Discrete Applied Mathematics 96–97 (1999) 177–193

DISCRETE
APPLIED
MATHEMATICS

The symmetry rule in propositional logic

Alasdair Urquhart *

Philosophy & Computer Science, University of Toronto, Toronto, Ont., Canada M5S 1A4

Received 1 August 1996; revised 1 December 1997; accepted 5 October 1998

Abstract

The addition of the symmetry rule to the resolution system sometimes allows considerable shortening in the length of refutations. We prove exponential lower bounds on the size of resolution refutations using two forms of a global symmetry rule. The paper also discusses the relationship of symmetry rules to the extension rule that allows the use of abbreviative definitions in proofs. © 1999 Elsevier Science B.V. All rights reserved.

1. Introduction

The symmetry rule arises naturally in proofs of combinatorial principles; in many cases it allows significant shortening of proofs. We discuss the efficiency of the rule and some of its variants in the context of the resolution proof system. We prove exponential lower bounds on the size of resolution proofs using two different forms of the symmetry rule. We also discuss the relationship of the rule to the extension rule that allows the use of abbreviative definitions in proofs.

Before proceeding to consideration of particular proof systems, let us fix notation. We assume an infinite supply of propositional variables and their negations; a variable or its negation is a *literal*. We say that a variable P and its negation $\sim P$ are *complements* of each other; we write the complement of a literal l as $\bar{l}$. A finite set of literals is a *clause*; it is to be interpreted as the disjunction of the literals contained in it. The *length* of a clause is the number of literals in it. We shall sometimes write a clause by juxtaposing the literals in it. An *assignment* is an assignment of truth-values to a set of propositional variables; some variables may remain unset under an assignment.

2. Symmetry in resolution proofs

The resolution rule is a simple form of the familiar cut rule. If Al and $B\bar{l}$ are clauses, then the clause AB may be inferred by the resolution rule, *resolving on* the literal l.

* *E-mail address:* urquhart@cs.toronto.edu. (A. Urquhart)

PII: S0166-218X(99)00039-6

A *resolution refutation* of a set of clauses Σ is a derivation of the empty clause Λ from Σ, using the resolution rule.

Although resolution operates only on clauses, it can be converted into a general purpose theorem prover for tautologies by employing an efficient method of conversion to conjunctive normal form, first used by Tseitin [18]. Let A be a formula containing various binary connectives such as $\rightarrow$ and $\equiv$; associate a literal with each subformula of A so that the literal associated with a subformula $\sim B$ is the complement of the literal associated with B. If the subformula is a propositional variable, then the associated literal is simply the variable itself. We write l_B for the literal associated with the subformula B. If B is a subformula having the form $C \circ D$, where $\circ$ is a binary connective, then $Cl(B)$ is the set of clauses making up the conjunctive normal form of $l_B \equiv (l_C \circ l_D)$. For example, if B has the form $(C \equiv D)$, then $Cl(B)$ is the set of clauses

$$\{\bar{l}_B\bar{l}_C l_D, \bar{l}_B l_C \bar{l}_D, l_B \bar{l}_C \bar{l}_D, l_B l_C l_D\}.$$

The set of clauses $Def(A)$ is defined as the union of all $Cl(B)$, where B is a subformula of A. If A is a tautology, then the set $Def(A) \cup \{\overline{l_A}\}$ is contradictory. We define a proof of A in the resolution system to be a proof of Λ from $Def(A) \cup \{\overline{l_A}\}$, and call it a proof by *resolution with limited extension* for the set of connectives (other than $\sim$) occurring in A.

If V is a set of variables, and σ a permutation of V, then for any clause C built from the variables in V, we define the clause $\sigma(C)$ to be the clause resulting from C by applying σ to each variable in C. For a set of clauses Γ, define $\sigma(\Gamma)$ to be $\{\sigma(C) \mid C \in \Gamma\}$.

The symmetry rule was introduced as an extension to the resolution system in a paper by Krishnamurthy [15]. The rule of symmetry allows the following inference. If a clause C has been derived from a set of clauses Γ, and $\sigma(\Gamma) = \Gamma$, then the clause $\sigma(C)$ can be inferred as the next step in the derivation. A proof from a set of clauses Γ in which each step is inferred by resolution from two earlier steps, or by the symmetry rule from an earlier step, is a *symmetric resolution* or *SR-I* proof.

The form of the symmetry rule just defined is designed to exploit global symmetries in a set of clauses. Krishnamurthy also defined a more general form of the symmetry rule that is able to exploit local symmetries. The local symmetry rule allows the following inference. Suppose that C is a clause derived from a set of clauses Γ, and for every clause A in Γ used in the derivation of C, $\sigma(A)$ is also in Γ. Then the local symmetry rule allows the derivation of $\sigma(C)$. A proof from a set of clauses Γ in which each step is inferred by resolution from two earlier steps, or by the local symmetry rule from an earlier step, is a *locally symmetric resolution proof* or *SR-II* proof.

The symmetry rule can also be generalized in another direction. If L is the set of literals based on a set of n variables, then L is closed under the complementation group, whose elements are the 2^n complementation operations; such an operation interchanges literals and their complements, for some subset of the literals in L. The symmetric group of all permutations of the variables acts in a natural way on the set of literals; hence this group can be enlarged to a group of order $2^n \cdot n!$ by adding the complementation operations. Following Harrison [13, Ch. 5], let us call this enlarged group the *group of permutations and complementations*. We can extend the symmetry rule (in either its global or local form) by allowing the inference of $\sigma(C)$ from C, where σ is an operation in the group of permutations and complementations under which Γ is invariant (or under which Γ is closed, when σ is applied to the appropriate subset of Γ, in the local form of the rule). Let us call the resulting proof systems *SRC-I* and *SRC-II*. For each of these proof systems, we define the *length* of a proof as the number of inferences in the proof; the *size* of a proof is the number of occurrences of symbols in it. For the inference systems defined above, the two measures of proof complexity are polynomially related.

The *extension rule*, first suggested by Tseitin [18], is a powerful addition to the resolution system that allows the use of literals as abbreviations for longer formulas. Let Γ be a set of clauses, let l_1, l_2, l_3 be literals such that neither l_1 nor its complement appears in Γ, and let $\circ$ be any binary connective. The *extension* of Γ with respect to l_1, l_2, l_3 and $\circ$ consists of the addition to Γ of the clauses making up the conjunctive normal form of the formula $l_1 \equiv (l_2 \circ l_3)$. The literals l_1 and $\overline{l_1}$ are said to be *introduced* by this extension. An *extended resolution derivation* of a clause C from a set of clauses Γ consists of a sequence of extensions of Γ followed by a resolution derivation of C from this extended set of clauses. The system of limited extension defined above is a restricted form of extended resolution. We define a proof of a tautology A by extended resolution to be an extended resolution refutation of $Def(A) \cup \{\overline{l_A}\}$.

3. The power of symmetry

Krishnamurthy [15] showed that the addition of the symmetry rule permits a considerable increase in efficiency over the simple resolution system in a number of cases. We illustrate this here with the propositional version of the pigeon-hole principle.

First, we define the graph-theoretical terminology used in this paper; our terminology is that of Bollobás [2]. A *graph* G is an ordered pair of finite sets (V, E) where E is a subset of the set of unordered pairs of V; the set $V = V(G)$ is the set of *vertices* of G, while $E = E(G)$ is the set of *edges* of G. If x, y are vertices, then we write xy for the edge containing x and y. We say that two edges are *adjacent* if they have exactly one vertex in common; a set of edges in a graph is *independent* if no two edges in the set are adjacent. A matching in a graph G is an independent subset of $E(G)$; the matching is *perfect* if every vertex in G belongs to one of the edges in the matching.

We can formulate the pigeon-hole principle in terms of certain finite graphs. Given a graph $G = (V, E)$, we can formulate the assertion that G has a perfect matching as a set of clauses, $PM(G)$. Where $x, y \in V$, the propositional variable P_{xy} is to be read as asserting: 'Vertex x is matched with vertex y'. We identify the variable P_{xy} with the variable P_{yx}. If x is a vertex in V, the disjunction $D_x = \bigvee\{P_{xy} | y \text{ adjacent to } x\}$ asserts that x is matched with one of its neighbors. Similarly, the disjunction

$E_{xyz} = (\sim P_{xy} \vee \sim P_{xz})$ asserts that x cannot be matched with both y and z. The set of clauses $PM(G)$ contains all the disjunctions D_x, for $x \in V$, together with all the disjunctions E_{xyz}, where $x, y, z \in V$, x is adjacent to y and z, and $y \neq z$. If G is a graph with n vertices, e edges and maximum degree d, then $PM(G)$ has size $O(e + d^2n)$.

If G has no perfect matching (for example, if G has an odd number of vertices) then $PM(G)$ is contradictory. Let $K(n+1, n)$ be the complete bipartite graph with $V = V_1 \cup V_2$, $|V_1| = n+1$, $|V_2| = n$, and $E = \{\{x, y\} \mid x \in V_1, y \in V_2\}$. The set of clauses $PM(K(n+1, n))$ is contradictory; the statement of this fact is a formulation of the pigeon-hole principle, so we shall refer to these clauses as the *pigeon-hole clauses* PHC_n. Armin Haken [12] proved the following result about the complexity of resolution refutations of PHC_n.

Theorem 3.1. *There is a* $c > 1$ *so that any resolution refutation of* PHC_n *contains at least* c^n *distinct clauses.*

The graph $K(n+1, n)$ is highly symmetric; we can use this fact to get a short *SR-I* refutation of PHC_n (an observation of Krishnamurthy). We formalize the following informal proof: 'If there is an injective map f from $\{1, \dots, n+1\}$ to $\{1, \dots, n\}$, then there is a k, $1 \leqslant k \leqslant n$, so that $f(n+1) = k$. By symmetry, we can assume that $k = n$. But then the map f' obtained by removing $\langle n+1, n \rangle$ from f is an injective mapping from $\{1, \dots, n\}$ into $\{1, \dots, n-1\}$. Hence the theorem follows by induction on n'.

Theorem 3.2. *There are SR-I refutations of length* $(3n+1)n/2$ *for the pigeon-hole clauses* PHC_n.

Proof. The proof is by induction on n; to simplify the notation, we shall assume that $V_1 = \{a_1, \dots, a_{n+1}\}$, $V_2 = \{b_1, \dots, b_n\}$, and that the propositional variables are written in the form $P_{i,j}$, where $a_i \in V_1$, $b_j \in V_2$.

The set of clauses PHC_1 has a resolution refutation of length 2. Assume that PHC_n has an *SR-I* refutation of length $f(n) = (3n+1)n/2$. To refute PHC_{n+1}, we begin by deriving the clauses $\sim P_{1,1} \vee P_{2,2} \vee \cdots \vee P_{2,n+1}, \sim P_{1,1} \vee P_{3,2} \vee \cdots \vee P_{3,n+1}, \dots, \sim P_{1,1} \vee P_{n+2,2} \vee \cdots \vee P_{n+2,n+1}$; this takes $n+1$ steps. By induction hypothesis, we can derive $\sim P_{1,1}$ from this set of clauses in $f(n)$ steps. By the symmetry rule, we can derive $\sim P_{1,2}, \sim P_{1,3}, \sim P_{1,4}, \dots, \sim P_{1,n+1}$ in n steps, then in $n+1$ further steps, we can derive the empty clause. The total length of this *SR-I* derivation is $f(n) + 3n + 2 = f(n+1)$. □

Krishnamurthy exhibits other interesting examples of sets of clauses where the symmetry rule produces significant shortening of proofs. Nevertheless, it is not very hard to defeat the symmetry rule. To do this, we can employ the sets of clauses based on graphs introduced by Tseitin [18].

If G is a graph, then a *labeling* G' of G is an assignment of distinct variables to the edges of G, together with an assignment Charge(x) $\in \{0, 1\}$ to each of the vertices x in G. If G' is a labeled graph, and x a vertex in G', and $l_1, \ldots, l_k$ the literals labeling the edges attached to x, then Clauses(x) is the set of clauses equivalent to the conjunctive normal form of the modulo 2 equation $l_1 \oplus \cdots \oplus l_k = \text{Charge}(x)$. That is to say, a clause C in Clauses(x) contains the literals $l_1, \ldots, l_k$, and the parity of the number of complemented literals in $\{l_1, \ldots, l_k\}$ in C is opposite to that of Charge(x). The set of clauses Clauses(G') is the union of all the sets Clauses(x), for x a vertex in G. Let us write Charge(G') for the sum modulo 2 of the charges on the vertices of G'; a labeling G' of G is *even* or *odd* depending on whether Charge(G') is 0 or 1.

If G is a connected graph, then Clauses(G') is contradictory if the labeling G' is odd. If we sum the left-hand side of all the mod 2 equations associated with the vertices of G, the result is 0, because each literal is attached to exactly two vertices, and so appears twice in the sum. On the other hand, the right-hand side sums to 1, by assumption, so the set of equations, and so the set of clauses, is contradictory.

It is easy to see that any symmetry of Clauses(G') obtained by permuting variables arises from a symmetry of the underlying graph G. We can obtain a lower bound for the length of symmetric resolution refutations by constructing a family of graphs with no symmetries for which the corresponding set of clauses Clauses(G') require long resolution refutations.

The graphs used in the lower bound for resolution are the expander graphs used by Galil [11] to prove an exponential lower bound for regular resolution, with a small modification to simplify the proof. The expander graph H_m is a simple bipartite graph in which each vertex has degree at most 5 and each side contains m^2 vertices (for brevity we write $n = m^2$). The particular family of expander graphs used here was first defined by Margulis [16]. The exact definition of the graphs is not needed; for the lower bound all that is needed is the expanding property proved by Margulis and stated in the next lemma.

Lemma 3.3. *There is a constant $d > 0$ such that if V_1 is contained in one side of H_m, $|V_1| \leqslant n/2$, and V_2 consists of all the vertices in the other side of H_m that are connected to vertices of V_1 by an edge, then $|V_2| \geqslant (1+d)|V_1|$.*

Proof. See Gabber and Galil [10], who also provide a numerical lower bound for the expansion factor d. □

The graph G_m is obtained from H_m by the following modifications. We add $n-1$ edges to each side of the graph so that each side forms a connected chain. The graph we obtain by adding the side edges may still have some symmetries. To destroy any remaining symmetries, add a single vertex and a single edge attaching it to the last vertex on one side; call the resulting graph G_m. Let Ω_m be Clauses(G_m); Ω_m contains at most $128n$ clauses of length at most 7, so the entire set of clauses has size O(n).

Theorem 3.4. *There is a constant $c > 1$ such that for sufficiently large m any SR-I refutation of Ω_m contains c^n distinct clauses.*

Proof. Since the set of clauses Ω_m has no symmetries under the group of all variable permutations, no non-trivial application of the symmetry rule is possible. The argument in Urquhart [19,20] shows that there is a constant $c > 1$ so that for sufficiently large m, any resolution refutation of Ω_m contains c^n distinct clauses (actually, the graphs used in the papers cited above do not contain the extra vertex and edge used to destroy symmetries, but it is easy to see that this addition does not affect the original arguments). □

4. The complementation rule

The sets of clauses based on graphs used in the previous section to provide lower bounds on symmetrical resolution have efficient refutations if we enlarge the symmetry group to include complementations.

Theorem 4.1. *If G' is a connected graph with an odd labelling, with n vertices and m edges, then there is an SRC-I refutation of Clauses(G') of length $2m - n + 1$.*

Proof. Choose a spanning tree T for G. Starting from the leaves of T, use the resolution rule on edges of the tree to derive a clause α in which the only variables are those not occurring in the spanning tree. This takes $n - 1$ resolution steps. Choose an edge e not in the spanning tree; let us suppose that $\alpha = \beta l$, where l contains the variable attached to e. Let C be a cycle to which e belongs, but all the other edges belong to T. Clauses(G') is invariant under the transformation that interchanges the variables in the cycle C with their complements (such a transformation leaves the parity condition unchanged). Hence, we can derive $\beta\bar{l}$ by the complementation rule, and so β by resolution. Repeating this sequence of moves for each edge not in the spanning tree, we can derive the empty clause in a total of $(n - 1) + 2(m - n + 1) = 2m - n + 1$ steps in the *SRC-I* system. □

To defeat the complementation rule, we can employ sets of clauses based on graphs without a perfect matching. If G is a graph in which every vertex has degree at least 3, then $PM(G)$ has no non-trivial symmetries under the complementation group. It follows that if the graph G itself has no non-trivial automorphisms, then $PM(G)$ has no non-trivial automorphisms under the group of permutations and complementations.

Hence, to prove an exponential lower bound on the size of *SRC-I* refutations, it is sufficient to find a sequence of graphs having no perfect matchings, in which all vertices are of degree at least three, where the clauses $PM(G)$ require exponentially long resolution refutations. Here, we show that such examples can be found easily by using ideas from the theory of random graphs. The following important theorem of Wright [22] provides us with a large stock of graphs of the kind that we need. Let $U_M = U_{n,M}$ be the number of unlabeled graphs with n vertices and M edges, let $L_M = L_{n,M}$ be the number of labeled graphs: $L_M = \binom{N}{M}$, where $N = \binom{n}{2}$.

Theorem 4.2. *Suppose* $\omega(n) \to \infty$ *and*

$$n \log n/2 + \omega(n)n \leqslant M \leqslant N - n \log n/2 - \omega(n)n.$$

Then

$$U_M \sim L_M/n!$$

Proof. See [3, Ch. IX, Theorem 4]. □

Corollary 4.3. *If* $\omega(n)$ *and* M *satisfy the conditions of Theorem* 4.2, *then almost every labeled graph with* n *vertices and* M *edges has a trivial automorphism group.*

Proof. If the automorphism group of an unlabeled graph is non-trivial then the graph is isomorphic to at most $n!/2$ labeled graphs. Hence the result of Theorem 4.2 implies that almost every unlabeled graph with n vertices and M edges (where M satisfies the stated inequalities) has a trivial automorphism group, so the same conclusion follows for the corresponding labeled graphs. □

There are two commonly used models of random graphs. In the first model, the probability space consists of all graphs with n vertices and M edges, with the uniform distribution. In the second model, the independent edge model, the edges in a graph with n vertices appear independently with probability p.

Lemma 4.4. *Almost all graphs with* n *vertices and* $M = \lfloor 0.99N \rfloor$ *edges have minimum degree at least* $9n/10$.

Proof. Consider the independent edge model where an edge appears with probability $p = 0.99$. The degree of a vertex x in a random graph in this model has a binomial distribution. By the Chernoff bound on the tail of the binomial distribution [3, pp. 11–12],

$$\mathbf{Pr}[\text{Degree}(x) < 9n/10] < 2\mathrm{e}^{-n/100}.$$

It follows that almost all random graphs in the independent edge model have minimum degree at least $9n/10$. Since this last property is monotone increasing, we can transfer the result just proved to the first model of random graphs, where $M = \lfloor 0.99N \rfloor$ by using the results of Bollobás [3, Ch. II, Theorem 2]. □

In view of the last two lemmas, to prove a lower bound for *SRC-I*, it is sufficient to prove a lower bound for the ordinary resolution system using the sets of clauses $PM(G)$, for appropriate graphs G. We demonstrate such a lower bound for almost all sets of clauses $PM(G)$, where G is a graph with n vertices and $M = \lfloor 0.99N \rfloor$ edges, where $N = \binom{n}{2}$, and n is odd. The lower bound argument is adapted from the work of Buss and Turán [4] generalizing Haken's lower bound for the pigeon-hole clauses [12]. In the remainder of this section, all graphs G are assumed to have n vertices, where n

is odd (so that G has no perfect matching), and G has minimum degree $\lfloor dn \rfloor$, where $d = 9/10$.

Let P_{xy} be the propositional variable associated with the vertices x and y in the graph G. A matching M in G determines an assignment of truth values to the propositional variables P_{xy} by the rule: If x is matched with y in M, then P_{xy} is true, otherwise P_{xy} is false. We shall identify a matching with the assignment it determines, so that if C is a clause, we write $M(C)$ for the truth value assigned to C by M. We denote by $M(r)$ the set of matchings M with $|M| = r$. If C is a clause expressed in terms of the matching variables P_{xy}, and x is a vertex, we write $E(C,x)$ for the set $\{y \mid P_{xy} \in C\}$.

Lemma 4.5. *If N is a matching in G, and $0 < c < d$, then in any refutation of $PM(G)$, there is a clause C such that*

1. $N(C) = 0$.
2. *If x is not covered by N, then $|E(C,x)| \leqslant \lfloor cn \rfloor$.*
3. *There is exactly one vertex x not covered by N so that $|E(C,x)| = \lfloor cn \rfloor$.*

Proof. In any refutation of $PM(G)$, there is a subsequence of clauses $C_1, \ldots, C_t$ so that $M(C_i) = 0$, each C_i is a premiss for C_{i+1}, C_1 is an initial clause and $C_t = \Lambda$. Because M is a matching, $C_1 = \bigvee\{P_{xy} \mid \{x,y\} \in E(G)\}$ for some vertex x not covered by M. Let C be the last clause in the sequence so that for some x in G not covered by M, $|E(C,x)| \geqslant \lfloor cn \rfloor$. Then C satisfies all three conditions of the Lemma because a resolution inference can eliminate at most one variable from a clause. □

For N a matching, and R a resolution refutation of $PM(G)$, we define C_N to be the first clause in R satisfying the conditions of Lemma 4.5, where $c = \frac{1}{5}$. For $M \in M(\lfloor n/5 \rfloor)$, let C^M be the first clause in the refutation of the form C_N where $N \in M(\lfloor dn/2 \rfloor)$ and $M \subseteq N$. We say that a clause of the form C^M, $M \in M(\lfloor n/5 \rfloor)$, is a *complex clause*.

Any matching M in G, where $|M| < \lfloor dn/2 \rfloor$, can be extended to a matching of size $\lfloor dn/2 \rfloor$. It follows from this that for any $M \in M(\lfloor n/5 \rfloor)$, there is a complex clause C^M in a refutation of $PM(G)$. We shall prove an exponentially small bound on the fraction of M for which a given complex clause is C^M; this will imply an exponential lower bound on the size of resolution refutations of $PM(G)$.

Lemma 4.6. *If C is a complex clause in a refutation of $PM(G)$, then there are at least $\lfloor n/20 \rfloor + 1$ vertices $x \in G$ so that either $\sim P_{xy} \in C$, for some y, or $|E(C,x)| \geqslant \lfloor n/5 \rfloor$.*

Proof. Let C^M be a complex clause, for $M \in M(\lfloor n/5 \rfloor)$, $N \in M(\lfloor dn/2 \rfloor)$, where $M \subseteq N$, $N(C^M) = 0$ and $C_N = C^M$. Define

$$V^- = \{x \in G \mid \exists y (\sim P_{xy} \in C^M)\},$$

$$V^+ = \{x \in G \mid x \not\in V^- \wedge |E(C^M,x)| \geqslant \lfloor n/5 \rfloor \wedge x \text{ is covered by } N\},$$

$x_0 =$ the unique vertex not covered by N such that $|E(C^M, x_0)| = \lfloor n/5 \rfloor$.

The sets V^-, V^+ and $\{x_0\}$ are pairwise disjoint. We wish to show that $|V^-| + |V^+| \geqslant \lfloor n/20 \rfloor$. If this condition fails, then we claim that there is an edge $\{y,z\} \in N \setminus M$ such that: (1) $P_{x_0 y}$ does not occur in C^M, and (2) $y \notin V^- \cup V^+$. Condition (1) rules out at most $\lfloor n/5 \rfloor$ edges in $N \setminus M$, while by our assumption (2) rules out less than $\lfloor n/20 \rfloor$ edges. On the other hand,

$$|N \setminus M| \geqslant \lfloor dn/2 \rfloor - \lfloor n/5 \rfloor = \lfloor 9n/20 \rfloor - \lfloor n/5 \rfloor.$$

Since $\lfloor n/5 \rfloor + \lfloor n/20 \rfloor \leqslant \lfloor 9n/20 \rfloor - \lfloor n/5 \rfloor$, the claim follows. Let $N' = (N \setminus \{yz\}) \cup \{x_0 y\}$. By construction, neither of the variables P_{yz} nor $P_{x_0 y}$ occur in C^M, so that $N'(C^M) = 0$. Thus, $M \subseteq N'$, $N'(C^M) = 0$, and if x is not covered by N' then $|E(C,x)| < \lfloor n/5 \rfloor$. Thus, $C_{N'}$ is a clause preceding C^M in the refutation, in contradiction to the definition of C^M. □

Theorem 4.7. *There is a $c > 1$ so that for almost all graphs G with n vertices and $0.99N$ edges, where n is odd and $N = \binom{n}{2}$, any SRC-I refutation of $PM(G)$ contains at least c^n distinct clauses, for sufficiently large n.*

Proof. By Corollary 4.3 and Lemma 4.4, almost all graphs G satisfying the conditions of the theorem have minimum degree at least $9n/10$, and have no non-trivial automorphisms. Hence, it is sufficient to show that if G is a graph with n vertices, of minimum degree $9n/10$, where n is odd, then at least c^n resolution steps are required in a resolution refutation of $PM(G)$.

Let M be a matching in $M(\lfloor n/5 \rfloor)$, and C^M the complex clause corresponding to M. We show that the matchings M' for which $C^M = C^{M'}$ form an exponentially small fraction of all matchings in $M(\lfloor n/5 \rfloor)$.

A matching $M \in M(\lfloor n/5 \rfloor)$ is determined by the following process. First, choose a set D of $\lfloor n/5 \rfloor$ vertices in G, then choose a set of $\lfloor n/5 \rfloor$ vertices that are matched with the vertices in D. By Lemma 4.6, there is a set H of $\lfloor n/20 \rfloor$ vertices so that for $x \in H$, either $\sim P_{xy} \in C^M$ for some y, or $|E(C^M, x)| \geqslant \lfloor n/5 \rfloor$. If $x \in D \cap H$, and x has degree f, then there are at most $f - \lfloor n/5 \rfloor$ choices for a vertex y so that $\{x, y\} \in M'$ and $M'(C^M) = 0$. On the other hand, without the condition that $M'(C^M) = 0$, there are at least $f - 2\lfloor n/20 \rfloor$ choices for a vertex y so that $\{x, y\} \in M'$. Hence, the ratio of the number of matchings in $M(\lfloor n/5 \rfloor)$ such that $C^{M'} = C^M$ to $|M(\lfloor n/5 \rfloor)|$ is bounded by

$$\sum_{i=0}^{l} \binom{k}{i} \binom{n-k}{l-i} \binom{n}{l}^{-1} p^i,$$

where $k = \lfloor n/20 \rfloor$, $l = \lfloor n/5 \rfloor$ and $p = 9/10$, since

$$\frac{f - \lfloor n/5 \rfloor}{f - 2\lfloor n/20 \rfloor} \leqslant 9/10$$

for n sufficiently large.

We can find a bound for this sum by adapting Chvátal's elegant bound [5] for the tail of the hypergeometric distribution. First, we establish an inequality

$$\begin{aligned}
&\sum_{i=0}^{l-j} \binom{k}{i} \binom{n-k}{l-i} \binom{l-i}{j} \binom{n}{l}^{-1} \\
&\quad = \binom{n-k}{j} \sum_{i=0}^{l-j} \binom{k}{i} \binom{n-k-j}{l-i-j} \binom{n}{l}^{-1} \\
&\quad = \binom{n-k}{j} \binom{n-j}{l-j} \binom{n}{l}^{-1} \\
&\quad = \binom{n-k}{j} \binom{l}{j} \binom{n}{j}^{-1} \\
&\quad \leqslant \binom{l}{j} \left(\frac{n-k}{n}\right)^{j}.
\end{aligned}$$

The bound on the ratio follows from this inequality by the computation

$$\begin{aligned}
&\sum_{i=0}^{l} \binom{k}{i} \binom{n-k}{l-i} \binom{n}{l}^{-1} p^{i} \\
&\quad = p^{l} \sum_{i=0}^{l} \binom{k}{i} \binom{n-k}{l-i} \binom{n}{l^{-1}} \sum_{j=0}^{l-i} \binom{l-i}{j} \left(\frac{1}{9}\right)^{j} \\
&\quad = p^{l} \sum_{j=0}^{l} \sum_{i=0}^{l-j} \binom{k}{i} \binom{n-k}{l-i} \binom{l-i}{j} \binom{n}{l}^{-1} \left(\frac{1}{9}\right)^{j} \\
&\quad \leqslant p^{l} \sum_{j=0}^{l} \binom{l}{j} \left(\frac{n-k}{n}\right)^{j} \left(\frac{1}{9}\right)^{j} \\
&\quad = p^{l} \left(1 + \frac{n-k}{9n}\right)^{l} \\
&\quad = \left(p + \frac{n-k}{10n}\right)^{l}.
\end{aligned}$$

Since $p+(n-k)/10n < 0.996$ for sufficiently large n, it follows that there is a $c > 1$ so that any resolution refutation of $PM(G)$ contains c^n complex clauses, for n sufficiently large. □

5. The extension rule

In his paper, introducing the symmetry rule [15], Krishnamurthy compares the power of symmetry with that of extension. He discusses a number of interesting examples of sets of clauses where the symmetry rule produces an exponential speedup over the simple resolution system. In all cases except one (this exception is discussed below), he shows that there are also efficient refutations using the extension rule. In the present section, we generalize these results by showing that extended resolution can simulate the system *SRC-I* efficiently. In proving this simulation result, it is convenient to use a more flexible form of proof system.

Let us fix on a language for propositional logic, say the language based on the connectives $\{\vee, \wedge, \rightarrow, \equiv, \neg\}$. We define a *Frege system* to consist of a finite set of schematic inference rules that is sound and complete for inferences in two-valued logic. The familiar text-book systems of logic with a finite number of axiom schemes, together with the rule of *modus ponens* are typical examples of Frege systems.

Let $\mathscr{F}$ be a Frege system. If $\Gamma \cup \{A\}$ is a set of formulas of $\mathscr{F}$, then a sequence of formulas ending in A is a *proof of A from Γ in $\mathscr{F}$ with extension* if each formula in the sequence either belongs to Γ, or is inferred from earlier formulas in the sequence by one of the rules of $\mathscr{F}$ or has the form $P \equiv B$, where P is a variable not in appearing in $\Gamma \cup \{A\}$, nor in any earlier formula in the sequence. In the case of a step of the last type, the variable is said to be introduced by the *extension rule*. We shall refer to the system with the addition of the extension rule as an *extended Frege system.*

The substitution rule is another natural rule that appears in the earliest systems for propositional logic, such as those of Frege [9] and Whitehead and Russell [21]. The rule allows the inference of $\sigma(A)$ from A, where σ is any substitution (that is, σ is a map from variables into formulas).

To compare the relative efficiency of proof systems for the tautologies, we define a notion of efficient simulation. If S_1 and S_2 are both proof systems for the classical tautologies, then we say that S_1 *p-simulates* S_2 if whenever there is a proof P_2 of a tautology A in the system S_2 there is a proof P_1 of A in the system S_1, where the size of P_1 is bounded by a fixed polynomial in the size of P_1 (the size of a proof is defined to be the number of occurrences of symbols in it). If S_1 and S_2 p-simulate each other, then we say that they are *p-equivalent.*

(A more restrictive definition of p-simulation, requiring an efficient translation function between the two systems, is used by Cook and Reckhow [7] and Urquhart [20]).

It is not hard to prove that a Frege system with the addition of the substitution rule can p-simulate the same system with the extension rule added. Surprisingly, the converse simulation also holds, a result due to Dowd [8].

Theorem 5.1. *Any two systems from the following classes are p-equivalent*: *extended resolution*, *extended Frege systems*, *Frege systems with substitution.*

Proof. See [14]. □

The p-equivalence of extended resolution and Frege systems with extension now allows an easy simulation of the symmetry rule.

Theorem 5.2. *Extended resolution p-simulates the system SRC-I.*

Proof. Let R be an *SRC-I* refutation of a set of clauses Γ. We show by induction on the length of R that if the clause C is derived in n steps in the *SRC-I* system, then the implication $\bigwedge \Gamma \to C$ is derivable in a Frege system with substitution, $\mathscr{FS}$, by a proof of size $n^{O(1)}$.

A resolution inference is easy to simulate in $\mathscr{FS}$, so we need to deal only with the case of a symmetry inference. Let us suppose that σ is an operation in the group of permutations and complementations such that $\sigma(\Gamma) = \Gamma$, and that $\sigma(C)$ is inferred by the symmetry rule from C. By assumption, we have an $\mathscr{FS}$ proof of $\bigwedge \Gamma \to C$ of size $n^{O(1)}$. By using the substitution rule, and eliminating double negations, we can derive the implication $\bigwedge \Gamma \to \sigma(C)$; the number of steps required is linear in the length of the implication.

The proof of p-simulation is completed by employing the p-simulation of $\mathscr{FS}$ by extended resolution. □

Krishnamurthy in his paper shows that there are polynomial-size symmetric resolution refutations of sets of clauses derived from Ramsey's theorem. He conjectures that they have polynomial-size extended resolution refutations; the theorem just proved shows that they do.

6. Symmetries of random sets of clauses

How useful is the symmetry rule in practice in deciding cases of the satisfiability problem? Although the results above suggest that in some cases, the symmetry rule may prove very efficient, there are at least two drawbacks to its use. The first is that checking for symmetries is known to be computationally expensive. The second is that the existence of global symmetries in a randomly chosen set of clauses is improbable, provided the set does not contain too few or too many clauses. In this section, we prove a result to this effect; it follows as a corollary that for sets of clauses with the number of clauses within a certain range, almost all such sets require long *SR-I* refutations.

We shall consider sets of clauses constructed from a set of n variables. In the remainder of this section, by a *clause* we shall always mean a clause containing three literals in which all the variables are distinct (thus ignoring tautologous clauses). A set containing M clauses will be said to have *size* M. We shall consider the action of the symmetric group S_n of all permutations of the set of variables $\{p_1, \ldots, p_n\}$. The group S_n acts in a natural way on the set of all clauses, and hence on sets of clauses. If two sets of clauses are equivalent under S_n, then (by analogy with graph theory) we shall say that they represent the same unlabeled clause-set. In other words, the family of unlabeled clause-sets in n variables corresponds to the orbits of S_n acting on the set of all clause-sets; we shall refer to clause-sets in the usual sense as *labeled* clause-sets.

We denote by N the number of all clauses in n variables, so that $N = 8\binom{n}{3}$. We write $L_M = L_{n,M} = \binom{N}{M}$ for the number of labeled clause-sets of size M in n variables, and $U_M = U_{n,M}$ for the number of unlabeled clause-sets of size M in n variables. Our main aim in this section is to show that under suitable conditions on M we have

$$U_M \sim L_M/n! = \binom{N}{M}/n!. \tag{1}$$

Since every unlabeled clause-set is isomorphic to a set of at most $n!$ labeled clause-sets,

$$U_M \geqslant L_M/n!.$$

By the argument of Corollary 4.3, (1) implies that almost every clause-set of size M (labeled or unlabeled) has a trivial automorphism group.

For a permutation ρ in S_n, let $\mathrm{Fix}(\rho)$ be the set of labeled clause-sets of size M invariant under ρ and put $I(\rho) = |\mathrm{Fix}(\rho)|$. By Burnside's lemma,

$$U_M = \frac{1}{n!} \sum_{\rho \in S_n} I(\rho).$$

For the identity permutation $1 \in S_n$, we have $I(1) = L_M$, so (1) holds if and only if

$$\sum_{\substack{\rho \in S_n \\ \rho \neq 1}} I(\rho) = \mathrm{o}(L_M). \tag{2}$$

The following theorem is an adaptation of Wright's theorem for graphs (Theorem 4.2); the result we prove here actually corresponds to a weaker version of Wright's theorem, which is best possible. The proof we give is adapted from Bollobás's proof of the corresponding result for graphs [3, Ch. IX, Theorem 3].

Theorem 6.1. *If $c > 1$ is a constant and*

$$cn \log n \leqslant M \leqslant N - cn \log n,$$

then

$$U_m \sim L_M/n!.$$

Proof. Let ρ be a permutation in S_n. As a permutation acting on the set of variables, it has m_j orbits of size j, $j = 1,\ldots,n$, and as a permutation acting on the set of clauses, it has M_j orbits of size j, $j = 1,\ldots,N$. Thus we have

$$m_1 + 2m_2 + \cdots + nm_n = n$$

and

$$M_1 + 2M_2 + \cdots + NM_N = N.$$

Denote by $S_n^{(m)}$ the set of all permutations moving m variables, so fixing $n - m$ variables; note that $n - m = m_1$. Then $S_n^{(0)} = \{1\}$ and $S_n^{(1)} = \emptyset$. If $\rho \in S_n^{(m)}$, then the m variables moved by ρ can be selected in $\binom{n}{m}$ ways, and there are at most $m!$ permutations moving a fixed set of m variables. Hence

$$|S_n^{(m)}| \leqslant \binom{n}{m} m! = n^{\underline{m}}, \tag{3}$$

where $n^{\underline{m}}$ denotes the falling factorial $n(n-1)(n-2)\ldots(n-m+1)$.

Since a clause-set is invariant under ρ if and only if it is the union of a set of orbits of ρ acting on the set of clauses, it follows that

$$I(\rho) = \left[\prod_{j=1}^{N} (1 + X^j)^{M_j} \right]_M ,$$

where $[F(X)]_k$ is the coefficient of X^k in the polynomial $F(X)$.

If a polynomial $F(X)$ has non-negative coefficients and $x > 0$, then

$$[F(X)]_k \leqslant x^{-k} F(x).$$

Setting $x = p/q$, where $p = M/N$ and $q = 1 - p$, we obtain from this inequality

$$\begin{aligned} I(\rho) &\leqslant (p/q)^{-M} \prod_{j=1}^{N} \{1 + (p/q)^j\}^{M_j} \\ &= p^{-M} q^{M-M_1} \prod_{j=2}^{N} \{1 + (p/q)^j\}^{M_j} \\ &\leqslant p^{-M} q^{M-M_1} \prod_{j=2}^{N} \{1 + (p/q)^2\}^{jM_j/2} \\ &= p^{-M} q^{-(N-M)} (p^2 + q^2)^{(N-M_1)/2}. \end{aligned}$$

The second inequality holds since $1 + x^j \leqslant (1 + x^2)^{j/2}$ for any real number x and $j \geqslant 2$, and the second equality is true since $\sum_{j=1}^{N} jM_j = N$.

Let $\rho \in S_n^{(m)}$, $m \geqslant 2$; we wish to bound M_1 from above. In a clause fixed under ρ, there are three possibilities for the cycle structure of the set of variables in the clause. All three variables may be fixed, or one may be fixed, and the other two are mapped into each other, or all three may form a cycle of size three. Hence,

$$M_1 = 8 \binom{m_1}{3} + 4m_1 m_2 + 2m_3. \tag{4}$$

Two cases arise here. In the first case, where $m_1 = 0$, the first two terms on the right-hand side of (4) are zero, so $M_1 = 2m_3$, hence $M_1 \leqslant 2n/3$. In the second case, $m_1 > 0$. In this latter case, if $m_3 > 1$, then the permutation ρ contains at least two cycles containing three variables. Let ρ' be the permutation resulting from ρ by replacing these two cycles by three cycles of size two containing the same variables. Then

$$\begin{aligned} M_1' &= 8 \binom{m_1}{3} + 4m_1(m_2 + 2) + 2(m_3 - 1) \\ &= M_1 + 6, \end{aligned}$$

so that we can assume that ρ contains at most one cycle of length three. Hence

$$\begin{aligned} M_1 &\leqslant 8\binom{m_1}{3} + 4m_1m_2 + 2 \\ &\leqslant 8\binom{n-m}{3} + 4(n-m)m/2 + 2 \\ &= 8\binom{n-m}{3} + 2(n-m)m + 2. \end{aligned}$$

Since this last expression dominates $2n/3$ for $n > 1$ and $m > 2$, we can assume $m_1 > 0$ so that

$$\begin{aligned} N - M_1 &\geqslant 8\binom{n}{3} - 8\binom{n-m}{3} - 2(n-m)m - 2 \\ &= 2m[2m^2/3 + 2n^2 + 3m + 4/3 - 2mn - 5n - 1/m] \\ &= N(m). \end{aligned} \tag{5}$$

By estimating binomial coefficients [3, p. 4], we have

$$L_M \geqslant 8^{-1/2} p^{-M} q^{-(N-M)} (pqN)^{-1/2}.$$

Hence, by (3) we have

$$\begin{aligned} \sum_{\rho \in S_n^{(m)}} I(\rho)/L_M &\leqslant |S_n^{(m)}|(p^2+q^2)^{N(m)/2} 8^{1/2} (pqN)^{1/2} \\ &\leqslant n^{\underline{m}} (p^2+q^2)^{N(m)/2} 2n^{3/2} \\ &\leqslant 2n^{m+3/2}(p^2+q^2)^{N(m)/2}. \end{aligned} \tag{6}$$

Here, we have used the inequality

$$pqN \leqslant N/4 \leqslant n^3/3.$$

We now estimate $\log(p^2+q^2)$ by making use of the restriction on M. By assumption,

$$\frac{3c\log n}{4(n-1)(n-2)} \leqslant p \leqslant 1 - \frac{3c\log n}{4(n-1)(n-2)}.$$

Hence,

$$p^2 + q^2 \leqslant 1 - \frac{3c\log n}{2(n-1)(n-2)}\left(1 - \frac{3c\log n}{4(n-1)(n-2)}\right).$$

Thus for n sufficiently large,

$$\begin{aligned} \log(p^2+q^2) &\leqslant -\frac{3c\log n}{2(n-1)(n-2)} + \mathrm{O}\left(c^3\left(\frac{\log n}{(n-1)(n-2)}\right)^3\right) \\ &\leqslant -\frac{3c\log n}{2n^2}. \end{aligned} \tag{7}$$

Combining inequalities (6) and (7), we have

$$\sum_{\rho \in S_n^{(m)}} I(\rho)/L_M \leqslant 2n^{m+3/2} \exp\{-(3cm/2)(\log n)Q\},$$

where

$$Q = [2m^2/3n^2 + 2 + 3m/n^2 + 4/3n^2 - 2m/n - 5/n - 1/mn^2].$$

It is not hard to check that for sufficiently large n,

$$(3cm/2)Q \geqslant m + 3/2 + c$$

for all m, $2 \leqslant m \leqslant n$. Hence if n is large enough, then

$$\sum_{\rho \in S_n^{(m)}} I(\rho)/L_M \leqslant 2n^{-c}$$

so that

$$\sum_{\rho \neq 1} I(\rho)/L_M \leqslant \sum_{m=2}^{n} \sum_{\rho \in S_n^{(m)}} I(\rho)/L_M \leqslant n^{1-c} = \mathrm{o}(1),$$

showing that (2) holds. □

We can use the above results to obtain a lower bound on randomly generated clause-sets by combining them with a recent result of Beame and Pitassi [1]. Simplifying and extending earlier work of Chvátal and Szemerédi [6], they proved the following theorem about random sets of clauses in 3-CNF, as a special case of a general theorem about random sets of clauses in k-CNF.

Theorem 6.2. *Let* $\varepsilon > 0$. *Then almost all clause-sets of size at most* $n^{8/7-\varepsilon}$ *have no resolution refutation of size less than* $2^{\Omega(n^{\varepsilon/6})}$.

In combination with our previous results, this immediately yields a lower bound on *SR-I* refutations of random clause-sets.

Theorem 6.3. *Let* $c > 1$, $\varepsilon > 0$. *Then almost all clause-sets of size between* $cn \log n$ *and* $n^{8/7-\varepsilon}$ *are contradictory and require SR-I refutations of size at least* $2^{\Omega(n^{\varepsilon/6})}$.

In contrast to Theorem 6.1, it is to be expected that a random set of clauses should contain a lot of local symmetries. Furthermore, the lower bound arguments offered earlier for the global symmetry rules do not seem to adapt in any obvious way to the local symmetry rules. The complexity of the systems *SR-II* and *SRC-II* remain as challenging open problems.

7. For Further Reading

The following reference is also of interest to the reader: [17]

Acknowledgements

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

References

[1] P. Beame, T. Pitassi, Simplified and improved resolution lower bounds, in: Proceedings of the 37th Annual IEEE Symposium on the Foundations of Computer Science, 1996, pp. 274–282.

[2] B. Bollobás, Graph Theory, Springer, Berlin, 1979.

[3] B. Bollobás, Random Graphs, Academic Press, New York, 1985.

[4] S.R. Buss, G. Turán, Resolution proofs of generalized pigeonhole principles, Theoret. Comput. Sci. (1988) 311–317.

[5] V. Chvátal, The tail of the hypergeometric distribution, Discrete Math. 25 (1979) 285–287.

[6] V. Chvátal, E. Szemerédi, Many hard examples for resolution, J. Assoc. Comput. Machinery 35 (1988) 759–768.

[7] S.A. Cook, R.A. Reckhow, The relative efficiency of propositional proof systems, J. Symbol. Logic 44 (1979) 36–50.

[8] M. Dowd, Model-theoretic aspects of $\mathscr{P} \neq \mathscr{NP}$, unpublished MS, 1985.

[9] G. Frege, Begriffsschrift, eine der arithmetischen nachgebildete Formelsprache des reinen Denkens, Nebert, Halle, 1879.

[10] O. Gabber, Z. Galil, Explicit constructions of linear size superconcentrators, in: Proceedings of the 20th Annual Symposium on Foundations of Computer Science, IEEE, New York, 1979, pp. 364–370.

[11] Z. Galil, On the complexity of regular resolution and the Davis–Putnam procedure, Theoret. Comput. Sci. 4 (1977) 23–46.

[12] A. Haken, The intractability of resolution, Theoret. Comput. Sci. 39 (1985) 297–308.

[13] M.A. Harrison, Introduction to Switching and Automata Theory, McGraw-Hill, New York, 1965.

[14] J. Krajíček, P. Pudlák, Propositional proof systems, the consistency of first order theories and the complexity of computations, J. Symbol. Logic 54 (1989) 1063–1079.

[15] B. Krishnamurthy, Short proofs for tricky formulas, Acta Informatica 22 (1985) 253–275.

[16] G.A. Margulis, Explicit construction of concentrators, Problems Inform. Transmission 9 (1973) 325–332.

[17] J. Siekmann, G. Wrightson (Eds.), Automation of Reasoning, Springer, New York, 1983.

[18] G.S. Tseitin, On the complexity of derivation in propositional calculus, in: A.O. Slisenko (Ed.), Studies in Constructive Mathematics and Mathematical Logic, Part 2, Consultants Bureau, New York, 1970, pp. 115–125. Reprinted in J. Siekmann, G. Wrightson (Eds.), Automation of Reasoning, Springer, New York, 1983, vol. 2, pp. 466–483.

[19] A. Urquhart, Hard examples for resolution, J. Assoc. Comput. Machinery 34 (1987) 209–219.

[20] A. Urquhart, The complexity of propositional proofs, Bull. Symbol. Logic 1 (1995) 425–467.

[21] A.N. Whitehead, B. Russell, Principia Mathematica, second ed., vols. 1–3, Cambridge University Press, Cambridge, 1925, pp. 1910–1913.

[22] E.M. Wright, Graphs on unlabelled nodes with a given number of edges, Acta Math. 126 (1971) 1–9.