Valiant-Vazirani theorem

Posov Ilya
Faculty of Mathematics and Mechanics
Chair of software engineering
(system programming)
Original paper

Contents

• Statement of the theorem
• Words before the proof
• The 1st proof
• The 2nd proof
• Open questions
Leslie Valiant & Vijay Vazirani

• Leslie G. Valiant
  http://people.deas.harvard.edu/~valiant/
  – Ph.D., Warwick university in CS, 1974
  – T. Jefferson Coolidge Professor of Computer Science and Applied Mathematics in the Division of Engineering and Applied Sciences, Harvard University

• Vijay V. Vazirani
  http://www-static.cc.gatech.edu/~vazirani/
  – Ph.D., University of California, Berkeley, 1983
  – Professor of CS at Georgia Tech and McKey Visiting Professor at the University of California, Berkeley
Theorem statement

\[ F \text{ in CNF} \]
\[ \text{can be constructed in polynomial time} \]
\[ \text{(probabilistic construction)} \]
\[ F_1, F_2, \ldots, F_m \text{ in CNF} \]

- If \( F \) is unsatisfiable, then all \( F_i \) are unsatisfiable
- If \( F \) is satisfiable, then with probability greater than \( \frac{1}{2} \) at least one of \( F_i \) is uniquely-satisfiable
Solving SAT

• Consider u-solver, an algorithm:
  – $u\text{-solver}(F) = \text{yes}$, if $F$ has exactly one solution
  – $u\text{-solver}(F) = \text{no}$, if $F$ has no solutions
  – $u\text{-solver}(F) = \text{yes/no}$ (unpredictable), otherwise

• Meaning of u-solver: tests for satisfiability assuming that given formula has at most one solution

• u-solver solves “promise problem” UNIQUE-SAT
Solving SAT (continue)

\( \text{a) } F \text{ is unsatisfiable} \)

- V-V construction
- \( F_1, F_2, \ldots, F_m \)
- \( 0, 0, 0 \)
- u-solver
- no, no, \ldots, no

\( \text{b) } F \text{ is satisfiable} \)

- V-V construction
- \( F_1, F_2, \ldots, F_m \)
- \( 0, 1, >1 \)
- u-solver
- no, yes, \ldots, yes/no

- So, if \( F \) is unsatisfiable, \( u\)-solver will say no for all \( F_i \)
- If \( F \) is satisfiable, with probability more than \( \frac{1}{2} \), \( u\)-solver will say yes for some \( F_i \)
Result

- $\text{SAT} \in \text{RP}^{\text{UNIQUE-SAT}}$
- $\text{NP} \subset \text{RP}^{\text{UNIQUE-SAT}}$
- $\text{NP} \subset \text{BPP}^{\text{UNIQUE-SAT}}$
Thoughts

• To solve SAT u-solver can be replaced by
  – Solver that tests whether the formula has exactly one satisfying assignment
  – Solver that tests whether the formula has odd number of satisfying assignments
Proof of the Theorem
Hyperplanes $\eta_S$

- Let $S \subseteq \{x_1, x_2, \ldots, x_n\}$
- Hyperplane $\eta_S$ is a boolean formula in CNF, stating that an even number of $x_i$ in $S$ is true
- Example: $n = 4$, $S = \{x_1, x_2, x_4\}$

\[(y_0) \land (y_1 \Leftrightarrow (y_0 \oplus x_1)) \land (y_2 \Leftrightarrow (y_1 \oplus x_2)) \land (y_3 \Leftrightarrow y_2) \land (y_4 \Leftrightarrow (y_3 \oplus x_4)) \land (y_4)\]
Notation

• $F$ is a formula in CNF with variables $x_1, x_2, ..., x_n$
• $T$ is a set of its satisfying assignments
• $D = |T|$ – number of its satisfying assignments
• $S_i$ are randomly selected subsets of $\{x_1, x_2, ..., x_n\}$ $(i = 1...n+1)$
• $F_0 = F$
• $F_1 = F \land \eta_{S_1}$
• $F_2 = F \land \eta_{S_1} \land \eta_{S_2}$
• $...$
• $F_{n+1} = F \land \eta_{S_1} \land \eta_{S_2} \land ... \land \eta_{S_{n+1}}$
Proof continue

- $F_0 = F$
- $F_1 = F \land \eta_{S_1}$
- $F_2 = F \land \eta_{S_1} \land \eta_{S_2}$
- ...
- $F_{n+1} = F \land \eta_{S_1} \land \eta_{S_2} \ldots \land \eta_{S_{n+1}}$
- Obviously, if $F$ is unsatisfiable, all $F_i$ are unsatisfiable
- We proof that if $F$ is satisfiable, if $2^k \leq D \leq 2^{k+1}$ then $F_{k+2}$ is uniquely-satisfiable with probability at least $\frac{1}{8}$
1/8 vs. 1/2

- $F_1(1), F_2(1), F_3(1), \ldots, F_{n+1}(1)$
- $\ldots$
- $F_1(6), F_2(6), F_3(6), \ldots, F_{n+1}(6)$

- Each set has no uniquely-satisfiable formula with probability at most $\frac{7}{8}$
- Sets constructed independently, so probability that there are no uniquely-satisfiable formulas at all is at most $(\frac{7}{8})^6 < \frac{1}{2}$
- Probability, that there is at least one uniquely-satisfiable formula is at least $\frac{1}{2}$
Evaluations (1/3)

- \( F_{k+2} = F \land \eta_{s_1} \land \eta_{s_2} \ldots \land \eta_{s_{k+2}} \quad \text{P}(\text{F}_{k+2} \text{ is uniquely-satisfiable}) = ? \)

- take \( t \in T \) some truth assignment of \( F \)

- \( P \{ t \text{ is the only satisfying assignment of } F_{k+2} \} = \)

\[
P \{ \forall i \ \eta_{s_i}(t) = \text{true} \ \& \ \forall t' \in T \setminus \{ t \} \ \exists i \ \eta_{s_i}(t') \neq \eta_{s_i}(t) \} =
\]

\[
P \{ \forall i \ \eta_{s_i}(t) = \text{true} \} \cdot P \{ \forall t' \in T \setminus \{ t \} \ \exists i \ \eta_{s_i}(t') \neq \eta_{s_i}(t) \} =
\]

\[
P_1 \cdot P_2
\]
Evaluations (2/3)

- \( F_{k+2} = F \land \eta_{s_1} \land \eta_{s_2} \ldots \land \eta_{s_{k+2}} \)
  \( P\{F_{k+2} \text{ is uniquely-satisfiable}\} = ? \)
- take \( t \in T \) some truth assignment of \( F \)
- \( P_1 = P \{ \forall i \ \eta_{s_i}(t) = \text{true} \} = \)

\[
(P \{ \eta_{s}(t) = \text{true} \})^{k+2} \geq \frac{1}{2^{k+2}}
\]

\( t = \bullet\bullet\bullet\bullet\bullet\bullet\bullet\)

Exactly one half of all subsets of variables have even number of true-variables
Evaluations (3/3)

\[ P_2 = P \{ \forall t' \in T \setminus \{t\} \exists i \eta_{S_i}(t') \neq \eta_{S_i}(t) \} = \]

\[ 1 - P \{ \exists t' \in T \setminus \{t\} \forall i \eta_{S_i}(t') = \eta_{S_i}(t) \} = \]

\[ 1 - P \left\{ \left( \forall i \eta_{S_i}(t_1) = \eta_{S_i}(t) \right) \lor \ldots \lor \left( \forall i \eta_{S_i}(t_{|T|-1}) = \eta_{S_i}(t) \right) \right\} \geq \]

\[ 1 - (|T| - 1) P \{ \forall i \eta_{S_i}(t') = \eta_{S_i}(t) \} > \]

\[ 1 - 2^{k+1} \left( P \{ \eta_S(t') = \eta_S(t) \} \right)^{k+2} = \]

\[ 1 - 2^{k+1} \cdot \frac{1}{2^{k+2}} = \frac{1}{2} \]

Exactly one half of all subsets \((S)\) of variables are such that \(\eta_S(t) = \eta_S(t')\)
Ending of the proof...

- If we take arbitrary \( t \in T \) truth assignment of \( F \),

\[
P\{t \text{ is the only satisfying assignment of } F_{k+2}\} = P_1 \cdot P_2 > \frac{1}{2^{k+2}} \cdot \frac{1}{2} = \frac{1}{2^{k+3}}
\]

- But \( |T| \geq 2^k \), so

\[
P\{\exists t \in T : t \text{ is the only satisfying assignment of } F_{k+2}\} > \frac{2^k}{2^{k+3}} = \frac{1}{8}
\]
Construction of $F_i$

- $i$ is a random number from $[0\ldots n]$
- $b_i = 4 \cdot 2^i n^2$
- $p_i$ is a random number in $[1\ldots b_i]$
- $r_i$ is a random number in $[1\ldots b_i]$
- $x$ is a bit sequence $x_1 x_2 \ldots x_n$ ($0 = \text{false}, 1 = \text{true}$)
- new random formula: $F' = F \land (x \mod p_i = r_i)$
- Let’s show that $F'$ is one-satisfiable with
probability $\geq \frac{1}{32n^4 + 32n^3}$
Preliminaries (1/2)

• $i$ is a random number in $[0...n]$

• $2^{i-1} < |T| = D \leq 2^i$ with probability $\frac{1}{n+1}$.

We will assume that this happened

$$F' = F \land (x \mod p_i = r_i)$$
Preliminaries (2/2)

- \( b_i = 4 \cdot 2^i n^2 \)
- Number of primes in the \([1 \ldots b_i]\) is at least:

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

\[ p \mid t^{(j)} - t^{(1)} \]

\[ \geq 2^{i+1} n \text{ primes in } [1\ldots b_i] \]

- inner circles: number of primes \( \leq n(D-1) < n2^i \)
- rest of primes \( \geq n2^{i+1} - n2^i = n2^i \)

\[ F' = F \land (x \mod p_i = r_i) \]
Proof

• \( t^{(1)} \): at least \( n2^i \) pairs \((p, r)\) that would make \( t^{(1)} \) the only satisfying assignment
• ...
• \( t^{(D)} \): at least \( n2^i \) pairs \((p, r)\) that would make \( t^{(D)} \) the only satisfying assignment

• overall number of such “lucky” pairs

\[
\geq n2^i D > n2^i 2^{i-1} = n2^{2i-1}
\]

• overall number of pairs = \( b_i b_i = 16 \cdot 2^{2i} n^4 \)
• \( P \{ \text{to choose a “lucky” pair} \} = n2^{2i-1}/16 \cdot 2^{2i} n^4 = 1/32n^3 \)

\[ F' = F \land (x \mod p_i = r_i) \]
Ending of the proof

- $P\{F' = F \land (x \mod p_i = r_i)\}$ is uniquely-satisfiable \geq \frac{1}{32n^3} \cdot \frac{1}{n+1} = \frac{1}{32n^4 + 32n^3}$
  $$P\{A\} \geq P\{A \land B\} = P\{A | B\} \cdot P\{B\}$$

- Probability of the converse (bad) situation
  \leq 1 - \frac{1}{32n^4 - 32n^3}$

- Repeat generation of $F'$ $O(n^4)$ times, probability that one of the generated formulas is uniquely-satisfiable:
  \begin{equation}
  \geq 1 - \left(1 - \frac{1}{32n^4 - 32n^3}\right)^{O(n^4)} = \text{const}
  \end{equation}
Open Questions
3-CNF

• $F \rightarrow \{F_i\}$
• $F$ is in 3-CNF then $F_i$ are not always in 3-CNF
• Translation to 3-CNF can significantly increase the number of variables in $F_i$
• Is there such a reduction to the set of formulas in 3-CNF that number of variables would increase only by $o(n)$?
Derandomization

• How to remove randomness from the algorithm?
• Maybe, working time of the algorithm would be $poly(|F|) \cdot c^n$ for some $c < 2$
Thank you for attention

Questions?