We began by finishing the discussion of multi-round coin flipping and the Baton Passing and Lightest Bin protocols, and saw how multi-round coin flipping is equivalent to leader election. We discussed adaptive coin-flipping and the bias of various functions. We conjectured that majority is optimal. We also discussed Santha Vazirani sources and found lower bounds for the bias in this case. Then we moved on to Mixed Sources and discussed strong impossibility results.

1 Multi-round coin flipping

Remember from the last lecture that we showed that 1-round coin flipping cannot tolerate $\Omega\left(\frac{n}{\log n}\right)$ bad players [KKL]. We will no show that the above is not true for multi-round coin flipping. We will start again with the example of Baton Passing.

**Baton Passing [Saks89, AL93]:** $P_1$ holds the baton and passes it to a random player $P_i$, eliminating himself. $P_i$ does the same, and so on, and the last player left is the leader and flips a coin. Clearly, bad guys will eliminate good guys, and good guys will eliminate random guys, so the bias is proportional to $\Pr(\text{bad guy is a leader})$.

Let $F(s, t) = \Pr(\text{bad guy is a leader when } s \text{ good guys and } t \text{ bad guys and good guys starts})$. Then, $f(s, t) = \frac{s}{s+t} \cdot f(s-1, t) + \frac{t}{s+t} \cdot f(s-1, t-1)$ because either the good guys will choose another good guy, eliminating him and leaving the bad guys, or the good guy will choose a bad guy who will eliminate a good guy, so both bad and good guys will go down.

[Saks 89] showed that $f(s, t) \leq \frac{t \log t + 1}{s+1}$ by doing an induction. Therefore, if $t < \frac{cs}{\log s}$ this implies that $f(s, t) < \epsilon$. Since $t + s = n$, then $t < \frac{cs}{\log n}$ implies that $f(s, t) = O(\epsilon)$.

[AL93]: The exact solution is $f(s, t) \leq \frac{9}{s+t} \sum_k kx^k$ where $x = \frac{2t \log s}{s+t} < \frac{2t \log n}{n}$.

If $t < \frac{n}{(2+\delta) \log n} \Rightarrow x < 1 \Rightarrow \sum_k kx^k = O(1) \Rightarrow f(s, t) = O\left(\frac{t}{s+t}\right) < O\left(\frac{1}{\log n}\right) = o(1)$. This already breaks the KKL lower bound.

In general, it is easy to see by induction that you can’t tolerate more than $\frac{n}{2}$ bad guys.

[Feige 99]:

1. If there are $\frac{n}{2}(1 + \delta)$ good guys, then there is a protocol where the fairness, which is $\min(\Pr(\text{coin= 0}), \Pr(\text{coin= 1}))$ is $\Omega(\delta^{c_1})$ where $c_1 \approx 1.65$.

2. Fairness must be $\leq O(\delta^{1-\epsilon}), \forall \epsilon > 0$.

3. You can achieve the bound in the first part with only $\log^* n$ rounds (essentially, $O(1)$).

**Lightest Bin Protocol [Feige 99]:** This is the idea for needing $\sim \log n$ rounds. Each player chooses a random bin 0 or 1. Players in the lightest bin recurse. At the beginning,
since the majority is good guys and they will be random so they will split basically evenly, the bad guys will also need to split almost evenly in half in order to keep playing.

There is, however, some small subtlety in defining ”half” when \( n \) is not a power of 2. In this case we define: \( \text{Half}(n, c) \) where \( n \) is number of players in the round and \( c \) is committee size as \( \text{Half}(n, c) = c \mod (c + 1) \). So when \( c = 1 \), as before, at each round, if the size of bin \( 0 \leq \text{Half}(n, c) \), bin 0 recurses. Otherwise, bin 1 recurses.

More generally, this extends to selecting a committee of \( c \) people with at least one honest person on the committee. (Our target is then to get \( c = 1 \)).

**Theorem 1** In general, for a committee of size \( c \) where number of good players \( \geq \frac{n}{c+1} \),
\[
\Pr(\text{elected committee has at least 1 good player}) = \delta^{O(\log \frac{1}{\delta})}
\]

For the proof, see Lemmas 7 and 8 and Theorem 9 in [Feige 99].

**Corollary 2** If \( s > \frac{n}{2} \) and you elect a committee of size 2, \( \Pr(\text{good}) = \Omega(1) \) and \( \delta = \text{constant.} \)

**Corollary 3** Up to a constant coin-flipping is equivalent to leader election.

**Proof:**
1. Leader Election \( \rightarrow \) Coin-Flipping: Elect a leader and let the leader flip a coin.
2. Coin-Flipping \( \rightarrow \) Leader Election: Use the Lightest Bin Protocol to elect a committee of size 2. Then use Coin-Flipping to select one of the 2 members of the committee.

Feige describes a clever monotone circuit game that can be used by the elected committee of size 2 to choose a leader from the \( n \) original players.

For fairness of \( \Omega(1) \) we can see that Feige is best. For fairness of \( \frac{1}{2} - o(1) \Rightarrow \) we know we can tolerate only \( t = o(n) \) and there exist previous protocols in [AN 93] with bias = \( O(\frac{1}{n}) \), but we won’t cover them.

2 Adaptive coin flipping

Before: \( b \) out of \( n \) players are bad and they are chosen at the beginning. This is called static corruption.

Adaptive Corruptions:
- \( \forall \) starts honest
- Attacker \( A \) corrupts \( \leq b \) players during execution

It turns out that most existing static protocols are insecure because they are based on leader election. Therefore, even for \( b = 1 \), just corrupt the leader.

How many people, \( b \) can you tolerate? Starting point: assume in each round, 1 (fixed) person sends 1 bit (random) and we ignore efficiency. This is called an LLS-source.
3 LLS-Source

An LLS-source can be thought of as the following process:
Nature flips $n$ random bits. Attacker is allowed $b$ history-dependent “interventions”. Meaning, the attacker observes the bits and based on the first $b_0 \ldots b_{i-1}$ bits he can decide whether or not to corrupt the $b_i$th bit. This is called an $(n, b)$-LLS source or $(n, b)$-control-limited source.

Let $q_f(b, n)$ be the fairness of $f(x) : \{0, 1\}^n \rightarrow \{0, 1\}$, with $\leq b$ interventions.

We want to find: $q(b, n) = \min_A \max_f (\text{fairness of } f(x))$.

Examples:

- $f$-parity: Clearly, $b = 1 \rightarrow q = 0$ since the attacker can just wait for the last bit and decide whether to send 0 or 1.
- $f$-random: We can think of $f$ as a tree whose leaves are the output of $f$ and the path to the leaf is the input. Since $f$ is random, we expect the bottom subtrees to contain both 0’s and 1’s as leaves. Therefore, the attacker can wait until the end and then determine whether the output will be 0 or 1 by choosing a path to 0 or 1. Therefore, $b = \omega(1) \rightarrow q = o(1)$.
- $f$-majority: Clearly, the adversary will fix $x_1, x_2, \ldots x_b = 1$. However, since the standard deviation is $\sqrt{n}$, up to $\sqrt{n}$ guys don’t matter.

$$\exists c_1, c_2 \text{ s/t } b = c_1 \sqrt{n} \rightarrow q = \frac{1}{2} - o(1), \quad b > c_2 \sqrt{n} \rightarrow q = o(1)$$

In fact, majority turns out to be optimal.

**Theorem 4 (LLS)**: Majority is the optimal bit-extractor for $(n, b)$-control-limited source. Optimal $b = \theta(\sqrt{n})$.

**Theorem 5 (LLS)**: Given $f : \{0, 1\}^n \rightarrow \{0, 1\}$ let $p = \Pr_{x \in \{0, 1\}^n} (f(x) = 1)$. Then with $b = O(\sqrt{n \log(\frac{1}{p})})$ can force $f(x)$ to 1 with probability $1 - o(1)$.

In fact, $E[ \# \text{ of interventions to force } 1 \text{ with } pr = 1] = O(\sqrt{n \log(\frac{1}{p})})$

In fact, [LLS], for any $p$, we can achieve the above bound with the following $f$. Define $f(x) = 1$ if $x$ has $\geq i$ 1’s and

$$p = \frac{\sum_{j=0}^{i} \binom{n}{j}}{2^n}$$

Otherwise $f(x) = 0$. We can visualize this function using a hypercube of dimension $n$. Position the hypercube so that vertices with the least weight are on the top and vertices with greatest weight are on the bottom. Starting from the bottom, we can add layer after layer where $f(x) = 1$. After $\sum_{j=0}^{i} \binom{n}{j}$ vertices have been passed, all the remaining vertices fulfill $f(x) = 0$. This function turns out to be optimal.

Clearly, this function corresponds to majority for $p = \frac{1}{2}$. 

L6-3
Conjecture 6 Returning to the general problem: Majority is optimal for general adaptive coin-flipping. Thus, we can only tolerate $\sqrt{n}$ bad guys.

4 Santha-Vazarani Source

Before (LLS): each bit was either completely perfect or completely bad.
Now: $x_1, x_2, \ldots, x_n$, each $x_i$ is at most $\delta$-biased. The bias, while $\leq \delta$, depends on history.

Definition 7 $X = x_1 \ldots x_n$ is a $\delta$-SV ($\delta$-bias limited) source if

$$\forall i \forall a_1 \ldots a_{i-1} Pr(x_i = 1 | x_1 \ldots x_{i-1} = a_1 \ldots a_{i-1}) \in \left[\frac{1}{2} - \delta, \frac{1}{2} + \delta\right]$$

Examples:

- Parity: clearly, only the last step matters. Therefore, $q = \frac{1}{2} - \delta$.
- Random: not great, but not bad.

Theorem 8 (AR89) $[BN93] \forall \delta > 0 \exists c > 0$ s/t with $pr(1 - 2^{-n}) q_f(\delta) \geq c$

- Majority: Adversary will bias every bit to 1. By Chernoff bound $pr(f(x) = 1) = 1 - 2^{-\Omega(n)}$. This is really bad! In fact, [AR89] Majority is the worst $f$.

Note that so far we could not get bias $\leq \delta$. Unfortunately, this must be the case, irrespective of $n!$

Theorem 9 $\forall n, \forall f : \{0, 1\}^n \rightarrow \{0, 1\} q_f(\delta) \leq \frac{1}{2} - \delta$.

This means that parity or even $f(x) = x_1$ is optimal. The attacker can always bias the result by at least $\delta$. Therefore, when $\delta = \Omega(1)$ we can’t extract even a single, almost unbiased bit.

To prove above, define 2 useful sources:

Definition 10 Assume $S \subseteq \{0, 1\}^n, |S| = 2^{n-1}$. Define $Z_S$ ($\delta$ half-space source): pick $b = 1$ with $pr(\frac{1}{2} + \delta$ and 0 otherwise. If $b = 1$, pick random $x$ from $S$. Else, $x \leftarrow \{0, 1\}^n \setminus S$.

Definition 11 Strong $\delta$-SV source: $\forall a_1 \ldots a_{i-1} \forall a_{i+1} \ldots a_n = a_{-i} \Pr(x_i = 1|x_{i-1} = a_{i-1}) \in \left[\frac{1}{2} - \delta, \frac{1}{2} + \delta\right]$ and $Pr(x_i = 1 | x_{-i} = a_{-i}) \in \left[\frac{1}{2} - \delta, \frac{1}{2} + \delta\right]$.

Lemma 12 $\forall S, Z_S$ is a strong $\delta$-SV source.

Proof: fix $a_{-i}$. It is enough to prove that:

$$\frac{1}{2} - \delta \leq \Pr(x_i = 1 | a_{-i}) \leq \frac{1}{2} + \delta$$
$$\frac{1}{2} + \delta \leq \Pr(x_i = 0 | a_{-i}) \leq \frac{1}{2} - \delta$$

L6-4
by multiplying by \( \frac{\Pr(a_{-i})}{\Pr(a_{-i})} \) we get:

\[
\frac{\frac{1}{2} - \delta}{\frac{1}{2} + \delta} \leq \frac{\Pr(1a_{-i})}{\Pr(0a_{-i})} \leq \frac{\frac{1}{2} + \delta}{\frac{1}{2} - \delta}.
\]

However, this is true by the definition of \( \delta \)-half-space since \( 1a_{-i} \) and \( 0a_{-i} \) are either in the same or different partition so clearly \( \frac{\Pr(1a_{-i})}{\Pr(0a_{-i})} \in \left\{ \frac{\frac{1}{2} - \delta}{\frac{1}{2} + \delta}, 1, \frac{\frac{1}{2} + \delta}{\frac{1}{2} - \delta} \right\} \).

Now we can prove that for SV sources, bias \( \geq \delta \).

**Proof:** Take \( \forall f \). WLOG, assume that \( f \) is balanced (hardest case). Then \( |\{x|f(x) = 0\}| = |\{x|f(x) = 1\}| \) Let \( S = \{x|f(x) = 0\}, |S| = 2^{n-1} \). Then we can pick a \( \delta \)-halfspace source \( Z_S \) at \( S \).

This means that \( \Pr(f(Z_S) = 1) = \frac{1}{2} + \delta \).

But by the previous lemma, a \( \delta \)-halfspace source is also a \( \delta \)-SV source.

5 Mixed Sources

Both previous sources were kind of restricted. Now we introduce a source that combines both LLS and SV.

**Definition 13** \((\delta, b, n)\)-bias-control-limited source. A has \( b \) interventions, otherwise can bias by at most \( \delta \).

Here we have a much stronger impossibility result.

**Theorem 14**

\[
\forall f \ q_f(\delta, b) \leq \frac{2}{(1 + 2\delta)^b} = \frac{1}{2^{\Omega(bb) - 1}}
\]

Thus, if \( b\delta = \omega(1) \) then \( \forall \) extractors can fail with \( pr \ (1 - o(1)) \). Like in SV, this is independent of \( n \).

This gives a very negative message for deterministic randomness extraction.