Collective Coin Flipping and the KKL Theorem (lecture notes) **[Edited 2025-10-31]**

Course: Analysis of Boolean Functions, Autumn 2025, University of Chicago
Instructor: William Hoza (`williamhoza@uchicago.edu`)

1 The Poincaré inequality and the Kahn-Kalai-Linial theorem

Suppose n parties wish to play a game of chance via group chat. However, there might be a few dishonest parties, so no individual party can be trusted to roll the dice. There is no public source of randomness. What should they do?

Let's focus on the case of generating just one shared random bit – the "collective coin flipping" problem. We will investigate the following approach. Each party $i \in [n]$ is instructed to generate a random bit $x_i \in \{\pm 1\}$. Then, the shared random bit is $f(x_1, \dots, x_n)$ for some function $f \colon \{\pm 1\}^n \to \{\pm 1\}$. Pessimistically, we suppose that the dishonest parties manage to observe all of the other x_i values before choosing their own x_i values. Is there a choice of f that prevents the dishonest parties from significantly biasing the shared random bit?

Let's begin by supposing there is just one dishonest party $i_* \in [n]$. In this case, the probability that the dishonest party has control over the outcome is precisely $\mathrm{Inf}_{i_*}[f]$. Therefore, we are looking for a near-balanced function f in which every variable has tiny influence. The majority function is a decent choice; each variable has influence $O(1/\sqrt{n})$. We can do better using the "tribes" function.

Definition 1.1 (Tribes)**.** $\mathrm{Tribes}_{w,s} \colon (\{\pm 1\}^w)^s \to \{\pm 1\}$ is defined by

$$\mathrm{Tribes}_{w,s}(x) = \bigvee_{i=1}^{s} \bigwedge_{j=1}^{w} x_{i,j}.$$

Let $s = \lceil (\ln 2) \cdot 2^w \rceil$ and $n = ws$. Then

$$\Pr_x[\mathrm{Tribes}_{w,s}(x) = +1] = (1 - 2^{-w})^{\lceil (\ln 2) \cdot 2^w \rceil} = \frac{1}{2} \pm o(1),$$

so $\mathrm{Tribes}_{w,s}$ is near-balanced. But, at the same time,

$$\mathrm{Inf}_i[\mathrm{Tribes}_{w,s}] \le 2^{-(w-1)} = O\left(\frac{\log n}{n}\right).$$

Is there a near-balanced Boolean function with even smaller influences? There is an elementary $\Omega(1/n)$ influence lower bound. More precisely, we can prove a lower bound in terms of the *variance* of the random variable $f(x)$ when x is chosen uniformly at random, which we denote $\mathrm{Var}[f]$. The following observation confirms that $\mathrm{Var}[f]$ is a good way to quantify "how well-balanced" f is.

Lemma 1.2. *Let $f \colon \{\pm 1\}^n \to \{\pm 1\}$ and let $\delta \in [0, 1]$.*

- *If $-1 + \delta \le \mathbb{E}[f] \le 1 - \delta$, then $\mathrm{Var}[f] \ge \delta$. For example, if $\mathbb{E}[f] = 0$, then $\mathrm{Var}[f] = 1$.*
- *If $\mathrm{Var}[f] \ge \delta$, then $-1 + \frac{\delta}{2} \le \mathbb{E}[f] \le 1 - \frac{\delta}{2}$.*

Proof. Let $\beta = 1 - |\mathbb{E}[f]|$. Then

$$\mathrm{Var}[f] = \mathbb{E}[f^2] - \mathbb{E}[f]^2 = 1 - \mathbb{E}[f]^2 = 1 - (1 - \beta)^2 = \beta \cdot (2 - \beta) \in [\beta, 2\beta]. \qquad \square$$

Proposition 1.3 (Poincaré inequality)**.** *For any $f \colon \{\pm 1\}^n \to \{\pm 1\}$, we have $\mathrm{I}[f] \ge \mathrm{Var}[f]$, hence there is some $i \in [n]$ such that $\mathrm{Inf}_i[f] \ge \mathrm{Var}[f]/n$.*

Proof. We use a convenient Fourier formula for variance:

$$\mathrm{Var}[f] = \mathbb{E}[f^2] - \mathbb{E}[f]^2 = \sum_{S \neq \varnothing} \widehat{f}(S)^2.$$

Meanwhile, recall that we also have a Fourier formula for total influence:

$$\mathrm{I}[f] = \sum_{k=0}^{n} k \cdot W^k[f] \geq \sum_{k=1}^{n} W^k[f] = \mathrm{Var}[f]. \qquad \square$$

The KKL theorem gives a tight $\Omega((\log n)/n)$ lower bound.

Theorem 1.4 (Kahn-Kalai-Linial)**.** *For every $f\colon \{\pm 1\}^n \to \{\pm 1\}$, there is some $i \in [n]$ such that $\mathrm{Inf}_i[f] \geq \Omega(\mathrm{Var}[f] \cdot \frac{\log n}{n})$.*

Proof. Let $c \in (0,1)$ be an appropriate constant. Case 1: Suppose $\mathrm{I}[f] > c \cdot \mathrm{Var}[f] \cdot \log n$. The best case is at least as good as the average case, so we are done.

Case 2: Suppose $\mathrm{I}[f] \leq c \cdot \mathrm{Var}[f] \cdot \log n$. Intuition: Friedgut's junta theorem tells us that f is close to a k-junta where $k = 2^{O(\mathrm{I}[f])} \leq \sqrt{n}$. If f actually *were* a k-junta, then we could apply the Poincaré inequality to conclude that f has a variable with influence at least $\mathrm{Var}[f]/k$. To deal with the error in Friedgut's junta theorem, we'll need to re-do the *proof* of the Poincaré inequality. The details follow.

Let $\varepsilon = \mathrm{Var}[f]/2$. By Friedgut's junta theorem, there is a set $J \subseteq [n]$ of size $2^{O(\mathrm{I}[f]/\varepsilon)} \leq \sqrt{n}$ such that f is ε-concentrated on the subsets of J. Therefore,

$$\begin{aligned}\max_i \mathrm{Inf}_i[f] \geq \frac{1}{\sqrt{n}} \cdot \sum_{i \in J} \mathrm{Inf}_i[f] = \frac{1}{\sqrt{n}} \cdot \sum_{i \in J} \sum_{S \ni i} \widehat{f}(S)^2 &\geq \frac{1}{\sqrt{n}} \sum_{\varnothing \neq S \subseteq J} \widehat{f}(S)^2 \\ &= \frac{1}{\sqrt{n}} \left(\sum_{S \neq \varnothing} \widehat{f}(S)^2 - \sum_{S \not\subseteq J} \widehat{f}(S)^2 \right) \\ &= \frac{\mathrm{Var}[f] - \varepsilon}{\sqrt{n}} \\ &= \frac{\mathrm{Var}[f]}{2\sqrt{n}}. \qquad \square\end{aligned}$$

2 Limitations of resilient functions

Having proven the KKL theorem, let us return to the collective coin flipping problem and consider the case of multiple dishonest parties. We will use the KKL theorem to prove that if 1% of the parties are dishonest, then the dishonest parties can control the outcome with probability $1 - o(1)$. We emphasize that the elementary Poincaré inequality would *not* suffice for this argument! The log-factor distinction between Poincaré and KKL might appear minor at first glance, but it has a significant qualitative impact.

2.1 The monotone case

We begin with the simplest case: f is monotone and the dishonest parties wish to cause f to output $+1$. Throughout this section, we use the following convenient notation. If $J \subseteq [n]$, $x \in \{0,1\}^J$, and $y \in \{0,1\}^{[n] \setminus J}$, then xy denotes the string in $\{0,1\}^n$ in which we put x in the J coordinates and y in the $\overline{J}$ coordinates.

Lemma 2.1. *Let $f\colon \{\pm 1\}^n \to \{\pm 1\}$ be a monotone Boolean function such that $\mathbb{E}[f] = -1 + \delta$, where $\delta \in (0, 2]$. For every $\varepsilon \in (0, 1/2)$, there exists $J \subseteq [n]$ of size $|J| = O(\frac{n}{\log n} \cdot \log(\frac{1}{\varepsilon\delta}))$ such that*

$$\mathop{\mathbb{E}}_{y \in \{0,1\}^{[n] \setminus J}} [f(1^J y)] \geq 1 - \varepsilon.$$

Proof. Let $f_0 = f$. In step j, we select the variable i that maximizes $\mathrm{Inf}_i[f_{j-1}]$. We set that variable to $+1$, giving us a function f_j, and we add that variable to J. We continue until we reach a function with $\mathbb{E}[f_j] \geq 1 - \varepsilon$.

Now let us compute how many steps this process takes. We think of each f_j as being on n variables (and just ignoring some of them). By the KKL theorem, we have

$$\mathbb{E}[f_j] = \mathbb{E}[f_{j-1}] + 2\max_i \mathrm{Inf}_i[f_{j-1}] \geq \mathbb{E}[f_{j-1}] + \Omega\left(\mathrm{Var}[f_{j-1}] \cdot \frac{\log n}{n}\right).$$

From here, we divide into two phases: the phase in which the expectation rises from $-1 + \delta$ up to 0, and the phase in which the expectation rises from 0 up to $1 - \varepsilon$.

To analyze the first phase, suppose $\mathbb{E}[f_{j-1}] < 0$, say $\mathbb{E}[f_{j-1}] = -1 + \delta_{j-1}$. By Lemma 1.2, we have $\mathrm{Var}[f_{j-1}] \geq \delta_{j-1}$, hence

$$\delta_j \geq \delta_{j-1} \cdot \left(1 + \Omega\left(\frac{\log n}{n}\right)\right).$$

By induction, this shows that if $\mathbb{E}[f_{j-1}] < 0$, then

$$\delta_j \geq \delta \cdot \left(1 + \Omega\left(\frac{\log n}{n}\right)\right)^j.$$

Let $q = q_0 q_1$, where $q_0 = O(n/\log n)$ and $q_1 = O(\log(1/\delta))$. Then by Bernoulli's inequality, we have

$$\delta \cdot \left(1 + \Omega\left(\frac{\log n}{n}\right)\right)^{q_0 q_1} \geq \delta \cdot \left(1 + \Omega\left(q_0 \cdot \frac{\log n}{n}\right)\right)^{q_1} \geq 1.$$

Thus, the first phase is complete within $O(\frac{n}{\log n} \cdot \log(1/\delta))$ steps.

Now we analyze the second phase. For simplicity of notation, assume without loss of generality that there is no first phase, i.e., $\mathbb{E}[f] \geq 0$. Write $\mathbb{E}[f_j] = 1 - \gamma_j$. By Lemma 1.2, we have $\mathrm{Var}[f_{j-1}] \geq \gamma_{j-1}$, hence

$$\gamma_j \leq \gamma_{j-1} \cdot \left(1 - \Omega\left(\frac{\log n}{n}\right)\right).$$

By induction, we get

$$\gamma_j \leq \gamma_0 \cdot \left(1 - \Omega\left(\frac{\log n}{n}\right)\right)^j \leq 1 \cdot \exp\left(-\Omega\left(\frac{j \log n}{n}\right)\right) \leq \varepsilon,$$

for a suitable $j = O(\frac{n}{\log n} \cdot \log(1/\varepsilon))$. Thus, the second phase is complete within $O(\frac{n}{\log n} \cdot \log(1/\varepsilon))$ steps. □

2.2 The non-monotone case

Now let's generalize to Boolean functions that are not necessarily monotone. We use the following concept.

Definition 2.2 (Monotonization)**.** Let $f\colon \{\pm 1\}^n \to \mathbb{R}$ and let $i \in [n]$. We define $f^{\sigma_i}\colon \{\pm 1\}^n \to \mathbb{R}$ by

$$f^{\sigma_i}(x) = \begin{cases} \max(f(x^{(i\mapsto +1)}), f(x^{(i\mapsto -1)})) & \text{if } x_i = +1 \\ \min(f(x^{(i\mapsto +1)}), f(x^{(i\mapsto -1)})) & \text{if } x_i = -1. \end{cases}$$

If $J \subseteq [n]$, say $J = \{i_1 < i_2 < \cdots < i_q\}$, then we define

$$f^{\sigma_J} = f^{\sigma_{i_1}\sigma_{i_2}\cdots\sigma_{i_q}}.$$

Lemma 2.3. *Let $f\colon \{\pm 1\}^n \to \mathbb{R}$ and $J \subseteq [n]$. Then $\mathbb{E}[f^{\sigma_J}] = \mathbb{E}[f]$.*

Proof. We prove it by induction on $|J|$. If $|J| = 1$, say $J = \{n\}$ without loss of generality, then

$$\begin{aligned}
\mathbb{E}[f^{\sigma_n}] &= \mathop{\mathbb{E}}_{x_1,\ldots,x_{n-1}}\left[\frac{\max(f(x^{(i\mapsto+1)}), f(x^{(i\mapsto-1)})) + \min(f(x^{(i\mapsto+1)}), f(x^{(i\mapsto-1)}))}{2}\right] \\
&= \mathop{\mathbb{E}}_{x_1,\ldots,x_{n-1}}\left[\frac{f(x^{(i\mapsto+1)}) + f(x^{(i\mapsto-1)})}{2}\right] \\
&= \mathbb{E}[f].
\end{aligned}$$

If $|J| > 1$, say $J = J_0 \cup \{i\}$ where $i = \max(J)$, then $\mathbb{E}[f^{\sigma_J}] = \mathbb{E}[f^{\sigma_{J_0}\sigma_i}] = \mathbb{E}[f^{\sigma_{J_0}}] = \mathbb{E}[f]$. □

Lemma 2.4. *Let $f\colon \{\pm1\}^n \to \mathbb{R}$, let $J \subseteq [n]$, and let $y \in \{\pm1\}^{\overline{J}}$. Then $f^{\sigma_{[n]}}(1^J y) \le f^{\sigma_J \sigma_{\overline{J}}}(1^J y)$.*

Proof sketch. This holds because $\max_a \min_b g(a,b) \le \min_b \max_a g(a,b)$. □

Lemma 2.5. *Let $f\colon \{\pm1\}^n \to \{\pm1\}$ with $\mathbb{E}[f] = -1+\delta$, where $\delta \in [0,2)$. For every $\varepsilon \in (0,1/2)$, there exists $J \subseteq [n]$ of size $|J| = O(\frac{n}{\log n}\cdot\log(\frac{1}{\varepsilon\delta}))$ such that*

$$\Pr_{y\in\{\pm1\}^{[n]\setminus J}}[\exists x \in \{\pm1\}^J \text{ such that } f(xy) = 1] \ge 1-\varepsilon.$$

Proof. The function $f^{\sigma_{[n]}}$ is monotone and $\mathbb{E}[f^{\sigma_{[n]}}] = -1+\delta$ by Lemma 2.3. Therefore, by Lemma 2.1, there exists J of size $O(\frac{n}{\log n}\cdot\log(\frac{1}{\varepsilon\delta}))$ such that

$$\begin{aligned}
1-2\varepsilon &\le \mathop{\mathbb{E}}_{y\in\{\pm1\}^{\overline{J}}}[f^{\sigma_{[n]}}(1^J y)] \\
&\le \mathop{\mathbb{E}}_{y\in\{\pm1\}^{\overline{J}}}[f^{\sigma_J\sigma_{\overline{J}}}(1^J y)] && \text{by Lemma 2.4} \\
&= \mathop{\mathbb{E}}_{y\in\{\pm1\}^{\overline{J}}}[f^{\sigma_J}(1^J y)] && \text{by Lemma 2.3} \\
&= \mathop{\mathbb{E}}_{y\in\{\pm1\}^{\overline{J}}}\left[\max_{x\in\{\pm1\}^J} f(xy)\right] && \text{by Definition 2.2.}
\end{aligned}$$

□

Finally, let us remove the assumption that the dishonest parties wish to cause f to output $+1$.

Definition 2.6 (Coalitional influence)**.** Let $f\colon \{\pm1\}^n \to \{\pm1\}$ and $J \subseteq [n]$. We define

$$\widetilde{\mathrm{Inf}}_J[f] = \Pr_{x\in\{\pm1\}^{\overline{J}}}[\exists y, y' \in \{\pm1\}^J \text{ such that } f(xy) = +1 \text{ and } f(xy') = -1].$$

Theorem 2.7. *Let $f\colon \{\pm1\}^n \to \{\pm1\}$. For every $\varepsilon \in (0,1)$, there exists a set $J \subseteq [n]$ of size $|J| = O(\frac{n}{\log n}\cdot\log(\frac{1}{\varepsilon\cdot\mathrm{Var}[f]}))$ such that $\widetilde{\mathrm{Inf}}_J[f] \ge 1-\varepsilon$.*

Proof. Apply Lemma 2.5 to f and $1-f$, and take the union of the two J sets. This works, because by Lemma 1.2, we have $-1+\frac{\mathrm{Var}[f]}{2} \le \mathbb{E}[f] \le 1-\frac{\mathrm{Var}[f]}{2}$. □

For example, if f is near-balanced and 1% of the parties are dishonest, then the dishonest parties can control the outcome with probability $1-o(1)$. Indeed, Theorem 2.7 says that for every $\mu \in (0,1)$, there exists $J \subseteq [n]$ such that $|J| \le \mu n$ and

$$\widetilde{\mathrm{Inf}}_J[f] \ge 1 - \frac{1}{\mathrm{Var}[f]\cdot n^{\Omega(\mu)}}.$$

Theorem 2.7 can also be reformulated in terms of the notion of a *resilient function*.

Definition 2.8 (Resilience)**.** Let $f\colon \{\pm1\}^n \to \{\pm1\}$. We say that f is (q,ε)*-resilient* if, for every $J \subseteq [n]$ with $|J| \le q$, we have $\widetilde{\mathrm{Inf}}_J[f] \le \varepsilon$.

Theorem 2.7 says that if f is a near-balanced $(q, 0.99)$-resilient function, then $q \le O(n/\log n)$. In the other direction, there are known constructions of resilient functions with $q = \Omega(n/\log^2 n)$. It is an open question to close the log-factor gap between these two bounds.