Note on the averaging and hybrid arguments and prediction vs. distinguishing.

March 30, 2006

Averaging argument Let f be some function. The averaging argument is the following claim: if we have a circuit C such that $C(x,y) = f(x)$ with probability at least ρ where x is chosen at random and y is chosen independently from some distribution Y over $\{0,1\}^m$ (which might not even be efficiently sampleable) then there exists a single string $y_0 \in \{0,1\}^m$ such that $\Pr_x[C(x,y_0) = f(x)] \geq \rho$.

Indeed, for every y define p_y to be $\Pr_x[C(x,y) = f(x)]$ then

$$\Pr_{x,y}[C(x,y) = f(x)] = \mathbb{E}_y[p_y]$$

and then this reduces to the claim that for every random variable Z, if $\mathbb{E}[Z] \geq \rho$ then $\Pr[Z \geq \rho] > 0$ (this holds since $\mathbb{E}[Z]$ is the weighted average of Z and clearly if the average of some values is at least ρ then one of the values must be at least ρ.

Hybrid argument The hybrid argument is the following: suppose that you have m distributions $H_1, \ldots, H_m$ (say over $\{0,1\}^n$) and some function $D : \{0,1\}^n \to \{0,1\}$. Then there exists i between 1 and $m-1$ such that

$$|\Pr[D(H_i) = 1] - \Pr[D(H_{i+1}) = 1]| > \frac{|\Pr[D(H_1) = 1] - \Pr[D(H_m) = 1]|}{m}$$

As we saw in class this follows by defining $p_i = \Pr[D(H_i) = 1]$ and noting that

$$|p_1 - p_m| = |p_1 - p_2 + p_2 \cdots - p_{m-1} + p_{m-1} - p_m| \leq |p_1 - p_2| + \cdots + |p_{m-1} - p_m|$$

Prediction vs. distinguishing Suppose that X is some distribution over $\{0,1\}^n$ and $D : \{0,1\}^n \to \{0,1\}$ such that $\Pr[D(X) = 1] - \Pr[D(U_n) = 1] \geq \epsilon$ then there exists P of comparable efficiency to D and i between 0 and $n-1$ such that

$$\Pr[P(X_{[1,i]}) = x_{i+1}] \geq \tfrac{1}{2} + \tfrac{\epsilon}{n}$$

To prove this we define H_i to be the distribution where the first i bits are chosen from X and the rest are chosen uniformly (denote $H_i = X_{[1,i]}U_{n-i}$), and by the hybrid argument ther's an i such that

$$\Pr[D(X_{[1,i+1]}U_{n-i-1}) = 1] - \Pr[D(X_{[1,i]}U_{n-i}) = 1] \geq \frac{\epsilon}{n}$$

(we can get rid of the absolute value by possibly negating D).

By the averaging argument there exists a fixing y_0 of the last $n-i-1$ bits of the uniform distribution such that

$$\Pr[D(X_{[1,i+1]}y_0) = 1] - \Pr[D(X_{[1,i]}U_1 y_0) = 1] \geq \frac{\epsilon}{n}$$

Our algorithm to compute x_{i+1} from $x_{[1,i]}$ will be the following: guess b at random from $\{0,1\}$ and run $D(x_{[1,i]}by_0)$ if the result is 1 then output b and otherwise output the complement of b, $\bar{b}$.

Define now p to be $\Pr[D(X_{[1,i+1]}y_0) = 1]$, $r = \Pr[D(X_{[1,i]}U_1 y_0) = 1]$ (and so $r < p - \frac{\epsilon}{n}$) and define q to be $\Pr[D(X_{[1,i]}\overline{X_{i+1}}y_0) = 1]$ (that is, the $i+1^{th}$ bit of X is flipped). Since a uniform bit will equal to X_i with probability half and $\overline{X_i}$ with probability half, we have that

$$r = \tfrac{1}{2}p + \tfrac{1}{2}q$$

which implies

$$\tfrac{1}{2}p + \tfrac{1}{2}q \leq p - \tfrac{\epsilon}{n}$$

or

$$q \leq p - \tfrac{2\epsilon}{n}$$

If $b = x_{i+1}$ our algorithm will answer the right answer if $D(x_{[1,i]}by_0) = 1$ and if $b = \overline{x_{i+1}}$ then our algorithm will provide the right answer if $D(x_{[1,i]}by_0) \neq 1$ and so the overall probability that we answer the right answer is

$$\frac{1}{2}p + \frac{1}{2}(1-q) \geq \frac{1}{2}p + \frac{1}{2}(1-p+\frac{2\epsilon}{n}) \geq \frac{1}{2} + \frac{\epsilon}{n}$$