18.405J/6.841J Advanced Complexity Theory	March 6, 2001
Lecture 8	
Lecturer: Daniel A. Spielman	*Scribe: Aram Harrow*

This lecture will prove the Valiant-Vazirani theorem and introduce hash functions.

8.1 The Valiant-Vazirani theorem

The Valiant-Vazirani theorem claims that if we can solve instances of SAT that are known to have only one satisfying assignment, then using randomization we can solve any problem in SAT. It is important both for historical reasons (it ended the question of whether nonlinear search could solve NP-complete problems) and because it introduces a useful tool that led to other so-called *isolation theorems* being proved.

Theorem 1 (Valiant-Vazirani) *If there exists an RP algorithm that can find a satisfying assignment of a SAT or CIRCUIT-SAT instance, given that there is only a single satisfying assignment, then NP=RP.*

Proof outline: We will consider the case of CIRCUIT-SAT, though this will only affect the notation used. The idea is to construct a polytime random algorithm that inputs a circuit $C(x_1 \ldots, x_n)$ and outputs $n+2$ circuits $C_1, \ldots C_{n+2}$ such that

(i) If C is unsatisfiable, then so are $C_1, \ldots, C_{n+2}$.

(ii) If C is satisfiable, then with probability at least $1/8$, one of the C_i will have exactly one satisfying assignment that also is a solution to C.

Now, if an RP algorithm exists to solve instances of CIRCUIT-SAT with a single satisfying assignment, we can use it to solve the general case of CIRCUIT-SAT with one-sided probability of $1/8$.

To construct the C_i, we will let $C_i = C \cap M_i$, for some masks M_i such that the number of solutions to C_i will be no more than 2^{-i+1} times the number of solutions to C.

8.2 Universal hash functions

To construct the masks we will need to develop the concept of a universal hash function. In general, a *hash function* is a function $h : \{0,1\}^n \to \{0,1\}^k$, where we would like that for any $S \subset \{0,1\}^n$ such that $|S| < 2^k$, we have $|h(S)| \approx 2^k$. This, of course, is not possible for a fixed h. For example, let S be the largest pre-image of anything in $\{0,1\}^k$ and $|S| \geq 2^{n-k}$, but $|h(S)| = 1$. Instead we will choose hash functions randomly from a probability distribution in which the action on all inputs are uniform and pairwise independant. More precisely,

Definition 2 *A family of functions $\mathcal{H} : \{0,1\}^n \to \{0,1\}^k$ is said to be* universal *if*

1. $\forall a \in \{0,1\}^n, \forall b \in \{0,1\}^k, Pr_{h \in \mathcal{H}}[h(a) = b] = 2^{-k}$

2. $\forall a_1 \neq a_2 \in \{0,1\}^n, \forall b_1, b_2 \in \{0,1\}^k, Pr_{h\in\mathcal{H}}[h(a_2) = b_2 | h(a_1) = b_1] = 2^{-k}$

$\mathcal{H}$ can also be called a family of pairwise independant functions.

From the definition, it immediately follows that for any distinct a_1 and a_2,

$$\begin{aligned} Pr[h(a_1) = h(a_2)] &= \sum_b Pr[h(a_1) = b \cap h(a_2) = b] \\ &= \sum_b Pr[h(a_1) = b | h(a_2) = b] Pr[h(a_2) = b] \\ &= \sum_b 2^{-k} \cdot 2^{-k} = 2^{-k} \end{aligned}$$

The specific family of hash functions we will use will be the set of all affine linear tranformations over the integers mod 2. So define

$$\mathcal{H} = \{h_{M,y} : M \in \{0,1\}^{k\times n}, y \in \{0,1\}^k$$

where

$$h_{M,y}(x) = Mx + y \pmod 2$$

So, h multiplies its input by a random matrix and adds a random vector, all mod 2. First, we prove that $\mathcal{H}$ is a univeral family of hash functions.

1. We must show that $\forall a, b Pr[h(a) = b] = 2^{-k}$. For this, all we need is the fact that we're adding a randomly chosen vector y.

$$Pr[h(a) = b] = Pr[Ma + y = b] = Pr[y = Ma + b] = 2^{-k}$$

2. $\forall a_1 \neq a_2, b_1, b_2$, such that $Ma_1 + y = b_1$ and $Ma_2 + y = b_2$, adding gives that $M(a_1 + a_2) = b_1 + b_2$.

So,

$$\begin{aligned} \Pr[Ma_2 + y = b_2 | Ma_1 + y = b1] &= \Pr[M(a_1 + a_2) = b_1 + b_2 | Ma_1 + y = b_1] \\ &= \frac{\Pr[M(a_1 + a_2) = b_1 + b_2 \cap Ma_1 + y = b_1]}{2^{-k}} \\ &= \Pr[M(a_1 + a_2) = b_1 + b_2] \end{aligned} \quad (8.1)$$

Since $a_1 \neq a_2$, we have that $a_1 + a_2$ has at least one nonzero component and thus $M(a_1 + a_2)$ is the sum of at least one column of M. Since each column is an independant uniformly distibuted vector drawn from $\{0,1\}^k$, the result is also uniformly distributed. Thus, eq. 8.1 becomes 2^{-k}, as desired.

The following lemma demonstrates how universal hash functions are useful in constructing instances of SAT with a single satisfying assignment.

Lemma 3 *Let $S \subset \{0,1\}^n$ such that $2^{k-2} \leq |S| < 2^{k-1}$ and $\mathcal{H}$ a universal family from $\{0,1\}^n \to \{0,1\}^k$. Then $Pr_{h\in\mathcal{H}}[|h^{-1}(0^k) \cap S| = 1] \geq 1/8$.*

Proof: Let $E_a = (h(a) = 0) \cap (\forall b \neq a, h(b) \neq 0^k)$.

An equivalent probability to the one we want is

$$\Pr_{h\in\mathcal{H}}[\exists! a \in S : h(a) = 0^k] = \Pr_{h\in\mathcal{H}}[\exists a \in S : h(a) = 0^k \cap \forall b \neq a, h(b) \neq 0^k]$$

Since all the E_a are disjoint, the probability that any is true is simply

$$\begin{aligned}
\sum_{a\in S} \Pr_{h\in\mathcal{H}}[E_a] &= \sum_{a\in S} \Pr_{h\in\mathcal{H}}[h(a)=0]\Pr_{h\in\mathcal{H}}[\forall b\neq a, h(b)\neq 0|h(a)=0] \\
&= \sum_{a\in S} 2^{-k}\left(1-\Pr_{h\in\mathcal{H}}[\exists b\neq a \text{ s.t. } h(b)\neq 0|h(a)=0]\right) \\
&\geq \sum_{a\in S} 2^{-k}\left(1-\sum_{b\neq a}\Pr_{h\in\mathcal{H}}[h(b)\neq 0|h(a)=0]\right) \\
&= \sum_{a\in S} 2^{-k}\left(1-(|S|-1)2^{-k}\right) = |S|2^{-k}\left(1+2^{-k}-|S|2^{-k}\right) \\
&\geq |S|2^{-k}\left(1-|S|2^{-k}\right) \geq |S|2^{-k}\left(\frac{1}{2}\right) \geq \left(\frac{1}{4}\right)\left(\frac{1}{2}\right) = \frac{1}{8}
\end{aligned}$$

■

Now we return to the theorem. To construct M_k, choose a hash function h_k at random from n bits to k bits. Since h_k is computable in polynomial time we can easily construct a circuit (or boolean function, if you prefer) M_k such that $M_k(x) = h_k(x)$.

The first statement that we need to prove is that if C has no satisfying assignment then no C_i does. This follows trivially from the fact that $C_i = C \cap M_i$.

We also need the probability of at least one C_k having a unique satisfying assignment to be at least 1/8. If we let $S = \{x \in \{0,1\}^n : C(x) = 1\}$, then lemma 3 implies that k such that $2^{k-2} \leq |S| < 2^{k-1}$ will suffice and obviously one such k exists between 1 and $n+2$. Q.E.D.

A random closing note. The universal family of hash functions that we chose requires $O(kn)$ random bits, but it's possible to bring this down to $O(n+k)$.