Valiant-Vazirani theorem

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

Original paper

- L.G. Valiant and V.V. Vazirani,
  NP is as Easy as Detecting Unique Solutions.
  Theoretical Computer Science,
  47(1986), 85-94.

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 Engeneering and Applied Sciences, Harvard University

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

Theorem statement

F in CNF

$\downarrow$ *can be constructed in polynomial time (probabilistic construction)*

$F_1, F_2, \ldots, F_m$ in CNF

- If F is unsatisfiable, then all F_i are unsatisfiable
- If F is satisfiable, then with probability greater than ½ at least one of F_i is uniquely-satisfiable

Solving SAT

- Consider u-solver, an algorithm:
  - *u-solver(F) = yes*, if *F* has exactly one solution
  - *u-solver(F) = no*, if *F* has no solutions
  - *u-solver(F) = 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)

a *F is unsatisfiable*

$\downarrow$ V-V construction

F_1, F_2, …, F_m

0 0 0

u - solver

no no … no

b *F is satisfiable*

$\downarrow$ V-V construction

F_1, F_2, …, F_m

0 1 >1

u - solver

no yes … yes/no

- So, if *F* is unsatisfiable, *u-solver* will say *no* for all F_i
- If F is satisfiable, with probability more than ½ *u-solver* will say *yes* for some F_i

Result

- $\mathrm{SAT} \in \mathrm{RP}^{\mathrm{UNIQUE-SAT}}$
- $\boxed{\mathrm{NP} \subset \mathrm{RP}^{\mathrm{UNIQUE-SAT}}}$
- $\boxed{\mathrm{NP} \subset \mathrm{BPP}^{\mathrm{UNIQUE-SAT}}}$

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 η_S

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

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

- $$\begin{tikzcd} y_0 \arrow[rr, bend left] & x_1 & y_1 \arrow[rr, bend left] & x_2 & y_2 \arrow[rr, bend left] & & y_3 \arrow[rr, bend left] & x_4 & y_4 \\ t & & & & & & & & t \end{tikzcd}$$

Notation

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

Proof continue

- $F_0 \quad = F$
- $F_1 \quad = F \wedge \eta_{S_1}$
- $F_2 \quad = F \wedge \eta_{S_1} \wedge \eta_{S_2}$
- $\quad \ldots$
- $F_{n+1} = F \wedge \eta_{S_1} \wedge \eta_{S_2} \cdots \wedge \eta_{S_{n+1}}$
- 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 ⅛

1/8 vs. 1/2

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

Evaluations (1/3)

- $F_{k+2} = F \wedge \eta_{S_1} \wedge \eta_{S_2} \dots \wedge \eta_{S_{k+2}}$ *P{F$_{k+2}$ is uniquely-satisfiable} = ?*
- take $t \in T$ some truth assignment of F
- $\underset{S_i}{P}\{t \text{ is the only satisfying assignment of } F_{k+2}\} =$

$$\underset{S_i}{P}\{\forall i\ \eta_{S_i}(t) = true \ \&\ \forall t' \in T \setminus \{t\}\ \exists i\ \eta_{S_i}(t') \neq \eta_{S_i}(t)\} =$$

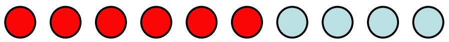
$$\underset{S_i}{P}\{\forall i\ \eta_{S_i}(t) = true\} \cdot \underset{S_i}{P}\{\forall t' \in T \setminus \{t\}\ \exists i\ \eta_{S_i}(t') \neq \eta_{S_i}(t)\} =$$

$$P_1 \cdot P_2$$

Evaluations (2/3)

- $F_{k+2} = F \wedge \eta_{S_1} \wedge \eta_{S_2} \cdots \wedge \eta_{S_{k+2}}$ *P{F_{k+2} is uniquely-satisfiable} = ?*
- take $t \in T$ some truth assignment of F
- $P_1 = \underset{S_i}{P}\{\forall i\ \eta_{S_i}(t) = true\} =$

$$\left(\underset{S}{P}\{\eta_S(t) = true\}\right)^{k+2} \geq \frac{1}{2^{k+2}}$$

t = 

Exactly one half of all subsets of variables have even number of true-variables

Evaluations (3/3)

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

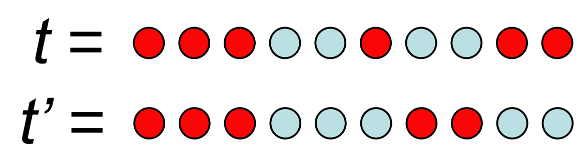
$$1 - \underset{S_i}{P}\{\exists t' \in T \setminus \{t\}\ \forall i\ \eta_{S_i}(t') = \eta_{S_i}(t)\} =$$

$$1 - \underset{S_i}{P}\Big\{ (\forall i\ \eta_{S_i}(t_1) = \eta_{S_i}(t)) \vee \ldots \vee (\forall i\ \eta_{S_i}(t_{|T|-1}) = \eta_{S_i}(t)) \Big\} \geq$$

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

$$1 - 2^{k+1} (\underset{S}{P}\{\eta_S(t') = \eta_S(t)\})^{k+2} =$$

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



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

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

$\blacksquare$

Second Proof

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 =`false`, 1=`true`)
- new random formula : $F' = F \wedge (x \bmod p_i = r_i)$
- Let's show that *F'* is one-satisfiable with probability $\geq \dfrac{1}{32n^4 + 32n^3}$

Preliminaries (1/2)

- i is a random number in $[0 \ldots n]$
- $2^{i-1} < |T| = D \leq 2^{i}$ with probability $\frac{1}{n+1}$.
- We will assume that this happened

$F' = F \wedge (x \bmod p_i = r_i)$

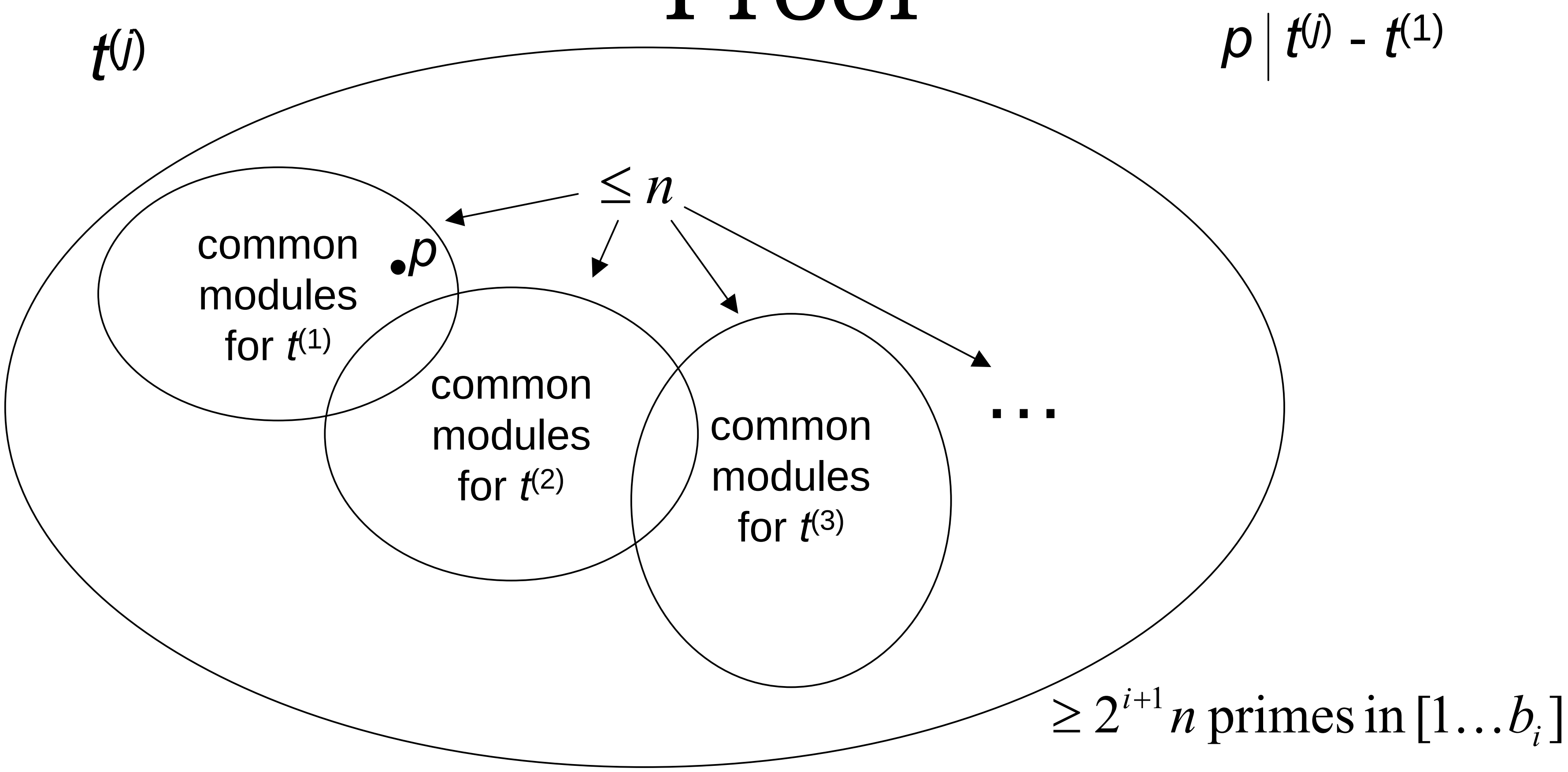
Preliminaries (2/2)

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

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

$F' = F \wedge (x \bmod p_i = r_i)$

Proof



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

$F' = F \wedge (x \bmod p_i = r_i)$

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 $= b_i b_i = 16 \cdot 2^{2i} n^4$
- $P\{$to choose a "lucky" pair$\} = n2^{2i-1}/16 \cdot 2^{2i} n^4 = 1/32n^3$

$$F' = F \wedge (x \bmod p_i = r_i)$$

Ending of the proof

- $P\{F' = F \wedge (x \bmod p_i = r_i) \text{ is uniquely-satisfiable}\} \geq$
  $$\frac{1}{32n^3}\frac{1}{n+1} = \frac{1}{32n^4 + 32n^3}$$
  $$\boxed{P\{A\} \geq P\{A \,\&\, B\} = P\{A \mid B\} \cdot P\{B\}}$$
- 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:
  $$\geq 1 - \left(1 - \frac{1}{32n^4 - 32n^3}\right)^{O(n^4)} = const$$

■

Open Questions

3-CNF

- $F \longrightarrow \{F_i\}$
- 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?