Y, E)$ be a bipartite (r, d, c)-boundary expander with $c > 2$ and $|X| > |Y|$. Let G have a matching that covers all vertices from the part Y. Then the formula PMP_H is unsatisfiable and the width of its resolution refutation is at least $cr/2$.

Proof. Parts X and Y have different number of vertices, hence there are no perfect matchings in G and PMP_G is unsatisfiable.

We call an assignment to variables of PMP_G proper if for every vertex v at most one edge incident to v has value 1. For some subset $S \subseteq V$ and for a clause C we say that S properly implies C if any proper assignment that satisfies all constraints in vertices from S, also satisfies C. We denote it as $S \vdash C$.

Now we define a measure on clauses from a resolution refutation of PMP_G: $\mu(C) = \min\{|S \cap X| \mid S \vdash C\}$.

The measure μ has the following properties:

1) The measure of any clause from PMP_G equals 0 or 1.

2) Semiadditivity: $\mu(C) \le \mu(C_1) + \mu(C_2)$, if C is obtained by applying of resolution rule to C_1 and C_2.

Let $S_1 \vdash C_1$, $|S_1 \cap X| = \mu(C_1)$ and $S_2 \vdash C_2$, $|S_2 \cap X| = \mu(C_2)$. Hence $S_1 \cup S_2 \vdash C_1$ and $S_1 \cup S_2 \vdash C_2$, so $S_1 \cup S_2 \vdash C$, therefore $\mu(C) \le |S_1 \cap X| + |S_2 \cap X| = \mu(C_1) + \mu(C_2)$.

3) The measure of the empty clause $\Box$ is more than r.

Let $\mu(\Box) \le r$, then there is such $S \subseteq V$ that $S \vdash \Box$ and $|S \cap X| \le r$. For all $A \subseteq S \cap X$ the following holds $|\Gamma(A)| \ge |\delta(A)| \ge (c-1)|A| \ge |A|$, and Hall's Lemma (Lemma 2.1) implies that there is a matching in H that covers all $S \cap X$. By construction of H it has a matching that covers all vertices of Y, therefore Lemma 3.1 implies that there exists a matching that covers $S \cap X$ and Y, hence it covers S. This matching corresponds to an assignment that satisfies all constraints for vertices from S, but it is impossible to satisfy the empty clause and we get a contradiction with the fact that $\mu(\Box) \le r$.

The semiadditivity of the measure implies that any resolution proof of the formula PMP_G contains a clause C with the measure in the interval $\frac{r}{2} \le \mu(C) \le r$. Let $S \vdash C$ and $|S \cap X| = \mu(C)$. For the sake of brevity let $A = S \cap X$. Since G is a (r, c)-boundary expander, $\delta(A) \ge c|A|$. Let F denote the set of edges between A and $\delta(A)$. Every vertex from $\delta(A)$ has exactly one incident edge leading to A, therefore $|F| = |\delta(A)|$. Consider one particular edge $f \in F$, let $f = (u, v)$, where $u \in A$. Since $|(S \setminus \{u\}) \cap X| < |S \cap X|$, clause C is not properly implied from the set $S \setminus \{u\}$, i. e. there exists a proper assignment σ that satisfies all restrictions in the vertices $S \setminus \{u\}$, but refutes the clause C. Such assignment σ cannot satisfy the constraint in the vertex u, since otherwise σ would satisfy S and therefore satisfy C. Since σ is a proper assignment, σ assigns value 0 to all edges that are incident with u .

We consider two cases: 1) σ refutes a constraint in the vertex v; 2) σ satisfies a constraint in the vertex v.

In the first case we consider another assignment σ' that differs from σ in the value of the edge f. Note that σ' is proper and satisfies all constraints from S, so it satisfies C. Since σ does not satisfy C, the variable f is contained in C.

In the second case σ satisfies v. There is an edge e incident to v such that $\sigma(e) = 1$. The vertex v is a boundary vertex for A, therefore the other endpoint of e does not belong to A. Consider an assignment σ'' that is obtained from σ by changing the values of f and e, σ'' is proper and it satisfies all constraints from S, and hence it satisfies C. Thus C contains either e or f. Thus for all $v \in \delta(A)$ at least one of the edges incident to v occurs in C. Therefore the size of the clause C is at least $|\delta(A)| \ge c|A| \ge cr/2$.

$\Box$

We say that a graph is explicit if it can be constructed in time polynomial in the number of its vertices.

Lemma 3.3 ([IS11], lemma 6.2)**.** For all d large enough and for all m there exists explicit construction of $(r, 0.5d)$-boundary expander $G(X, Y, E)$ with $|X| = |Y| = m$, $r = \Omega(m)$ such that degrees of all vertices from X are at most d and degrees of all vertices from Y are at most d^2.

Corollary 3.1. For all d large enough and for all C and all n and $m \in [n+1, Cn]$ there is an explicit construction of $(r, 0.4d)$-boundary expander $G(X, Y, E)$ with $|X| = m$, $|Y| = n$

and $r = \Omega(n)$ such that degrees of all vertices from X are at most d and degrees of all vertices from Y are at most d^2.

Proof. The required graph can be obtained from Lemma 3.3 by deleting several vertices from the part Y. $\square$

Proof of Theorem 3.1. Consider some $d > 5$ that satisfies Corollary 3.1; consider $(r, 0.4d)$-boundary expander H from the Corollary 3.1 that has m and n vertices in parts. Let graph G be obtained from H by adding any matching that covers all vertices from the part Y. Graph G is a $(r, c-1)$-boundary expander, since the addition of a matching increases degrees of vertices in X at most by 1 and for every $A \subseteq X$ the size of $\delta(A)$ decreases by at most $|A|$.

Lemma 3.2 implies that the width of any resolution proof of PMP_G is at least $\Omega(n)$. Theorem 2.1 implies that the size of any resolution proof of PMP_G is at least $2^{\Omega(n)}$. $\square$

4 Subgraph extraction

Let $G(V, E)$ be an undirected graph and h be a function $V \to \mathbb{N}$ such that for every vertex $v \in V$, $h(v)$ is at most the degree of v. We consider formula $\Psi_G^{(h)}$; its variables corresponds to edges of G. $\Psi_G^{(h)}$ is a conjunction of the following statements: for every $v \in V$ exactly $h(v)$ edges that are incident to v have value 1. Formula PMP_G is a particular case of $\Psi_G^{(h)}$ for $h \equiv 1$.

Lemma 4.1. For all $d \in \mathbb{N}$ and for all n large enough for any set V of cardinality n and any function $h : V \to \{1, 2, \ldots, d\}$ there exists explicit construction of a graph $G(V, E)$ with the following properties: 1)V consists of two disjoint sets U and T with no edges between them; 2)The degree of every vertex $u \in U$ equals $h(u) - 1$ and the degree of every vertex $v \in T$ equals $h(v)$; 3) $|U| \geq \frac{n}{2} - 2d^2$.

Proof. Let $n \geq 4d^2$ and the vertices $v_1, v_2, \ldots, v_n$ be arranged in non-decreasing order of $h(v_i)$. Let k be the largest number that satisfies the inequality $\sum_{i=1}^{k}(h(v_i) - 1) < \sum_{i=k+1}^{n} h(v_i) - d(d-1)$. We denote $U = \{v_1, v_2, \ldots, v_k\}$ and $T = V \setminus U$. Obviously, $|U| = k \geq n/2 - d(d-1)$. Now we construct a graph G based on the set of vertices V. We start with an empty graph and will add edges one by one. For every vertex $v \in T$ we call co-degree of v the difference between $h(v)$ and the current degree of v. From every $u \in U$ we add $h(u) - 1$ edges to G that lead from u to distinct vertices of $V \setminus U$. Doing so, we maintain degrees of all $v \in T$ under the value $h(v)$. This always can be done since by the construction of U the total co-degree of all vertices from T is greater than $d(d-1)$, hence for all big enough n there exists at least d vertices with co-degree at least 1.

While the number of vertices in T with positive co-degree is greater than d, we will choose one of those vertices $w \in T$ and add to graph exactly co-degree of w edges that connect w with other vertices from T. Finally we have that T contains at most d vertices with co-degrees at most d. Now we connect them with distinct vertices from the set U, remove that vertices from U and add them to T. It is possible that in the last step some vertex $v \in T$ is already connected with several vertices from U, in that case we should connect v with new vertices. By this operation we deleted at most d^2 vertices from U and therefore $|U| \geq n/2 - 2d^2$. $\square$

Theorem 4.1. For all $d \in \mathbb{N}$ there is such $D \in \mathbb{N}$ that for all n large enough and for any function $h : V \to \{1, 2, \dots, d\}$, where V is a set of cardinality n, there exists such explicit graph $G(V, E)$ with maximum degree at most D, that formula $\Psi_G^{(h)}$ is unsatisfiable and the size of any resolution proof for $\Psi_G^{(h)}$ is at least $2^{\Omega(n)}$.

Proof. By Lemma 4.1 we construct a graph $G_1(V, E_1)$ and a set $U \subseteq V$ of size at least $\frac{n}{2} - 2d^2$ such that for all $v \in U$, the degree of v is equal to $h(v) - 1$ and for all $v \in V \setminus U$ the degree of v is equal to $h(v)$. Consider graph $G(U, E_2)$ from Theorem 3.1 with U as the set of its vertices. Define a new graph $G(V, E)$, where the set of edges E equals $E_1 \cup E_2$. Recall that edges from the set E_2 connect vertices of the set U and edges from E_1 do not connect pairs of vertices from U (that follows from the construction of the graph in Lemma 4.1).

For every vertex $v \in V \setminus U$ its degree equals $h(v)$. Therefore if $\Psi_G^{(h)}$ is satisfiable, then in any satisfying assignment of $\Psi_G^{(h)}$ all edges that are incident to vertices $V \setminus U$ must have the value 1. After substitution the value 1 for all these variables $\Psi_G^{(h)}$ becomes equal to the formula PMP_{G_2} that is unsatisfiable because of Theorem 3.1.

Formula PMP_{G_2} is obtained from $\Psi_G^{(h)}$ by substitution of several variables, thus Lemma 2.2 implies that the size of any resolution proof of $\Psi_G^{(h)}$ is at least the size of the minimal proof for PMP_G, that is at least $2^{\Omega(n)}$ by Theorem 3.1. $\square$

4.1 Colloraries

Tseitin formulas. A Tseitin formula $T_G^{(f)}$ can be constructed by an arbitrary graph $G(V, E)$ and a function $f : V \to \{0, 1\}$; variables of $T_G^{(f)}$ corresponds to edges of G. The formula $T_G^{(f)}$ is a conjunction of the following conditions: for every vertex v we write down a CNF condition that encode that the parity of the number of edges incident to v that have value 1 is the same as the parity of $f(v)$.

Based on the function $f : V \to \{0, 1\}$ we define a function $h : V \to \{1, 2\}$ by the following way: $h(v) = 2 - f(v)$. In other words if $f(v) = 1$, then $h(v) = 1$, and if $f(v) = 0$, then $h(v) = 2$. By Theorem 4.1 there exists such number D, that for all n large enough it is possible to construct graph G with n vertices of degree at most D such that the size of any resolution proof of the formula Ψ_G^h is at least $2^{\Omega(n)}$.

Note that every condition corresponding to a vertex of the formula $T_G^{(h)}$ is implied from the condition corresponding to the formula Ψ_G^h. Since the resolution proof system is implication complete, every condition of $T_G^{(h)}$ may be derived from a condition of Ψ_G^h by derivation of size at most 2^D Hence all clauses of the Tseitin formula may be obtained from clauses of formula Ψ_G^h by the derivation of size $O(n)$. Thus the size of any resolution proof of $T_G^{(f)}$ is at least $2^{\Omega(n)}$. This lower bound was proved in the paper [Urq87].

Complete graph. Let K_n be a complete graph with n vertices and $h : V \to \{0, 1, \dots, d\}$, where d is a some constant. Let formula $\Psi_{K_n}^{(h)}$ be unsatisfiable. By Theorem 4.1 there exists D such that for all n large enough there exists an explicit graph G with n vertices of degree at most D that the size of any resolution proof of Ψ_G^h is at least $2^{\Omega(n)}$. The graph G can be obtained from K_n by removing of several edges, hence the formula $\Psi_G^{(h)}$ can be obtained from $\Psi_{K_n}^{(h)}$ by the substitution zeroes to edges that do not present in G. Therefore by Lemma 2.2 the size of the resolution proof of $\Psi_{K_n}^{(h)}$ is at least $2^{\Omega(n)}$.

Acknowledgements

The authors are grateful to Vsevolod Oparin for fruitfull discussions.

References

[Ale04] Michael Alekhnovich. Mutilated chessboard problem is exponentially hard for resolution. *Theor. Comput. Sci.*, 310(1-3):513–525, January 2004.

[BSW01] E. Ben-Sasson and A. Wigderson. Short proofs are narrow — resolution made simple. *Journal of ACM*, 48(2):149–169, 2001.

[DR01] Stefan S. Dantchev and Søren Riis. "planar" tautologies hard for resolution. In *FOCS*, pages 220–229, 2001.

[Hak85] Armin Haken. The intractability of resolution. *Theoretical Computer Science*, 39:297–308, 1985.

[HLW06] S. Hoory, N. Linial, and A. Wigderson. Expander graphs and their applications. *Bulletin of the American Mathematical Society*, 43:439–561, 2006.

[IS11] Dmitry Itsykson and Dmitry Sokolov. Lower bounds for myopic DPLL algorithms with a cut heuristic. In *Proceedings of the 22nd international conference on Algorithms and Computation*, ISAAC'11, pages 464–473, Berlin, Heidelberg, 2011. Springer-Verlag, available as ECCC Report TR12-141.

[MCW02] S. Vadhan M. Capalbo, O. Reingold and A. Wigderson. Randomness conductors and constant-degree expansion beyond the degree/2 barrier. In *Proceedings of the 34th Annual ACM Symposium on Theory of Computing*, pages 659–668, 2002.

[Raz01a] Ran Raz. Resolution lower bounds for the weak pigeonhole principle. Technical Report 01-021, Electronic Colloquium on Computational Complexity, 2001.

[Raz01b] Alexander A. Razborov. Resolution lower bounds for the weak pigeonhole principle. Technical Report 01-055, Electronic Colloquium on Computational Complexity, 2001.

[Raz03] Alexander A. Razborov. Resolution lower bounds for the weak functional pigeonhole principle. *Theoretical Computer Science*, 303(1):233—243, 2003.

[Raz04] Alexander A. Razborov. Resolution lower bounds for perfect matching principles. *Journal of Computer and System Sciences*, 69(1):3–27, 2004.

[SB97] T. Pitassi S. Buss. Resolution and the weak pigeonhole principle. In *Proceedings of the CSL97, Lecture Notes in Computer Science*, volume 1414, page 149–156, 1997.

[Urq87] A. Urquhart. Hard examples for resolution. *JACM*, 34(1):209–219, 1987.

[Urq03] Alasdair Urquhart. Resolution proofs of matching principles. *Annals of Mathematics and Artificial Intelligence*, 37(3):241–250, March 2003.