Valiant-Vazirani Theorem

Ilya Posov

June 24, 2006

1 Introduction

Leslie G. Valiant and Vijay V. Vazirani in 1986 wrote a paper with the name 'NP is as Easy as Detecting Unique Solutions' [?]. The theorem they proved became the classical theorem in the complexity theory, so sometimes it's even called a lemma instead of a theorem. In this text it will be presented the statement of the theorem, two different proofs, and also it would be some discussion.

Both L.G. Valiant and V.V. Vazirani are professors of computer science, L.G. Valiant works at the Harvard University, V.V. Vazirani works at the Georgia Tech and at the University of California, Berkley. They have their homepages and more information about them can be found there: http://people.deas.harvard.edu/∼valiant/, http://www-static.cc.gatech.edu/∼vazirani/.

2 Statement of the Theorem

Before we give the proof of the theorem, let us think of its statement. The theorem deals with the satisfiability problem (SAT). Given a Boolean formula one is to say whether there is an assignment to its variables that would make the formula true. Such assignments will be called satisfying assignments. If the formula has no satisfying assignments, it will be called unsatisfiable. If the formula has exactly one satisfying assignment, it will be called uniquely-satisfiable. The conjunctive normal form (CNF) of the formula is the other well-known concept, the formula is said to be in the CNF, if it is a conjunction of a set of clauses, where clause is a disjunction of a set of variables and negations of variables. As an example to all said above, F is a uniquely-satisfiable formula in CNF with the only satisfying assignment $x = \text{true}, y = \text{false}, z = \text{true}$:

$$F = (x) \wedge (\bar{x} \vee z) \wedge (\bar{x} \vee \bar{y} \vee \bar{z})$$

Theorem 1 (Valiant-Vazirani) *Given a Boolean formula F in CNF it can be constructed in polynomial time a set of formulas $F_1, F_2, \ldots, F_m$ (all in CNF) such that*

- *if F is satisfiable, than with probability more than $1/2$ one of F_i is uniquely-satisfiable.*
- *if F is unsatisfiable, than all F_i are unsatisfiable too.*

The construction that is mentioned in the theorem is polynomial. It means that m, that is the size of the set $\{F_i\}$, is polynomial to the size of input, and the sizes of formulas F_i are also polynomial to the size of input. The construction is probabilistic; it means that if we run it several times on the same formula F we would obtain different resulting sets $\{F_i\}$.

3 Solving SAT with Valiant-Vazirani theorem

Imagine we want to solve the satisfiability problem by means of the construction from the Valiant-Vazirani theorem. Consider the algorithm u-solver() that accepts Boolean formulas as the input and returns the answer in the following way:

- u-solver(F) = Yes, if F has exactly one satisfying assignment
- u-solver(F) = No, if F has no satisfying assignments
- u-solver(F) = Yes/No (unpredictable), otherwise

u-solver has the meaning that can be described as follows: it test the given formula for satisfiability, assuming that it has not more than one satisfying assignment. If we look on the definition of the u-solver we see that it works in unpredictable way, if the given formula has more than one solution. The kind of problem u-solver solves called promise problem: we promise the algorithm something about the input, in this case promise is about the number of solutions of the given formula (not more than one). It's not a simple task to test whether the formula has not more than one solution, so if u-solver dosn't want to do it, it can simply believe the promise. The problem u-solver solves is called UNIQUE-SAT.

Common sense hints that UNIQUE-SAT is to be simpler than SAT, and actually there are algorithms for UNIQUE-SAT (u-solvers) that work faster than SAT algorithms. Now we are going to show that Valiant-Vazirani theorem reduces SAT to UNIQUE-SAT.

Imagine we have a formula F, let us make a Valiant-Vazirani construction and obtain a set of formulas $\{F_i\}$. Now let us apply a u-solver to every F_i. We would obtain a set of answers a_i. There are two different cases:

- formula F is unsatisfiable. Then, as Valiant-Vazirani theorem says, all F_i are unsatisfiable and, based on the definition of u-solver, all a_i would be No.
- formula F is satisfiable. Then, again as Valiant-Vazirani theorem says, with probability more than 1/2 one of F_i would be uniquely-satisfiable. u-solver on such formulas returns Yes as an answer, it means that with probability more than 1/2 one of a_i would be Yes.

Now we can make the decision about the satisfiability of the formula F based on whether there are Yeses in $\{a_i\}$. If there are no Yeses, we say that formula is unsatisfiable, if there are some, we say that formula is satisfiable.

Of cause, we are not always right in our decision about the satisfiability of F, but let us analyze our answers. If F is unsatisfiable, we would always say 'unsatisfiable', if F is satisfiable, we would sometimes say the wrong answer, but with probability less than 1/2. It reminds us the definition of the RP class, the right and false answers are to be distributed in the same way there. So we have the result that SAT is in RP class, but with an oracle that solves a UNIQUE-SAT problem:

$$\mathbf{SAT} \in \mathbf{RP}^{\mathbf{UNIQUE-SAT}}$$

Sat is an NP-complete problem, thus any problem of NP can be solved by means of u-solver() in the already discussed way, if it's first of all reduced to some instance of SAT:

$$\mathbf{NP} \subset \mathbf{RP}^{\mathbf{UNIQUE-SAT}}$$

To understand the next result one is just to remind herself the inclusion **RP** $\subset$ **BPP**:

$$\mathbf{NP} \subset \mathbf{BPP}^{\mathbf{UNIQUE-SAT}}$$

UNIQUE-SAT is a promise problem, machine that solves it works unpredictably on inputs that are promised not to be given to the machine. By the way, machine that solves SAT solves UNIQUE-SAT too. There are two other normal (not promise) machines for UNIQUE-SAT. The first tests whether the formula has exactly one satisfying assignment (USAT problem from the UP complexity class), the second tests, whether the formula has odd number of satisfying assignment (⊕SAT problem from ⊕P complexity class). That leads us to two last results about the inclusion of NP:

$$\mathbf{NP} \subset \mathbf{BPP}^{\mathbf{UP}},\ \mathbf{NP} \subset \mathbf{BPP}^{\oplus\mathbf{P}}$$

4 First Proof

The first proof is almost similar to the one given in the book of Papadimitriu [?]. We would use the concept of hyperplanes, so now we are going to define them.

Definition 1 *Let $S \subseteq \{x_1, x_2, \dots, x_n\}$. Hyperplane η_S is a Boolean formula in CNF, stating that an even number of x_i in S is true.*

Consider an example. Let $n = 4$ and $S = \{x_1, x_2, x_4\}$.

$$\eta_S = (y_0) \wedge (y_1 \Leftrightarrow (y_0 \oplus x_1)) \wedge (y_2 \Leftrightarrow (y_1 \oplus x_2)) \wedge (y_3 \Leftrightarrow y_2) \wedge (y_4 \Leftrightarrow (y_3 \oplus x_4)) \wedge (y_4)$$

η_S is not in CNF and it is to be converted in CNF. But all properties of it are better seen when it's written in this form. It's not very hard to check that in every satisfying assignment of η_S there are even number of true variables of set S. Indeed, in every satisfying assignment, variables y_0 and y_4 are to be true. Variables y_0 and y_1 are equal unless x_1 is true. y_1 and y_2 are equal unless x_2 is true. y_2 and y_3 are equal in every satisfying assignment, y_3 and y_4 are equal unless x_4 is true. So, if we consequently look on the truth values of $y_0, y_1, \dots, y_4$ we see that in the beginning and in the end it would be true, and changing of the truth value occurs if the corresponding x_i is true. Truth value of y_i changed even number of times and thus there are even number of true x_i.

For other values of n and for other S the hyperplane η_S can be constructed in the same way.

The first proof of Valiant-Vazirani Theorem

We are given a formula F in CNF, it has variables $x_1, x_2, \dots, x_n$. Let T be a set of satisfying assignments of the formula F. $D = |T|$ is a number of its satisfying assignments.

We are going to construct a set of formulas $\{F_i\}$ from the statement of the Valiant-Vazirani theorem. For this purpose we choose $n + 1$ random subsets S_i of $\{x_1, \dots, x_n\}$ $(1 \le i \le n + 1)$. Construction of F_i is as follows:

$$\begin{aligned} F_0 &= F \\ F_1 &= F \wedge \eta_{S_1} \\ F_2 &= F \wedge \eta_{S_1} \wedge \eta_{S_2} \\ &\dots \\ F_{n+1} &= F \wedge \eta_{S_1} \wedge \eta_{S_2} \cdots \wedge \eta_{S_{n+1}} \end{aligned}$$

Every F_i is a formula in CNF because it's a conjunction of the formula F that is in CNF and some set of hyperplanes that are in CNF by definition. One obvious thing is that if F was unsatisfiable, than all F_i are unsatisfiable too. So, to prove the theorem we are to show that if F is satisfiable, than with high probability one of F_i is uniquely-satisfiable.

If F is satisfiable, it has $D > 0$ satisfying assignments. Let k be such an integer that $2^k \leq D \leq 2^{k+1}$. We are going to show that with probability more than 1/8 the formula F_{k+2} is uniquely satisfiable.

1/8 is not the desired probability, but we can make the construction of $\{F_i\}$ several times. The probability that every time we build a set without uniquely-satisfiable formulas is not greater than 7/8, so after 6 independent constructions this probability would be not greater than $(7/8)^6 < 1/2$. Thus it suffices to give a proof about the 1/8 probability.

We are going to prove that the formula F_{k+2} is uniquely-satisfiable with probability greater than 1/8.

$$F_{k+2} = F \wedge \eta_{S_1} \wedge \eta_{S_2} \wedge \ldots \wedge \eta_{S_{k+2}}$$

Let us bound the probability $\mathbb{P}_{S_i}\{F_{k+2} \text{ is uniquely satisfiable}\}$. For this let us take any satisfying assignment t of the initial formula F. There are several cases. t can be a satisfying assignment of F_{k+2} if it satisfies all hyperplanes η_{S_i} for $1 \leq i \leq k+2$. It can be not a satisfying assignment of F_{k+2} if it doesn't satisfy some η_{S_i}, and it can be the only satisfying assignment of F_{k+2}. The probability of this is:

$$\begin{aligned}
&\mathbb{P}_{S_i}\{t \text{ is the only satisfying assignment of } F_{k+2}\} = \\
&\mathbb{P}_{S_i}\{\forall i\ \eta_{S_i}(t) = \mathit{true}\ \&\ \forall t' \in T \setminus \{t\} \exists i\ \eta_{S_i}(t') \neq \eta_{S_i}(t)\} = \\
&\mathbb{P}_{S_i}\{\forall i\ \eta_{S_i}(t) = \mathit{true}\} \cdot \mathbb{P}_{S_i}\{\forall t' \in T \setminus \{t\} \exists i\ \eta_{S_i}(t') \neq \eta_{S_i}(t)\} = \\
&\mathbb{P}_1 \cdot \mathbb{P}_2
\end{aligned}$$

The first equality here means that t would be the only satisfying assignment of F_{k+2} if and only if it satisfies all hyperplanes η_{S_i} for $1 \leq i \leq k+2$ and any other satisfying assignment t' of the initial formula F doesn't satisfy at least one hyperplane η_{S_i}. The last fact, that t' doesn't satisfy some hyperplane is coded in the following way: there is such hyperplane η_S that $\eta_S(t) \neq \eta_S(t')$, we can do it because we know that t satisfies all hyperplanes.

Second equality follows from the independency of the two events. This and all other independencies of events in this text wouldn't be proved, though all independencies would be quite natural and the reader can prove them by herself if she likes.

Now we are going to bound probabilities $\mathbb{P}_1$ and $\mathbb{P}_2$ separetly. Starting with $\mathbb{P}_1$:

$$\mathbb{P}_1 = \mathbb{P}_{S_i}\{\forall i\ \eta_{S_i}(t) = \mathit{true}\} = (\mathbb{P}_S\{\eta_S(t) = \mathit{true}\})^{k+2}$$

All subsets S_i are chosen independently, so it's quite natural, that all event $\eta_{S_i}(t) = \mathit{true}$ are independent. We used it in this equality without proof as was promised.

To evaluate $\mathbb{P}_1$ further we are to think of a combinatorial essence of the obtained probability. We have a fixed truth assignment t and the question is, what is the probability, that it would be an even number of true variables in a randomly chosen subset S of variables. There are two answers to the question. If we have truth assignment t that assigns false to every variable, then in every subset there are zero true variables and the probability of the event is 1. For every other truth assignment t it's claimed that there is exactly one half of all subsets with an even number of true variables. To prove this first we are to look on subsets consisting only of true variables of t. For such subsets it's obvious that exactly one half of them has even number of variables. The rest of the proof is left to the reader as an exercise.

So, probability $\mathbb{P}_S\{\eta_S(t) = \mathit{true}\}$ is 1 or 1/2 depending on t, we would say that it's not less than 1/2 and as the result we can write that

$$\mathbb{P}_1 = (\mathbb{P}_S\{\eta_S(t) = \mathit{true}\})^{k+2} \geq \frac{1}{2^{k+2}}$$

Almost the same can be done with $\mathbb{P}_2$. We are going to do some formal rewritings of the expression for $\mathbb{P}_2$.

$$\begin{aligned}\mathbb{P}_2 = \mathbb{P}_{S_i}\{\forall t' \in T \setminus \{t\} \exists i \; \eta_{S_i}(t') \neq \eta_{S_i}(t)\} =\\ 1 - \mathbb{P}_{S_i}\{\exists t' \in T \setminus \{t\} \forall i \; \eta_{S_i}(t') = \eta_{S_i}(t)\} =\\ 1 - \mathbb{P}_{S_i}\{(\forall i \; \eta_{S_i}(t_1) = \eta_{S_i}(t)) \vee \ldots \vee (\forall i \; \eta_{S_i}(t_{|T|-1}) = \eta_{S_i}(t))\} \geq\\ 1 - (|T|-1)\mathbb{P}_{S_i}\{\forall i \; \eta_{S_i}(t') = \eta_{S_i}(t)\} >\\ 1 - 2^{k+1}(\mathbb{P}_S\{\eta_S(t') = \eta_S(t)\})^{k+2}\end{aligned}$$

First we used the formula $\mathbb{P}\{\bar{A}\} = 1 - \mathbb{P}\{A\}$, then we rewrote an existence of t' by means of disjunctions, then we used the formula $\mathbb{P}\{A \vee B\} \leq \mathbb{P}\{A\} + \mathbb{P}\{B\}$ and finally we used the independency of events $\eta_{S_i}(t') = \eta_{S_i}(t)$ for $1 \leq i \leq k+2$.

t and t' are two fixed different truth assignments and $\mathbb{P}_S\{\eta_S(t') = \eta_S(t)\}$ can be evaluated in the same way as it was done for $\mathbb{P}_1$. Again it occurs that exactly one half of all subsets of variables is such that $\eta_S(t') = \eta_S(t)$. Thus,

$$\mathbb{P}_2 > 1 - 2^{k+1}(\mathbb{P}_S\{\eta_S(t') = \eta_S(t)\})^{k+2} = 1 - 2^{k+1} \cdot \frac{1}{2^{k+2}} = \frac{1}{2}$$

Finally we can remind ourselfs the probability we were initially bounding:,

$$\mathbb{P}_{S_i}\{t \text{ is the only satisfying assignment of } F_{k+2}\} = \mathbb{P}_1 \cdot \mathbb{P}_2 > \frac{1}{2^{k+2}} \cdot \frac{1}{2} = \frac{1}{2^{k+3}}$$

To end the proof let us remember that $D = |T| \geq 2^k$ and do final evaluations:

$$\begin{aligned}\mathbb{P}_{S_i}\{F_{k+2} \text{ is uniquely-satisfiable}\} =\\ \mathbb{P}_{S_i}\{\exists t \in T: \; t \text{ is the only satisfying assignment of } F_{k+2}\} >\\ \frac{2^k}{2^{k+3}} = \frac{1}{8}\end{aligned}$$

□

5 Second Proof

The second proof in russian is presented in [?].

The second proof of Valiant-Vazirani Theorem

Second proof uses numeric theory and doesn't have so many evaluations. In this proof we construct only one random formula F' based on the given formula F and we will show that with probability not less than $\frac{1}{32n^4+32n^3}$ constructed formula is uniquely-satisfiable. n again is a number of varaibles in F. If we repeat construction of F' for $O(n^4)$ times, we can make constant probability that we would have a uniquely-satisfiable formula: $1 - (1 - \frac{1}{32n^4+32n^3})^{O(n^4)}$.

So, now we are to show how to construct the F'. Let i be a random integer from the segment $[\,0 \ldots n\,]$. Let $b_i = 4 \cdot 2^i n^2$, let p_i and r_i be random integers from the segment $[\,1 \ldots b_i\,]$.

Truth assignments of the formula F can be thought as integer numbers with n bits in binary representation each bit representing true value of the corresponding variable. For instance, let 1 mean true and 0 mean false. To construct F' let $F' = F \wedge (x \mod p_i = r_i)$. Here $(x \mod p_i = r_i)$ means a Boolean formula in CNF of variables x. We are not going to show the exact way how to construct it as it was done with hyperplanes from the previous proof. One is just to encode multiplication of some unknown number y (new introduced variables) by p_i, then encode the addition of r_i and the comparison of the result with x.

If F is unsatisfiable, F' is unsatisfiable too. In the other case number of truth assignments of F is between some degrees of 2: $2^{j-1} < D \leq 2^j$. j can vary in the segment $[0 \dots n]$. So, if we are lucky, our initially chosen number i equals to j and $2^{i-1} < D \leq 2^i$. This occurs with probability $\frac{1}{n+1}$ and for all further proof we will assume that this happened.

How to bound the number of primes in the segment $[1 \dots b_i]$? There is a formula in the numeric theory, that number of primes in such segment is at least $0.92129 b_i / \ln b_i$. We can simlify this expression:

$$0.92129 b_i / \ln b_i > b_i / \log_2 b_i = 4 \cdot 2^i n^2 / (i + 2 + 2 \log_2 n) > 4 \cdot 2^i n^2 / 2n = 2^{i+1} n$$

Now we came to the very proof of the theorem. We want to evaluate the probability that F' is uniquely-satisfiable. Let us name elements of T as $t^{(j)} \quad 1 \leq j \leq |T| = D$. Now we fix j and thus choose some $t^{(j)} \in T$. As it was in previous proof, $t^{(j)}$ can be the satisfying assignment of F', it can be not a satisfying assignment of F' and it can be the only satisfying assignment of F'. We prefer the last case. Imagine, chosen p_i proved to be prime. There are some prime numbers that if p_i is such number, $t^{(j)}$ would never be the only satisfying assignment of F' (independently of choosing of r_i). Consider primes p such that $p \mid t^{(j)} - t^{(1)}$ $(j \neq 1)$. If b_i is such a prime, two equalities $t^{(1)} \mod b_i = r_i$ and $t^{(j)} \mod b_i = r_i$ both either hold or not. So, $t^{(j)}$ is either not a satisfying assignment of F' at all, or is not the only satisfying assignment of F'.

In the same way we can show that we don't like p_i to be such that $p_i \mid t^{(j)} - t^{(l)}$ for any $l \neq j$. By the way, all other primes are good for us and if we are lucky in choosing r_i such that $t^{(j)} \mod p_i = r_i$ holds, $t^{(j)}$ is the only satisfying assignment of F'. We can count the number of 'bad' prime numbers. Number of primes such that $p \mid t^{(j)} - t^{(1)}$ is not greater than n, because $t^{(j)}$ and $t^{(1)}$ are n-bit numbers and all primes are at least two. Now we sum up the number of 'bad' primes corresponding to different $t^{(l)}, l \neq j$ and the resulting number of overall 'bad' primes is not greater than $n(D-1) < n2^i$.

We have at least $2^{i+1}n$ primes, so there are at least $2^{i+1}n - n2^i = n2^i$ primes left that can make $t^{(j)}$ the only satisfying assignment. The result: there are at least $n2^i$ pairs of p_i and r_i that make $t^{(j)}$ the only satisfying assignment. There are different lucky pairs for different t^j, thus there are at least $n2^iD > n2^i2^{i-1} = n2^{2i-1}$ pairs that will make F' uniquely-satisfiable. Overall number of pairs is $b_ib_i = 16 \cdot 2^{2i}n^4$ and finally the probability that we chose the lucky pair is $\frac{n2^{2i-1}}{16 \cdot 2^{2i} n^4} = \frac{1}{32n^3}$.

Here is the very place to remember that all evaluations were done in the assumption that in the beginning we were lucky to choose the right i.

$$\begin{aligned}\mathbb{P}\{F' \text{ is uniquely satisfiable}\} \geq \\ \mathbb{P}\{F' \text{ is uniquely satisfiable \& the right } i \text{ was chosen}\} = \\ \mathbb{P}\{F' \text{ is uniquely satisfiable} \mid \text{the right } i \text{ was chosen}\} \cdot \mathbb{P}\{\text{the right } i \text{ was chosen}\} \geq \\ \frac{1}{32n^3}\frac{1}{n+1} = \frac{1}{32n^4 + 32n^3}\end{aligned}$$

□

6 Open Questions

We already saw that Valiant-Vazirani theorem reduces SAT to the UNIQUE-SAT problem. There are solvers for UNIQUE-SAT that work faster than solvers for SAT. They work even faster if the formula on input is in 3-CNF (all clauses have not more than three variables). So the desired thing is to have a Valiant-Vazirani transform that would produce formulas $\{F_i\}$ in 3-CNF. There is a well-known method to translate any formula in CNF in 3-CNF, but it may sometimes significantly increase the number of variables. If a solver works for, say, $O((1.5)^n)$ and number of variables increases only twice, the working time becomes $O((2.25)^n)$, so may be better idea was to solve the initial formula without any Valiant-Vazirani reduction.

The open question is, is there such a Valiant-Vazirani reduction to the set of formulas in 3-CNF that number of variables would increase only by $o(n)$.

The second open question concerns derandomization. Is there a deterministic reduction instead of probabilistic. The working time is not supposed now to be polynomial, it may be $poly(|F|) \cdot c^n$ for some constant $c < 1$ instead. May be reduction would be not to the UNIQUE-SAT problem, but to some weaker problem, for example if the formula have an odd or zero number of satisfying assignments.