

Lecture Notes for
COMBINATORIAL METHODS IN COMPLEXITY THEORY
(16:198:540)
Spring, 1995
Taught by: Eric Allender

These notes were prepared by the following Rutgers graduate students who took this course: Ramkrishna Chatterjee, Malka Rosenthal, Martin Strauss, Jing Wu, and Shiyu Zhou. Attention in the lectures focused on the results and techniques involved, instead of on the literature where these results and techniques were developed. As a consequence, although a few literature pointers are provided, correct attribution and citations are often not present.

The course began with a brief discussion of the basic results concerning Kolmogorov complexity. We do not repeat this material here, but refer the reader to the book *An Introduction to Kolmogorov Complexity and its Applications* by Ming Li and Paul Vitanyi, (Springer Verlag, 1993).

A goal of complexity theory is to present tight lower bounds on the circuit size required to compute a function $f : \{0, 1\}^* \rightarrow \{0, 1\}$ (i.e., on the size of the smallest circuit C_n that computes f on input of length n). For general circuits, essentially no interesting lower bounds are known. However, good lower bounds are known for *constant depth* circuits of various types. First we consider constant-depth circuits of AND and OR gates, and then we consider augmenting these circuits, first with MOD p gates where p is a prime, and then with MOD m gates where m is any integer. No superpolynomial lower bound is known for any problem in NP for more general classes of circuits.

It is an easy observation that any family $\{C_n\}$ of constant-depth circuits of AND, OR, and NOT gates is equivalent to a *leveled* family $\{D_n\}$ (of possibly greater, but still constant, depth), where a circuit family is said to be “leveled” if

- The only NOT gates appear at the input level (call this level zero of the circuit). Equivalently, we may assume that each input x_i is given both negated and non-negated, and that there are no other NOT gates in the circuit.
- Level 1 of the circuit contains only OR gates. (The *bottom fan-in* of the circuit is the largest number of wires that feeds into any of these

OR gates on level 1.)

- Levels alternate, with AND gates on level 2, OR gates on level 3, etc. The fan-in on all of the gates on these levels is unrestricted.

The next section of the notes has a statement of a “Switching Lemma”. Here, we will show that, under the assumption that this Switching Lemma holds, no constant-depth circuit of less than exponential size can compute the parity of n bits of input.

Theorem: Let C be a leveled circuit having

- depth k
- n inputs ($n \geq \max\{17^{3(k-1)}, (\frac{2^c 17}{\log 18/17})^{k-1}\}$, where c is the constant from the Switching Lemma))
- bottom fan-in $\leq t = \frac{n^{1/(k-1)}}{17}$
- at most 2^t gates in levels 2 and above.

Then C does not compute parity or its negation.

This theorem is proved by induction on k . The basis case ($k \leq 2$) is trivial. Thus, we’ll start with the inductive step.

Let C be a leveled depth k circuit with $m \leq 2^t$ AND gates on level 2. Let $s = t$ and let $l = n^{\frac{k-2}{k-1}}$. A routine calculation (below) shows that

$$\left(\frac{n-l+s}{8tl}\right)^s > 2^c 2^s \geq 2^c m,$$

and thus the hypothesis of the lemma holds. (More specifically, $(\frac{n-l+s}{8tl})^s = 2^s (\frac{17}{16}(1 - (n^{-1/k-1} - n^{-k/k-1}/17)))^s$, which for our choice of n is greater than $2^s (18/17)^s$, which, again by our choice of n is greater than $2^s 2^c$.)

Let us assume that C computes the parity or the negated parity of its n inputs. We will show that this contradicts the induction hypothesis.

Let ρ be a Kolmogorov-random element of R^l (the set of all restrictions on n variables leaving l variables free). Note that the induced circuit $C|_\rho$ computes either the parity or the negated parity of l variables. By the switching lemma, each of the subfunctions computed by the AND gates on level two of $C|_\rho$ is computed by an OR of ANDs, where the ANDs have fan-in $\leq s$.

If we replace each of the AND of ORs in the bottom two levels of $C|_\rho$ by an equivalent subcircuits that is an OR of ANDs, then we obtain a circuit C' with two adjacent levels of OR gates (on levels 2 and 3). These levels can be merged (by directly connecting each OR gate g on level 3 of C' to all of the AND gates h on level 1 such that there is a path of length 2 from h to g in C') to get a circuit of depth $k - 1$. Call this depth $k - 1$ circuit C'' , and note that it computes either parity or the negation of parity on l variables. However, C'' is not a leveled circuit, since its bottom level consists of AND gates. However, if we negate C'' and apply DeMorgan's laws to push the NOTs down to the inputs, then we obtain a leveled circuit C''' of size at most $2^t = 2^{l^{1/k-2}/17}$ with bottom fan-in at most $l^{1/k-2}/17$, computing either parity or the negation of parity on l inputs. Since this contradicts the induction hypothesis, we have now proved the theorem. The next set of notes proves the switching lemma.