Bullet Notes on Computational Complexity

Albert Atserias,
Universitat Politècnica de Catalunya

MIRI, MAMME, MPAL
February-June, 2020.
Last modified: March 17, 2020.

1 Probabilistic computation

1.1 The model

- The model of non-deterministic TM will also serve as our model of randomized algorithm.
- Let $M = (Q, \Gamma, \delta_0, \delta_1, q_0, q_F)$ be an NTM.
- Think of the machine as making an independent and fair coin-flip at each step.
- Let $c_i \in \{0,1\}$ be the outcome of the i-th coin-flip.
- The machine takes the random computation path given by the sequence $\delta_{c_1}, \ldots, \delta_{c_t}$.
- Fix an input $x \in \Gamma^*$ and let $t = T_M(x)$.
- For $c = (c_1, c_2, \ldots, c_t) \in \{0,1\}^t$:
- Notation: $M_c(x)$: the output of M on input x when it uses δ_{c_i} in its i-th step.
- Notation: $\Pr[\ E\ ] := |E|/2^t$ for any *event* $E \subseteq \{0,1\}^t$.
- For example, for $y \in \Gamma^*$ and $E = \{c \in \{0,1\}^t : M_c(x) = y\}$, what is $\Pr[\ E\ ]$?
- It's the probability that (a random computation path of) M on input x outputs y.
- In this interpretation, if $L \in \mathrm{NP}$ and M is a NTM that decides L with $t_M(n) \leq p(n)$, then:
- For every input x we have
- 1) if $x \in L$, then $\Pr[\ M(x) = 1\ ] > 0$,
- 2) if $x \notin L$, then $\Pr[\ M(x) = 1\ ] = 0$.
- But note that, in case $x \in L$, the probability $\Pr[\ M(x) = 1\ ]$ can be as small as $1/2^{p(|x|)}$.
- If $p(n)$ is, say, n^2, this probability could be useless even for rather small n.
- For $n = 200$, it is smaller than the probability of the planet exploding in the next second.
- We want NTMs that for $x \in L$ achieve good probability of acceptance.
- Say 0.99, instead of $1/2^{40000}$.

1.2 Example: primality testing

- COMPOSITENESS/PRIMALITY:
- Input: An m bit number n.
- Output: Is n composite or prime?

- The naive algorithm that tests $x|n$ for all $x \leq \lfloor\sqrt{n}\rfloor$ takes exponential time: $O(2^{m/2})$.

- Recall Miller-Rabin test for compositeness:
- 1. given an odd $n \geq 3$,
- 2. write $n-1 = 2^s q$ where q is odd; i.e., repeatedly divide $n-1$ by 2 until odd,
- 3. choose a random $a \in \{1, \dots, n-1\}$,
- 4. compute $x_0 := a^q \mod n$ by modular repeated squaring,
- 5. for $i = 0, 1, 2, \dots, s-1$, compute $x_{i+1} := x_i^2 \mod n$,
- 6. if we find some $i \in \{0, \dots, s-1\}$ with $x_i \neq \{+1, -1\}$ and $x_{i+1} = 1$, then output 'composite'.
- 7. else output 'probably prime'.

- The test is sound:
- If n is prime, then the only two roots of $x^2 - 1$ mod n are $+1$ and -1.
- This follows from the fact that $\mathbb{Z}/n\mathbb{Z}$ is a field when n is prime.
- The test succeeds with good probability:
- If n is not prime, then at least $3/4$ fraction of $a \in \{1, \dots, n-1\}$ output 'composite'.
- This follows from a little bit of basic number theory (beyond the scope here).
- The probability of error can be made exponentially small in t by repeating the test t many times.

- How is this implemented in a NTM?
- Modular arithmetic has efficient algorithms; for exponentiation we use repeated squaring.
- But how is $a \in \{1, \dots, n-1\}$ chosen uniformly at random?
- It is not:
- 1) find k such that $2^k \leq n-1 < 2^{k+1}$,
- 2) draw $k+1$ many independent coin-flips and interpret them as a number $x \in \{0, \dots, 2^{k+1}-1\}$,
- 3) if $x \notin \{1, \dots, n-1\}$, repeat; else, output x.
- The probability that nothing is output after t iterations is $\leq (1-(n-1)/2^{k+1})^t \leq (1/2)^t$.
- Conditioned on success: x is uniformly distributed in $\{1, \dots, n-1\}$.
- If we stop after t unsuccessful iterations, the probabilities get biased by no more than $1/2^t$.

1.3 Example: polynomial identity testing

- POLYNOMIAL IDENTITY TESTING:
- Input: An arithmetic expression F with variables $x_1, \ldots, x_n$ and constants $+1$ and -1,
- Output: Does F compute the identically zero polynomial in $\mathbb{R}[x_1, \ldots, x_n]$?

- Example 1: $(x_1 + x_2)(x_2 - x_3) - x_1x_2 + x_1x_3 - x_2^2 + x_2x_3$ is identically zero.
- Example 2: $x_1x_3x_5 \cdots x_{n-1} - \prod_{i=1}^{n/2}(x_{2i-1} - x_{2i}) + x_2x_4x_6 \cdots x_n$ is not identically zero.
- The second example shows that naively expanding the expression could take exponential time.

- The "mindless" test:
- 1. given an arithmetic expression $F(x_1, \ldots, x_n)$ with n variables and m operations,
- 2. for $i = 1, \ldots, n$, choose a random $a_i \in \{1, \ldots, 20m\}$, independently,
- 3. evaluate $F(x_1/a_1, \ldots, x_n/a_n)$,
- 4. if output is not zero, output 'not the identically zero polynomial'
- 5. else, output 'probably the identically zero polynomial'.

- The test is sound:
- This is obvious: how could $F(x_1, \ldots, x_n)$ be identically 0 if $F(x_1/a_1, \ldots, x_n/a_n) \neq 0$?
- The test succeeds with high probability:
- This relies on the following two facts.

- Lemma 1:
- Assume $F(x_1, \ldots, x_n)$ is an arithmetic expression with n variables and m subexpressions.
- Then F computes a polynomial $p \in \mathbb{R}[x_1, \ldots, x_n]$ of degree at most $2m - 1$.
- Proof:
- Let size(F) denote the number of subexpressions of F.
- Let $\deg(F)$ denote the degree of the polynomial computed by F.
- Proof is by induction on size(F).
- Base case: F is a variable or a constant. Obvious.
- Inductive cases: $F = G + H$ or $F = G \times H$ for subexpressions F and H.
- Let $m_1 = \text{size}(F)$ and $m_2 = \text{size}(G)$, so $m = m_1 + m_2 + 1$.
- $F = G + H$: Then $\deg(F) = \max\{\deg(G), \deg(H)\} \leq \max\{2m_1 - 1, 2m_2 - 1\} \leq 2m - 1$.

- $F = G \times H$: Then $\deg(F) = \deg(G) + \deg(H) \leq 2m_1 - 1 + 2m_2 - 1 = 2m - 1$.
- QED

- Lemma 2 [Schwartz-Zippel Lemma]:
- Assume $p \in \mathbb{R}[x_1, \ldots, x_n]$ has degree at most d and let $S \subseteq \mathbb{R}$.
- Then p has at most $d|S|^{n-1}$ many roots in S^n, unless it is identically zero.
- Proof: Induction on n.
- Base case: $n = 1$.
- This follows from the fundamental theorem of algebra:
- Over fields, non-zero univariate polynomials of degree d have at most d roots.
- Inductive case: $n \geq 2$.
- Write $p = \sum_{i=0}^{d} p_i(x_1, \ldots, x_{n-1})x_n^i$ and assume p is not identically zero.
- Then there exists a maximal $d^* \in [d]$ so that p_{d^*} is not identically zero.
- Note that p_{d^*} has degree at most $d - d^*$ and at most $n - 1$ variables.
- Now fix a root $(a_1, \ldots, a_n) \in S^n$ of p.
- Then, either $(a_1, \ldots, a_{n-1})$ is a root of p_{d^*}, or it isn't and a_n is a root of $\sum_{i=0}^{d^*} p_i(a_1, \ldots, a_{n-1})x_n^i$.
- Of the first type we have no more than $(d - d^*)|S|^{n-2}|S|$ (by the induction hypothesis).
- Of the second type we have no more than $|S|^{n-1}d^*$ (by the base case).
- This leaves a total of at most $(d - d^*)|S|^{n-2}|S| + |S|^{n-1}d^* = d|S|^{n-1}$.
- QED

- The test succeeds with high probability (continued):
- Assume F is not identically zero.
- By Lemma 1, we have $\deg(F) \leq 2m - 1$.
- By Lemma 2 with $S = \{1, \ldots, 20m\}$ we have:
- For random and independent $a_1, \ldots, a_n \in S$:
- The probability that $F(x_1/a_1, \ldots, x_n/a_n) = 0$ is at most $(2m - 1)(20m)^{n-1}/(20m)^n \leq 1/10$.
- Thus the algorithm outputs "probably not identically zero" with probability at least $9/10$.

1.4 Probabilistic complexity classes: BPP, RP, co-RP, ZPP

- BPP: Bounded-error Probabilistic Polynomial-time.
- Class of all $L \subseteq \{0,1\}^*$ for which there exist NTM M and $c \geq 0$ such that $t_M = O(n^c)$ and:
- For all $x \in \{0,1\}^*$:
- 0) $\Pr[\ M(x) \in \{0,1\}\ ] = 1$.
- 1) if $x \in L$, then $\Pr[\ M(x) = 1\ ] \geq 3/4$ (hence $\Pr[\ M(x) = 0\ ] \leq 1/4$),
- 2) if $x \notin L$, then $\Pr[\ M(x) = 1\ ] \leq 1/4$ (hence $\Pr[\ M(x) = 0\ ] \geq 3/4$).

- RP: Randomized Polynomial-time with 1-sided error and no false positives.
- Class of all $L \subseteq \{0,1\}^*$ for which there exist NTM M and $c \geq 0$ such that $t_M = O(n^c)$ and:
- For all $x \in \{0,1\}^*$:
- 0) $\Pr[\ M(x) \in \{0,1\}\ ] = 1$.
- 1) if $x \in L$, then $\Pr[\ M(x) = 1\ ] \geq 1/2$ (hence $\Pr[\ M(x) = 0\ ] \leq 1/2$),
- 2) if $x \notin L$, then $\Pr[\ M(x) = 1\ ] = 0$ (hence $\Pr[\ M(x) = 0\ ] = 1$).

- RP': Randomized Polynomial-time with 1-sided error and no false negatives.
- Class of all $L \subseteq \{0,1\}^*$ for which there exist NTM M and $c \geq 0$ such that $t_M = O(n^c)$ and:
- For all $x \in \{0,1\}^*$:
- 0) $\Pr[\ M(x) \in \{0,1\}\ ] = 1$.
- 1) if $x \in L$, then $\Pr[\ M(x) = 1\ ] = 1$ (hence $\Pr[\ M(x) = 0\ ] = 0$),
- 2) if $x \notin L$, then $\Pr[\ M(x) = 1\ ] \leq 1/2$ (hence $\Pr[\ M(x) = 0\ ] \geq 1/2$).

- ZPP: Zero-error Probabilistic Polynomial-time.
- Class of all $L \subseteq \{0,1\}^*$ for which there exist NTM M and $c \geq 0$ such that $t_M = O(n^c)$ and:
- For all $x \in \{0,1\}^*$:
- 0) $\Pr[\ M(x) \in \{0,1,?\}\ ] = 1$ and $\Pr[\ M(x) = ?\ ] \leq 1/2$.
- 1) if $x \in L$, then $\Pr[\ M(x) = 0\ ] = 0$ (hence $\Pr[\ M(x) = 1\ ] \geq 1/2$),
- 2) if $x \notin L$, then $\Pr[\ M(x) = 1\ ] = 0$ (hence $\Pr[\ M(x) = 0\ ] \geq 1/2$).
- I.e., algorithm is never wrong (zero-error), but may fail to give a definite (i.e. 0/1) answer.

- Obvious relationships:
- RP = co-RP$'$ and RP$'$ = co-RP.
- RP $\subseteq$ NP and co-RP $\subseteq$ co-NP.

- RP $\subseteq$ BPP and co-RP $\subseteq$ BPP.

- More:
- Theorem: ZPP $=$ RP $\cap$ co-RP
- Think about it: proof given in the next version of these notes.