Many Hard Examples for Resolution

VAŠEK CHVÁTAL
Rutgers University, New Brunswick, New Jersey

AND

ENDRE SZEMERÉDI
Rutgers University, New Brunswick, New Jersey and Hungarian Academy of Sciences,
Budapest, Hungary

Abstract. For every choice of positive integers c and \( k \), such that \( k \geq 3 \) and \( c2^{-k} \geq 0.7 \), there is a positive number \( \epsilon \) such that, with probability tending to 1 as \( n \) tends to \( \infty \), a randomly chosen family of \( cn \) clauses of size \( k \) over \( n \) variables is unsatisfiable, but every resolution proof of its unsatisfiability must generate at least \((1 + \epsilon)n\) clauses.

Categories and Subject Descriptors: F.2.2 [Analysis of Algorithms and Problem Complexity]: Non-numerical Algorithms and Problems—complexity of proof procedures

General Terms: Algorithm, Theory, Verification

Additional Key Words and Phrases: Resolution, satisfiability

1. Introduction

A truth assignment \( f \) is a mapping \( f \) that assigns 0 or 1 to each variable in its domain. For each such variable \( x \), we define \( f(\overline{x}) = 1 - f(x) \) and refer to both \( x \) and \( \overline{x} \) as literals; a clause is a set of literals. A truth assignment \( f \) satisfies a clause \( C \) if and only if \( f(w) = 1 \) for at least one literal \( w \) in \( C \); the assignment \( f \) satisfies a family \( F \) of clauses if and only if it satisfies every clause in \( F \). A family of clauses is called satisfiable if it is satisfied by at least one truth assignment; otherwise, it is called unsatisfiable.

If \( A, B \) are clauses and \( x \) is a variable such that \( x \in A, \overline{x} \in B \), then the clause \((A - \{x\}) \cup (B - \{\overline{x}\})\) is called a resolvent of \( A \) and \( B \). (It is often required that \( x \notin B, \overline{x} \notin A \) and that there be no variable \( y \) other than \( x \) such that \( y \in A \cup B \), \( \overline{y} \notin A \cup B \). The definition we use is simpler and its adoption certainly brings about no loss of generality in what we are about to do.) Obviously, every truth assignment satisfying both \( A \) and \( B \) satisfies all their resolvents.

Authors' present addresses: V. Chvátal, Department of Computer Science, Rutgers University, New Brunswick, NJ 08903; E. Szemerédi, Department of Computer Science, Rutgers University, New Brunswick, NJ 08903 or Mathematical Institute, Hungarian Academy of Science, Reáltanoda utca 13-15, Budapest, Hungary.

Permission to copy without fee all or part of this material is granted provided that the copies are not made or distributed for direct commercial advantage, the ACM copyright notice and the title of the publication and its date appear, and notice is given that copying is by permission of the Association for Computing Machinery. To copy otherwise, or to republish, requires a fee and/or specific permission.

© 1988 ACM 0004-5411/88/1000-0759 $01.50

Now let $F$ be a family of clauses and $C_1, C_2, \ldots, C_N$ be a sequence of clauses such that

—each $C_k$ belongs to $F$ or is a resolvent of some $C_i, C_j$ such that $i < k, j < k$,
—$C_N$ is the empty clause.

Straightforward induction on $k$ shows that every truth assignment satisfying $F$ must satisfy each $C_k$; since no truth assignment satisfies the empty clause $C_N$, it follows that $F$ is unsatisfiable. For this reason, the sequence $C_1, C_2, \ldots, C_N$ is called a resolution proof of unsatisfiability of $F$. (It is also easy to show that every unsatisfiable $F$ admits a resolution proof of unsatisfiability. This observation is often credited to Robinson [15], even though it follows instantly from an analysis of a procedure designed by Davis and Putnam [5]; Robinson defined the notion of resolution and proved a more general theorem concerning predicate calculus. Incidentally, the Davis–Putnam procedure was also proposed some fifty years earlier by Löwenheim [11–13]. An account of Löwenheim's work can be found in Hammer and Rudeanu [9]; we are grateful to Yves Crama for this information. We are also grateful to Wolfgang Bibel for informing us that resolution was introduced before Robinson by Blake [2]; see Bibel [1, p. 205]). By the resolution complexity of an unsatisfiable family $F$ of clauses, we mean the smallest $N$ such that there is a resolution proof $C_1, C_2, \ldots, C_N$ of unsatisfiability of $F$.

Haken [7] was the first to prove that there is an infinite sequence of families of clauses whose resolution complexity increases faster than every polynomial in the size of the input; his lower bound was exponential in the cube root of the input size. Later on, Urquhart [17] used a different construction to improve the lower bound to an exponential in the input size. (Urquhart's construction evolves from an idea of Tseitin [16], who constructed an infinite sequence of families of clauses for which the complexity of so-called regular resolution grows at least as fast as an exponential in the square root of the input size; Tseitin's lower bound was subsequently improved by Galil [6] to an exponential in the input size.) The aim of our paper is to prove that randomly generated sparse families of clauses are very likely to have the property of Urquhart's examples.

2. The Theorem and An Outline of Its Proof

Let us call a clause $C$ ordinary if there is no variable $x$ such that $x \in C$ and $\bar{x} \notin C$; let $n, m, k$ be positive integers and let $X$ be a set of size $n$. The random family of $m$ clauses of size $k$ over $n$ variables consists of independent random variables $C_1, C_2, \ldots, C_m$ such that each $C_i$ is distributed uniformly over all $\binom{n}{k} 2^k$ ordinary clauses of size $k$ with variables coming from $X$. (We have chosen this definition partly because it suggests a reasonably practical way of generating random families of clauses and partly because it simplifies our subsequent references to random hypergraphs. The proof of our result can be easily adapted to other definitions of a random family.)

**Theorem.** For every choice of positive integers $c$ and $k$ such that $k \geq 3$ and $c^2^{-k} \geq 0.7$ there is a positive number $\epsilon$ such that, with probability tending to one as $n$ tends to infinity, the random family of $cn$ clauses of size $k$ over $n$ variables is unsatisfiable and its resolution complexity is at least $(1 + \epsilon)^n$.

Proving that, with probability tending to 1 as $n$ tends to $\infty$, the random family $F$ is unsatisfiable is a straightforward exercise: every truth assignment $f$ whose domain consists of all $n$ variables satisfies each $C_i$ with probability $1 - 2^{-k}$, and so it satisfies
Many Hard Examples for Resolution

F with probability \((1 - 2^{-k})^m\). Since there are precisely \(2^n\) choices of \(f\), the probability that \(F\) is satisfiable is at most \(t^n\) with

\[ t = 2(1 - 2^{-k})^m < 2 \exp(-c2^{-k}) \leq 2e^{-0.7} < 0.999, \]

and the desired conclusion follows. (Here, the assumption that \(k \geq 3\) is superfluous.)

The remainder of this paper is devoted to proving that, with probability tending to 1 as \(n\) tends to \(\infty\), the resolution complexity of \(F\) is at least \((1 + \epsilon)^n\). (Here, the assumption that \(c2^{-k} \geq 0.7\) becomes superfluous, but the assumption that \(k \geq 3\) becomes essential: as pointed out by Cook [4], the Davis-Putnam procedure requires only a polynomial time to test satisfiability of any family of clauses of size at most 2; in case the family turns out to be unsatisfiable, the procedure produces a resolution proof of length at most \(n\).) Our proof comes in two parts: first we show that the random family is very likely to have certain properties (Lemma 4) and then we show that these properties impose a lower bound on resolution complexity (Lemma 5).

Lemma 4 guarantees that there are numbers \(a, d\) such that \(0 < d < a/8\) and such that \(F\) is very likely to have the following properties:

- For every family \(F'\) of at most \(an\) clauses from \(F\), there are at least \(\frac{1}{4} |F'|\) variables \(x\) such that \(x\) is involved in precisely one clause from \(F'\).
- There is a "dense" collection of sets \(D\) of \(dn\) variables such that, for every family \(F'\) of at most \(an\) clauses from \(F\), every truth assignment with domain \(D\) has an extension that satisfies \(F'\).

To prove this lemma, we show that all "locally sparse" families of clauses have these properties (Lemma 3) and check by a routine computation that \(F\) is very likely to be locally sparse (Lemma 1).

The strategy used in our proof of Lemma 5 goes back to Haken: select a large family of "special assignments" and find a not-too-many-to-one mapping from this family to the set of clauses in the resolution proof. Actually, it was Urquhart's variation on Haken's theme that inspired our proof: if there is a reasonably uniformly distributed family of linear-size sets \(D\) such that every truth assignment with domain \(D\) is special and if, for every special assignment \(f\), the resolution proof includes a linear-size clause \(C\) that is not satisfied by \(f\), then the mapping that sends \(f\) onto \(C\) is not-too-many-to-one. To find \(C\), Urquhart seemed to rely heavily on a special property of his families of clauses: these families include many clauses whose deletion produces a satisfiable family. Unfortunately, the random \(F\) is far from having this property; fortunately, Urquhart's rule may be reformulated in terms that make sense in any \(F\): choose the first \(C\) in the resolution proof such that deriving \(C\) from \(F\) subject to \(f\) requires a large (but not too large) number of clauses from \(F\).

3. Random Hypergraphs Are Locally Sparse

A hypergraph is a set \(X\) along with a family of not necessarily distinct subsets \(E_i\) of \(X\); elements of \(X\) are called the vertices of the hypergraph and the sets \(E_i\) are called the edges. (We consider edges \(E_i, E_j\) to be distinct if \(i \neq j\), even though we may have \(E_i = E_j\) in this case.) The hypergraph is said to be \(k\)-uniform if all its edges have size \(k\). We say that a hypergraph with \(n\) vertices is \((x, y)\)-sparse if every set of \(s\) vertices such that \(s \leq xn\) contains at most \(ys\) edges.

Let \(n, m, k\) be positive integers; let \(X\) be a set of size \(n\). The random \(k\)-uniform hypergraph with \(n\) vertices and \(m\) edges consists of \(X\) along with independent
random variables $E_1, E_2, \ldots, E_m$ such that each $E_i$ is distributed uniformly over all ($2^k$) subsets of $X$ that have size $k$.

**Lemma 1.** For every choice of positive integers $c$ and $k$ and for every number $y$ such that $(k - 1)y > 1$, there is a positive $x$ such that, with probability tending to 1 as $n$ tends to $\infty$, the random $k$-uniform hypergraph with $n$ vertices and $cn$ edges is $(x, y)$-sparse.

**Proof.** Write

$$\epsilon = y - (k - 1)^{-1},$$
$$x = \left( \frac{1}{2e} \right) \left( \frac{y}{ce} \right)^{1/(k-1)c},$$
$$f(n) = e^{\left( \frac{ce}{y} \right) n^{-1}},$$
$$g(n) = n^{1/2}.$$

The probability that the hypergraph is not $(x, y)$-sparse is at most

$$\sum_{k \leq s \leq xn} a(n, s)$$

with

$$a(n, s) = \left( \frac{n}{s} \right) \sum_{i \geq s} \left( \begin{array}{l} cn \\ i \end{array} \right) \left( \frac{k}{n} \right)^{i} \left( 1 - \left( \frac{k}{n} \right) \right)^{s}.$$

Using the inequality

$$\sum_{i \geq m} \left( \frac{m}{i} \right) p^i (1 - p)^{m-i} \leq \left( \frac{ep}{t} \right)^m,$$

valid whenever $p < t \leq 1$ (a simple proof can be found, for instance, in Chvátal [3]), with $m = cn$, $p = \left( \frac{1}{n} \right)^{y}$, and $t = ys/cn$, we find that

$$a(n, s) \leq \left( \frac{n}{s} \right) \left( \frac{ce^{k-1}}{y} \right)^{ys}.$$

Next, using the elementary bound $(\frac{s}{n}) < (en/s)^s$, we obtain

$$a(n, s) \leq \left( \frac{ce}{y} \right)^s \left( \frac{k-1}{n} \right)^s.$$

Our choice of $x$ guarantees that $a(n, s) \leq \left( \frac{1}{n} \right)^s$ whenever $s \leq xn$, and so

$$\sum_{g(n) \leq s \leq xn} a(n, s) \leq 2^{1 - g(n)} \rightarrow 0. \quad (3.1)$$

On the other hand, we have $a(n, s) \leq (f(n))^s$ whenever $s \leq g(n)$, and so

$$\sum_{k \leq s \leq g(n)} a(n, s) \leq f(n)^{k}(1 - f(n))^{-1} \rightarrow 0. \quad (3.2)$$

The desired conclusion follows from (3.1) and (3.2). \qed

4. **A Lemma on Systems of Distinct Representatives**

A system of distinct representatives (SDR) of a family $(E_i: i \in I)$ of not necessarily distinct sets is a set of distinct points $x_i(i \in I)$ such that each $x_i$ belongs to $E_i$. The

4. A Lemma on Systems of Distinct Representatives
classical theorem of Hall [8] asserts that \((E_i : i \in I)\) has an SDR if and only if

\[
\left| \bigcup_{i \in J} E_i \right| \geq |J| \tag{4.1}
\]

for all subsets \(J\) of \(I\). In the next section, we use the “if” part of the following corollary of Hall’s theorem.

**Lemma 2.** A family \((E_i : i \in I)\) has an SDR with at most \(t\) points in a set \(S\) if and only if it has an SDR and

\[
|J| - \left| \bigcup_{i \in J} (E_i - S) \right| \leq t \tag{4.2}
\]

for all subsets \(J\) of \(I\).

**Proof.** The “only if” part is obvious; to prove the “if” part, we may assume that \(|S| > t\) (otherwise the conclusion is trivial). Now enlarge \(I\) into a set \(I^*\) of size \(|I| + |S| - t\) and set \(E_i = S\) whenever \(i \in I^* - I\). Clearly \((E_i : i \in I)\) has an SDR with at most \(t\) points in \(S\) if and only if \((E_i : i \in I^*)\) has an SDR. Hence Hall’s theorem reduces our task to proving that (4.1) holds for all subsets \(J\) of \(I^*\). By assumption, \((E_i : i \in I)\) has an SDR, and so (4.1) holds whenever \(J \subseteq I\). On the other hand, if \(J \not\subseteq I\), then

\[
\left| \bigcup_{i \in J} E_i \right| = \left| \bigcup_{i \in J \cap I} (E_i - S) \right| + |S|,
\]

and so assumption (4.2) with \(J \cap I\) in place of \(J\) implies

\[
\left| \bigcup_{i \in J} E_i \right| \geq |J \cap I| - t + |S| = |J \cap I| + |I^* - I| \geq |J|;
\]

hence (4.1) holds again. \(\square\)

Lemma 2 is a special case of a theorem of Hoffman and Kuhn [10]; in turn, as shown by Welsh [18], the Hoffman–Kuhn theorem may be seen as a special case of an earlier theorem of Rado [14].

5. **Properties of Locally Sparse Hypergraphs**

The boundary of a family \(F\) of edges in a hypergraph is the set of all the vertices that belong to precisely one edge in \(F\).

We say that a hypergraph with \(n\) vertices has property \(P(a)\) if every family of \(m\) edges such that \(m \leq an\) has boundary of size at least \(m/2\). We say that a hypergraph with \(n\) vertices has property \(Q(a, b)\) if at least 50% of all sets \(S\) of \(\lfloor bn \rfloor\) vertices have the following property: there is a subset \(D\) of \(S\) such that \(|S - D| \leq (a/32) \cdot |S|\) and such that every family of at most \(an\) edges has an SDR disjoint from \(D\).

**Lemma 3.** Let \(H\) be a \(k\)-uniform hypergraph with \(n\) vertices and \(cn\) edges. If \(H\) is \((ak, 4/(2k + 1))-sparse and (x, 0.5 + (a/512))-sparse, then it has properties \(P(a)\) and \(Q(a, b)\) with \(b = \min(x/2k, a/64ck^3, a/8)\).

**Proof.** Showing that \(H\) has property \(P(a)\) is a straightforward exercise: consider any family of \(m\) edges of \(H\) and let \(pm\) denote the size of its boundary. Clearly, the family covers at most \((k + p)m/2\) vertices; if \(m \leq an\), then it covers at most \(akn\) vertices, and so \(p \geq \frac{1}{2}\) since \(H\) is \((ak, 4/(2k + 1))-sparse.
To prove that $H$ has property $Q(a, b)$, set $s = \lfloor bn \rfloor$ and, for each set $S$ of $s$ vertices, let $N(S)$ denote the number of edges that intersect $S$ in at least two vertices. Then let $\bar{N}$ denote the average $N(S)$ and call $S$ normal if $N(S) \leq 2\bar{N}$. Clearly, at least 50% of all sets of $s$ vertices are normal; hence we only need to find, in each normal $S$, a subset $D$ such that $|S - D| \leq as/32$ and such that every family of at most $an$ edges has an SDR disjoint from $D$.

Note that

$$\left(\frac{n}{s}\right)\bar{N} \leq cn\left(\frac{k}{2}\right)\left(\frac{n - 2}{s - 2}\right),$$

and so

$$\bar{N} \leq \frac{ck^2s^2}{2n} \leq \left(\frac{ck^2b}{2}\right) \cdot s \leq \left(\frac{a}{128k}\right)s. \quad (5.1)$$

Now consider an arbitrary but fixed normal $S$. By a cluster, we mean any family of edges whose boundary is contained in $S$. Clearly, for each subset $D$ of $S$, every minimal family of edges with no SDR disjoint from $D$ is a cluster. Hence we only need find a subset $D$ of $S$ such that $|S - D| \leq as/32$ and such that every cluster of at most $an$ edges has an SDR disjoint from $D$. For this purpose, let $(E_i : i \in I)$ be the union of all clusters that have at most $an$ edges; we only need prove that $(E_i : i \in I)$ has an SDR with at most $as/32$ points in $S$. \quad (5.2)

To prove (5.2), note first that

$$|E_i| \leq 2s \quad \text{because } H \text{ has property } P(a),$$

then that

$$4s = an \quad \text{because } b \leq a/8.$$  

Trivially, property $P(a)$ guarantees that every family of at most $an$ edges has an SDR; in particular, $(E_i : i \in I)$ has an SDR. Hence, Lemma 2 reduces proving (5.2) to proving that

$$|J| - \left| \bigcup_{i \in J} (E_i - S) \right| \leq \frac{as}{32} \quad (5.6)$$

for all subsets $J$ of $I$.

To prove (5.6), write

$$P = \bigcup_{i \in J} (E_i \cap S), \quad Q = \bigcup_{i \in J} (E_i - S).$$

Trivially, (5.5) guarantees that $|P| + |Q| \leq 2sk$; since $H$ is $(x, 0.5 + (a/512))$-sparse, it follows that

$$|J| \leq \left(\frac{1}{2} + \frac{a}{512}\right)(|P| + |Q|).$$
Many Hard Examples for Resolution

and so

\[ |P| + |Q| \geq \left(2 - \frac{a}{128}\right)|J|. \]  \hspace{1cm} (5.7)

Clearly, \(|J| \geq |P| - kN(S)|; since \(S\) is normal, it follows that

\[ |J| \geq |P| - 2kN. \]  \hspace{1cm} (5.8)

Finally, (5.7), (5.8), (5.1), and (5.5) imply

\[ |J| - |Q| \leq |P| - \left(1 - \frac{a}{128}\right)|J| \leq 2kN + \frac{a}{128} |J| \leq \frac{as}{32}, \]

and so (5.6) is proved. \(\square\)

We use the following consequence of Lemmas 1 and 3; the assumption that \(k \geq 3\) is used here and only here.

**Lemma 4.** For every choice of positive integers \(c\) and \(k\) such that \(k \geq 3\), there are positive numbers \(a, b\) with \(b \leq a/8\) such that, with probability tending to one as \(n\) tends to \(\infty\), the \(k\)-uniform hypergraph with \(n\) vertices and \(cn\) edges has properties \(P(a)\) and \(Q(a, b)\).

**Proof.** By Lemma 1, there is a positive \(x'\) such that, with probability tending to 1 as \(n\) tends to \(m\), the hypergraph is \((x', 4/(2k + 1))-sparse; set \(a = x'/k\). By Lemma 1 again, there is a positive \(x\) such that, with probability tending to 1 as \(n\) tends to \(\infty\), the hypergraph is \((x, 0.5 + (a/512))-sparse. The rest follows from Lemma 3. \(\square\)

6. A Lower Bound on Resolution Complexity

When \(C\) is a clause, let \(E(C)\) denote the set of all variables \(x\) such that precisely one of \(x\) and \(\bar{x}\) belongs to \(C\). Next, let \(H\) be a hypergraph with edges \(E_1, E_2, \ldots, E_m\). We say that a family \(C_1, C_2, \ldots, C_m\) of clauses is based on \(H\) if each \(C_i\) is an ordinary clause with \(E(C_i) = E_i\).

**Lemma 5.** Let \(H\) be a hypergraph with \(n\) vertices and let \(F\) be an unsatisfiable family of clauses based on \(H\). If \(H\) has properties \(P(a)\) and \(Q(a, b)\) with \(b \leq a/8\), then \(F\) has resolution complexity at least

\[ \frac{1}{4} \left(\frac{e}{2}\right)^{\frac{a}{b}bn1/16}. \]

**Proof.** Write

\[ s = |bn1, \quad d = s - \left\lfloor \frac{as}{32}\right\rfloor. \]

and call a set \(S\) of \(s\) variables special if there is a subset \(D\) of \(S\) such that \(|D| = d\) and such that every family of at most \(an\) clauses from \(F\) can be satisfied by a truth assignment whose domain is disjoint from \(D\). For each special \(S\), choose one \(D\) with this property and call it \(D(S)\). By a special pair, we mean any pair \((S, f)\) such that \(S\) is a special set and \(f\) is a truth assignment with domain \(D(S)\). Since \(H\) has
property $Q(a, b)$, there are at least $\frac{1}{2}(\binom{n}{s}2^d)$ special sets; it follows that there are at least

$$\frac{1}{2} \binom{n}{s}2^d$$

(6.1)
special pairs.

Now consider any resolution proof $C_1, C_2, \ldots, C_N$ of unsatisfiability of $F$. Our plan is to assign one $C_k$ to each special pair in such a way that each $C_k$ is assigned to at most

$$2^\left(\frac{\sqrt{n}}{16}\binom{n}{s}2^d + \frac{1}{2}\binom{n}{s}2^d\right)$$

(6.2)
special pairs. As soon as we do this, the desired lower bound on $N$ follows at once: since $e^2 < 8$, quantity (6.2) is at most

$$2^\left(\frac{\sqrt{n}}{16}\binom{n}{s}2^d\right)$$

and so (6.1) divided by (6.2) is at least

$$\frac{1}{4} \left(\frac{e}{2}\right)^{\frac{\sqrt{n}}{16}}.$$

To implement this plan, we only need prove that

for every special pair $(S, f)$, some $C_k$
not satisfied by $f$ has size at least $an/8$;

(6.3)
then we can assign to each $(S, f)$ a clause $C_k$ with these properties. To verify that each $C_k$ is assigned to at most (6.2) special pairs, let $N_i$ denote the number of special pairs $(S, f)$ such that $C_k$ is assigned to $(S, f)$ and $|D(S) \cap E(C_k)| = i$; we claim that

$$\sum_{i=as/32} N_i \leq \left(\frac{2}{e}\right)^{\frac{as}{16}}\binom{n}{s}2^d$$

(6.4)
and

$$\sum_{i=as/32} N_i \leq \binom{n}{s}2^{d-as/32}.$$ 

(6.5)
To justify these claims, write $m = |E(C_k)|$. We may assume that $m \geq an/8$, for otherwise every $N_i$ is zero by definition. Now note that $|D(S) \cap E(C_k)| \leq as/32$ implies $|S \cap E(C_k)| \leq as/16$, and so

$$\sum_{i=as/32} N_i \leq \sum_{j=as/16} \binom{m}{j} \binom{n-m}{s-j}2^d.$$ 

Hence (6.4) follows from a bound on the tail of the hypergeometric distribution (a simple proof of this bound can be found in Chvátal [3]). Next, if $C_k$ is assigned to $(S, f)$, then $f$ does not satisfy $C_k$, and so $f(x) = 0$ whenever $x \in D(S)$, $x \in C_k$ and $f(x) = 1$ whenever $x \in D(S)$, $x \in C_k$. Hence (6.5) follows at once.

To prove (6.3), consider an arbitrary but fixed special pair $(S, f)$. We say that a family $F'$ of clauses implies a clause $C$ subject to $f$ if every extension of $f$ satisfying $F'$ satisfies $C$; we say that a clause $C$ is complex if no family of at most $an/2$ clauses from $F$ implies $C$ subject to $f$. Since $(S, f)$ is a special pair, every family of
at most \( \frac{an}{2} \) clauses from \( F \) is satisfied by some extension of \( f \); hence the empty clause is complex. It follows that there is a smallest subscript \( k \) such that \( C_k \) is complex; since no complex clause is satisfied by \( f \), we only need prove that

\[
| C_k | \geq \frac{an}{8}.
\]  

(6.6)

To prove (6.6), note first that no clause in \( F \) is complex as each clause implies itself subject to \( f \) (we may assume that \( \frac{an}{2} \geq 1 \), for otherwise the desired lower bound on resolution complexity of \( F \) is less than 1). Hence \( C_k \) is a resolvent of some \( C_i, C_j \) such that \( i < k, j < k \). By minimality of \( k \), neither of \( C_i, C_j \) is complex.

That is to say, there are families \( F_i, F_j \) of clauses in \( F \) such that \( | F_i | \leq \frac{an}{2}, | F_j | \leq \frac{an}{2} \), every extension of \( f \) satisfying \( F_i \) satisfies \( C_i \), and every extension of \( f \) satisfying \( F_j \) satisfies \( C_j \). Since every truth assignment satisfying both \( C_i \) and \( C_j \) satisfies \( C_k \), it follows that \( F_i \cup F_j \) implies \( C_k \) subject to \( f \). Now let \( F_k \) be a smallest family of clauses from \( F \) such that \( F_k \) implies \( C_k \) subject to \( f \). Since \( | F_k | \leq | F_i \cup F_j | \leq an \) and since \( H \) has property \( P(a) \), there is a set \( W \) of at least \( \frac{1}{2} | F_k | \) variables such that for each \( x \) in \( W \) there is precisely one \( C \) in \( F_k \) with \( x \in E(C) \). Since \( C_k \) is complex, we have \( | F_k | > \frac{an}{2} \), and so \( | W | > \frac{an}{4} \); since \( b \leq a/8 \), it follows that \( | W - S | > \frac{an}{8} \).

We complete the proof of (6.6) by proving that

\[
W - S \subseteq E(C_k).
\]  

(6.7)

To prove (6.7), consider any variable \( x \) in \( W - S \). By definition of \( W \), there is precisely one clause \( C \) in \( F_k \) with \( x \in E(C) \). By minimality of \( F_k \), some extension \( g \) of \( f \) satisfies \( F_k - \{C\} \) without satisfying \( C_k \). Setting \( h(x) = 1 - g(x) \) and \( h(y) = g(y) \) whenever \( y \neq x \), observe that

- \( g \) does not satisfy \( C \)
  
  (since it satisfies \( F_k - \{C\} \) without satisfying \( C_k \)), and so

  \( h \) satisfies \( C \)
  
  (since \( g \) and \( h \) differ on \( x \) and since \( x \in E(C) \)). Next, observe that

  \( h \) satisfies \( F_k - \{C\} \)
  
  (since \( g \) and \( h \) agree on all variables involved in these clauses), and so

  \( h \) satisfies \( C_k \)
  
  (since \( F_k \) implies \( C_k \) subject to \( f \) and since \( x \notin D(S) \)). Finally, since \( g \) and \( h \) differ only on \( x \), and since precisely one of them satisfies \( C_k \), we conclude that \( x \in E(C_k) \). \( \Box \)

REFERENCES


RECEIVED JULY 1987; REVISED JANUARY 1988; ACCEPTED JANUARY 1988