# Lecture 10. Circuit Complexity 2

In last lecture we proved exponential lower bound for depth-3 circuit. The method doesn’t extend to larger depth. In this lecture, we show how to prove exponential lower bounds for constant-depth circuits.

## DNF, CNF, and Switching Lemma

Recall:

CNF: , where each is a literal, and each is a clause. The function is called a -CNF if each .

DNF: , where each is a monomial. The function is called a -DNF if each .

In general, a -CNF is not necessarily also a *k*-DNF. For example, the AND function is a 1-CNF, but an *n*-DNF. The Switching Lemma says that if we fix some variables of a *t*-CNF, then we obtain a subfunction which is an *s*-DNF for some small *s*. We can actually use a *random* restriction. A *p*-random restriction makes each bit unfixed with probability *p*, and fixed with probability . In the latter case, the bit is fixed to be 0 or 1 each equal probability. We use to denote a random restriction, and the resulting subfunction. The following lemma was given by Hastad [Has89].

**Lemma 1.1**. If is a -CNF, and is a *p*-random restriction, then

The original proof uses probabilistic arguments. Also see Razborov’s elegent proof [Raz95] using a combinatorial method.

Recall that is the degree of the function represented as a polynomial in over . Equivalently, it is the largest where the numbers are the Fourier coefficients.

We now give another lemma.

**Lemma 1.2**. Under the condition of Lemma 1.1,

## Application of Switching Lemma

Recall that certificate complexity of a function on an input is

where . Further define

and

To get familiar with the concept, consider some specific functions:

* AND:
* OR:
* Parity:
* Majority:

**Theorem 2.1**. If *f* can be computed by a depth- circuit of size *S*, then

Using the parameters for Parity, we immediately get the following corollary.

**Corollary**. If a circuit with depth *d* computes the Parity function, then the circuit size is at least

Now we sketch the proof for Theorem 2.1.

*Proof* *idea* (of Theorem 2.1). Repeatedly apply the Switching Lemma, in a bottom up manner, to reduce the depth. Use the lemma with , and . Once we replace a CNF by a DNF, we’ll see two consecutive layers of OR gates, thus we can collapse these two layers. Each round leaves about *p*-fraction of variables unfixed, thus finally we get a depth-2 circuit which computes a subfunction of variables. We need some special handling for the first step, which can also be done as an application of the switching lemma. And finally the *s*-DNF function can be made constant by restricting variables. Thus overall we restricted variables and obtained a constant function. By definition of , we get the claimed statement.

Next we show exponential lower bounds for more general functions, superseding the previous result for Parity. It’s interesting also because it links circuit complexity and Fourier coefficients. This famous result was given in [LMN93].

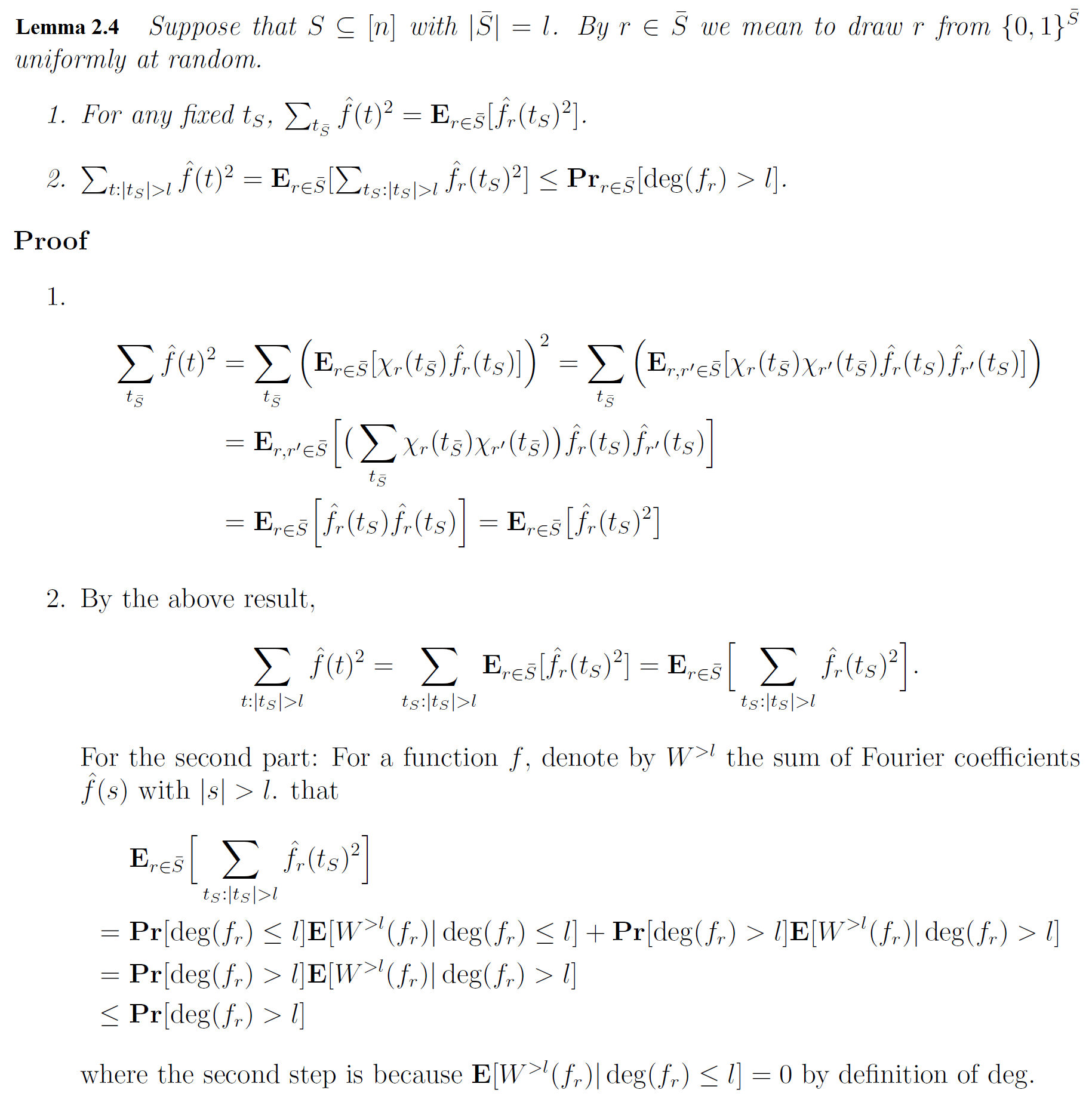
**Theorem 2.2**. If a circuit with depth *d* and size *M* computes a function , then

Note that for Parity function, there is only one nonzero Fourier coefficient:  . Thus we can take and obtain a lower bound of .

We’ll need a couple of lemmas to prove this theorem.

**Lemma 2.3**. .

*Proof*. Think of T also as a random variable distributed according to Fourier weights  . (We identify a string with a subset .) Then



**Lemma 2.5**. A *p*-random restriction gives a subfunction of with probability at least . Here .

This can be proven by a similar argument as in the proof of Theorem 2.1; one just need to use Lemma 1.2 instead of Lemma 1.1. See [LMN93] for details.

*Proof of Theorem 2.2*. Let be the distribution on by setting each coordinate to be 1 with probability . Let , . Note that we identify a string and a subset .

(Lemma 2.3)

(Lemma 2.4)

(Lemma 2.5)

## References

[Has89] J. Hastad, **Almost optimal lower bounds for small depth circuits**, *Advances in Computing Research*, vol. 5, pp. 143–170, 1989.

[Raz95] A. A. Razborov, **Bounded arithmetics and lower bounds in boolean complexity**, in *Proceedings of Workshop on Feasible Mathematics II*, 1995.

[LMN93] N. Linial, Y. Mansour, and N. Nisan, **Constant depth circuits, Fourier transforms and learnability**, *Journal of the ACM*, vol. 40, pp. 607–620, 1993.