On Unique Satisfiability and Randomized Reductions*

Richard Chang† Pankaj Rohatgi

Department of Computer Science, Cornell University
Ithaca, New York 14853, USA

Abstract

Ever since Valiant and Vazirani [VV86] showed that there exists a random reduction from SAT to USAT, the complexity of USAT has been cited as "USAT is complete for $\mathrm{D^P}$ under randomized reductions." However, the definition of the randomized reduction was never quite satisfying because the probability of a "correct" reduction can approach zero as the length of the formula increases. The discrepancy between the Valiant-Vazirani definition and the earlier Adleman-Manders [AM77] definition has been noted previously [Joh85]. This column reflects on recent results about the complexity of USAT and of $\mathrm{D^P}$ which shed a new light on the meaning of completeness under randomized reductions. For example, it is pointed out that, under randomized reductions, USAT is complete for $\mathrm{P}^{\mathrm{SAT}[\log n]}$ as well. These results also show that the non-robustness of $\mathrm{D^P}$ creates many difficulties in defining a randomized reduction which gives a meaningful notion of completeness.

1 An Historical Account

The central question in structural complexity theory is of course the P =? NP question. One way to consider this problem is to investigate the complexity of the NP-complete set SAT. In addition to studying the complexity of detecting a satisfiable Boolean formula, much research has been devoted to studying the complexity of computing the actual number of satisfying assignments. As a special case, the unique satisfiability problem is the problem of detecting if a Boolean formula has exactly one satisfying assignment.

From the beginning, the study of the complexity of unique satisfiability has been tied to the class $\mathrm{D^P}$ and to randomized reductions. Papadimitriou and Yannakakis [PY84] first defined $\mathrm{D^P}$ to study the complexity of the facets of polytopes.

*This research was supported in part by NSF Research Grant CCR 88-23053.

†Current Address: Department of Computer Science, University of Maryland, Baltimore County Campus, Baltimore, MD 21228, USA.

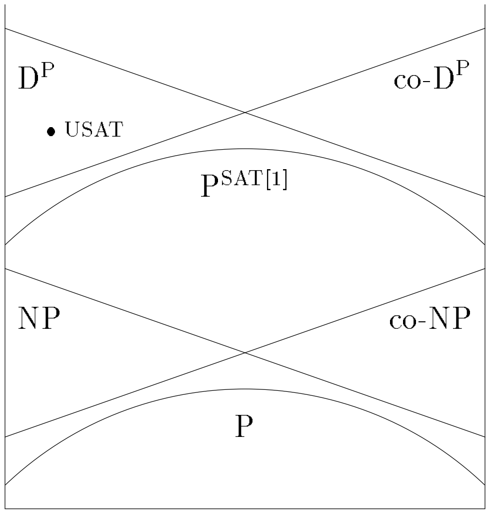

Figure 1: USAT and related complexity classes.

Definition: The definitions of $\mathrm{D^P}$, co-$\mathrm{D^P}$ are given below. The languages $\mathrm{SAT}\wedge\overline{\mathrm{SAT}}$ and $\overline{\mathrm{SAT}}\vee\mathrm{SAT}$ are $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete for $\mathrm{D^P}$ and co-$\mathrm{D^P}$ respectively.

$$\begin{aligned}
\mathrm{D^P} &= \{L_1 \cap \overline{L_2} \mid L_1, L_2 \in \mathrm{NP}\} \\
\text{co-}\mathrm{D^P} &= \{\overline{L_1} \cup L_2 \mid L_1, L_2 \in \mathrm{NP}\}
\end{aligned}$$

$$\begin{aligned}
\mathrm{SAT}\wedge\overline{\mathrm{SAT}} &= \{(F_1, F_2) \mid F_1 \in \mathrm{SAT} \text{ and } F_2 \in \overline{\mathrm{SAT}}\ \} \\
\overline{\mathrm{SAT}}\vee\mathrm{SAT} &= \{(F_1, F_2) \mid F_1 \in \overline{\mathrm{SAT}} \text{ or } F_2 \in \mathrm{SAT}\ \}.
\end{aligned}$$

Papadimitriou and Yannakakis also noticed that the set of uniquely satisfiable Boolean formulas, USAT, is contained in $\mathrm{D^P}$. This is easily seen from the definition by letting L_1 be SAT and L_2 be the set of formulas with two or more satisfying assignments. Then, $\mathrm{USAT} = L_1 - L_2$. So, the natural question to ask is: Can USAT be complete for $\mathrm{D^P}$?

Blass and Gurevich [BG82] answered this question partially. They noticed that since $\overline{\mathrm{SAT}} \leq_{\mathrm{m}}^{\mathrm{P}} \mathrm{USAT}$ and since the conjunction of uniquely satisfiable formulas is also uniquely satisfiable,

$$\mathrm{USAT} \text{ is } \leq_{\mathrm{m}}^{\mathrm{P}}\text{-complete for } \mathrm{D^P} \iff \mathrm{SAT}\wedge\overline{\mathrm{SAT}} \leq_{\mathrm{m}}^{\mathrm{P}} \mathrm{USAT} \iff \mathrm{SAT} \leq_{\mathrm{m}}^{\mathrm{P}} \mathrm{USAT}.$$

So, the question of whether USAT can be $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete for $\mathrm{D^P}$ hinges on whether there is a $\leq_{\mathrm{m}}^{\mathrm{P}}$-reduction from SAT to USAT. Then, they showed that there are oracle worlds where no such reduction can exist. This meant a non-relativizing proof technique would be needed to answer the question—a formidable obstacle, indeed.

Valiant and Vazirani [VV86] did not surmount this obstacle, but they did manage to circumvent it. Although, it may be difficult to construct a $\leq_m^P$-reduction from SAT to USAT (assuming one even exists), they were able to construct a *randomized reduction.* In particular, they constructed a polynomial function f such that

$$x \in \mathrm{SAT} \Longrightarrow \mathrm{Prob}_z[\ f(x,z) \in \mathrm{USAT}\ ] \geq 1/(4|x|)$$
$$x \notin \mathrm{SAT} \Longrightarrow \mathrm{Prob}_z[\ f(x,z) \notin \mathrm{USAT}\ ] = 1.$$

Thus, USAT becomes complete for $\mathrm{D^P}$ under randomized reductions[1]. However, this variety of randomized reduction is not quite satisfying, because the probability of the reduction being "correct" can approach zero as the length of x increases. One would have expected a probability bound of 1/2 (in keeping with the Adleman-Manders [AM77] definition). The justification for the Valiant-Vazirani definition is that in many situations the probability bound can be amplified, in which case, the definitions would be equivalent. Before we continue, we need to introduce some notation and terminology to facilitate our discussion of randomized reductions with different probability bounds.

Definition: We say that A randomly reduces to B (written $A \leq_m^{rp} B$) with probability δ, if there exists a polynomial time function f and a polynomial bound q such that

$$x \in A \Longrightarrow \mathrm{Prob}_z[\ f(x,z) \in B\ ] \geq \delta$$
$$x \notin A \Longrightarrow \mathrm{Prob}_z[\ f(x,z) \notin B\ ] = 1,$$

where z is chosen uniformly over $\{0,1\}^{q(n)}$.

In this terminology, Valiant and Vazirani showed that SAT randomized reduces to USAT with probability $1/(4n)$. As a special case, we will write $A \leq_m^{vv} B$ if $A \leq_m^{rp} B$ with probability $1/p(n)$ for some polynomial bound p. We will reserve the term "the Valiant-Vazirani reduction" to name the randomized reduction from SAT to USAT. Similarly, the Adleman and Manders definition of randomized reductions would be randomized reductions with probability 1/2. Also, in statements where the exact probability bound is not important, we will use the terms 1/poly and 1/exp to indicate that the statement holds for any inverse polynomial and inverse exponential function. As we mentioned before, under certain conditions, $\leq_m^{vv}$-reductions and randomized reductions with probability 1/2 are equivalent.

Definition: For any language B, we define the following classes.

$$\begin{aligned}
\mathrm{OR}_2(B) &= \{\langle x,y\rangle \mid x \in B \text{ or } y \in B\} \\
\mathrm{OR}_\omega(B) &= \{\langle x_1,\ldots,x_n\rangle \mid \text{for some } i,\ 1 \leq i \leq n,\ x_i \in B\} \\
\mathrm{AND}_2(B) &= \{\langle x,y\rangle \mid x \in B \text{ and } y \in B\} \\
\mathrm{AND}_\omega(B) &= \{\langle x_1,\ldots,x_n\rangle \mid \text{for all } i,\ 1 \leq i \leq n,\ x_i \in B\}.
\end{aligned}$$

[1] Valiant and Vazirani credit Alan Selman for this application of their randomized reduction.

We say that the set B has OR_2 if $\mathrm{OR}_2(B) \leq_{\mathrm{m}}^{\mathrm{P}} B$, and similarly for OR_ω, AND_2 and AND_ω.

Lemma 1. If $A \leq_{\mathrm{m}}^{\mathrm{vv}} B$ and B has OR_ω, then $A \leq_{\mathrm{m}}^{\mathrm{rp}} B$ with probability $1 - 1/\exp$.

Proof (Sketch): Let f be the $\leq_{\mathrm{m}}^{\mathrm{vv}}$-reduction from A to B. The idea is to exploit the fact that f makes only one-sided errors and that B has OR_ω. One can construct a randomized reduction g which simulates f repeatedly. The outputs from f are then joined together using the OR_ω function and reduced to B. Then, one can show that polynomially many repetitions diminish the error to inverse exponential. □

Robust languages such as SAT and $\overline{\mathrm{SAT}}$ have both OR_ω and AND_ω. Thus, in cases where one randomly reduces to a nice language, it doesn't matter which definition of randomized reduction is used. However, USAT is not known to have OR_ω. So, there wasn't an obvious way to amplify the Valiant-Vazirani reduction from SAT to USAT.

Nevertheless, the $\leq_{\mathrm{m}}^{\mathrm{vv}}$-reduction from SAT to USAT proved to be useful in many areas of research. For example, Richard Beigel [Bei88] used it to show that SAT is superterse unless RP = NP. Also, Toda [Tod89] used a similar reduction in his proof that $\mathrm{PH} \subseteq \mathrm{P}^{\#\mathrm{P}[1]}$. This result, in turn, led to the Lund, Fortnow, Karloff and Nisan [LFKN90] result: $\mathrm{PH} \subseteq \mathrm{IP}$. So, there should be little doubt in the reader's mind regarding the usefulness of the Valiant-Vazirani reduction. The more pertinent questions are: What does this reduction mean? Does USAT being $\leq_{\mathrm{m}}^{\mathrm{vv}}$-complete for D^{P} mean that it is somehow representative of the whole class? How does the complexity of $\leq_{\mathrm{m}}^{\mathrm{vv}}$-complete sets compare with the $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete languages?

Recent results about the complexity of USAT and of D^{P} shed a new light on these questions. Under the assumption that the Polynomial Hierarchy has infinitely many levels, much has been discovered about $\mathrm{SAT} \wedge \overline{\mathrm{SAT}}$, the D^{P} $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete set. For example, Kadin [Kad88, CK90a] showed that

$$\mathrm{D}^{\mathrm{P}} = \text{co-}\mathrm{D}^{\mathrm{P}} \implies \text{PH collapses.}$$

So, $\mathrm{SAT} \wedge \overline{\mathrm{SAT}} \notin \text{co-}\mathrm{D}^{\mathrm{P}}$ unless PH collapses. Similarly, one can show that $\mathrm{SAT} \wedge \overline{\mathrm{SAT}}$ cannot have OR_ω unless PH collapses [CK90b]. These results show that $\mathrm{SAT} \wedge \overline{\mathrm{SAT}}$ does not have the same robust properties of SAT. So, how does USAT, the $\leq_{\mathrm{m}}^{\mathrm{vv}}$-complete set for D^{P}, compare with the $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete set? As it turns out, Chang and Kadin [CK90c] recently showed that

USAT $\notin \text{co-}\mathrm{D}^{\mathrm{P}}$ unless PH collapses,

USAT does not have OR_ω unless PH collapses.

From these results it would appear that $\leq_{\mathrm{m}}^{\mathrm{vv}}$-complete sets behave much like the $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete sets and this is true *in spite of* the fact that the Valiant-Vazirani reduction cannot be amplified by repeated trials (since USAT does not have OR_ω unless PH collapses). Can these results be generalized for $\leq_{\mathrm{m}}^{\mathrm{vv}}$-complete sets in general? Or do these results only apply to $\leq_{\mathrm{m}}^{\mathrm{vv}}$-complete sets for D^{P}? We will investigate these questions in the next section.

2 A Random Complete Set for co-D^P

In this section we will describe the behavior of a set that is complete for co-D^P under randomized reductions. We will show that its behavior is drastically different from that of D^P $\leq_\mathrm{m}^\mathrm{vv}$-complete sets. The set we have in mind is $\mathrm{SAT}\oplus\overline{\mathrm{SAT}}$ the disjoint union of SAT and $\overline{\mathrm{SAT}}$:

$$\mathrm{SAT}\oplus\overline{\mathrm{SAT}} = \{\ 0F \mid F \in \mathrm{SAT}\ \} \cup \{\ 1F \mid F \in \overline{\mathrm{SAT}}\ \}.$$

Lemma 2. $\mathrm{SAT}\oplus\overline{\mathrm{SAT}}$ is complete for co-D^P under randomized reductions. In particular, $\overline{\mathrm{SAT}}\vee\mathrm{SAT} \leq_\mathrm{m}^\mathrm{rp} \mathrm{SAT}\oplus\overline{\mathrm{SAT}}$ with probability $1/2 + 2^{-n^2}$.

Proof (Sketch): Recall that $\overline{\mathrm{SAT}}\vee\mathrm{SAT}$ is $\leq_\mathrm{m}^\mathrm{P}$-complete for co-$\mathrm{D}^\mathrm{P}$, so we need to display a randomized reduction from $\overline{\mathrm{SAT}}\vee\mathrm{SAT}$ to $\mathrm{SAT}\oplus\overline{\mathrm{SAT}}$. It is simple to construct a randomized reduction with probability greater than or equal to 1/2, because

$$\langle F_1, F_2\rangle \in \overline{\mathrm{SAT}}\vee\mathrm{SAT} \iff F_1 \in \overline{\mathrm{SAT}} \text{ or } F_2 \in \mathrm{SAT}.$$

Thus, a randomized function can choose F_1 or F_2 with equal probability, then output $1F_1$ or $0F_2$. If $\langle F_1, F_2\rangle$ is indeed an element of $\overline{\mathrm{SAT}}\vee\mathrm{SAT}$, then

$$\mathrm{Prob}_{i\in\{0,1\}}[\ iF_{2-i} \in \mathrm{SAT}\oplus\overline{\mathrm{SAT}}\ ] \geq 1/2.$$

On the other hand, if $\langle F_1, F_2\rangle \notin \overline{\mathrm{SAT}}\vee\mathrm{SAT}$, then neither case holds. Thus,

$$\mathrm{Prob}_{i\in\{0,1\}}[\ iF_{2-i} \in \mathrm{SAT}\oplus\overline{\mathrm{SAT}}\ ] = 0.$$

To improve the probability beyond 1/2, simply observe that if $F_2 \in \mathrm{SAT}$, then there is a small probability of guessing a satisfying assignment. This fact can be used to improve the proability to $1/2 + 2^{-n^2}$. See [CR90] for details. $\square$

Note that the probability bound for the reduction described above is much better than the one for reducing $\mathrm{SAT}\wedge\overline{\mathrm{SAT}}$ to USAT. Since USAT behaves so much like the D^P $\leq_\mathrm{m}^\mathrm{P}$-complete sets, one would expect $\mathrm{SAT}\oplus\overline{\mathrm{SAT}}$ to behave like co-D^P $\leq_\mathrm{m}^\mathrm{P}$-complete sets. In fact, $\mathrm{SAT}\oplus\overline{\mathrm{SAT}}$ *does not* resemble $\overline{\mathrm{SAT}}\vee\mathrm{SAT}$. $\mathrm{SAT}\oplus\overline{\mathrm{SAT}}$ can be computed in $\mathrm{P}^{\mathrm{SAT}[1]}$, the set of languages recognized by a polynomial time Turing machine which asks only one query to its SAT oracle. Moreover,

$$\mathrm{P}^{\mathrm{SAT}[1]} \subseteq \mathrm{D}^\mathrm{P} \cap \text{co-}\mathrm{D}^\mathrm{P}.$$

So, there are co-D^P $\leq_\mathrm{m}^\mathrm{vv}$-complete sets in D^P. In contrast, the assumption that USAT $\in$ co-D^P would collapse the Polynomial Hierarchy. Thus, we are left in an asymmetric position: D^P $\leq_\mathrm{m}^\mathrm{vv}$-complete sets behave like the $\leq_\mathrm{m}^\mathrm{P}$-complete sets, but being $\leq_\mathrm{m}^\mathrm{vv}$-complete for co-$\mathrm{D}^\mathrm{P}$ is next to meaningless. At this point, the skeptical reader might suggest that this asymmetry is due to some "special property" of USAT which $\mathrm{SAT}\oplus\overline{\mathrm{SAT}}$ does not enjoy. However, the behavior of USAT we mentioned above is actually a property of *any* $\leq_{\mathrm{m}}^{\mathrm{vv}}$-complete set for D^{P}, not just of USAT. Still, this asymmetry seems very unnatural and we believe that it is an artifact of the definition of $\leq_{\mathrm{m}}^{\mathrm{vv}}$-reductions. The following theorem [CR90] illustrates our point.

Theorem 3. If $\overline{\mathrm{SAT}}\vee\mathrm{SAT} \leq_{\mathrm{m}}^{\mathrm{rp}} \mathrm{SAT}\wedge\overline{\mathrm{SAT}}$ with probability $1/2 + 1/p(n)$ for some polynomial bound p, the Polynomial Hierarchy collapses.

Now, consider a set $G \in$ co-D^{P} such that $\overline{\mathrm{SAT}}\vee\mathrm{SAT} \leq_{\mathrm{m}}^{\mathrm{rp}} G$ with probability $1/2 + 1/\mathrm{poly}$. Then, the theorem shows that G cannot be in D^{P} unless PH collapses. Thus, G is much more representative of co-D^{P} than $\mathrm{SAT}\oplus\overline{\mathrm{SAT}}$. These theorems demonstrate a kind of *threshold* for the probability bounds of randomized reductions. If we restrict our attention to randomized reductions with probability above $1/2 + 1/\mathrm{poly}$, then the languages that are complete for co-D^{P} under this notion of randomized reducibility behave like the $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete sets. However, if we allow randomized reductions with probabilities below this threshold, then even trivial sets like $\mathrm{SAT}\oplus\overline{\mathrm{SAT}}$ can be complete. Thus, when we consider $\leq_{\mathrm{m}}^{\mathrm{rp}}$-complete sets for co-$\mathrm{D}^{\mathrm{P}}$, the smallest non-trivial probability bound is $1/2 + 1/\mathrm{poly}$. In contrast, the smallest non-trivial probability bound for D^{P} $\leq_{\mathrm{m}}^{\mathrm{rp}}$-complete sets is $1/\mathrm{poly}$. It would appear that these thresholds, above which completeness starts making sense, are different for different complexity classes. This still leaves open the question of whether Valiant and Vazirani made the correct decision when they chose $1/\mathrm{poly}$ as the threshold for D^{P} $\leq_{\mathrm{m}}^{\mathrm{rp}}$-complete sets.

To address this question, we return to USAT. Suppose someone were to construct a randomized reduction from SAT to USAT with probability $1/2 + 1/\mathrm{poly}$. Then, USAT would be complete for D^{P} in a much stronger sense. In fact, such a theorem would answer the frequently posed question of whether USAT has OR_2 [CH86, GW86, CGH+89, GNW90]. (It is known that $\mathrm{SAT}\wedge\overline{\mathrm{SAT}}$ does not have OR_2 unless PH collapses [CK90b].)

Corollary 4. If $\mathrm{SAT} \leq_{\mathrm{m}}^{\mathrm{rp}} \mathrm{USAT}$ with probability $1/2 + 1/p(n)$ for some polynomial bound p, then USAT does not have OR_2 unless PH collapses.

Proof: We know that $\overline{\mathrm{SAT}} \leq_{\mathrm{m}}^{\mathrm{P}} \mathrm{USAT}$. By assumption, $\mathrm{SAT} \leq_{\mathrm{m}}^{\mathrm{rp}} \mathrm{USAT}$ with probability $1/2+1/\mathrm{poly}$. If USAT has OR_2, then these two reductions can be combined into a randomized reduction from $\overline{\mathrm{SAT}}\vee\mathrm{SAT}$ to USAT with probability $1/2+1/\mathrm{poly}$. Since $\mathrm{USAT} \in \mathrm{D}^{\mathrm{P}}$, this also gives a randomized reduction from $\overline{\mathrm{SAT}}\vee\mathrm{SAT}$ to $\mathrm{SAT}\wedge\overline{\mathrm{SAT}}$ with probability $1/2 + 1/\mathrm{poly}$. Then, by Theorem 3, PH collapses. $\Box$

So, if we were to call a set $\leq_{\mathrm{m}}^{\mathrm{rp}}$-complete only when the probability bounds are at least $1/2 + 1/\mathrm{poly}$, then we would restore symmetry to our world. However, considering the usefulness of the Valiant-Vazirani reduction from SAT to USAT, one would hesitate to say that they made the wrong definition of $\leq_{\mathrm{m}}^{\mathrm{rp}}$-completeness for D^{P}. However, one could lament the fact that they did not provide a stronger reduction from SAT to USAT. Then, our world could be made nice, sane and symmetric again.

3 A Note on BPP reductions

So far, we have been discussing randomized reductions with one-sided error. In this section, we show that similar results apply to randomized reductions with two-sided error. Traditionally, the BP$\cdot$ operator on a class $\mathcal{C}$ has been defined as follows. A language A is in BP$\cdot\mathcal{C}$ if there exists a language $B \in \mathcal{C}$ and a constant $\varepsilon < \frac{1}{2}$ such that

$$\mathrm{Prob}_z[\ x \in A \iff (x,z) \in B\ ] \geq 1 - \varepsilon.$$

Frequently, a fixed constant such as 1/3 or 1/4 is chosen for ε. Sometimes, ε is allowed to be as large as $1/2 - 1/\mathrm{poly}$. Recently, Toda and Ogiwara defined a stronger operator which they called $\widehat{\mathrm{BP}}\cdot$ in which the error probability is required to be very small:

$$A \in \widehat{\mathrm{BP}}\cdot\mathcal{C} \Longrightarrow \forall p,\ \exists B \in \mathcal{C},\ \mathrm{Prob}_z[\ x \in A \iff (x,z) \in B\ ] \geq 1 - 2^{-p(n)}.$$

We know that if the class $\mathcal{C}$ is closed under majority reductions, then all of the reductions above are equivalent [Sch86]. However, for classes not known to be closed under majority reductions, it makes sense to consider $\widehat{\mathrm{BP}}\cdot$ operations separately. In their paper, Toda and Ogiwara showed that $\mathrm{PH} \subseteq \widehat{\mathrm{BP}}\cdot\mathcal{K}$ where $\mathcal{K}$ is any of the counting classes: PP, $\oplus$P, C$_=$P, or MOD$_g$P. Moreover, they use a version of the Valiant-Vazirani reduction to derive this result. Their proof is particularly interesting, because it does not depend on whether these counting classes are closed under majority reductions.[2] To overcome this obstacle, they showed that by repeating polynomially many Valiant-Vazirani type reductions, the probability of having at least one of the reductions being "correct" is $1 - 1/\exp$. Moreover, using exact counting they can detect whether such a "correct" reduction occurred. Thus, in this case, the power of counting allows one to amplify the probability bounds of randomized reductions. For details, see [TO90].

As the reader may suspect, there are problems in defining $\leq_{\mathrm{m}}^{\mathrm{bpp}}$-reductions in non-robust classes like $\mathrm{D^P}$ and co-$\mathrm{D^P}$. Since $\mathrm{D^P}$ and co-$\mathrm{D^P}$ do not have the power of exact counting, the amplification technique described above do not work for $\mathrm{D^P}$ and co-$\mathrm{D^P}$. The following theorems [CR90] illustrate our point.

Lemma 5. There exists a polynomial time function f such that

$$\mathrm{Prob}_z[\ x \in \overline{\mathrm{SAT}} \vee \mathrm{SAT} \iff f(x,z) \in \mathrm{SAT} \oplus \overline{\mathrm{SAT}}\ ] \geq 2/3.$$

Proof:

Let g be the $\leq_{\mathrm{m}}^{\mathrm{rp}}$-reduction with probability 1/2 from $\overline{\mathrm{SAT}} \vee \mathrm{SAT}$ to $\mathrm{SAT} \oplus \overline{\mathrm{SAT}}$ described in Lemma 2. Our $\leq_{\mathrm{m}}^{\mathrm{bpp}}$-reduction f will always output a member of $\mathrm{SAT} \oplus \overline{\mathrm{SAT}}$ (independent of the input) with probability 1/3. For the remaining 2/3 probability, f simply simulates g. This converts an $\leq_{\mathrm{m}}^{\mathrm{rp}}$-reduction with 1/2 probability and one-sided error into a $\leq_{\mathrm{m}}^{\mathrm{bpp}}$-reduction with probability 2/3 and two-sided error. $\square$

[2] Recently, PP was shown to be closed under intersection and majority reductions [BRS90].

Once again, the existence of a trivial reduction from $\overline{\text{SAT}} \vee \text{SAT}$ to $\text{SAT} \wedge \overline{\text{SAT}}$ indicates that one should consider randomized reductions with a higher probability bound. In fact, $2/3 + 1/\text{poly}$ is the threshold for $\leq_{\text{m}}^{\text{bpp}}$-reductions to $\text{SAT} \wedge \overline{\text{SAT}}$.

Theorem 6. Suppose there exists a polynomial time function f and a polynomial bound p such that

$$\text{Prob}_z[\ x \in \overline{\text{SAT}} \vee \text{SAT} \iff f(x,z) \in \text{SAT} \wedge \overline{\text{SAT}}\ ] \geq 2/3 + 1/p(|x|).$$

Then, the Polynomial Hierarchy collapses.

4 Conclusion

In this column we have investigated the meaning of completeness under randomized reductions. We say that a notion of completeness "makes sense" if the complete languages are in some way representative of the whole complexity class. We have argued that for some classes, completeness under randomized reductions "makes sense" only if the randomized reductions are required to have probability bounds above a certain threshold. Otherwise, even trivial sets can be complete sets under randomized reductions. For the class co-D^{P}, we have shown that this threshold is $1/2 + 1/\text{poly}$. For other classes, we would expect the threshold to be different. Hence we must insist on a different threshold for the notion of completeness under randomized reduction for different complexity classes. For example, USAT is $\leq_{\text{m}}^{\text{vv}}$-complete for both D^{P} and $\text{P}^{\text{SAT}[\log n]}$. Since USAT is not representative of the class $\text{P}^{\text{SAT}[\log n]}$, we should insist on a threshold much higher than inverse polynomial for the class $\text{P}^{\text{SAT}[\log n]}$. For D^{P}, there is some evidence that $\leq_{\text{m}}^{\text{vv}}$-completeness makes sense. However, we should keep in mind that, for some classes, this notion of completeness is strictly weaker than completeness under randomized reductions with probability $1/2 + 1/\text{poly}$ (assuming the Polynomial Hierarchy does not collapse).

5 Acknowledgements

The authors would like to thank Juris Hartmanis for this opportunity to expound their views and for his unwavering guidance and support. They would also like to thank Desh Ranjan for suggesting $\leq_{\text{m}}^{\text{bpp}}$-reductions, Suresh Chari and Radhakrishnan Jagadeesan for enlightening discussions, and Jim Kadin for asking, "What do we know about USAT, anyway?"

References

[AM77] L. M. Adleman and K. Manders. Reducibility, randomness, and intractibility [*sic*]. In *ACM Symposium on Theory of Computing*, pages 151–163, 1977.

[Bei88] R. Beigel. NP-hard sets are p-superterse unless R = NP. Technical Report 4, Department of Computer Science, The Johns Hopkins University, 1988.

[BG82] A. Blass and Y. Gurevich. On the unique satisfiability problem. *Information and Control*, 55(1–3):80–88, 1982.

[BRS90] R. Beigel, N. Reingold, and D. Spielman. PP is closed under intersection. Technical Report TR-803, Department of Computer Science, Yale University, June 1990.

[CGH+89] J. Cai, T. Gundermann, J. Hartmanis, L. Hemachandra, V. Sewelson, K. Wagner, and G. Wechsung. The Boolean hierarchy II: Applications. *SIAM Journal on Computing*, 18(1):95–111, February 1989.

[CH86] J. Cai and L. A. Hemachandra. The Boolean hierarchy: Hardware over NP. In *Structure in Complexity Theory*, Springer-Verlag *Lecture Notes in Computer Science #223*, pages 105–124, 1986.

[CK90a] R. Chang and J. Kadin. The Boolean hierarchy and the polynomial hierarchy: a closer connection. In *Proceedings of the 5th Structure in Complexity Theory Conference*, pages 169–178, July 1990.

[CK90b] R. Chang and J. Kadin. On computing Boolean connectives of characteristic functions. Technical Report 90-1118, Department of Computer Science, Cornell University, May 1990.

[CK90c] R. Chang and J. Kadin. On the structure of uniquely satisfiable formulas. Technical Report 90-1124, Department of Computer Science, Cornell University, May 1990.

[CR90] R. Chang and P. Rohatgi. Random reductions in the Boolean hierarchy are not robust. Technical Report 90-1154, Department of Computer Science, Cornell University, October 1990.

[GNW90] T. Gundermann, N. Nasser, and G. Wechsung. A survey of counting classes. In *Proceedings of the 5th Structure in Complexity Theory Conference*, pages 140–153, July 1990.

[GW86] T. Gundermann and G. Wechsung. Nondeterministic Turing machines with modified acceptance. In *Proceedings of Mathematical Foundations of Computer Science 1986*, Springer Verlag *Lecture Notes in Computer Science #233*, pages 396–404, 1986.

[Joh85] D. S. Johnson. The NP-completeness column: An ongoing guide. *Journal of Algorithms*, 6:291–305, 1985.

[Kad88] J. Kadin. The polynomial time hierarchy collapses if the Boolean hierarchy collapses. *SIAM Journal on Computing*, 17(6):1263–1282, December 1988.

[LFKN90] C. Lund, L. Fortnow, H. Karloff, and N. Nisan. Algebraic methods for interactive proof systems. To appear in *Proceedings of the IEEE Symposium on Foundations of Computer Science*, 1990.

[PY84] C. Papadimitriou and M. Yannakakis. The complexity of facets (and some facets of complexity). *Journal of Computer and System Sciences*, 28(2):244–259, April 1984.

[Sch86] U. Schöning. *Complexity and Structure*. Lecture Notes in Computer Science #211. Springer-Verlag, 1986.

[TO90] S. Toda and M. Ogiwara. Counting classes are at least as hard as the polynomial-time hierarchy. Technical Report 90-09, Department of Computer Science and Information Mathematics, University of Electro-Communications, July 1990.

[Tod89] S. Toda. On the computational power of PP and $\oplus$P. In *Proceedings of the IEEE Symposium on Foundations of Computer Science*, pages 514–519, 1989.

[VV86] L. G. Valiant and V. V. Vazirani. NP is as easy as detecting unique solutions. *Theoretical Computer Science*, 47(1):85–93, 1986.