Regular and General Resolution: An Improved Separation

Alasdair Urquhart*

Department of Computer Science
University of Toronto
Toronto, Ontario M5S 1A4,
Canada
urquhart@cs.toronto.edu

Abstract. This paper gives an improved separation between regular and unrestricted resolution. The main result is that there is a sequence $\Pi_1, \Pi_2, \ldots, \Pi_i, \ldots$ of sets of clauses for which the minimum regular resolution refutation of Π_i has size $2^{\Omega(R_i/(\log R_i)^7)}$, where R_i is the minimum size of an unrestricted resolution refutation of Π_i. This improves earlier lower bounds for which the separations proved were of the form $2^{\Omega(\sqrt[3]{R})}$ and $2^{\Omega(\sqrt[4]{R}/(\log R)^3)}$.

1 Introduction

1.1 The Regularity Restriction

This paper proves an improved separation between the size of regular and unrestricted resolution refutations of sets of clauses. This provides a nearer approach to an optimal separation between these two propositional proof systems than earlier results.

The regularity restriction was first introduced by Grigory Tseitin in a groundbreaking article [1], the published version of a talk given in 1966 at a Leningrad seminar. This restriction is very natural, in the sense that algorithms such as that of Davis, Logemann and Loveland [2] (the prototype of almost all satisfiability algorithms used in practice today) can be understood as a search for a regular refutation of a set of clauses. If refutations are represented as trees, rather than directed acyclic graphs, then minimal-size refutations are regular, as can be proved by a simple pruning argument [3, p. 436].

The main result of Tseitin's paper [1] is an exponential lower bound for regular resolution refutations of contradictory CNF formulas based on graphs. Tseitin makes the following remarks about the heuristic interpretation of the regularity restriction:

> The regularity condition can be interpreted as a requirement for not proving intermediate results in a form stronger than that in which they

* The author gratefully acknowledges the support of the Natural Sciences and Engineering Research Council of Canada.

H. Kleine Büning and X. Zhao (Eds.): SAT 2008, LNCS 4996, pp. 277–290, 2008.

are later used (if A and B are disjunctions such that $A \subseteq B$, then A may be considered to be the stronger assertion of the two); if the derivation of a disjunction containing a variable ξ involves the annihilation of the latter, then we can avoid this annihilation, some of the disjunctions in the derivation being replaced by "weaker" disjunctions containing ξ.

These remarks of Tseitin suggest that there is always a regular resolution refutation of minimal size, as in the case of tree resolution. Consequently, some researchers tried to extend Tseitin's results to general resolution by showing that regular resolution can simulate general resolution efficiently. However, these attempts were doomed to failure.

The first example of a contradictory CNF formula whose shortest resolution refutation is irregular was given by Wenqi Huang and Xiangdong Yu [4]. Subsequently, Andreas Goerdt [5] gave the first super-polynomial separation between regular resolution and unrestricted resolution by constructing a family of formulas that have polynomial-size resolution refutations, but require super-polynomial size regular resolution refutations.

Goerdt's results were improved to an exponential separation in a paper by Alekhnovich, Johannsen, Pitassi and Urquhart [6]. The paper in fact contains two separate proofs of an exponential separation. The first presents a sequence $GT'_{n,\rho}$ of sets of clauses that have general resolution refutations with size $O(n^3)$, but require regular resolution refutations of size $2^{\Omega(n)}$. The second gives an infinite sequence of sets of clauses $Stone(G, S)$ based on a pebbling problem that have general resolution refutations with size $O(n^4)$, but require regular resolution refutations of size $2^{\Omega(n/(\log n)^3)}$.

Hence, the best separations so far between regular and general resolution are of the form $2^{\Omega(\sqrt[3]{R})}$, and $2^{\Omega(\sqrt[4]{R}/(\log R)^3)}$, where R is the size of the smallest general resolution refutation of the set of clauses in question. It is natural to ask whether we can improve these separations. In fact, we know that we cannot do better than a $2^{\Omega(R \log\log R/\log R)}$ separation. This is because Ben-Sasson, Impagliazzo and Wigderson [7] showed that if R is the size of a general resolution refutation of a set of clauses, then there is a tree resolution refutation with size $2^{O(R \log\log R/\log R)}$. Since a tree resolution refutation of minimal size is regular, it follows that the same upper bound holds for regular resolution.

The present paper makes a closer approach to a matching lower bound. The main result is that there is a sequence of contradictory sets of clause Π_i, with an associated unbounded parameter $n = n(i)$, so that Π_i has a general resolution refutation with size $O(n(\log n)^7)$, but any regular resolution refutation has size $2^{\Omega(n/[(\log n)^2 \log\log n])}$ The proof of this result is an amalgamation and extension of ideas underlying the two previous separation results.

1.2 Preliminaries

A *literal* is a propositional variable x or its negation $\neg x$. A *clause* is a set of literals, interpreted as the disjunction of the set. For clauses containing exactly one positive literal, we use the implication $p_1, \ldots, p_k \rightarrow q$ as alternative notation

for the clause $\neg p_1 \vee \cdots \vee \neg p_k \vee q$. The *resolution rule* allows us to derive the *resolvent* $C \vee D$ from the clauses $C \vee x$ and $D \vee \neg x$ by *resolving on* the variable x; a clause $C \vee D$ can also be derived from a clause C by *weakening*. A *resolution derivation* of a clause C from a set of clauses Σ consists of a sequence of clauses in which each clause is either a clause of Σ, or derived from earlier clauses by resolution or weakening, and C is the last clause in the sequence; it is a *refutation* of Σ if C is the empty clause Λ. The *size* $|\mathcal{R}|$ of a refutation $\mathcal{R}$ is the number of resolvents in it. We can represent it as a directed acyclic graph (dag) where the nodes are the clauses in the refutation, each clause of F has out-degree 0, and any other clause has one or two arcs pointing to the clause or clauses from which it is derived. Resolution is a *sound* and *complete* propositional proof system, that is to say, a set of clauses Σ is unsatisfiable if and only if there is a resolution refutation for Σ.

A resolution refutation is *regular* if on any path from Λ to a clause in F (in the directed acyclic graph associated with the refutation), each variable is resolved on at most once along the path.

It is sometimes helpful to view a regular resolution refutation as a branching program. Representing the refutation as a dag, let us say that a variable x is *queried at a node* q in the dag if q is labelled with a clause $C \vee D$, derived from parent clauses $C \vee x$ and $D \vee \neg x$ by resolving on x. Starting from the empty clause Λ at the root of the dag, we can construct a path in the refutation by answering the queries occurring in the path; the answers determine an assignment to the variables queried along the path. The path is chosen so that the assignment falsifies all the clauses in the path. Thus, if the variable x is queried at a node, and the answer is "false," then the next node in the path is labelled with the parent clause containing the literal x; similarly for the answer "true." If $C \vee D$ is derived by weakening from C, then the path continues to C. The path constructed in this way must end with an initial clause falsified by this assignment.

An *assignment* (*restriction*) for a set of clauses is a Boolean assignment to some of the variables in the set; the assignment is *total* if all the variables in the set are assigned values. If C is a clause, and σ an assignment, then we write $C \restriction \sigma$ for the result of applying the assignment to C, that is, $C \restriction \sigma = 1$ if $\sigma(l) = 1$ for some literal l in C, otherwise, $C \restriction \sigma$ is the result of removing all literals set to 0 by σ from C. If Σ is a set of clauses, then $\Sigma \restriction \sigma$ is the set of clauses $C \restriction \sigma$, C a clause in Σ.

If $\mathcal{R}$ is a resolution refutation of Σ, and σ a restriction for Σ, then we define the *restriction* $\mathcal{R} \restriction \sigma$ of $\mathcal{R}$ to be the sequence of clauses resulting from $\mathcal{R}$ by replacing all of the clauses C in $\mathcal{R}$ by $C \restriction \sigma$, and then removing all of the clauses set to 1. It is easy to verify that $\mathcal{R} \restriction \sigma$ is a resolution refutation of $\Sigma \restriction \sigma$, and that $\mathcal{R}$ is regular, if $\mathcal{R}$ is regular.

If Σ is a set of clauses, and x, y are variables in Σ, or the propositional constant $\bot$, then we say that there is an *implicational chain from x to y in Σ* if there is a sequence $x = x_0, \ldots, x_k = y$ of variables (or constants) and a sequence $C_1, \ldots, C_k$ of clauses so that for all i, $0 < i \leq k$, x_{i-1} occurs negatively and x_i positively in C_i.

The notation $\log x$ stands for the base two logarithm of x, and $\ln x$ the natural logarithm of x.

2 Pebbling Games and Pebbling Formulas

2.1 The Pebbling Game

A *pointed graph* G is a directed acyclic graph where all nodes have indegree at most two, having a unique sink, or target node, to which there is a directed path from all the nodes in G. It is *binary* if all nodes except for the source nodes have indegree two. If v is a node in a pointed graph G, then $G\restriction v$ is the subgraph of G restricted to the nodes from which there is a directed path to v.

The *pebbling game* played on a pointed graph G is a one-player game in the course of which pebbles are placed on or removed from nodes in G. The rules of the game are as follows;

1. A pebble may be placed on a source node at any time.
2. If all predecessors of a node u are marked with pebbles, then a pebble may be placed on node u.
3. A pebble may be removed from a node at any time.

A *move* in the game consists of the placing or removing one of the pebbles in accordance with one of the three rules. The *configuration* at a given stage in the game is the set of nodes in G that are marked with a pebble. The goal of the game is to place a pebble on the sink node t, while minimizing the number of pebbles used (that is, minimizing the number of pebbles on the graph at any stage of the game). Thus a successful play of the game can be presented as a sequence of configurations $C_0, \ldots, C_k$, where $C_0 = \emptyset$ and $t \in C_k$.

A *strategy* for the game is a sequence of moves following the rules of the game that ends in pebbling the target node. The *cost* of such a strategy is the minimum number of pebbles required in order to execute it, that is to say, the size of the largest configuration in the sequence of configurations produced by following the strategy. The *pebbling number* of G, written as $\sharp G$, is the minimum cost of a strategy for the pebbling game played on G.

2.2 Pebbling Formulas

We associate a contradictory set of clauses with every pointed graph G. Each node in G except the target t is assigned a distinct variable; to simplify notation, we identify a node with the variable associated with it, and use the notation $\mathrm{Var}(G)$ for the set of these variables. We associate the constant $\bot$ (falsum) with the target node t, and make the identification $t = \bot$.

Definition 1. *If G is a pointed graph, $Peb(G)$ is a set of clauses expressed in terms of the variables $Var(G)$, so that $Peb(G) = \{Clause(v) : v \in G \setminus \{t\}\}$.*

1. *If v is a source node of G, then $Clause(v) = v$.*

2. If v is a node in G, with predecessor u, then $Clause(v) = u \to v$.
3. If v is a node in G, with predecessors u, w, then $Clause(v) = u, w \to v$.

If we set some variables in $\mathrm{Peb}(G)$, then the resulting set of clauses is not necessarily of the form $\mathrm{Peb}(G')$, where G' is a subgraph of G. We shall focus on a family of special assignments, called *pebbling assignments*, that preserve this property. If $v \in G$, $v \neq t$, then we define the assignment $[\![v := 1]\!]$ to be the assignment defined by first setting the variable v to 1, and then setting to 1 any variable u for which there is no implicational chain from u to $\bot$ in the resulting clause set. The assignment $[\![v := 0]\!]$ is defined as follows: first, choose a directed path $\pi = (v, \ldots, t)$ from v to the target t, set all the nodes in the path to 0, and in addition set any node from which v is not reachable, but not in the path π, to 1. The assignment $[\![v := 0]\!]$ is not uniquely determined by this construction, since it depends on the path chosen – however, this is not important, since the set of clauses $\mathrm{Peb}(G)\restriction [\![v := 0]\!]$ resulting from the restriction is independent of the path. A *pebbling assignment* results from a sequence of restrictions of the form $[\![v := 0]\!]$ and $[\![w := 1]\!]$.

The effect of the restrictions just defined can be described directly as an operation on the underlying graph. If G is a pointed graph, and $v \in G$, $v \neq t$, $G[v := 1]$ is the graph resulting from G by first removing v, together with all edges entering or leaving v, and then restricting the resulting graph to the nodes from which the target node t is accessible. $G[v := 0]$ is the pointed graph $G\restriction v$.

Lemma 1. *1. For $b = 0, 1$, $Peb(G)\restriction [\![v := b]\!] = Peb(G[v := b])$.*
2. If G is a pointed graph, and $v \in G$, then

$$\sharp G \leq \max\{\sharp G[v := 0], \sharp G[v := 1] + 1\}.$$

Proof. The first part of the lemma follows straightforwardly from the definitions. For the second part, we employ the following strategy in the pebble game on G. First, follow a minimum cost strategy to pebble v in $G[v := 0]$. Second, leaving a pebble on v, but removing all other pebbles, follow a minimum cost strategy in the pebbling game on $G[v := 1]$ to pebble the target node in G, using the extra pebble for any moves where a pebble is needed on v to justify a placement. The cost is at most $\max\{\sharp G[v := 0], \sharp G[v := 1] + 1\}$. □

If Σ is a set of clauses, then a *C-critical assignment* is an assignment to the variables in Σ that makes all the clauses true, except C. In the case of $\mathrm{Peb}(G)$, we are interested in a particular family of critical assignments. Let v be a vertex in G, and $\pi = (v, \ldots, t)$ a directed path in G from v to the target node t. Set all the nodes in the path π to 0, and all other nodes in G to 1. This assignment makes all of the clauses in $\mathrm{Peb}(G)$ true, except for $\mathrm{Clause}(v)$. An assignment determined by the path π we shall call a *v-critical assignment*, since the clause that it falsifies is associated with the node v. Since we have assumed that G is a pointed graph, such v-critical assignments exist for all the nodes v in G, so that $\mathrm{Peb}(G)$ is minimally inconsistent.

Lemma 2. *If G is a pointed graph with $\sharp G = p$, then there are at least p vertices v in G for which there is a v-critical assignment for $Peb(G)$.*

Proof. Every pebbling strategy for G must contain a configuration with p pebbles, so there must be at least p vertices in G. For every vertex v in G, we can construct a v-critical assignment for Peb(G) by choosing a path from v to the target node. □

If G is a binary pointed graph, then the clause set Peb(G) contains both 3-literal clauses and unit clauses. It is convenient, in view of a later construction, to convert it into a set of 3-literal clauses.

Definition 2. *Let Σ be a set containing both 3-literal clauses and unit clauses. Then Σ^* is the set of clauses obtained from Σ by the following construction. First, introduce for each unit clause l in Σ, a pair of new auxiliary variables x_l and y_l. Second, replace the unit clause l by the set of four 3-literal clauses $\{l \vee x_l \vee y_l, l \vee \overline{x_l} \vee y_l, l \vee x_l \vee \overline{y_l}, l \vee \overline{x_l} \vee \overline{y_l}\}$.*

We write Peb$^*(G)$ for Peb$(G)^*$. Let G be a binary pointed graph. If v is a node in G that is not a source node, then we write Clauses(v) for $\{u, w \rightarrow v\}$, where u, w are the predecessors of v, and if v is a source node, then Clauses(v) is defined to be the set of four clauses $\{v \vee x_v \vee y_v, v \vee \overline{x_v} \vee y_v, v \vee x_v \vee \overline{y_v}, v \vee \overline{x_v} \vee \overline{y_v}\}$. If X is a subset of the nodes in G, then Clauses(X) is defined to be $\bigcup\{\text{Clauses}(v) : v \in X\}$.

3 Constructing Hard Problems

3.1 Earlier Constructions

In this section, we construct the problems that produce our improved separation between general and regular resolution. The overall approach is derived from the first separation result described above in §1; the proof of this result is based on the following idea. The construction begins with a sequence of problems GT_n that are hard for tree resolution but not for regular resolution. The set of clauses GT_n asserts that there is a directed acyclic ordering on n nodes that has no sink; these problems were introduced in the proof complexity literature by Krishnamurthy [8], who conjectured that they require superpolynomial-size resolution refutations. That conjecture was refuted by Stålmarck, who showed that they in fact have linear size resolution refutations [9]. However, Bonet and Galesi [10] showed that they require exponentially large tree resolution refutations, thus showing an exponential separation between general and tree resolution.

The exponential lower bound for tree resolution shows that any tree refutation for GT_n must contain exponentially many paths starting from the root of the tree. Although this fact does not force regular resolution refutations to be large, as Stålmarck showed, nevertheless we can convert the GT_n examples into hard problems for regular resolution by making a small modification. The idea is to add new literals to certain clauses in such a way as to force the exponentially many paths in a tree refutation not to overlap, at least in their initial segments. The new sets of clauses $GT'_{n,\rho}$ require exponentially large regular resolution refutations, though the general resolution size remains linear, as in the case of the original GT_n problems.

The construction in the present paper follows the outline above, but this time starting from the pebbling formulas. The second lower bound proof in [6] also began from the pebbling formulas, but used a somewhat different construction to convert them into hard examples for regular resolution. The present result combines features of both proofs; the construction proceeds in two stages.

3.2 Xorification of Clause Sets

The construction starts from $\mathrm{Peb}(G)$, for G a pointed graph. The first stage applies to $\mathrm{Peb}(G)$ a construction of Alekhnovich and Razborov.

Definition 3. *Let Σ be a set of clauses, and $k > 1$ a positive integer. For each variable x in Σ, introduce a set of k distinct variables $\{x_1, \cdots, x_k\}$. Then the set of clauses $\Sigma^{k\oplus}$, the k-*xorification of Σ*, is defined as follows: first, substitute the formula $x_1 \oplus \cdots \oplus x_k$ for all of the variables x occurring in Σ, second, convert the resulting formula into conjunctive normal form.*

If C is a clause containing m literals, then $\{C\}^{k\oplus}$ contains $2^{m(k-1)}$ clauses, each of length mk. Hence, when G is a binary pointed graph with n nodes, $\mathrm{Peb}^*(G)^{k\oplus}$ contains nk variables, and $n2^{3(k-1)}$ clauses, each of length $3k$.

The special case of Definition 3 where $k = 2$ is the original construction of Alekhnovich and Razborov [11]. They observed that it could be used to produce hard problems for resolution from clause sets requiring refutations of large width. Let $\mathrm{Width}(\Sigma)$ be the size of the largest clause in Σ, and $\mathrm{Width}(\Sigma \vdash 0)$ the minimum width of a resolution refutation of Σ.

Theorem 1. (Alekhnovich and Razborov) *If Σ is contradictory, then any resolution refutation of $\Sigma^{2\oplus}$ has size* $\exp[\Omega(\mathit{Width}(\Sigma \vdash 0) - \mathit{Width}(\Sigma))]$.

More important in the present context is the fact that the construction can be used to produce examples that separate tree resolution from general resolution.

Theorem 2. *If G is a pointed graph with n nodes and pebbling number p, then the set of clauses $\mathit{Peb}(G)^{2\oplus}$ has general resolution refutations of size $O(n)$, but every tree resolution refutation of $\mathit{Peb}(G)^{2\oplus}$ has size $2^{\Omega(p)}$.*

Proof. The theorem can be proved by imitating the proof of Ben-Sasson, Impagliazzo and Wigderson [7]. Their result involves clause sets that are the "orification" $\mathrm{Peb}(G)^{\vee}$ of $\mathrm{Peb}(G)$ rather than the xorification $\mathrm{Peb}(G)^{2\oplus}$; however, the steps in their proof can be imitated almost word for word in the case of $\mathrm{Peb}(G)^{2\oplus}$ to produce essentially the same result as their main theorem. □

An assignment μ for $\mathrm{Peb}^*(G)^{k\oplus}$ is defined to be *full* if whenever v is a vertex in G, and μ assigns a value to some variable v_j associated with v, then all the variables attached to v are assigned values by μ. If μ is such a full assignment, then we can construct an assignment for $\mathrm{Peb}(G)$ from μ by setting $\sigma(v) = \mu(v_1 \oplus \cdots \oplus v_k)$. In this case, we say that the constructed assignment is the *projection* of μ, written $\pi(\mu)$. We shall say that an assignment μ for $\mathrm{Peb}^*(G)^{k\oplus}$ is a *pebbling assignment* if its projection $\pi(\mu)$ is a pebbling assignment for $\mathrm{Peb}(G)$.

Lemma 3. *Let G be a binary pointed graph. If σ is a v-critical assignment for $Peb(G)$, $v \in G$, and C is in $Clauses(v)^{k\oplus}$, then there is a C-critical assignment μ for $Peb^*(G)^{k\oplus}$ so that $\pi(\mu) = \sigma$.*

Proof. If v is a source node in G, and D is a clause in Clauses(v), then we can construct a D-critical assignment for $\mathrm{Peb}^*(G)$ by giving the appropriate values to the auxiliary variables x_l and y_l. If v is not a source node, then σ is already a v-critical assignment for $\mathrm{Peb}^*(G)$.

Starting from a v-critical assignment for $\mathrm{Peb}^*(G)$, we can construct an assignment μ that assigns values to $u_1, \ldots, u_k$, for all nodes $u \in G$, so as to make C false, but all other clauses in $\mathrm{Peb}^*(G)^{k\oplus}$ true, and in addition, this assignment μ satisfies $\pi(\mu) = \sigma$. □

3.3 Adding Random Literals

The second stage of the construction starts from $\mathrm{Peb}^*(G)^{k\oplus}$, for a binary pointed graph G and suitable k, and replaces each clause C in the set with a pair of clauses, $C \vee \rho(C)$ and $C \vee \neg\rho(C)$, where $\rho(C)$ is a variable associated with C by the function ρ. For the second stage to work (that is to say, for the resulting sets of clauses to require exponentially large regular resolution refutations), it is essential that ρ have a special property, namely that the image of a large set of clauses has a large intersection with a large set of variables. The easiest way to construct such a function is by a probabilistic argument, given in the following lemma.

Lemma 4. *If G is a binary pointed graph with n nodes, $\delta = 5/3$ and $k = \lceil \delta \log\log n \rceil + 1$, define $\Sigma = Peb^*(G)^{k\oplus}$, and $V = Var(\Sigma)$. Then for sufficiently large n, there exists a map ρ from Σ to V satisfying the condition: For all $A \subseteq G$ with $|A| = \lfloor n/4\log n \rfloor$, and $B \subseteq V$, with $|B| = \lfloor n/4\log n \rfloor$, $|\rho(Clauses(A)) \cap B| \geq n/8\log n$.*

Proof. If $A \subseteq G$ with $|A| = \lfloor n/4\log n \rfloor$, and $x \in A$, then Clauses(x) contains $2^{3(k-1)} = 2^{5\lceil \log\log n \rceil} \geq (\log n)^5$ clauses, so that |Clauses(A)| contains $\Theta(n(\log n)^4)$ clauses, $|\Sigma| = \Theta(n(\log n)^5)$, and $|V| = nk = n(\lceil \delta \log\log n \rceil + 1) \leq 2n \log\log n$, for sufficiently large n.

Consider the space $\mathcal{R}$ of all random maps from Σ to V; that is to say, for each $C \in \Sigma$, a variable $\rho(C) \in V$ is chosen uniformly at random. For $A \subseteq G$ with $|A| = \lfloor n/4\log n \rfloor$, and $B \subseteq V$, with $|B| = \lfloor n/4\log n \rfloor$, we say that ρ is *bad for A and B* if $|\rho(\mathrm{Clauses}(A)) \cap B| < n/8\log n$.

We establish the existence of the map ρ by a probabilistic argument; to accomplish this, we need to prove exponentially small upper bounds on the probability that a random map is bad for some sets A and B. In proving this, it helps to view the construction of a random map as resulting from a series of independent experiments, each of them consisting in the construction of a random map from a subset of Σ.

We partition Clauses(x) as $\Xi_1(x), \ldots, \Xi_q(x)$, where $q = \lfloor (\log n)^3 \rfloor$, so that each set $\Xi_j(x)$ in the sequence contains at least $(\log n)^2$ clauses. For fixed j,

$1 \leq j \leq q$, let Σ_j be the union of all the $\Xi_j(x)$, for $x \in G$, and for $A \subseteq G$, $|A| = \lfloor n/4 \log n \rfloor$, let $\text{Clauses}_j(A)$ be the union of all the $\Xi_j(x)$, for $x \in A$. Then $\text{Clauses}_j(A)$ contains $\Theta(n \log n)$ clauses. Let ρ_j be a random map from Σ_j to V; we take ρ to be the union of the sequence $\rho_1, \ldots, \rho_q$ of independently constructed random maps.

For a given j, where $1 \leq j \leq q$, let Z be the random variable representing the number of variables in B not in the image of $\text{Clauses}_j(A)$ under ρ_j:

$$Z(\rho_j) = |\{x \in B |\, x \notin \rho_j(\text{Clauses}_j(A))\}|.$$

For $B = \{b_1, b_2, \ldots, b_i, \ldots, b_m\}$, where $m = \lfloor n/4 \log n \rfloor$, define an indicator random variable Θ_i by:

$$\Theta_i(\rho_j) = \begin{cases} 1, \text{ if } b_i \notin \rho_j(\text{Clauses}_j(A)) \\ 0, \text{ if } b_i \in \rho_j(\text{Clauses}_j(A)), \end{cases}$$

so that $Z = \Theta_1 + \cdots + \Theta_m$. We estimate the expected value of Θ_i by

$$\begin{aligned} E(\Theta_i) &= \left(1 - \frac{1}{|V|}\right)^{|\text{Clauses}_j(A)|} \\ &\leq \left(1 - \frac{1}{2n \log\log n}\right)^{\Theta(n \log n)} \\ &\leq \exp\left(-\Omega\left(\frac{\log n}{\log\log n}\right)\right), \end{aligned}$$

showing that

$$E(Z) \leq m \cdot \exp\left(-\Omega\left(\frac{\log n}{\log\log n}\right)\right) = m \cdot o(1).$$

It follows that for any given positive γ, $E(Z) < \gamma m$, for sufficiently large n. For the remainder of the proof, we assume that n is chosen sufficiently large so that $E(Z) < m/8$.

We need to show that the random variable Z is tightly concentrated around its mean. To do this, we employ a large deviation bound for martingales, following [12].

Order $\text{Clauses}_j(A)$ as $\{C_1, \ldots, C_p\}$. For $\rho \in \mathcal{R}$, and $1 \leq j \leq p$, define $\rho \restriction j$ to be the restriction of ρ to the set $\{C_1, \ldots, C_j\}$. Define an equivalence relation $\equiv_j$ on $\mathcal{R}$ by setting

$$\rho \equiv_j \sigma \iff \rho \restriction j = \sigma \restriction j,$$

for $1 \leq j \leq p$, and let $\equiv_0$ be the universal relation on $\mathcal{R}$. Let $\mathcal{F}_j$ be the finite Boolean algebra whose atoms are the blocks of the partition of $\mathcal{R}$ induced by $\equiv_j$, for $0 \leq j \leq p$. Now define a sequence of random variables $Z_0, \ldots, Z_p$ by setting $Z_j = E(Z|\mathcal{F}_j)$. Then $Z_0 = E(Z)$, $Z_p = Z$, and the sequence $Z_0, \ldots, Z_p$ forms a martingale, with $|Z_{j+1} - Z_j| \leq 1$. Consequently, by the martingale tail inequality of Hoeffding and Azuma [13, p. 221],

$$\begin{aligned} P(Z \geq m/2) &\leq P(Z - E(Z) > 3m/8) \\ &< \exp(-(3m/8)^2/2p) \\ &\leq \exp(-\Omega(n/(\log n)^3)). \end{aligned}$$

Let W be the random variable representing the number of variables in B not in the image of Clauses(A) under ρ:

$$W(\rho) = |\{x \in B |\ x \notin \rho(\text{Clauses}(A))\ \}|.$$

Since the maps $\rho_1, \ldots, \rho_q$ are constructed independently, it follows that

$$P(W \geq m/2) \leq [\exp(-\Omega(n/(\log n)^3))]^q = \exp(-\Omega(n)).$$

We can now complete the proof of the existence of a map ρ satisfying the condition of the lemma. The probability that a random map $\rho \in \mathcal{R}$ is bad for some A and B is bounded by

$$\binom{n}{\lfloor n/4 \log n \rfloor} \binom{n \log \log n}{\lfloor n/4 \log n \rfloor} \exp(-\Omega(n)).$$

Let $H(x) = x \log(1/x) + (1-x)\log(1/(1-x))$ be the binary entropy function. Then the first binomial coefficient above can be bounded by

$$\begin{aligned} \binom{n}{\lfloor n/4 \log n \rfloor} &\leq \exp(O(nH(n/\lfloor n/4 \log n \rfloor)) \\ &= \exp(O(nH(1/\log n))) \\ &= \exp(O(n \log \log n/\log n)). \end{aligned}$$

A similar computation shows that the second binomial coefficient has the same upper bound. Hence, the probability can be bounded above by

$$\exp(O(n \log \log n/\log n)) \exp(-\Omega(n)) = \exp(-\Omega(n)).$$

Consequently, the probability that a random map ρ is bad for some A and B is exponentially small for sufficiently large n, showing that a map satisfying the condition of the lemma must exist. □

3.4 Construction of the Hard Problems

Let's say that for $\Sigma = \text{Peb}^*(G)^{k\oplus}$, a map ρ is *good for* Σ if it satisfies the condition of Lemma 4. This lemma states that for $\delta = 5/3$, $k = \lceil \delta \log \log n \rceil + 1$, and sufficiently large n, there is a map that is good for $\Sigma = \text{Peb}^*(G)^{k\oplus}$. This enables us to construct our set of hard problems for regular resolution. The construction is based on the following result of Paul, Celoni and Tarjan.

Theorem 3. *[14] There is a sequence of binary pointed graphs $G_1, G_2, \ldots, G_i, \ldots$ with pebbling number $\Omega(n(i)/\log n(i))$, where $n(i) = |G_i| = O(i2^i)$.*

We construct our sequence $\Pi_1, \Pi_2, \ldots, \Pi_i, \ldots$ by applying the earlier constructions to $G_1, G_2, \ldots, G_i, \ldots$.

Definition 4. *Let $G_1, G_2, \ldots, G_i, \ldots$ be the sequence of graphs of Theorem 3, $k(i) = \lceil \delta \log\log n(i) \rceil + 1$, and ρ_i a map that is good for $\Sigma_i = Peb^*(G_i)^{k(i)\oplus}$. Then Π_i is defined to be the set of clauses*

$$\{C \vee \rho_i(C) : C \in \Sigma_i\} \cup \{C \vee \neg\rho_i(C) : C \in \Sigma_i\}.$$

The set of clauses Π_i contains $\Theta(n(\log n)^5)$ clauses, and $\Theta(n \log\log n)$ variables, where $n = n(i)$ is the size of the pointed graph G_i. By a "pebbling assignment for Π_i" we mean a pebbling assignment for $\Sigma_i = \mathrm{Peb}^*(G_i)^{k(i)\oplus}$.

4 Lower Bound for Regular Resolution

4.1 Destroying Large Clauses by Restrictions

In this section, to avoid notational clutter, we adopt the following conventions. We assume that we are dealing with the set of clauses $\Pi = \Pi_i$, for sufficiently large i, write G for G_i, and n for $n(i) = |G_i|$. Define a clause to be *large* if it contains at least $n/8 \log n$ literals.

Lemma 5. *If Σ is a set of clauses in the language of Π, containing fewer than $2^{n/[64(\log n)^2 \log\log n]}$ clauses, then there is a pebbling assignment μ so that:*

1. *$\Sigma\restriction\mu$ contains no large clauses.*
2. *$G\restriction\pi(\mu)$ has pebbling number at least $n/2\log n$.*

Proof. There are at most $2n \log\log n$ variables in Π, and so at most $4n \log\log n$ literals involving those variables. If we choose a literal at random and set it to 1, then the probability this assignment sets a large clause C to 1 is at least $1/r$, where $r = 32 \log n \log\log n$. Hence, the average number of large clauses in Σ set to 1 is at least $|\Sigma|/r$.

Choose a literal l achieving at least this average, and set it to 1. Suppose that l contains a variable v_j, where $v \in G$. Set the remaining variables in the set of variables $\{v_1, \ldots, v_k\}$ so as to maximize $\sharp G[v := b]$, where $b = v_1 \oplus \cdots \oplus v_k$. Now extend this assignment to produce a pebbling assignment for Π whose projection to $\mathrm{Peb}(G)$ is $[\![v := b]\!]$. Then the set Σ' resulting from this restriction contains at most $(1 - 1/r)|\Sigma|$ large clauses, and by Lemma 1, $\sharp G[v := b]$ is at most one less than $\sharp G$.

If we repeat this procedure $\lfloor n/2 \log n \rfloor$ times, resulting in a restriction μ, then the set contains at most

$$(1 - 1/r)^{\lfloor n/2 \log n \rfloor} 2^{n/[64(\log n)^2 \log\log n]}$$

large clauses. However, this last expression is bounded above by

$$\exp\left[-\frac{n}{(\log n)^2}\left(\frac{0.9 - \ln 2}{64 \log\log n}\right)\right] < 1,$$

showing that $\Sigma\restriction\mu$ contains no large clauses. By construction, the pebbling number of $G\restriction\pi(\mu)$ is at least $n/2\log n$. □

4.2 Large Clauses

Lemma 6. *Let $\mathcal{R}$ be a regular resolution refutation of $\Pi\restriction\mu$, where μ is a pebbling assignment, and $G\restriction\pi(\mu)$ has pebbling number $\geq n/2\log n$. Then $\mathcal{R}$ contains a clause with at least $n/8\log n$ literals.*

Proof. Viewing $\mathcal{R}$ as a branching program, we describe a strategy for constructing a path in $\mathcal{R}$, starting with the root, and concurrently constructing a full assignment to certain variables in π. The strategy is as follows. We suppose that the path has been constructed as far as a node p, and that σ is the current full assignment. We extend the path and the assignment according to these rules:

1. If the clause labelling p is derived by weakening, then continue the path to the unique parent node; the assignment remains unchanged.
2. If the variable queried at p is already assigned a value by σ, answer the query according to σ, and continue the path according to this answer.
3. If the variable queried at p is not assigned a value by σ, then it must be associated with a node $v \in G\restriction\pi(\sigma)$. Extend σ to a pebbling assignment σ' so that $\pi(\sigma') = [\![v := b]\!]$, choosing b so as to maximize the pebbling number of $(G\restriction\pi(\mu\cup\sigma))\restriction[\![v := b]\!])$. Then extend the path in accordance with σ'.

Continue according to these rules until $\lfloor n/4\log n\rfloor$ nodes in G have been queried (that is to say, variables attached to the nodes have been queried), let C be the clause at the end of the resulting path, and τ the resulting assignment.

By Lemma 2, there are at least $n/4\log n$ vertices $v \in G\restriction\pi(\tau)$ for which there is a v-critical assignment for $\mathrm{Peb}(G\restriction\pi(\tau))$. If ϕ is such a critical assignment, then $\pi(\tau)\cup\phi$ is a v-critical assignment for $\mathrm{Peb}(G)$. Let A be the set of all nodes in G satisfying this condition, and B the set of variables assigned values by τ. Since $|A|, |B| \geq \lfloor n/4\log n\rfloor$, by Lemma 4, $|\rho(\mathrm{Clauses}(A)) \cap B| \geq n/8\log n$.

Let x be a variable in $\rho(\mathrm{Clauses}(A)) \cap B$. We claim that x must occur in C. Suppose not. By assumption, there is a $D \in \mathrm{Clauses}(v)$, for some $v \in A$, so that $\rho(D) = x$, and $D \vee x, D \vee \overline{x} \in \Pi$. Let's assume that $\tau(x) = 0$ (the case $\tau(x) = 1$ is symmetrical). By Lemma 3, there is a D-critical assignment ϕ for $\mathrm{Peb}^*(G)^{k\oplus}$ that extends τ, and so is a $D \vee x$-critical assignment for Π. Extend the path in $\mathcal{R}$ from C by answering queries in accordance with ϕ. This path must terminate in a node labelled with $D \vee x$. But since x does not occur in C, it follows that it must have been resolved on twice along the path, violating regularity. This contradiction proves that x must occur in C, showing that C contains at least $n/8\log n$ literals. □

4.3 Lower Bound

Theorem 4. *Let $\Pi_1, \Pi_2, \ldots, \Pi_i, \ldots$ be the sequence of contradictory sets of clauses based on the pointed graphs $G_1, G_2, \ldots, G_i, \ldots$ of Paul, Celoni and Tarjan, where $n = n(i)$ is the size of the graph G_i. Then:*

1. *There are resolution refutations of Π_i with size $O(n(\log n)^7)$.*
2. *Every regular resolution refutation of Π_i has size $2^{\Omega(n/[(\log n)^2 \log\log n])}$*

Proof. The set of clauses $\mathrm{Peb}(G)$ has a refutation using unit resolution (where at least one of the premisses in every resolution step is a unit clause), with $O(n)$ steps and in which every clause contains at most three literals. We can imitate this refutation to produce a refutation of $\mathrm{Peb}(G)^{k\oplus}$; in this refutation, a single resolution step in the original refutation corresponds to multiple resolution steps in the new refutation. Let us suppose that in the original refutation of $\mathrm{Peb}(G)$, the clause $b \vee c$ was inferred from a and $\overline{a} \vee b \vee c$, where a, b, c are literals. Then in the new refutation, we infer $\{b \vee c\}^{k\oplus}$ from $\{\overline{a} \vee b \vee c\}^{k\oplus}$ and $\{a\}^{k\oplus}$. The set of clauses $\{a\}^{k\oplus} \cup \{\overline{a}\}^{k\oplus}$ consists of all the clauses in a fixed set of k variables, so it takes $O(2^k) = O((\log n)^{5/3})$ steps to deduce the empty clause from this set. Hence, a single clause in $\{b \vee c\}^{k\oplus}$ can be derived in $O((\log n)^{5/3})$ steps. It follows that the derivation of $\{b \vee c\}^{k\oplus}$ takes $O((\log n)^5 (\log n)^{5/3})$ resolution steps, showing that the entire refutation has size $O(n(\log n)^{20/3})$. By adding some extra resolution inferences, we can produce a resolution refutation of Π_i with the same size bound.

For the second part of the theorem, let us assume that $\mathcal{R}$ is a regular resolution refutation of Π_i, with size less than $2^{n/[64(\log n)^2 \log\log n]}$. By Lemma 5 there is a pebbling assignment μ so that $\mathcal{R}\restriction \mu$ contains no large clauses, but $G_i \restriction \pi(\mu)$ has pebbling number at least $n/2 \log n$. However, Lemma 6 shows that $\mathcal{R}\restriction \mu$ must contain a large clause, showing that a regular refutation of this size cannot exist. □

It is interesting to ask how close Theorem 4 comes to the optimum. We already observed in §1 that if R is the minimum size of a resolution refutation of a set of clauses, then the size of a regular refutation is bounded above by $2^{O(R \log\log R/\log R)}$. If we express the lower bound in these terms, then we find that the lower bound on regular refutations has the form $2^{\Omega(R/(\log R)^7)}$. So, the separation we have proved is certainly much closer to the optimum than previous bounds, but there is definitely room for improvement.

References

1. Tseitin, G.: On the complexity of derivation in propositional calculus. In: Slisenko, A.O. (ed.) Studies in Constructive Mathematics and Mathematical Logic, Part 2, pp. 115–125. Consultants Bureau, New York (1970); Reprinted in[15], vol. 2, pp. 466-483
2. Davis, M., Logemann, G., Loveland, D.: A machine program for theorem proving. Communications of the Association for Computing Machinery 5, 394–397 (1962); Reprinted in [15], vol. 1, pp. 267-270
3. Urquhart, A.: The complexity of propositional proofs. The Bulletin of Symbolic Logic 1, 425–467 (1995)
4. Huang, W., Yu, X.: A DNF without regular shortest consensus path. SIAM Journal on Computing 16, 836–840 (1987)
5. Goerdt, A.: Regular resolution versus unrestricted resolution. SIAM Journal on Computing 22, 661–683 (1993)
6. Alekhnovich, M., Johannsen, J., Pitassi, T., Urquhart, A.: An exponential separation between regular and general resolution. Theory of Computing 3, 81–102 (2007); Preliminary version. In: Proceedings of the 34th Annual ACM Symposium on Theory of Computing, May 19-21, 2002, Montréal, Québec, Canada (2002)

7. Ben-Sasson, E., Impagliazzo, R., Wigderson, A.: Near optimal separation of tree-like and general resolution. Combinatorica, 585–603 (2004); Preliminary version, ECCC TR00-005 (2000)
8. Krishnamurthy, B.: Short proofs for tricky formulas. Acta Informatica 22, 253–275 (1985)
9. Stålmarck, G.: Short resolution proofs for a sequence of tricky formulas. Acta Informatica 33, 277–280 (1996)
10. Bonet, M.L., Galesi, N.: Optimality of size-width tradeoffs for resolution. Computational Complexity 10, 261–276 (2001); Preliminary version: Proceedings 40th FOCS (1999)
11. Ben-Sasson, E.: Size Space Tradeoffs For Resolution. In: Proceedings of the 34th ACM Symposium on the Theory of Computing, pp. 457–464 (2002)
12. Kamath, A., Motwani, R., Palem, K., Spirakis, P.: Tail bounds for occupancy and the satisfiability threshold conjecture. Random Structures and Algorithms 7, 59–80 (1995)
13. McDiarmid, C.: Concentration. In: Habib, M., McDiarmid, C., Ramirez-Alfonsin, J., Reed, B. (eds.) Probabilistic Methods for Algorithmic Discrete Mathematics, vol. 16, pp. 195–248. Springer, Heidelberg (1998); Algorithms and Combinatorics 16
14. Paul, W., Tarjan, R., Celoni, J.: Space bounds for a game on graphs. Mathematical Systems Theory 10, 239–251 (1977)
15. Siekmann, J., Wrightson, G. (eds.): Automation of Reasoning. Springer, New York (1983)