On the Structure of Uniquely Satisfiable Formulas

Richard Chang*
Jim Kadin**

TR 90-1124
May 1990

Department of Computer Science
Cornell University
Ithaca, NY 14853-7501

*Department of Computer Science, Cornell University, Ithaca, NY 14853. Supported in part by an IBM Graduate Fellowship and by NSF Research Grant CCR-88-23053.
**Department of Computer Science, University of Maine, Orono, ME 04469.
On the Structure of Uniquely Satisfiable Formulas

Richard Chang\textsuperscript{1} \quad Jim Kadin\textsuperscript{1}

May 7, 1990

Abstract. This paper presents some new results on the computational complexity of the set of uniquely satisfiable Boolean formulas (USAT). Valiant and Vazirani showed that USAT is complete for the class $\text{D}^P$ under randomized reductions. In spite of the fact that the probability bound of this reduction is low, we show that USAT captures many properties possessed by $\text{D}^P$ many-one complete sets. We show that the structure of USAT can affect the structure of $\text{D}^P$ and the entire Polynomial Hierarchy (PH) as well. That is,

1. if $\text{USAT} \equiv_m^P \overline{\text{USAT}}$, then $\text{D}^P = \text{co-D}^P$ and PH collapses.
2. if $\text{USAT} \in \text{co-D}^P$, then PH collapses.
3. if USAT is closed under disjunctive reductions, then PH collapses.

The third result implies that the probability bound in the Valiant-Vazirani reduction cannot be amplified by repeated trials unless the Polynomial Hierarchy collapses. These results show that even sets complete under "weak" randomized reductions can capture properties of many-one complete sets.

1 Introduction

USAT is the set of Boolean formulas with exactly one satisfying assignment. The investigation on the computational complexity of USAT in relation to $\text{D}^P$ began when Papadimitriou and Yannakakis showed that USAT was in $\text{D}^P$ [PY82]. The class $\text{D}^P$, $\text{co-D}^P$ and the canonical $\leq_m^P$-complete languages for these two classes are defined below.

Definition

\[
\text{D}^P = \{ L_1 \cap \overline{L_2} \mid L_1, L_2 \in \text{NP} \}
\]

\[
\text{SAT} \wedge \overline{\text{SAT}} = \{ (F_1, F_2) \mid F_1 \in \text{SAT} \text{ and } F_2 \in \overline{\text{SAT}} \}
\]

\[
\text{co-D}^P = \{ L_1 \cup L_2 \mid L_1, L_2 \in \text{NP} \}
\]

\[
\overline{\text{SAT}} \vee \text{SAT} = \{ (F_1, F_2) \mid F_1 \in \overline{\text{SAT}} \text{ or } F_2 \in \text{SAT} \}
\]

\textsuperscript{1}Department of Computer Science, Cornell University, Ithaca, NY 14853. Supported in part by an IBM Graduate Fellowship and by NSF Research Grant CCR 88-23053.

\textsuperscript{1}Department of Computer Science, University of Maine, Orono, ME 04469.
Apparently USAT was once conjectured to be $\leq_{m}^{P}$-complete for $\Delta_{2}^{P}$.

We note here that the precise complexity of UNIQUE SAT is a persistent open question. Our observation that it is in $D^{P}$ casts doubt on the recurring conjecture that it is complete for $\Delta_{2}^{P}$ [PY82].

This motivated Blass and Gurevich [BG82] to show that there exist oracle worlds where USAT is not $\leq_{m}^{P}$-complete for $D^{P}$, hence, not $\leq_{m}^{P}$-complete for $\Delta_{2}^{P}$.\(^1\) Thus, there is some evidence that USAT may not be $\leq_{m}^{P}$-complete for $D^{P}$. Nevertheless, Valiant and Vazirani went on to prove that USAT is complete for $D^{P}$ under randomized reductions [VV86]. We define some standard reductions formally below.

**Definition [VV86]** $A$ is random reducible to $B$, written $A \leq_{m}^{P} B$, if there exists a probabilistic polynomial time function $f$ and a polynomial $p$ such that

$$x \in A \implies \text{Prob}[f(x) \in B] \geq 1/p(|x|)$$

$$x \not\in A \implies \text{Prob}[f(x) \not\in B] = 1.$$ 

**Definition [LLS75]** $A$ is disjunctive reducible to $B$, written $A \leq_{\text{dis}}^{P} B$, if there is a polynomial time function $f$ such that for all $x$, $f(x) = (y_1, \ldots, y_m)$ and

$$x \in A \iff \exists i, 1 \leq i \leq m, y_i \in B.$$ 

We abuse the terminology and say that a set $B$ is closed under disjunctive reducibilities if $A \leq_{\text{dis}}^{P} B \implies A \leq_{m}^{P} B$. Similarly, $A$ is conjunctive reducible to $B$, written $A \leq_{\text{con}}^{P} B$,

\(^1\)From recent work [Kad88], we have more convincing evidence that USAT is not $\leq_{m}^{P}$-complete for $\Delta_{2}^{P}$—if it were, the Polynomial Hierarchy would collapse.
if there is a polynomial time function $f$ such that for all $x$, $f(x) = (y_1, \ldots, y_m)$ and $x \in A \iff \forall i, 1 \leq i \leq m, y_i \in B$.

One would expect the definition of $\leq_P^m$-reductions to be different from the one used by Valiant and Vazirani, because it is more natural to consider the definition where $x \in A$ implies $\text{Prob}_y[f(x) \in B] \geq 1/2$. However, the definition they use is strong enough to give the corollary $\text{USAT} \in \text{RP} \implies D^P = \text{NP} = \text{RP}$. Furthermore, if $A \leq_P^m B$ and $B$ is closed under disjunctive reductions, then the results of polynomially many $\leq^m_P$-reductions can be joined into one $\leq^m_P$-reduction to $B$. So, the $\leq^m_P$-reduction $A$ to $B$ can be amplified—i.e., for any polynomials $p$, there exists $f'$ such that

$$x \in A \implies \text{Prob}_y[f'(x) \in B] \geq 1 - 2^{-p(n)}.$$ 

In any case, the following theorem shows that USAT is $\leq^m_P$-complete for $D^P$.

**Fact 1** (Valiant, Vazirani [VV86]) There is a polynomial time function $f$ such that

$$x \in \text{SAT} \land \overline{\text{SAT}} \implies \text{Prob}_y[f(x, y) \in \text{USAT}] \geq 1/(4|x|)$$

$$x \not\in \text{SAT} \land \overline{\text{SAT}} \implies \text{Prob}_y[f(x, y) \not\in \text{USAT}] = 1.$$

From this result, one would be tempted to say that USAT is “almost” many-one complete for $D^P$. However, the $\leq^m_P$-reduction does not reduce strings in $\text{SAT} \land \overline{\text{SAT}}$ to USAT with high probability. In fact, the probability tends toward zero as the length of the formula increases. At first glance, it is not clear how closely this completeness result relates the structure of USAT to the structure of $D^P$. For example, it is not clear whether USAT can be in co-$D^P$, or even $P^{SAT[1]}$. Thus, the “precise complexity” of USAT is still open. In this paper, we make another step towards resolving this open question and show that USAT does indeed behave like $D^P \leq^m_P$-complete sets in several ways.

First, we show that if USAT is equivalent to its complement under many-one reductions, then $D^P = \text{co-D}^P$. This quick theorem was our first piece of evidence that the structure of USAT can affect the structure of all the languages in $D^P$. Note that $D^P = \text{co-D}^P$ implies that the Polynomial Hierarchy ($\text{PH}$) [Sto77] collapses to $\Delta_3^P$ [Kad88,CK89]. So, one should consider it very unlikely that $\text{USAT} \equiv^m_P \text{USAT}$.

Our second theorem, suggests that USAT is not in co-$D^P$. We show that if USAT $\in \text{co-D}^P$, then $\text{PH} \subseteq \Delta_3^P$. This parallels the result of Kadin [Kad88], which showed that if $\text{SAT} \land \overline{\text{SAT}} \in \text{co-D}^P$, then $\text{PH} \subseteq \Delta_3^P$. We conclude that the structure of USAT can affect the structure of the entire Polynomial Hierarchy in the same manner that $\text{SAT} \land \overline{\text{SAT}}$ does.

In our third theorem, we investigate the structure of USAT under conjunctive and disjunctive reductions. $NP$ and co-$NP$ are known to be closed under conjunctive and disjunctive reductions. $D^P$, on the other hand, is closed under conjunctive reductions, but not under disjunctive reductions unless $\text{PH} \subseteq \Delta_3^P$ [CK90]. Also, DeMorgan’s Law implies that co-$D^P$ is closed under disjunctive reductions, but not conjunctive reductions (with the same caveat). It is easy to show that USAT is closed under conjunctive reductions, and in our third theorem we show that USAT is not closed under disjunctive reductions unless

---

2 We write $P^{SAT[i]}$ for the set of languages accepted by polynomial time machines that query the SAT oracle only $i$ times.
PH \subseteq \Sigma^P_3$. Thus, compared to the \( \leq^P_m \)-complete languages of the four complexity classes surrounding USAT, we find that the structure of USAT under conjunctive and disjunctive reductions is most similar to that of the D^P \( \leq^P_m \)-complete languages.

The third theorem also suggests that the probability bound of the Valiant-Vazirani reduction cannot be amplified in the standard way (repeating and combining the result of many reductions), because USAT is not closed under disjunctive reductions unless PH collapses. So, this is evidence that there may not exist an \( \leq^P_m \)-reduction from SAT \& SAT to USAT with high probability bound. Yet, USAT does capture some properties of \( \leq^P_m \)-complete sets despite the fact that the probability bound is so low.

The intuitive thread behind the last two theorems begins with the Valiant-Vazirani \( \leq^P_m \)-reduction from SAT \& SAT to USAT. Using this reduction one can show that if USAT \( \in \text{co-D}^P \), then every set in D^P \( \leq^P_m \)-reduces to SAT \lor SAT (the canonical co-D^P \( \leq^P_m \)-complete set). Since SAT \lor SAT is closed under disjunctive reductions, this \( \leq^P_m \)-reduction can be amplified. We know from Kadin’s “hard/easy formulas” proof that if SAT \& SAT \( \leq^P_m \)-reduces to SAT \lor SAT, then PH collapses. By extending this proof to \( \leq^P_m \)-reductions with high probability bounds, it can be shown that if SAT \& SAT \( \leq^P_m \)-reduces to SAT \lor SAT, then PH collapses. Similarly, if USAT is closed under disjunctive reductions, there is an \( \leq^P_m \)-reduction from SAT \lor SAT to USAT which can be amplified. Since USAT \( \leq^P_m \) SAT \& SAT, this gives an \( \leq^P_m \)-reduction from SAT \lor SAT to SAT \& SAT with high probability bounds. Again, this collapses PH using a generalization of the “hard/easy” proof.

2 Unique Satisfiability and co-D^P

In this section, we investigate structure of USAT in relation to co-D^P. In the following theorem, the hypothesis that USAT \( \equiv^P_m \) USAT is stronger than the assumption that USAT \( \in \text{co-D}^P \), but the consequences are stronger, as well.

Theorem 1 If USAT \( \equiv^P_m \) USAT, then D^P = co-D^P and PH \subseteq \Delta^P_3.

Proof: One can show that SAT \( \leq^P_m \) USAT by constructing a function which adds exactly one satisfying assignment to a Boolean formula. Hence, SAT \( \leq^P_m \) USAT. Assuming USAT \( \equiv^P_m \) USAT, both SAT and SAT \( \leq^P_m \)-reduces to USAT. Since USAT is closed under conjunctive reductions, SAT \& SAT \( \leq^P_m \)-reduces to SAT \& SAT. So, USAT is \( \leq^P_m \)-complete for D^P. However, we assumed that USAT \( \equiv^P_m \) USAT, so D^P = co-D^P and the Polynomial Hierarchy collapses to \( \Delta^P_3 \) by Kadin [Kad88].

The following lemma shows the standard way of amplifying the probability bounds of \( \leq^P_m \)-reductions.

Lemma 1 If A \( \leq^P_m \) B and B is closed under disjunctive reductions, then for all polynomials \( p'(n) \), there exist a polynomial time function \( f' \) and a polynomial \( q'(n) \) such that

\[
\begin{align*}
    x \in A &\implies \text{Prob}_x[f'(x, z) \in B] \geq 1 - 2^{-p'(n)} \\
    x \notin A &\implies \text{Prob}_x[f'(x, z) \notin B] = 1,
\end{align*}
\]

4
where \( n = |x| \) and \( z \) is chosen uniformly over \( \{0,1\}^{q(n)} \).

**Proof:** Let \( f \) be the \( \leq^p_m \)-reduction from \( A \) to \( B \). That is, there are polynomials \( p \) and \( q \) such that
\[
x \in A \implies \Pr_{z}[ f(x,z) \in B ] \geq 1/p(n)
x \notin A \implies \Pr_{z}[ f(x,z) \notin B ] = 1,
\]
where \( n = |x| \) and \( z \) is chosen uniformly over \( \{0,1\}^{q(n)} \). Consider the set
\[
D = \{(x_1, \ldots, x_m) \mid \exists i, 1 \leq i \leq m, x_i \in B \}.
\]
Clearly, \( D \leq^p_m B \). So, by assumption, \( D \leq^p B \) via some polynomial time function \( g \). Now, define \( r(n) = p(n) \cdot p'(n) \) and \( q'(n) = r(n) \cdot q(n) \). We construct the new \( \leq^p_m \)-reduction \( f' \) as follows. On input \( (x,z) \), where \( z \in \{0,1\}^{q(n)} \) and \( n = |x| \), \( f' \) divides \( z \) into \( r(n) \) segments \( z_1, \ldots, z_{r(n)} \) of length \( q(n) \). Let
\[
f'(x,z) = g( f(x,z_1), f(x,z_2), \ldots, f(x,z_{r(n)}) ),
\]
where \( g \) is the \( \leq^p_m \)-reduction from \( D \) to \( B \). Clearly, if \( x \notin A \) then for all \( i \), \( f(x,z_i) \notin B \). So,
\[
x \notin A \implies \forall z \in \{0,1\}^{q'(|x|)}, f'(x,z) \notin B \implies \Pr_z[ f(x,z) \notin B ] = 1.
\]
Suppose \( x \in A \), then \( \Pr_z[ f(x,z) \in B ] \geq 1/p(n) \), where \( z \) is chosen uniformly over \( \{0,1\}^{q(n)} \). So, the probability that for some \( i, 1 \leq i \leq r(n) \), \( f(x,z_i) \in B \) is bounded below by:
\[
1 - \Pr_z[z_1, \ldots, z_{r(n)} \mid \forall i, 1 \leq i \leq r(n), f(x,z_i) \notin B]
\geq 1 - (1 - 1/p(n))^{r(n)}
\geq 1 - ((1 - 1/p(n))^{p(n)})^{p'(n)},
\]
Since \( (1 - 1/p(n))^{p(n)} \) converges to \( e^{-1} \), we have
\[
x \in A \implies \Pr_z[ f'(x,z) \in B ] \geq 1 - e^{-p'(n)} \geq 1 - 2^{-p'(n)}
\]
where \( z \) is chosen uniformly over \( \{0,1\}^{q'(n)} \).
\( \square \)

Before we go on, we need to define some probabilistic and nonuniform classes.

**Definition** For any class \( C \), \( A \in \text{BP} \cdot C \) if there exists \( B \in C \) and a constant \( \varepsilon \) such that
\[
\forall x, \Pr_y[ x \in A \iff (x,y) \in B ] > 1/2 + \varepsilon.
\]

**Definition** Let \( C \) be any class of languages and let \( f \) a polynomially bounded function (i.e., there exists \( k \) such that \( |f(y)| \leq |y|^k + k \)). \( A \in C/f \) if there exists \( B \in C \) such that
\[
\forall x, x \in A \iff (x,f(|x|)) \in B.
\]

5
$f$ is called the advice function and $f(1^{|x|})$ the advice string. Note that the advice string depends only on the length of $x$. Also, we write $\mathcal{C}/\text{poly}$ for the union of $\mathcal{C}/f$ over all possible polynomially bounded advice functions.

The “hard/easy formulas” proof, which showed that $\text{D}^p = \text{co-D}^p$ implies $\text{PH}$ collapses, used the following line of reasoning. Suppose $\text{D}^p = \text{co-D}^p$, then there is a many-one reduction from $\text{SAT} \land \overline{\text{SAT}}$ to $\text{SAT} \lor \overline{\text{SAT}}$. With the help of an advice function $f$, this reduction can be converted into a reduction from $\overline{\text{SAT}}$ to $\text{SAT}$. Thus, $\overline{\text{SAT}} \in \text{NP}/f$. Then, by a theorem due to Yap [Yap83], $\text{PH}$ collapses to $\Sigma^p_3$. In the next theorem, we will show that the $\leq_{\text{fp}}^p$-reduction from $\text{SAT} \land \overline{\text{SAT}}$ to $\text{SAT} \lor \overline{\text{SAT}}$ can be converted into an $\leq_{\text{fp}}^p$-reduction from $\overline{\text{SAT}}$ to $\text{SAT}$ (with help from an advice function). It follows that $\overline{\text{SAT}}$ is contained in the rather awkward class $\text{BP}-(\text{NP}/f)$. A generalization of a theorem due to Schöning relates $\text{BP}-(\text{NP}/f)$ to nonuniform Polynomial Hierarchies.

**Fact 2** (Schöning [Sch89])
For all polynomially bounded $f$, if $\overline{\text{SAT}} \in \text{BP}-(\text{NP}/f)$ then $\Sigma^p_2/f = \Pi^p_2/f$.

Now, we are ready to show that if USAT were in $\text{co-D}^p$, then the entire Polynomial Hierarchy would collapse. This consequence is weaker than the one in Theorem 1, since it does not imply that $\text{D}^p = \text{co-D}^p$.

**Theorem 2** If USAT $\in \text{co-D}^p$, then $\text{PH} \subseteq \Delta^p_3$.

**Proof:** Suppose USAT $\in \text{co-D}^p$. Since $\overline{\text{SAT}} \lor \text{SAT}$ is $\leq_{\text{fp}}^p$-complete for $\text{co-D}^p$, there is a $\leq_{\text{fp}}^p$-reduction from USAT to $\overline{\text{SAT}} \lor \text{SAT}$. Moreover, $\text{SAT} \land \overline{\text{SAT}} \leq_{\text{fm}}^p \text{USAT}$, so there is an $\leq_{\text{fm}}^p$-reduction from $\text{SAT} \land \overline{\text{SAT}}$ to $\overline{\text{SAT}} \lor \text{SAT}$. Since $\overline{\text{SAT}} \lor \text{SAT}$ is closed under disjunctive reductions, the probability bound of this $\leq_{\text{fp}}^p$-reduction can be amplified by Lemma 1. (Recall that the original probability bound was $1/(4n)$.) That is, using the disjunctive reduction to combine the results of polynomially many $\leq_{\text{fm}}^p$-reductions, we can construct a polynomial time function $h$ and a polynomial $q$ such that

$$(F_1, F_2) \in \text{SAT} \land \overline{\text{SAT}} \implies \Pr[h(F_1, F_2, z) \in \overline{\text{SAT}} \lor \text{SAT}] \geq 1 - 2^{-n}$$

$$(F_1, F_2) \in \overline{\text{SAT}} \lor \text{SAT} \implies \Pr[h(F_1, F_2, z) \in \text{SAT} \land \overline{\text{SAT}}] = 1$$

where $n = |(F_1, F_2)|$ and $z$ is chosen uniformly over $\{0, 1\}^{q(n)}$.

To prove the theorem, we will construct an advice function $f$ computable in $\Delta^p_3$ such that $\overline{\text{SAT}} \in \text{BP}-(\text{NP}/f)$. Then, by Fact 2, $\Sigma^p_2/f = \Pi^p_2/f$ which implies that $\Sigma^p_3/f \subseteq \Sigma^p_2/f$. However, $f$ is computable in $\Delta^p_3$, so a $\Delta^p_3$ machine can compute the advice for itself. Thus, $\Sigma^p_3 \subseteq \Sigma^p_2/f \subseteq \Sigma^p_2/f \subseteq \Delta^p_3$. So, $\text{PH} \subseteq \Delta^p_3$.

Now, we construct the advice function $f$. We call $F$ easy if $F \in \overline{\text{SAT}}$ and

$$\exists x, y \text{ such that } |x| = |F|, y \in \{0, 1\}^{q(n)}, \pi_2(h(x, F, y)) \in \text{SAT},$$

where $\pi_i$ is the $i^{th}$ projection function (i.e., $\pi_i(x_1, \ldots, x_m) = x_i$). $F$ is called easy in this case because there is “existential evidence” that $F$ is unsatisfiable. If $F \in \overline{\text{SAT}}$ and $F$ is not easy, then we call $F$ a hard string. On input $1^n$, the advice function simply outputs the lexically smallest hard string of length $n$ if it exists. Otherwise, it outputs the empty
string, \( \varepsilon \). From the definition of easy, it is clear that checking whether a string is hard is a co-NP question. So, using binary search and an NP oracle, the advice function \( f \) can be computed in \( \Delta^p_3 \).

Now, consider the following NP program. On input \((F, H, z)\), \(N\) treats \(F\) as a Boolean formula of length \(n\), takes \(H\) as an advice string of length 0 or \(n\), and parses \(z\) into a \(q(n)\) bit long guess string. (If the input does not conform to this syntax, \(N\) rejects outright.) Then, \(N\) does the following.

1. If the advice string \(H\) is the empty string, then accept if and only if
   \[ \exists x, y \text{ such that } |x| = n, \ y \in \{0,1\}^{q(n)}, \ \pi_2(h(x, F, y)) \in \text{SAT}. \]
2. If \(|H| = n\), then accept if and only if \(\pi_1(h(F, H, z)) \in \text{SAT}\).

**Claim:** The NP program above shows that \(\overline{\text{SAT}} \in \text{BP-}(\text{NP} / f)\). That is,

\[
\text{Prob}_F[ F \in \overline{\text{SAT}} \iff N(F, f(1^n), z) \text{ accepts } ] \geq 1 - 2^{-n}.
\]

Note that whether there is a hard string of length \(n\) does not depend on the guess string \(z\). So, we can analyze the program in two cases.

**Case 1:** Consider the case where all the strings in \(\overline{\text{SAT}}\) of length \(n\) are easy—i.e., \(f(1^n) = \varepsilon\). If the input \(F \in \overline{\text{SAT}}\), then \(F\) must also be easy which means the appropriate \(x\) and \(y\) would be found in step 1. So,

\[ F \in \overline{\text{SAT}} \implies \text{Prob}_z[ N(F, \varepsilon, z) \text{ accepts } ] = 1. \]

If \(F \in \text{SAT}\), then for all \(x, (x, F) \in \overline{\text{SAT}} \cup \text{SAT}\). So, by the description of the reduction \(h\),

\[ \text{Prob}_F[ h(x, F, z) \in \text{SAT} \land \overline{\text{SAT}} ] = 1. \]

But, \(h(x, F, z) \in \text{SAT} \land \overline{\text{SAT}}\) implies that \(\pi_2(h(x, F, z)) \in \overline{\text{SAT}}\). So, \(N\) must reject in step 1. Thus, in the easy case \(\text{Prob}_z[ F \in \overline{\text{SAT}} \iff N(F, \varepsilon, z) \text{ accepts } ] = 1.\)

**Case 2:** Suppose the advice string \(H\) is a hard string of length \(n\). If \(F \in \overline{\text{SAT}},\) then \(F, H) \in \overline{\text{SAT}} \cup \text{SAT}\). By the description of the reduction \(h,\)

\[ \text{Prob}_F[ h(F, H, z) \in \text{SAT} \land \overline{\text{SAT}} ] = 1. \]

So, for all \(z\), \(\pi_1(h(F, H, z)) \in \text{SAT}\). Therefore, for all \(z\), \(N\) will accept in step 2 and

\[ F \in \overline{\text{SAT}} \implies \text{Prob}_z[ N(F, H, z) \text{ accepts } ] = 1. \]

If \(F \in \text{SAT},\) then \((F, H) \in \text{SAT} \land \overline{\text{SAT}}\) because \(H\) is hard implies that \(H \in \overline{\text{SAT}}\). Also, since \(H\) is hard,

\[ \forall x, |x| = n, \ \forall z, z \in \{0,1\}^{q(n)}, \ \pi_2(h(x, H, z)) \in \overline{\text{SAT}}. \]

So, for all choices of \(z\), \(h(F, H, z) \in \text{SAT} \land \overline{\text{SAT}} \iff \pi_1(h(F, H, z)) \in \text{SAT}\). Moreover, by the description of \(h\) and the fact that \((F, H) \in \overline{\text{SAT}} \cup \text{SAT}\),

\[ \text{Prob}_F[ h(F, H, z) \in \text{SAT} \land \overline{\text{SAT}} ] \leq 2^{-n}. \]
So, \( \Pr_x[ \pi_1(h(F, H, z)) \in \text{SAT} ] \leq 2^{-n} \). Thus,
\[
F \in \text{SAT} \implies \Pr_x[ N(F, H, z) \text{ accepts } ] < 2^{-n}.
\]
\( \square \)

Since USAT plays no special role in this proof, this theorem holds for all \( \text{D}^p \leq_{\text{m}}^p \)-complete sets.

**Corollary 1**

Let \( A \) be \( \leq_{\text{m}}^p \)-complete for \( \text{D}^p \). If \( A \in \text{co-D}^p \), then \( \text{PH} \subseteq \Delta_3^p \).

### 3 Unique Satisfiability and Disjunctive Reductions

In this section, we show that USAT is not closed under disjunctive reductions unless the Polynomial Hierarchy collapses. At first glance, the proof of this theorem may appear to be symmetric to the proof of Theorem 2, because the intermediate step constructs an \( \leq_{\text{m}}^p \)-reduction from \( \text{SAT} \lor \text{SAT} \) to \( \text{SAT} \land \text{SAT} \) (cf. \( \text{SAT} \land \text{SAT} \leq_{\text{m}}^p \text{SAT} \lor \text{SAT} \) in Theorem 2). As it turns out, this theorem is much harder. Nevertheless, we can push the proof through using a "hard/easy formulas" argument and another theorem from Schöning.

**Definition**\([\text{Sel82}]\) \( A \) is polynomial time positive reducible to \( B \), written \( A \leq_{\text{pos}}^p B \), if \( A = L(M^B) \) where \( M \) is a polynomial time machine which has the additional constraint that
\[
X \subseteq Y \implies L(M^X) \subseteq L(M^Y).
\]

**Fact 3** (Schöning [\text{Sch89}])

For any class \( \mathcal{C} \) closed under \( \leq_{\text{pos}}^p \)-reductions, \( \text{B.P} \cdot \mathcal{C} \subseteq \mathcal{C} / \text{poly} \).

In the following proof, we will use the fact that for all polynomially bounded \( f \), \( \text{NP} / f \) is closed under \( \leq_{\text{pos}}^p \)-reductions. Therefore, \( \text{B.P} \cdot (\text{NP} / f) \subseteq (\text{NP} / f) / \text{poly} = \text{NP} / \text{poly} \).

**Theorem 3** If USAT is closed under disjunctive reductions, then \( \text{PH} \subseteq \Sigma_3^p \).

**Proof:** First, we note that if USAT is closed under disjunctive reductions, then the probability bound in the Valiant-Vazirani \( \leq_{\text{m}}^p \)-reduction from SAT to USAT can be amplified by Lemma 1. That is, there is a polynomial time function \( f \) and a polynomial \( q \) such that
\[
x \in \text{SAT} \implies \Pr_y[ f(x, y) \in \text{USAT} ] \geq 1 - 2^{-n^2}
\]
\[
x \in \overline{\text{SAT}} \implies \Pr_y[ f(x, y) \in \overline{\text{USAT}} ] = 1
\]
where \( n = |x| \) and \( y \) is chosen uniformly over \( \{0, 1\}^{q(n)} \).

Also, USAT being closed under disjunctive reductions implies that there is an \( \leq_{\text{m}}^p \)-reduction from \( \text{SAT} \lor \text{SAT} \) to USAT. However, USAT \( \in \text{D}^p \), so there is an \( \leq_{\text{m}}^p \)-reduction from \( \overline{\text{SAT}} \lor \text{SAT} \) to \( \text{SAT} \land \overline{\text{SAT}} \). Combined with the observation on amplifying the Valiant-Vazirani reduction, this implies that there exist a polynomial time function \( h \) and a polynomial \( q \) such that
\[(F_1, F_2) \in \overline{\text{SAT}} \lor \text{SAT} \implies \text{Prob}_z[h(F_1, F_2, z) \in \text{SAT} \land \overline{\text{SAT}}] \geq 1 - 2^{-n^2}\]
\[(F_1, F_2) \in \text{SAT} \land \overline{\text{SAT}} \implies \text{Prob}_z[h(F_1, F_2, z) \in \overline{\text{SAT}} \lor \text{SAT}] = 1\]

where \(n = |(F_1, F_2)|\) and \(z\) is chosen uniformly over \(\{0, 1\}^q(n)\).

As in the proof of Theorem 2, we define hard and easy strings and construct an advice function \(f\). In this proof, we call a string \(F\) easy if \(F \in \overline{\text{SAT}}\) and

\[\exists x, |x| = |F|, \text{ Prob}_z[\pi_2(h(x, F, z)) \in \text{SAT}] > 2/3,\]

where \(\pi_i\) is the \(i^{th}\) projection function. As before, if \(F \in \overline{\text{SAT}}\) and not easy, we call \(F\) a hard string. We construct an advice function \(f\) which on input \(1^n\) outputs the lexically smallest hard string of length \(n\), if it exists. Then, we show that \(\overline{\text{SAT}} \in \text{BP}.(\text{NP}/f)\). In this case, however, we do not know that \(f\) can be computed in \(\Delta^p_3\). However, Fact 3 implies that \(\text{BP}.(\text{NP}/f) \subseteq \text{NP/poly}\). Thus, \(\text{SAT} \in \text{NP/poly}\) and by Yap [Yap83] \(\text{PH} \subseteq \Sigma^p_3\).

Consider the NP program \(N\). On input \((F, H, \vec{z})\), \(N\) treats \(F\) as a Boolean formula of length \(n\), \(H\) as an advice string, and parses \(\vec{z} = (z_1, z_2, z_3)\) into three \(q(n)\) bit long guess strings. Then, \(N\) does the following.

1. If the advice string \(H\) is empty, then accept if and only if
   \[\exists x, \text{ such that } |x| = n, \pi_2(h(x, F, z_1)) \in \text{SAT}.\]

2. If \(|H| = n\), then accept if and only if
   \[\text{ for each } i = 1, 2, 3, \pi_1(h(F, H, z_i)) \in \text{SAT}.\]

Note that step 1 in this program is different from the one in Theorem 2. The string \(z_1\) is not guessed existentially in step 1, but taken from \(\vec{z}\).

**Claim:** The NP program above demonstrates that \(\overline{\text{SAT}} \in \text{BP}.(\text{NP}/f)\). That is,

\[\text{Prob}_x[F \in \overline{\text{SAT}} \iff N(F, f(1^n), \vec{z}) \text{ accepts}] > 2/3.\]

**Case 1:** Consider the case where all the strings in \(\overline{\text{SAT}}\) of length \(n\) are easy (\(f(1^n) = \varepsilon\)). If the input \(F \in \overline{\text{SAT}}\), then \(F\) must also be easy. Let \(x\) be the witness that \(F\) is easy. Then, by the definition of easy,

\[\text{Prob}_z[\pi_2(h(x, F, z_1)) \in \text{SAT}] > 2/3.\]

So, \(\text{Prob}_z[\exists x, |x| = n, \pi_2(h(x, F, z_1)) \in \text{SAT}] > 2/3\). So the probability that the existential search in step 1 will be successful is greater than \(2/3\). Thus,

\[F \in \overline{\text{SAT}} \implies \text{Prob}_x[N(F, \varepsilon, \vec{z}) \text{ accepts}] > 2/3.\]

On the other hand, if \(F \in \text{SAT}\), then for all \(x, (x, F) \in \overline{\text{SAT}} \lor \text{SAT}\). Thus,

\[\text{Prob}_z[h(x, F, z_1) \in \text{SAT} \land \overline{\text{SAT}}] > 1 - 2^{-n^2}.\]

So, \(\text{Prob}_z[\pi_2(h(x, F, z_1)) \in \text{SAT}] < 2^{-n^2}\). However, \(2^{-n^2}\) is so small, we can move an existential quantifier inside the probability.
\[ \text{Prob}_z[ \exists x, |x| = |F|, \pi_2(\ell(x, F, z_1)) \in \text{SAT} ] < (1 - 2^{-n^2})^2. \]

Then, the following calculations give us

\[ 1 - (1 - 2^{-n^2})2^n = 2^{-n^2} \sum_{i=1}^{2^n} (1 - 2^{-n^2})^{i-1} < 2^{-n^2}2^n = 2^{n-n^2} \]

Thus, \( F \in \text{SAT} \implies \text{Prob}_x[ N(F, \varepsilon, \tilde{z}) \text{ accepts } ] < 2^{n-n^2}. \)

**Case 2:** Suppose there is a hard string \( H = f(1^n) \). If \( F \in \overline{\text{SAT}} \), then \( (F, H) \in \overline{\text{SAT}} \lor \text{SAT} \). So, by the description of \( h \)

\[ \text{Prob}_z[ h(F, H, z) \in \text{SAT} \land \overline{\text{SAT}} ] > 1 - 2^{-n^2}. \]

This means \( \text{Prob}_z[ \pi_1(h(F, H, z)) \in \text{SAT} ] > 1 - 2^{-n^2} \). So,

\[ \text{Prob}_{z_1, z_2, z_3}[ \text{for each } i = 1, 2, 3, \pi_1(h(F, H, z_i)) \in \text{SAT} ] > (1 - 2^{-n^2})^3 > 1 - 3 \cdot 2^{-n^2}. \]

So, the probability that all three trials checking if \( \pi_1(h(F, H, z_i)) \in \text{SAT} \) in step 2 are successful is greater than \( 1 - 3 \cdot 2^{-n^2} \). Thus,

\[ F \in \overline{\text{SAT}} \implies \text{Prob}_x[ N(F, H, \tilde{z}) \text{ accepts } ] > 1 - 3 \cdot 2^{-n^2}. \]

On the other hand, if \( F \in \text{SAT} \), then \( (F, H) \in \text{SAT} \land \overline{\text{SAT}} \). From the description of \( h \), this means \( \text{Prob}_z[ h(F, H, z) \in \overline{\text{SAT}} \lor \text{SAT} ] = 1 \). However, \( H \) is hard, so

\[ \text{Prob}_z[ \pi_2(h(F, H, z)) \in \overline{\text{SAT}} ] \geq 1/3. \]

Note that \( (G_1, G_2) \in \overline{\text{SAT}} \lor \text{SAT} \) and \( G_2 \in \overline{\text{SAT}} \) implies that \( G_1 \in \overline{\text{SAT}} \). So,

\[ \text{Prob}_z[ \pi_1(h(F, H, z)) \in \overline{\text{SAT}} ] \geq 1/3. \]

This yields the relation

\[ \text{Prob}_{z_1, z_2, z_3}[ \text{for each } i = 1, 2, 3, \pi_1(h(F, H, z_i)) \in \text{SAT} ] < (2/3)^3 < 1/3. \]

Thus, \( F \in \text{SAT} \implies \text{Prob}_x[ N(F, H, \tilde{z}) \text{ accepts } ] < 1/3. \)

\[ \square \]

As in Theorem 2, \( \text{USAT} \) plays no special role in the proof. With minor modifications, the preceding proof will also show the following corollary.

**Corollary 2**

Let \( A \) be \( \leq_m^p \)-complete for \( \text{D}^p \). If \( A \) is closed under disjunctive reductions, then the Polynomial Hierarchy collapses to \( \Sigma_3^p \).

**Proof:** (Sketch) In Theorem 3, we implicitly used the \( \leq_m^p \)-reduction from \( \overline{\text{SAT}} \) to \( \text{USAT} \) to construct an \( \leq_m^p \)-reduction from \( \overline{\text{SAT}} \lor \text{SAT} \) to \( \text{USAT} \). For a \( \text{D}^p \leq_m^p \)-complete set \( A \), there may only be an \( \leq_m^p \)-reduction from \( \overline{\text{SAT}} \) to \( A \). However, the \( \leq_m^p \)-reduction can be amplified by Lemma 1, because we are assuming that \( A \) is closed under disjunctive reductions. Thus, there exist a polynomial \( q \) and two polynomial time functions \( f \) and \( g \) such that
\[ x \in \text{SAT} \implies \Pr_y [ f(x, y) \in A ] \geq 1 - 2^{-n^2} \]
\[ x \notin \text{SAT} \implies \Pr_y [ f(x, y) \notin A ] = 1 \]
\[ x \in \overline{\text{SAT}} \implies \Pr_y [ g(x, y) \in A ] \geq 1 - 2^{-n^2} \]
\[ x \notin \overline{\text{SAT}} \implies \Pr_y [ g(x, y) \notin A ] = 1 \]

where \( n = |x| \) and \( y \) is chosen uniformly over \( \{0, 1\}^{q(n)} \). Consider the set
\[
D = \{(F_1, F_2) \mid F_1 \in A \text{ or } F_2 \in A \}
\]
Since \( D \leq_{s_{2^\infty}} A \), there is a \( \leq_{s_{2^\infty}}^P \)-reduction \( t \) from \( D \) to \( A \). Using \( t \), the two \( \leq_{s_{2^\infty}}^P \)-reductions \( f \) and \( g \) can be combined into one \( \leq_{s_{2^\infty}}^P \)-reduction from \( \overline{\text{SAT}} \lor \text{SAT} \) to \( A \):
\[
(F_1, F_2) \in \overline{\text{SAT}} \lor \text{SAT} \implies \Pr_y [ t(f(F_1, y), g(F_2, y)) \in A ] \geq 1 - 2^{-n^2}
\]
\[
(F_1, F_2) \in \text{SAT} \land \overline{\text{SAT}} \implies \Pr_y [ t(f(F_1, y), g(F_2, y)) \notin A ] = 1
\]

The rest of the proof would proceed in the same way as the proof of Theorem 3. \qed

### 4 A Technical Discussion

One way to remember Theorem 2 is:
\[
\text{SAT} \land \overline{\text{SAT}} \leq_{s_{2^\infty}}^P \text{USAT} \leq_{s_{2^\infty}}^P \overline{\text{SAT}} \lor \text{SAT} \implies \text{PH collapses.}
\]

We would like to say that the intuition behind these proofs is that not only does \( \text{D}^P \subseteq \text{co-D}^P \) collapse \( \text{PH} \), but so does \( \text{D}^P \subseteq \text{BP-co-D}^P \). Then, we could draw an analogy with the Polynomial Hierarchy, since both \( \Sigma_k^P \subseteq \Pi_k^P \) and \( \Sigma_k^P \subseteq \text{BP} \cdot \Pi_k^P \) collapse the Polynomial Hierarchy [Sch89]. However, to prove this is the correct intuition, we would also have to show that \( \text{co-D}^P \subseteq \text{BP} \cdot \text{D}^P \) collapses \( \text{PH} \). We are unable to prove this statement, because both the “hard/easy formulas” argument and the Valiant-Vazirani random reduction are one-sided—that is, there is an easy case and a hard case. When the easy cases match, everything works out (as in Theorem 2). When the cases do not match, life becomes difficult. So, we leave as an open question:
\[
\overline{\text{SAT}} \lor \text{SAT} \leq_{s_{2^\infty}}^P \text{USAT} \leq_{s_{2^\infty}}^P \text{SAT} \land \overline{\text{SAT}} \implies \text{PH collapses.}
\]

(Note that the hypothesis is weaker than the one in Theorem 3.) Such a theorem may very well resolve some open questions about the Counting Hierarchy described by Cai and Hemachandra [CH85].

### 5 Conclusion

We have shown that the complexity of USAT affects the structure of \( \text{D}^P \) and of the entire Polynomial Hierarchy in much the same way that \( \text{D}^P \leq_{s_{2^\infty}}^P \)-complete sets do. This happens
despite the fact that the Valiant-Vazirani $\leq_m^P$-reduction has a low probability bound. In fact, Corollaries 1 and 2 apply to all $D^P \leq_m^P$-complete sets. So, these results show that $\leq_m^P$-complete sets can capture some of the properties of $\leq_m^P$-complete sets even when the definition of $\leq_m^P$ allows reductions with low probabilities. It would be interesting to see if the $\leq_m^P$-complete sets of other complexity classes have this behavior.

6 Acknowledgements

The authors would like to thank Vijay Vazirani and Desh Ranjan for sitting through various versions of our proof, Steve Mitchell and Christine Piatko for helpful hints on probability, and Juris Hartmanis for his unwavering guidance and support.

References


