Non-uniform computational models

Lecture 1

- Definition of complexity classes P, NP, $coNP$, Σ_k^p, Π_k^p and the polynomial hierarchy PH.

Proof sketch:

Theorem 1. *If $P = NP$ then $P = PH$. If $\Sigma_k^p = \Pi_k^p$ then $\Sigma_k^p = PH$.*

- Definition of a Boolean circuit in de Morgan basis $\wedge, \vee, \neg$.
- Circuit computes a Boolean function $f : \{0,1\}^n \to \{0,1\}^m$. Size = number of gates. Depth = length of a longest directed path.
- Definition of $P/poly$ = languages computed by Boolean circuits of a polynomial size.

Exercise: PARITY$_n$ has a Boolean circuit of size $O(n)$ and depth $O(\log n)$.

Proof sketch:

Theorem 2. *$P \subseteq P/poly$.*

P/poly is uncountable and hence:

$$P/poly \not\subseteq P\,.$$

Lecture 2

Proof sketch:

Theorem 3 (Karp-Lipton)**.** *If $NP \subseteq P/poly$ then $PH = \Sigma_2^p$.*

The key ingredient is *self-reducibility* of SAT.

Theorem 4 (Shannon)**.** *There exists a Boolean function $f : \{0,1\}^n \to \{0,1\}$ which requires a circuit of size $\Omega(\frac{2^n}{n})$.*

Theorem 5. *Every Boolean function can be computed by a circuit of size at most $O(\frac{2^n}{n})$.*

- Definition of Boolean formula in basis $\wedge, \vee, \neg$.
- By de Morgan rules, negations can be moved to leaves.
- L(f) := minimum number of leaves in a formula computing f. $D(f)$:= minimum depth of a formula/circuit computing f (counting $\wedge, \vee$-gates on a path)
- L(f) captures total number of gates up to a constant factor.

$$L(f) \leq 2^{D(f)}$$

Lemma 6. *Given a binary tree T with $s \geq 2$ leaves, there exists a node v such that the subtree rooted at v has s_v leaves with*

$$s/3 < s_v \leq 2s/3 \,.$$

Theorem 7. $D(f) \leq O(\log L(f))$.

Lecture 3

Khrapchenko lower bound

Exercise: PARITY$_n$ has a $(\neg, \wedge, \vee)$-formula with n^2 leaves if n is a power of two. In general, $L(\text{PARITY}_n) \leq O(n^2)$.

Theorem 8 (Khrapchenko)**.** *For every n, $L(PARITY_n) \geq n^2$*

- $R = A \times B \subseteq \{0,1\}^\times\{0,1\}^n$ is a monochromatic rectangle if $a_i = 1$, $b_i = 0$ for every $(a,b) \in R$, or vice versa.
- $R_f = f^{-1}(0) \times f^{-1}0$

Lemma 9. *If $L(f) = s$ then R_f can be partitioned into s monochromatic rectangles.*

- $H := \{(a,b) \in \{0,1\}^\times\{0,1\}^n :$ a and b have Hamming distance 1.$\}$

$$S \subseteq \{0,1\}^\times\{0,1\}^n \,,\; \mu(S) := \frac{|H \cap S|^2}{|S|} \,.$$

Lemma 10. *(i). If R is a monochromatic rectangle then $\mu(R) \leq 1$.*

(ii). If S_1, S_2 are disjoint subsets of $\{0,1\}^\times\{0,1\}^n$ then $\mu(S_1 \cup S_2) \leq \mu(S_1) + \mu(S_2)$.

Corollary 11. $\mu(R_f) \leq L(f)$.

Nechiporuk lower bound

- Formulas with *arbitrary (binary) gates.*
- $f(X,Y)$ a Boolean function in disjoint sets of variables X, Y. *X-subfunction of f* is obtained by setting variables in Y to 0 or 1. $\mathrm{Sub}_X(f)$= the set of all X-subfunctions of f.

Lemma 12. *Assume that f has a formula (with arbitrary binary gates) in which the variables from X appear s_x times. Then $|Sub_X(f)| \leq 2^{4s_x}$.*

$n = 2^{k-1}k$. $a_1, \dots, a_{2^{k-1}} \in \{0,1\}^k$,

$$\mathrm{EDM}_n(a_1, \dots, a_{2^{k-1}}) = 1 \text{ iff all } a_i \text{ are distinct.}$$

Theorem 13 (Nechiporuk)**.** *EDM_n requires formula with arbitrary gates of size $\Omega(n^2/\log^2 n)$.*

- Note: the bound can be improved to $\Omega(n^2/\log n)$ by choosing n and k more carefully.

Lecture 4

- *AC_0* circuits - a constant depth d and unbounded $\neg, \wedge, \vee$ gates. *Size*= number of $\wedge, \vee$ gates.
- *AC_0* = languages decidable by by poly-size AC_0 circuits of a constant depth.

Exercise:

(i). PARITY_n has a depth-two circuit of size $2^{n-1}+1$, which is *tight.* This is both for DNF and CNF representation.

(ii). PARITY_n can be computed by depth-d circuit of size $2^{O(n^{1/(d-1)})}$ for every $d \geq 2$.

Without proof:

Theorem 14 (Hastad)**.** *$PARITY_n$ requires AC_0 circuits of size $2^{\Omega(n^{1/(d-1)})}$. Hence, $PARITY_n \notin AC_0$.*

$$\begin{aligned} \mathrm{MOD}_{m,n}(x_1, \dots, x_n) &= 1 \text{ if } \sum x_i \neq 0 \,\mathsf{mod}\, m \\ &= 0\,, \text{ otherwise.} \end{aligned}$$

- *$AC_0[m]$* circuits - in addition, unbounded MOD_m gates.
- *$AC_0[m]$* = languages decidable by poly-size $AC_0[m]$ circuits of a constant depth.

Theorem 15 (Razborov-Smolensky)**.** *$PARITY_n$ requires $AC_0[3]$ circuits of size $2^{\Omega(n^{1/2d})}$. Hence, $PARITY_n \notin AC_0[3]$.*

Finite fields interlude

$\mathbb{F}_q$ - a field with q elements.

- A q-element field exists iff q is a power of a prime number p. The field then has *characteristic* p (i.e., sum of p ones is zero).
- All finite fields of the same size are isomorphic.

Fermat's Little Theorem
$a^p = a \,\mathsf{mod}\, p$, if p is a prime. Hence, $a^p = a$ for every $a \in \mathbb{F}_p$, and $a^{p-1} \in \{0, 1\}$.

Fact:

(i). Every $f : \mathbb{F}_q^n \to \mathbb{F}$ can be uniquely represented as a polynomial with coefficients from $\mathbb{F}_q$ in which every variable has degree at most $q - 1$.

(ii). Every $f : \{0,1\}^n \to \{0,1\}$ can be uniquely represented as a multilinear polynomial with coefficients from $\mathbb{F}_q$ (this holds also over infinite fields).

Lecture 5

Proof of Theorem 15.

Lemma 16. *Assume that* $f : \{0,1\}^n \to \{0,1\}$ *has an* $AC[3]_0$*-circuit of depth* d *and size* s*. Then for every* $k \geq 2$*, there exists a proper polynomial* $\widehat{f}$ $\mathbb{F}_3$ *over* $\mathbb{F}_3$ *which has a) degree at most* $\leq (2k)^d$*, and b) agrees with* f *on at least* $(1 - \frac{s}{2^k})$*-fraction of inputs (and c) maps* $\{0,1\}^n$ *to* $\{0,1\}$*).*

Lemma 17. *Any polynomial over* $\mathbb{F}_3$ *of degree at most* $\sqrt{n}$ *agrees with* $PARITY_n$ *on at most* 0.99*-fraction of inputs.*

Generalizations:

- $\mathrm{MOD}_{p,n}$ is not in $AC_0[q]$ whenever p, q are distinct primes.
- $\mathrm{MAJORITY}_n$ is not in $AC_0[q]$ whenever q is a prime.

Open problem:

- superpolynomial lower bound on bounded-depth circuits with MOD_6 gates, or circuits using both MOD_3 and MOD_2 gates.

Other classes:

- ACC_0 (bounded-depth circuits with arbitrary MOD gates), TC_0 (threshold gates = majority gates).

$$AC_0 \subseteq ACC_0 \subseteq TC_0$$

Lecture 6

- Definition of *branching program* and decision trees. *Size*=number of vertices.

Exercise. PARITY_n has a BP of a linear size (and width 2).

Exercise. Branching programs lie between circuits and formulas:

(i). CircuitSize$(f) \leq O($BPsize(f),

(ii). BPsize$(f) \leq L(f)$.

Constant-width branching programs

- Definition of *layered* branching program. *Length*=number of layers (except the source). *Width*= maximum size of a layer.

Exercise. Branching programs of length ℓ and a constant width have a circuit of depth $O(\log \ell)$ (and hence a formula of size polynomial in ℓ).

Barrington's theorem

Puzzle: Hang a picture using two nails so that the picture falls down whenever a nail is removed.

- S_5= group of permutations on a five element set.
- Definition of a *program* over S5 of length ℓ that σ-computes a Boolean function; $e \neq \sigma \in S5$.
- A program over S5 of length ℓ gives a branching program of length ℓ.

Lemma 18. *(i). If σ is a cyclic permutation then so is σ^{-1}.*

(ii). If σ_1, σ_2 are cyclic permutations then there exists a permutation τ with $\sigma_2 = \tau\sigma\tau^{-1}$.

(iii). There exist cyclic permutations $\alpha, \beta \in S5$ such that $\alpha\beta\alpha^{-1}\beta^{-1}$ is cyclic.

Lemma 19. *Assume σ_1, σ_2 are cyclic. If P_1 σ_1-computes f then there exists a program of the same length that σ_2-computes f.*

Theorem 20 (Barrington)**.** *If f has a Boolean circuit of depth d (counting $\wedge, \vee, \neg$) then it has an S5-program of length at most 4^d.*

Corollary 21. *(i). If f has a Boolean circuit of depth d then it has a width-5 branching program of length at most 4^d*

(ii). Languages decided by polynomial size formulas = languages decidable by width-5 branching programs of polynomial size.

Lecture 7

- *Monotone* Boolean functions, circuits and formulas. $L_+, C_+ =$ monotone formula resp. circuit size.
- Majority, threshold functions, MATCHING_n, BipMATCHING_n, CLIQUE_n^k.

Exercise. MAJORITY_n has a monotone circuit of a polynomial size and a monotone formula of a quasipolynomial ($n^{O(\log n)}$) size.

Note. Theorem 7 holds also for monotone formula size and depth.

Theorem 22 (Valiant)**.** MAJORITY_n *has a monotone formula of a polynomial size.*

Lecture 8

- Definition of a monotone *slice function.*

Theorem 23 (Berkowitz)**.** *Let f be an n-variate slice function. Then $L_+(f) \leq L(f)\text{poly}(n)$ and $C_+(f) \leq \text{CircuitSize}(f) + \text{poly}(n)$.*

Some monotone lower bounds without proof:

- BipMATCHING_n requires monotone circuit size $n^{\Omega(\log n)}$ and monotone formula size $2^{\Omega(n)}$ (Razborov, Raz-Wigderson).
- If $k \leq \sqrt{n}$, CLIQUE_n^k requires monotone circuit of size $n^{\Omega(\sqrt{k})}$ (Razborov, Alon-Boppana).
- There exists a function with a poly-size circuit but no subexponential monotone circuit (Tardos).

A superpolynomial lower bound on monotone formula size

- A bipartite graph with vertices $U \cup V$ is *k-separated* if for every disjoint $a, a' \subseteq U$ of size k there exists $v \in V$ connected to every element of a but no element of a'.
- Paley graph is k-separated with $|U|, |V| = n$ and $k \sim \log n$.
- A is the collection of sets $a_0 \cup a_1$ with $a_0 \subseteq U$ of size k and $a_1 \subseteq V = \{v \in V; v \text{ connected to every } u \in a_0\}$.

$$f_G := \bigvee_{a \in A} \bigwedge_{w \in a} x_w \,.$$

Theorem 24. *Gal-Pudlak If G is k-separated then $L_+(f_G) \geq \binom{n}{k}$.*

For Paley graph, this gives $L_+(f_G) \geq n^{\Omega(\log n)}$.

Exercise: The disjointness matrices D_n and $D_{n,k}$ have full rank.

A monotone analogy of Lemma 26:

Lemma 25. *If $L_+(f) = s$ then R_f can be partitioned into s (+)-monochromatic rectangles.*

Lemma 26. *If M is a $f^{-1}(0) \times f^{-1}(1)$ matrix then*

$$L_+(f) \geq \frac{rk(M)}{\max_R rk(M_R)},$$

where the maximum is taken over (+)-monochromatic rectangles.