

Valiant Vazirani Theorem and Toda's Theorem

Algorithms and Complexity II

National Technical University of Athens

January 13, 2019

Overview

1 Valiant Vazirani Theorem

2 Toda's Theorem

- *USAT* is the satisfiability problem for boolean formulas that are promised to have at most one satisfying assignment.
- \mathbb{GF}_2^n is the vector space of dimension n over \mathbb{GF}_2 , the field of two elements.
- Let \mathbb{F} be a field, \mathbb{F}^n be a vector space over \mathbb{F} , and let E be a subset of \mathbb{F}^n . Then E is a subspace of \mathbb{F}^n if:
 - 1 The zero vector, $\mathbf{0}$, is in E .
 - 2 If \mathbf{x} and \mathbf{y} are elements of E , then the sum $\mathbf{x} + \mathbf{y}$ is an element of E .
 - 3 If \mathbf{x} is an element of E and c is a scalar from \mathbb{F} , then the scalar product $c\mathbf{x}$ is an element of E .
- For a set A of vectors, the orthogonal complement of A is the set $A^\perp =_{\text{def}} \{\mathbf{y} \mid \forall \mathbf{x} \in A \mathbf{x} \cdot \mathbf{y} = 0\}$, where \cdot denotes inner product.

Lemma

Let S be a nonempty subset of \mathbb{GF}_2^n . Let E_0, \dots, E_n be a random tower of linear subspaces of \mathbb{GF}_2^n ,

$$\{\mathbf{0}\} = E_0 \subset E_1 \subset \dots \subset E_n = \mathbb{GF}_2^n, \text{ with } \dim E_i = i.$$

Then $\Pr(\exists i | S \cap E_i| = 1) \geq \frac{3}{4}$.

How can we choose a tower of linear subspaces uniformly at random?

- Choose a random basis $\mathbf{x}_1, \dots, \mathbf{x}_n$ of \mathbb{F}^n . This can be done efficiently.
- Define $E_i = \{\mathbf{x}_1, \dots, \mathbf{x}_{n-i}\}^\perp$.
- Each E_i is represented by some random vectors $\mathbf{x}_1, \dots, \mathbf{x}_{n-i}$.
- It holds that $E_{i-1} = E_i \cap \{\mathbf{x}_{n-i+1}\}^\perp$.

For example, if $\mathbb{F}^n = \mathbb{GF}_2^n$, for $n = 4$, and the random basis is $\{(1, 0, 0, 0), (0, 1, 0, 0), (0, 0, 1, 0), (0, 0, 0, 1)\}$, then

$$F_0 = \{(1, 0, 0, 0), (0, 1, 0, 0), (0, 0, 1, 0), (0, 0, 0, 1)\}^\perp = \{(0, 0, 0, 0)\}$$

$$F_1 = \{(1, 0, 0, 0), (0, 1, 0, 0), (0, 0, 1, 0)\}^\perp = \{(0, 0, 0, 0), (0, 0, 0, 1)\}$$

$$F_2 = \{(1, 0, 0, 0), (0, 1, 0, 0)\}^\perp = \{(0, 0, 0, 0), (0, 0, 0, 1), (0, 0, 1, 0), (0, 0, 1, 1)\}$$

$$F_3 = \{(1, 0, 0, 0)\}^\perp =$$

$$\{(0, 0, 0, 0), (0, 0, 0, 1), (0, 0, 1, 0), (0, 1, 0, 0), (0, 1, 0, 1), (0, 1, 1, 0), (0, 0, 1, 1), (0, 1, 1, 1)\}$$

$$F_4 = \mathbb{GF}_2^4$$

Valiant Vazirani Theorem

Theorem ([Valiant and Vazirani, 1986])

$$NP \subseteq RP^{USAT}.$$

Proof. We show that $SAT \in RP^{USAT}$.

That is, we show that there is a polynomial-time bounded probabilistic oracle Turing machine M with oracle $USAT$ such that:

$$\begin{aligned}\phi \text{ is satisfiable} &\Rightarrow Pr(M \text{ accepts } \phi) \geq \frac{3}{4}, \\ \phi \text{ is unsatisfiable} &\Rightarrow Pr(M \text{ accepts } \phi) = 0.\end{aligned}$$

- Let ϕ be the input formula and w a string of random bits that M produces.
- $M(\phi \# w)$ constructs a random tower of linear subspaces $F_i \subseteq \mathbb{GF}_2^n$ (as in the Lemma), where n is the number of boolean variables x_1, \dots, x_n of ϕ .
- For each $0 \leq i \leq n$, M constructs a formula ψ_i , the satisfying assignments of which are the n -vectors of F_i .

Valiant Vazirani Theorem

Proof cont.

- This construction is a straightforward encoding of the inner product of (x_1, \dots, x_n) with the random vectors representing F_i .
- The machine M queries the oracle on the conjunctions $\phi \wedge \psi_i$ and accepts iff the oracle responds “yes” to any of these queries.
- Let S be the set of truth assignments satisfying ϕ .
 - 1 If $S \neq \emptyset$, then $Pr_w(M \text{ accepts } \phi \# w) = Pr(\exists i \phi \wedge \psi_i \in USAT) = Pr(\exists i |S \cap F_i| = 1) \geq \frac{3}{4}$.
 - 2 If $S = \emptyset$, then $Pr_w(M \text{ accepts } \phi \# w) = Pr(\exists i \phi \wedge \psi_i \in USAT) = Pr(\exists i |S \cap F_i| = 1) = 0$.



How we encode F_i by ψ_i ?

- Let $\mathbf{a}_1, \dots, \mathbf{a}_n$ be a random basis of \mathbb{GF}_2^n . Then,
 $F_{i-1} = \{\mathbf{a}_1, \dots, \mathbf{a}_{n-i+1}\}^\perp = F_i \cap \{\mathbf{a}_{i-n+1}\}^\perp$.
- For example, if ϕ has 4 variables, x_1, x_2, x_3, x_4 , and the basis chosen is $\{\mathbf{a}_1 = (1, 0, 0, 0), \mathbf{a}_2 = (0, 1, 0, 0), \mathbf{a}_3 = (0, 0, 1, 0), \mathbf{a}_4 = (0, 0, 0, 1)\}$, then

- 1 $F_4 = \mathbb{GF}_2^4$ is encoded by
 $\psi_4 = (x_1 \vee \neg x_1) \wedge (x_2 \vee \neg x_2) \wedge (x_3 \vee \neg x_3) \wedge (x_4 \vee \neg x_4)$, i.e. all truth assignments satisfy ψ_4 .
- 2 $F_3 = F_4 \cap \{(0, 0, 0, 1)\}^\perp$ is encoded by
 $\psi_3 = \psi_4 \wedge (x_1 \vee \neg x_1) \wedge (x_2 \vee \neg x_2) \wedge (x_3 \vee \neg x_3) \wedge (\neg x_4)$, i.e. all the satisfying truth assignments of ψ_3 correspond to vectors orthogonal to $(0, 0, 0, 1)$.
- 3 $F_2 = F_3 \cap \{(0, 0, 1, 0)\}^\perp$ is encoded by
 $\psi_2 = \psi_3 \wedge (x_1 \vee \neg x_1) \wedge (x_2 \vee \neg x_2) \wedge (\neg x_3) \wedge (x_4 \vee \neg x_4)$.
- 4 $F_1 = F_2 \cap \{(0, 1, 0, 0)\}^\perp$ is encoded by
 $\psi_1 = \psi_2 \wedge (x_1 \vee \neg x_1) \wedge (\neg x_2) \wedge (x_3 \vee \neg x_3) \wedge (x_4 \vee \neg x_4)$.
- 5 $F_0 = F_1 \cap \{(1, 0, 0, 0)\}^\perp = \{(0, 0, 0, 0)\}$ is encoded by
 $\psi_0 = \psi_1 \wedge (\neg x_1) \wedge (x_2 \vee \neg x_2) \wedge (x_3 \vee \neg x_3) \wedge (x_4 \vee \neg x_4)$.

Lemma

Fix a set $S \subseteq \mathbb{F}_2^n$, then for $\mathbf{x}_1, \dots, \mathbf{x}_{n+1} \in_R \mathbb{F}_2^n$,

(a) if $\mathbf{0} \in S$, then $\Pr(|S \cap \{\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_{n+1}\}^\perp| = 1) > \frac{1}{2}$

(b) if $\mathbf{0} \notin S$, and $2^{i-1} \leq |S| \leq 2^i$, then
 $\Pr(|S \cap \{\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_{i+1}\}^\perp| = 1) > \frac{1}{8}$.

Proof.(a) Since we always have $\mathbf{0} \in \{\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_{n+1}\}^\perp$, if $\mathbf{0} \in S$, then $\mathbf{0} \in S \cap \{\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_{n+1}\}^\perp$. For any $\mathbf{x} \in \mathbb{F}_2^n$, $\mathbf{x} \neq \mathbf{0}$, we have for any j that $\Pr(\mathbf{x}_j \cdot \mathbf{x} = 0) = \frac{1}{2}$. Therefore, since the \mathbf{x}_j are chosen independently, $\Pr(\mathbf{x}_1 \cdot \mathbf{x} = \mathbf{x}_2 \cdot \mathbf{x} = \dots = \mathbf{x}_{n+1} \cdot \mathbf{x} = 0) = \frac{1}{2^{n+1}}$. Thus

$$\Pr(\exists \mathbf{x} \in S - \{\mathbf{0}\}, \mathbf{x} \in \{\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_{n+1}\}^\perp) \leq \sum_{\mathbf{x} \in S - \{\mathbf{0}\}} \Pr(\mathbf{x} \in \{\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_{n+1}\}^\perp) = \frac{|S|-1}{2^{n+1}} < \frac{1}{2}.$$

It follows that with probability greater than $\frac{1}{2}$, $\mathbf{0}$ is the only element of $S \cap \{\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_{n+1}\}^\perp$.

Lemma

Fix a set $S \subseteq \mathbb{F}_2^n$, then for $\mathbf{x}_1, \dots, \mathbf{x}_{n+1} \in_R \mathbb{F}_2^n$,

(a) if $\mathbf{0} \in S$, then $\Pr(|S \cap \{\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_{n+1}\}^\perp| = 1) > \frac{1}{2}$

(b) if $\mathbf{0} \notin S$, and $2^{i-1} \leq |S| \leq 2^i$, then

$\Pr(|S \cap \{\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_{i+1}\}^\perp| = 1) > \frac{1}{8}$.

Proof.(b) Suppose that $\mathbf{0} \notin S$ and $2^{i-1} \leq |S| \leq 2^i$. Define $h(\mathbf{x}) = (\mathbf{x}_1 \cdot \mathbf{x}, \dots, \mathbf{x}_{i+1} \cdot \mathbf{x}) \in \mathbb{F}_2^{i+1}$. Then, $\Pr[h(\mathbf{x}) = \mathbf{0}] = \frac{1}{2^{i+1}}$.

Suppose now that $\mathbf{x} \neq \mathbf{y}$ and $\mathbf{x}, \mathbf{y} \neq \mathbf{0}$. Then,

$\Pr[h(\mathbf{x}) = h(\mathbf{y}) = \mathbf{0}] = 1/2^{2(i+1)}$ for $\mathbf{x}, \mathbf{y} \in S$, $\mathbf{x} \neq \mathbf{y}$.

$$\begin{aligned} & \text{Thus, } \Pr[\exists \mathbf{y} \in S \setminus \{\mathbf{x}\}. h(\mathbf{x}) = h(\mathbf{y}) = \mathbf{0}] \leq \\ & \leq \sum_{\mathbf{y} \in S \setminus \{\mathbf{x}\}} \Pr[h(\mathbf{x}) = h(\mathbf{y}) = \mathbf{0}] = \frac{|S|-1}{2^{2(i+1)}} < \frac{1}{2^{i+2}}, \text{ since } |S| \leq 2^i. \end{aligned}$$

Proof.(b) Therefore,

$$\begin{aligned} &Pr[h(\mathbf{x}) = \mathbf{0} \text{ and } \forall \mathbf{y} \in S \setminus \{\mathbf{x}\}. h(\mathbf{y}) \neq \mathbf{0}] = \\ &= Pr[h(\mathbf{x}) = \mathbf{0}] - Pr[\exists \mathbf{y} \in S \setminus \{\mathbf{x}\}. h(\mathbf{x}) = h(\mathbf{y}) = \mathbf{0}] > \frac{1}{2^{i+1}} - \frac{1}{2^{i+2}} = \frac{1}{2^{i+2}}. \end{aligned}$$

Taking the union of these events, which are disjoint, over all choices of $\mathbf{x} \in S$,

$$Pr[\exists \mathbf{x}. h(\mathbf{x}) = \mathbf{0} \text{ and } \forall \mathbf{y} \in S \setminus \{\mathbf{x}\}. h(\mathbf{y}) \neq \mathbf{0}] > \frac{|S|}{2^{i+2}} \geq \frac{2^{i-1}}{2^{i+2}} = \frac{1}{8}, \text{ since } |S| \geq 2^{i-1}.$$

Logspace analog of Valiant-Vazirani Theorem

Theorem ([Avi Wigderson, 1994])

$$STCONN \leq_{RL}^{1/n^3} UNIQUE - STCONN$$

That is, there is a logspace bounded probabilistic oracle Turing machine M with oracle $UNIQUE - STCONN$ such that

$$\begin{aligned} G \text{ has at least one } s\text{-}t \text{ path} &\Rightarrow Pr(M \text{ accepts } G) \geq \frac{1}{n^3}, \\ G \text{ has no } s\text{-}t \text{ path} &\Rightarrow Pr(M \text{ accepts } G) = 0. \end{aligned}$$

Lemma 2

Lemma (2)

$$BP \cdot \oplus P \subseteq P^{\#P}.$$

Proof. Let $L \in BP \cdot \oplus P$. Then there exists $A \in \oplus P$ such that for all x

- $x \in L \Rightarrow \exists^+ y : x; y \in A$
- $x \notin L \Rightarrow \exists^+ y : x; y \notin A$

where y has length $|x|^k$ for some $k \in \mathbb{N}$. Equivalently,

- $x \in L \Rightarrow |W(n^k, A, x)| \geq \frac{3}{4} \cdot 2^{|x|^k}$
- $x \notin L \Rightarrow |W(n^k, A, x)| \leq \frac{1}{4} \cdot 2^{|x|^k}$

where $W(n^k, A, x)$ is the witness set

$$W(n^k, A, x) =^{def} \{y \in \{0, 1\}^{|x|^k} : x; y \in A\}.$$

Lemma 2

Proof cont. Because $A \in \oplus P$, there exists a polynomial-time nondeterministic TM M such that $x, y \in A$ iff $\text{acc}_M(x, y)$ is odd.

We construct M' such that

- $\text{acc}_M(x, y) \equiv 1 \pmod{2} \Rightarrow \text{acc}_{M'}(x, y) \equiv -1 \pmod{2^{|x|^{k+1}}}$
- $\text{acc}_M(x, y) \equiv 0 \pmod{2} \Rightarrow \text{acc}_{M'}(x, y) \equiv 0 \pmod{2^{|x|^{k+1}}}$

How?

The machine M' has $h^m(\text{acc}_M(x, y))$, where $h(z) = 4z^3 + 3z^4$, and $m = \log(|x|^k + 1)$.

It holds that

$$z \text{ is odd} \Rightarrow h^m(z) \equiv -1 \pmod{2^{2^m}}$$

$$z \text{ is even} \Rightarrow h^m(z) \equiv 0 \pmod{2^{2^m}}$$

Now we can determine membership in L by a $P^{\#P}$ computation as follows:
we construct a new TM N that on input x of length n :

- 1 generates all possible strings $x; y$ with $|y| = n^k$ by nondeterministic branching, one computation path for each such string,
- 2 for each $x; y$, runs M' on $x; y$.

Lemma2

Proof cont.

$$\begin{aligned} acc_N(x) &= \sum_{|y|=n^k} acc_{M'}(x; y) \equiv \\ &\equiv \sum_{y: acc_M(x; y) \text{ odd}} -1 + \sum_{y: acc_M(x; y) \text{ even}} 0 \pmod{2^{|x|^{k+1}}} \equiv \\ &\equiv 2^{|x|^{k+1}} - |\{y : |y| = n^k \text{ and } acc_M(x; y) \text{ is odd}\}| \pmod{2^{|x|^{k+1}}} \\ &= 2^{|x|^{k+1}} - |\{y : |y| = n^k \text{ and } x, y \in A\}| = \\ &= 2^{|x|^{k+1}} - |W(n^k, A, x)|. \end{aligned}$$

If we know this quantity we can decide if $x \in L$. Why?

Lemma 2

Recall that $L \in BP \cdot \oplus P$.

Thus there exists $A \in \oplus P$ such that for all x

$$\bullet x \in L \Rightarrow \frac{3}{4} \cdot 2^{|x|^k} \leq |W(n^k, A, x)| \leq 2^{|x|^k} \Rightarrow$$


$$2^{|x|^k} \leq 2^{|x|^{k+1}} - |W(n^k, A, x)| \leq \frac{5}{4} \cdot 2^{|x|^k}$$

$$\bullet x \notin L \Rightarrow 0 \leq |W(n^k, A, x)| \leq \frac{1}{4} \cdot 2^{|x|^k} \Rightarrow$$

$$\frac{7}{4} \cdot 2^{|x|^k} \leq 2^{|x|^{k+1}} - |W(n^k, A, x)| \leq 2^{|x|^{k+1}}.$$

So a polynomial-time TM makes an oracle call for $acc_N(x)$ and computes $acc_N(x) \bmod 2^{|x|^{k+1}}$.

References

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

 Dexter Kozen
Theory of Computation
Springer, New York, 2006.

 Avi Wigderson
 $NL/poly \subseteq \oplus L/poly$
Structure in Complexity Theory Conference 1994: 59–62.