

COM-440, Introduction to Quantum Cryptography, Fall 2025

Exercise Solution # 6

1. Deterministic Extractors on Bit-Fixing Sources

- (a)
- We can think of generating X_0 by $n-t$ independent fair coin flips, so each of its strings occurs with equal probability 2^{t-n} and $H_{\min}(X_0) = -\log 2^{t-n} = n-t$.
 - The number of strings with an even number of 0s is equal to the number of strings with an odd number of 0s, so each of these is equal to 2^{n-1} . Thus the min-entropy of X_1 is $-\log \frac{1}{2^{n-1}} = (n-1)$.
 - As before, think of generating X_2 through a series of independent fair coin flips: it is fully determined by $\frac{n}{2}$ of them and so $H_{\min}(X_2) = \frac{n}{2}$.
- (b) Let us look at all the proposed answers consecutively. We're interested in finding which ones are distributed as a uniformly random bit.

- $f_0(X_0)$ — false. Since the first t bits of X_0 is fixed ($100 \cdots 00$), $f_0(X_0)$, the parity of the first t bits of X_0 , is always 1.
- $f_0(X_1)$ — true. The string X_1 can be seen as $n-1$ random bits followed by a bit that is fully determined by the previous $n-1$ bits. Therefore, the first $n-1$ bits of X_1 is distributed uniformly, and thus $f_0(X_1)$, the parity of the first $t \leq n-1$ bits of X_1 , is distributed uniformly.
- $f_0(X_2)$ — true. The first $\frac{n}{2}$ bits of X_2 is distributed uniformly, and thus $f_0(X_2)$, the parity of the first $t < \frac{n}{2}$ bits of X_2 , is distributed uniformly.
- $f_1(X_0)$ — true. Let $X_0 = x_1 \cdots x_n$. Then $f_1(X_0) = \left(\sum_{i=1}^{n/2} x_i x_{i+n/2} \right) \bmod 2 = (x_{1+n/2} + \sum_{i=t+1}^n x_i x_{i+n/2}) \bmod 2$. Since $x_{1+n/2}$ is a random bit, $f_1(X_0)$ is distributed as a uniformly random bit.
- $f_1(X_1)$ — it depends on n . If n is divisible by 4, $f_1(X_1)$ is not a uniformly random bit; otherwise, if n is even but not divisible by 4, $f_1(X_1)$ is a uniformly random bit. The reason is as follows.

The string X_1 can be seen as $n-1$ random bits followed by a bit that is fully determined by the previous $n-1$ bits. We can write it as $x_1 \cdots x_n$ where $x_n = (\sum_{i=1}^{n-1} x_i) \bmod 2$. Therefore,

$$\begin{aligned}
 f_1(X_1) &= \left(\sum_{i=1}^{n/2} x_i x_{i+n/2} \right) \bmod 2 \\
 &= \left(x_{n/2} \cdot \sum_{i=1}^{n-1} x_i + \sum_{i=1}^{n/2-1} x_i x_{i+n/2} \right) \bmod 2 \\
 &= \left(\sum_{i=1}^{n/2-1} (x_i + x_{n/2})(x_{i+n/2} + x_{n/2}) - (n/2 - 2)x_{n/2} \right) \bmod 2 .
 \end{aligned}$$

If n is divisible by 4, the above equation can be simplified to

$$\left(\sum_{i=1}^{n/2-1} ((x_i + x_{n/2})(x_{i+n/2} + x_{n/2}) \bmod 2) \right) \bmod 2 .$$

Each term in the summation is independent and identically distributed, and is 1 with probability 1/4, and is 0 with probability 3/4. Therefore, the parity of the terms in the summation is not a uniformly random bit (but becomes closer to uniformly random bit when n becomes bigger).

If n is not divisible by 4, the above equation can be simplified to

$$\left(\sum_{i=1}^{n/2-1} (x_i + x_{n/2})(x_{i+n/2} + x_{n/2}) - x_{n/2} \right) \bmod 2 .$$

Note that the following $n - 1$ random variables, $x_i + x_{n/2}$ ($i = 1, 2, \dots, n/2 - 1, n/2 + 1, \dots, n - 1$), $x_{n/2}$ are uniform random bits that are independent. Therefore, $f_1(X_1)$ is a uniform random bit.

- $f_1(X_2)$ — true. Since the first $\frac{n}{2}$ bits of X_2 are the same as the second half, we have $x_L \cdot x_R = \text{XOR}(x_L) = \text{XOR}(x_R)$ which is a uniformly random bit since the strings $x_L = x_R$ are random.
- $f_2(X_0)$ — true. Since the last $n - k$ bits of X_0 are fully random, the XOR of the entire string will result in a uniformly random bit.
- $f_2(X_1)$ — false. Since the number of 0's in the string is known the parity of the string (computed by the XOR) is 0 for n even.
- $f_2(X_2)$ — false. Since the first $\frac{n}{2}$ bits of X_2 are the same as the second half, the parity of the bit string is zero.

- (c) We divide X into $\lfloor \frac{n}{t+1} \rfloor$ blocks of length at least $t+1$, i.e. $X = Y_1 \parallel Y_2 \parallel \dots \parallel Y_{\lfloor \frac{n}{t+1} \rfloor}$ where each Y_i has length at least $t+1$. We define $g(Y)$ = the XOR of all the bits of Y and set $f(X) = g(Y_1) \parallel g(Y_2) \parallel \dots \parallel g(Y_{\lfloor \frac{n}{t+1} \rfloor})$.

From the construction, $f(X)$ is a deterministic function. Moreover, each $g(Y_i)$ is totally uncorrelated from Eve's bits as Eve learns at most t bits of X (so at least one bit of Y_i is hidden from Eve's view). Notice that each $g(Y_i)$ is independent as Y_i is independent. Therefore, $f(X)$ is uniformly random over strings of length $\lfloor \frac{n}{t+1} \rfloor$ and is totally uncorrelated from Eve's bits.