18.405J/6.841J Advanced Complexity Theory	March 10, 1998
Lecture 9	
Lecturer: Daniel A. Spielman	*Scribe: Venkatesan Guruswami*

1 Introduction

For every known NP-complete problem, the number of solutions over its instances varies over a large range, from zero to exponentially many. It is therefore natural to ask if the inherent intractability of NP-complete problems is caused by this wide variation in the number of possible solutions.

In this lecture we establish that the answer to this question is NO. In particular, we establish a result of Valiant and Vazirani [1] stating that deciding the satisfiability of SAT instances that are promised to have at most one satisfying assignment (let us call such instances as USAT instances in the sequel) is as difficult as deciding satisfiability of general SAT instances.

This is proved by exhibiting a randomized reduction from SAT to USAT, i.e we establish a randomized polynomial-time TM M such that if

$$\begin{aligned} \phi \notin \text{SAT} &\implies M(\phi) \notin \text{SAT (and hence } M(\phi) \notin \text{USAT)} \\ \phi \in \text{SAT} &\implies \text{Prob}[M(\phi) \in \text{USAT}] \geq \frac{1}{8} \end{aligned}$$

where the probability is taken over the internal coin tosses of the machine M.

The above implies that if there exists a polynomial-time randomized algorithm for distinguishing instances of SAT having zero or one satisfying assignment, then we will have $\mathbf{NP} = \mathbf{RP}$, since we can give a $\mathbf{RP}$ algorithm for SAT by first employing the above reduction M and then using the supposed algorithm for deciding USAT.

To give the above reduction, we will now develop some machinery from Universal Hashing which will also be useful in several other places.

2 Universal Hashing

This extremely useful tool was developed by Carter and Wegman.

Definition 1 (Universal Hashing)*: Given sets S and T, a family $\mathcal{H}$ of functions from S to T is a* universal family of hash functions *from S to T if*

- $\forall x \in S$, $\forall w \in T$
$$\text{Prob}_{h\in\mathcal{H}}[h(x) = w] = \frac{1}{|T|} \text{ \textit{(uniformity)}}$$
- $\forall x \neq y \in S$, $\forall w, z \in T$,
$$\text{Prob}_{h\in\mathcal{H}}[(h(x) = w) \wedge (h(y) = z)] = \frac{1}{|T|^2} \text{ \textit{(universal independence)}}$$

An example of a universal hash family: Let $S = \{0,1\}^n$, $T = \{0,1\}^k$, and for $x \in \{0,1\}^n$, let $h_{M,b}(x) = Mx + b$ where M is a $k \times n$ boolean matrix, b is a column vector in $\{0,1\}^k$ and all operations are mod 2. The family $\mathcal{H}$ is the set of functions $h_{M,b}$ for all possible values of M and b.

Proposition 2 *$\mathcal{H} = \{h_{M,b}\}$ is a universal family of hash functions from $\{0,1\}^n$ to $\{0,1\}^k$.*

Proof: We first check universality. For any fixed $x \in \{0,1\}^n - \vec{0}$ and $y \in \{0,1\}^k$ (the case $x = \vec{0}$ is trivial)

$$\begin{aligned}
\mathrm{Prob}_{h\in\mathcal{H}}[h(x) = y] &= \mathrm{Prob}_{M,b}[Mx + b = y] \\
&= \sum_{z\in\{0,1\}^k} \mathrm{Prob}_M[Mx = z] \cdot \mathrm{Prob}_b[b = y - z] \\
&= 2^k \cdot 2^{-k} \cdot 2^{-k} \\
&= 2^{-k}
\end{aligned}$$

To check universal independence, for $x \neq y \in \{0,1\}^n$ and $w, z \in \{0,1\}^k$, we have

$$\begin{aligned}
\mathrm{Prob}_{h\in\mathcal{H}}[(h(x) = w) \wedge (h(y) = z)] &= \mathrm{Prob}_{M,b}[Mx + b = w \wedge My + b = z] \\
&= \mathrm{Prob}_{M,b}[M(x - y) = w - z \wedge Mx + b = w] \\
&= \mathrm{Prob}_M[M(x - y) = w - z] \times \\
&\quad\ \mathrm{Prob}_{M,b}[Mx + b = w \mid M(x - y) = w - z] \\
&= 2^{-k} \times \mathrm{Prob}_{M,b}[Mx + b = w] \\
&= 2^{-k} \cdot 2^{-k} \\
&= 2^{-2k}
\end{aligned}$$

where the fourth equality follows since M is a random $k \times n$ matrix and $x - y$ is a fixed non-zero vector and the events $Mx + b = w$ and $M(x - y) = w - z$ are independent because of the random and independent (from M) choice of b. The next equality follows from the universality property proved earlier. □

We now prove that we do not need the random vector b if $x, y \neq \vec{0}$.

Proposition 3 *$\forall x \neq y \in \{0,1\}^n - \vec{0}$ and $\forall w, z \in \{0,1\}^k$, we have*

$$\mathrm{Prob}_M[Mx = w \wedge My = z] = \frac{1}{2^{2k}}.$$

Proof: If x and y are $e_1 = (1, 0, \ldots, 0)$ and $e_2 = (0, 1, 0, \ldots, 0)$, respectively, then the truth of the proposition is clear. Since neither x nor y is $\vec{0}$, they are linearly independent. Thus, there exists rank n matrix A such that $Ax = e_1$ and $Ay = e_2$. Because the matrix A has full rank, the distribution obtained by multiplying a unformly chosen random matrix M by A is the same as that obtained by just choosing M uniformly at random. So, the truth of the proposition for e_1 and e_2 implies the truth of the proposition in general. □

Proposition 4 *Let $S \subseteq \{0,1\}^n$ with $2^{k-2} \leq |S| \leq 2^{k-1}$. Then,*

$$\mathrm{Prob}[\exists\ !\ s \in S\ s.t\ Ms = \vec{0}] \geq \frac{1}{8}$$

where the probability is taken over the uniform choice of M from the set of all $k \times n$ boolean matrices.

Proof: The proof proceeds by distinguishing two cases.
Case 1: $\vec{0} \in S$. In this case $M\vec{0} = \vec{0}$

$$\begin{aligned}
\text{Prob}_M[\exists s \in S, s \neq \vec{0}, Ms = \vec{0}] &\leq \sum_{s \in S, s \neq \vec{0}} \text{Prob}_M[Ms = \vec{0}] \\
&\leq |S| \cdot 2^{-k} \\
&\leq \frac{1}{2}
\end{aligned}$$

and hence

$$\text{Prob}[\exists! s \in S \text{ s.t } Ms = \vec{0}] \geq \frac{1}{2}$$

Case 2: $\vec{0} \notin S$. Now for any fixed $s \in S$, $\text{Prob}_M[Ms = \vec{0}] = 2^{-k}$ and $\forall t \neq s \in S$, $\text{Prob}_M[Ms = \vec{0} \wedge Mt = \vec{0}] = 2^{-2k}$, which implies $\text{Prob}_M[Mt = \vec{0} \mid Ms = \vec{0}] = 2^{-k}$. Also,

$$\begin{aligned}
\text{Prob}_M[Ms = \vec{0} \wedge \forall t \neq s, Mt \neq \vec{0}] &= \text{Prob}_M[Ms = \vec{0}] \cdot \text{Prob}_M[\forall t \neq s, Mt \neq \vec{0} \mid Ms = \vec{0}] \\
&= 2^{-k} \cdot \left(1 - \text{Prob}_M[\exists t \neq s \in S, Mt = \vec{0} \mid Ms = \vec{0}]\right) \\
&\geq 2^{-k} \cdot \left(1 - \sum_{t \in S, t \neq s} \text{Prob}_M[Mt = \vec{0} \mid Ms = \vec{0}]\right) \\
&= 2^{-k} \left(1 - 2^{-k}(|S| - 1)\right) \\
&\geq 2^{-k-1}.
\end{aligned}$$

Now,

$$\begin{aligned}
\text{Prob}_M[\exists s, Ms = \vec{0} \wedge \forall t \neq s \in S, Mt \neq \vec{0}] &= \sum_{s \in S} \text{Prob}_M[Ms = \vec{0} \wedge \forall t \neq s, Mt \neq \vec{0}] \\
&\geq |S| \cdot 2^{-k-1} \\
&\geq \frac{1}{8},
\end{aligned}$$

where the first equality is because the considered events are all mutually exclusive. □

3 Deciding USAT in RP-time implies NP=RP

The idea is the following: Given an instance of SAT we repeatedly apply restrictions on the formula. Then we run the **RP** machine to detect whether the new formula has exactly one solution or not. The consequence of this is that any **NP** problem will be solved in **RP** time. Since $\mathbf{RP} \subseteq \mathbf{NP}$, this means $\mathbf{NP} = \mathbf{RP}$. Note that this will also imply an hierarchy collapse to the second level.

The successive restrictions are applied as follows. Given a CNF formula ϕ on n variables $\vec{x}$, choose $n+1$ random vectors $\vec{v}_1, \vec{v}_2, \cdots, \vec{v}_{n+1}$, and create the formulas ϕ_i for $1 \leq i \leq n+1$ as follows:

$$\phi_i = \phi \wedge (\vec{x} \cdot \vec{v}_1 = 0) \wedge (\vec{x} \cdot \vec{v}_2 = 0) \wedge \cdots \wedge (\vec{x} \cdot \vec{v}_i = 0)$$

Lemma 5 *If ϕ is not satisfiable, then none of the ϕ_i's are satisfiable.*

Proof: O.K. $\square$

Lemma 6 *If ϕ is satisfiable, then with probability at least 1/8, at least one of the ϕ_i's has a unique satisfying assignment.*

Proof: Let S be the set of satisfying assignments of ϕ: by hypothesis $|S| \geq 1$. Let k be such that $2^{k-2} \leq |S| < 2^{k-1}$. Then by Proposition 4, ϕ_k has a probability $\geq 1/8$ of having exactly one satisfying assignment. $\square$

The above two lemmas provide the randomized reduction of SAT to USAT, thus proving that detecting unique solutions is as hard as **NP**. In complexity–theoretic terms, we have just proved that **NP** is randomly reducible to **UP** where **UP** is the class of *promise problems* whose instances are promised to have either zero or one solution. Put more succinctly, the main results are

Theorem 7 $\mathbf{NP} \subseteq \mathbf{RP}^{\mathbf{UP}}$.

Theorem 8 *If* $\mathbf{UP} \subseteq \mathbf{RP}$, *then* $\mathbf{NP} = \mathbf{RP}$.

References

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