CS 744: Pseudorandomness Generators

Lecture Notes 17: Randomness Extractors

March 11, 2015

In this part of the course, we will be interested in the converse problem of what we had considered until now — suppose we have a distribution that is not the uniform distribution, but contains significant randomness, can we write a procedure which takes this input distribution and returns nearly the uniform distribution? Till now, we were concerned with "stretching" the uniform distribution on a few bits, the seed, to a pseudorandom distribution on many more bits. The current problem can be thought of as "condensing" a non-uniform distribution to the uniform distribution on shorter strings. These will be called *randomness extractors*.

Before we begin the complexity theoretic questions, we will look at a classical randomness extractor due to von Neumann.

Example 1. *(von Neumann randomness extractor)*

Consider a source $S \subseteq \Sigma^n$ which is independent and such that the bits in the strings from S are identically distributed. Let the probability that a bit is 0 be p, where p is unknown, and not necessarily 1/2.

Can we extract out bits which are iid and where the bits occur with equal probability?

Consider the experiment: For each pair of bits $s_n s_{n+1}$, if they are

1. *both 0, then output nothing,*
2. *01, then output 0,*
3. *10, then output 1,*
4. *both 1, then output nothing.*

Then 0 and 1 occur with equal probability in the output.

Question: What is the expected length of the output string?

The complexity theoretic perspective on extraction is different in that, first, instead of assuming an iid source, we will assume only that we have a source with "sufficiently high entropy", and second, in that we will be concerned with asymptotic bounds on the input and the output.

We will look at the notion of entropy that we need.

Definition 2. *The* Shannon entropy *of a source $S \subseteq \{0,1\}^n$ with probability distribution $P : S \to [0,1]$ is defined by*

$$H(S) = -\sum_{s \in S} P(s) \log P(s) = E_{s \in S}[\log 1/P(s)].$$

The min Entropy *of S is*

$$H_\infty(S) = min_{s \in S}[\log 1/P(s)].$$

Even though Shannon entropy is the most commonly encountered notion in information theory, assuming that a source has high Shannon entropy is not enough to extract randomness in the sense that we are interested in. Assuming that a source has high *min entropy* usually suffices. We now define what it means to extract randomness - the extracted output should be "fairly close to uniform".

Definition 3. *If $X, Y \subseteq \Sigma^m$ are distributions with probabilities P_X and P_Y respectively, then the statistical distance between X and Y is defined by*

$$||X - Y|| = \max_{T:\Sigma^m \to \Sigma} |P_X[T = 1] - P_Y[T = 1]|.$$

We say that X is ε-close to the uniform distribution U_m on Σ^m if

$$||X - U_m|| < \varepsilon$$

.

As usual in complexity theory, we will start with a few negative results. The first says that deterministic extraction is impossible. This is a simple combinatorial argument. We then look at extractors which use some randomness - based on some random "seed". The next result is an important lower bound on the length of the seed required in order for extraction to be possible. Of course, the second implies the first result, but it is useful to look at the first problem in isolation.

Definition 4. *Let $X \subseteq \{0,1\}^n$ be a source with probabilty distribution P. A single bit deterministic extractor for X is a function $E : \{0,1\}^n \to \{0,1\}$ such that*

$$||E(X) - U_1|| < \varepsilon.$$

Lemma 5. *There is no single bit deterministic extractor.*

The argument is that for every such deterministic function, we can design a random variable X whose support is entirely on $E^{-1}(0)$ or entirely on $E^{-1}(1)$, whichever has greater probability. We pick the larger to ensure that X has high min-entropy. Then E fails to extract a nearly uniform distribution from X, even though X has high min-entropy.

Hence we consider a seeded extractor.

Definition 6. *A function $E : \Sigma^n \times \Sigma^d$ is a (minentropy: k, bias: ε)* extractor *if for any distribution X with minentropy*