Valence of a Configuration

0-valent:
there is an adversary with a high probability for deciding 0
there is no adversary with a high probability for deciding 1

1-valent:
there is no adversary with a high probability for deciding 0
there is an adversary with a high probability for deciding 1

bivalent:
there is an adversary with a high probability for deciding 0
there is an adversary with a high probability for deciding 1

null-valent:
there is no adversary with a high probability for deciding 0
there is no adversary with a high probability for deciding 1
Valence of a Configuration

0-valent: only high probability for deciding 0
1-valent: only high probability for deciding 1
bivalent: high probability for deciding 0 and high probability for deciding 1
null-valent: not high probability for deciding 0 and not high probability for deciding 1

\[ \varepsilon_k = \frac{1}{n\sqrt{n}} - \frac{k}{(n-f)^3} \]

where \( k \) is the layer number
Back to the Big Picture

Initially

- bivalent
- null-valent

Deciding

- 0-valent
- 1-valent

w.h.p. null-valent bivalent

≥ n-f

hiding $p_i$
maybe $p_i$
failing $p_i$
no step of $p_i$
no step of $p_i$

f layers, each with at least $n-f$ steps $\Rightarrow f(n-f)$ steps
Remaining Null-Valent

• Assume we are in a null-valent configuration
• Our goal (as an adversary) is to choose an f-layer that reaches another null-valent configuration
• 3-valued one-round coin-flipping game: 
  \[ g: \{X_1 \cup \bot\} \times \{X_2 \cup \bot\} \times \ldots \times \{X_m \cup \bot\} \rightarrow \{1, 2, 3\} \]
  \(X_i\) is a random variable
• We will prove:
  one of the outcomes has high probability
Interpretation of the Coin-Flipping Game

\[ g : \{X_1 \cup \bot\} \times \{X_2 \cup \bot\} \times \ldots \times \{X_m \cup \bot\} \rightarrow \{1, 2, 3\} \]

- Product probability space = results of local coin-flips
- \( \bot \) stands for a process not taking a step in the layer

- Each layer implies a resulting configuration
- Partition into categories according to valence:
  - 0-valent or bivalent configuration \( \Rightarrow \) the outcome of \( g \) is 1
  - 1-valent configuration \( \Rightarrow \) the outcome of \( g \) is 2
  - Null-valent configuration \( \Rightarrow \) the outcome of \( g \) is 3

- one of the outcomes has high probability
  \( \Rightarrow \) some category can be forced (by hiding processes) w.h.p.
**Interpretation of the Coin-Flipping Game**

\[ g : \{X_1 \cup \bot\} \times \{X_2 \cup \bot\} \times \ldots \times \{X_m \cup \bot\} \to \{1, 2, 3\} \]

\[ \Rightarrow \text{some outcome can be forced (by hiding processes) w.h.p.} \]

But, we started from a null-valent configuration

1. not high probability of deciding 0
   \[ \Rightarrow \text{cannot have high probability for reaching a 0-valent configuration} \]

2. not high probability of deciding 1
   \[ \Rightarrow \text{cannot have high probability for reaching a 1-valent configuration} \]

\[ \Rightarrow \text{the null-valent category must be the one with high probability} \]
From Null-Valent to Null-Valent

- Null-valent configuration has probability for deciding 0 at most $1-\varepsilon_k$
- Assume 0-valent or bivalent configuration can be reached with probability $1-1/(n-f)^3$
- New configuration has probability for deciding 0 at least $1-\varepsilon_{k+1}$
- Together, the probability for deciding 0 from the null-valent configuration is:

$$
\geq \left(1-\frac{1}{(n-f)^3}\right)(1-\varepsilon_{k+1}) = \left(1-\frac{1}{(n-f)^3}\right)\left(1-\frac{1}{n\sqrt{n}} + \frac{k+1}{(n-f)^3}\right)
$$

$$
= 1-\frac{1}{n\sqrt{n}} + \frac{k}{(n-f)^3} + \frac{1}{(n-f)^3 n\sqrt{n}} - \frac{k+1}{(n-f)^6}
$$

$$
> 1-\frac{1}{n\sqrt{n}} + \frac{k}{(n-f)^3} = 1-\varepsilon_k
$$

Cannot have high probability for reaching a 0-valent or bivalent configuration
From Null-Valent to Null-Valent

- Same proof shows that the category that can be forced with high probability cannot be the category of 1-valent configurations.
- The category that can be forced with high probability must be of the null-valent configurations.
- We now prove the claim

one of the outcomes of the game has high probability
One Outcome has High Probability

The probability space $X = X_1 \times X_2 \times \ldots \times X_m$

$W^1 = \{\text{points where hiding } \leq t \text{ coordinates does not give outcome 1}\}$

$W^2$

$W^3$

We want to prove that for some $u$, $\Pr[W^u] < 1/m^3$

$x = x_1 \ldots x_m$

$g(x) \neq 1$

$|I| \leq t$ $x_I = x_1 \ldots \perp \ldots \perp \ldots x_m$

$g(x_I) \neq 1$
One Outcome has High Probability

\[ W_1 \]

\[ W_2 \]

\[ B(W_1, t/3) \]

\[ B(W^2, t/3) = \{ \text{points that differ in at most } t/3 \text{ coordinates from some point in } W^2 \} \]

\[ B(W_3, t/3) \]

\[ W^3 \]

\[ \forall \neq 1 \neq 2 \neq 3 \]

\[ g(y) = g(x_1) = g(x_2) = g(x_3) = ? \]

\[ \mathbf{y}_1 \]

\[ \mathbf{x}_2^1 \]

\[ \mathbf{x}_2^2 \]

\[ \mathbf{x}_3^1 \]

\[ \mathbf{x}_3^2 \]

We want to prove that for some \( u \), \( \Pr[W^u] < 1/m^3 \)

\( W^u \) – adversary cannot reach outcome \( u \).

Assume \( \Pr[W^u] \geq 1/m^3 \)

Isoperimetric inequality: if \( \Pr[W^u] \geq 1/m^3 \) then \( \Pr[B(W^u, t/3)] \geq 1-1/m^3 \)
One Outcome has High Probability

$W^u$ – adversary cannot reach outcome $u$.
For some $u$, $\Pr[W^u]<1/m^3$.
The adversary can reach the outcome $u$ with probability $\geq 1-1/m^3$.
Must be the null-valent category.
Isoperimetric inequality

• Still need to prove the isoperimetric inequality that we used

• If $\Pr[W^u] \geq 1/m^3$ then $\Pr[B(W^u, t/3)] \geq 1 - 1/m^3$

\[
t = 6\sqrt{2m \log(m^3)}
\]
Wrap-up

• The probability to continue $f/2$ layers is at least $1 - 1/\sqrt{n}$
  – The probability for each layer is at least $1 - 1/n\sqrt{n}$

• Therefore, the expected number of steps is:
  \[
  \left(1 - \frac{1}{\sqrt{n}}\right)\frac{f}{2} (n - f)
  \]
  which is $\Omega(n^2)$ for $f=n/2$
Isoperimetric inequality

• Still need to prove the isoperimetric inequality that we used

• If $\Pr[W^u] \geq 1/m^3$ then $\Pr[B(W^u,t/3)] \geq 1-1/m^3$

$$t = 6\sqrt{2m \log(m^3)}$$
Interlude - Martingales

- A **martingale** is a sequence of random variables $X_0, X_1, \ldots$, not necessarily **independent**, such that:

\[ E[X_{i+1} \mid X_0, \ldots, X_i] = X_i \]

- This can be thought of as a stochastic process having “no memory”.

- A nice fact about martingales is that for all $i$:

\[ E[X_i] = E[X_0] \]
Martingales - Example

• The sum of independent unbiased coin flips
  – When we analyzed the shared-coin algorithm last week, we had random variables $X_1, X_2, \ldots, X_m$, and analyzed the behavior of their sums $S_j = X_1 + \ldots + X_j$. The sequence $S_1, S_2, \ldots$ forms a martingale.
Doob Martingale

• Framework for constructing a martingale
  – Based on accumulating elements of a random combinatorial structure

• Let $X = X_1 \times \ldots \times X_m$ be a product probability space for which we are interested in some function $f : X \to \mathbb{R}$

• Let $z$ be a random vector taking values in $X$
  – Example: If $X$ is the probability space of Boolean vectors indexed by all pairs of nodes of a graph then $z$ represents a random graph.
  – The function $f$ could be any graph property, e.g., the chromatic number
Doob Martingale
Doob Martingale
Doob Martingale

- \( X = X_1 \times \ldots \times X_m \) product probability space
  
  We are interested in \( f: X \rightarrow \mathbb{R} \)

  \( z \) is drawn from \( X \)

- Let \( D = \{1, \ldots, m\} \)

- Define \( z: D \rightarrow X_1 \bigcup \ldots \bigcup X_m \) such that \( z(i) \) is in \( X_i \)

- Define a sequence of partial domains
  
  \( D_i = \{1, \ldots, i\} \)

- \( D_0 = \emptyset \)
Doob Martingale

- \( z : D \rightarrow X_1 \cup \ldots \cup X_m \) such that \( z(i) \) is in \( X_i \)
- A sequence of partial domains \( D_i = \{1, \ldots, i\} \)
- \( D_0 = \emptyset \)
- Choose a random element \( w \) according to the distribution \( X \), and define the sequence \( Y_0, \ldots, Y_m \) by

\[
Y_i = E \left[ f(z) \mid z \mid_{D_i} = w \mid_{D_i} \right]
\]
Doob Martingale

\[ Y_i = E\left[ f(z) \mid z_{D_i} = w_{D_i} \right] \]

We have:

• \( Y_0 = E\left[ f(z) \right] \)

• \( Y_m = f(w) \) with the probability of choosing \( w \)

• The sequence \( Y_0, ..., Y_m \) is a Martingale

\[ E\left[ Y_{i+1} \mid Y_0, ..., Y_i \right] = Y_i \]

• Called a **Doob Martingale**
Azuma’s Inequality

• In many cases we are interested in bounding large deviations of a martingale sequence

• If $|X_i - X_{i-1}| < c_i$ for every $i$, then

$$\Pr\left[ X_m - X_0 > t \right] < \exp\left( \frac{-t^2}{2 \sum_{i=1}^{m} c_i^2} \right)$$

• Applying twice and using union bound gives

$$\Pr\left[ |X_m - X_0| > t \right] < 2 \exp\left( \frac{-t^2}{2 \sum_{i=1}^{m} c_i^2} \right)$$
Doob Martingale

\[ Y_i = E \left[ f(z) \mid z_{|D_i} = w_{|D_i} \right] \]

- So, if \( |Y_i - Y_{i-1}| < c_i \) then Azuma’s inequality holds

\[
\Pr \left[ |Y_m - Y_0| > t \right] < 2 \exp \left( \frac{-t^2}{2 \sum_{i=1}^m c_i^2} \right)
\]

- The function \( f \) satisfies the **Lipschitz** condition if whenever \( z_1 \) and \( z_2 \) differ only in \( D_i \backslash D_{i-1} \) for some \( i \), then \( |f(z_1) - f(z_2)| \leq 1 \)

- The martingale Lipschitz condition says that if the Lipschitz condition holds then \( |Y_i - Y_{i-1}| \leq 1 \)
Isoperimetric inequality:
If $\Pr[W^u] \geq 1/m^3$ then $\Pr[B(W^u,t/3)] \geq 1 - 1/m^3$

• Let $A \subseteq X$ with $\Pr[z \in A] = c$, and let $\lambda_0 = \sqrt{2m \log \frac{2}{c}}$, then for $\ell \geq \lambda_0$ we have

$$\Pr\left[z \in B(A, \ell)\right] \geq 1 - 2 \exp\left(\frac{-(\ell-\lambda_0)^2}{2m}\right)$$

• Reminder: $t = 6\sqrt{2m \log (m^3)}$
Gives Inequality:

- Plug in the parameters
- Let \( A \subseteq X \) with \( \Pr[z \in A] = c \), and let \( \lambda_0 = \sqrt{2m \log \frac{2}{c}} \), then for \( \ell \geq \lambda_0 \) we have

\[
\Pr[z \in B(A, \ell)] \geq 1 - 2 \exp\left(\frac{-(\ell - \lambda_0)^2}{2m}\right)
\]

- We get that if \( \Pr[W^u] \geq 1/m^3 \) then
  \( \Pr[B(W^u, t/3)] \geq 1 - 1/m^3 \) by plugging \( c = 1/m^3 \),

\[
\lambda_0 = \sqrt{2m \log(2m^3)} \quad \text{and} \quad \ell = t / 3 = 2\sqrt{2m \log(2m^3)} = 2\lambda_0
\]
Isoperimetric inequality:
If $\Pr[W^u] \geq 1/m^3$ then $\Pr[B(W^u, t/3)] \geq 1 - 1/m^3$

- Let $A \subseteq X$ with $\Pr[z \in A] = c$, and let $\lambda_0 = \sqrt{2m \log \frac{2}{c}}$, then for $\ell \geq \lambda_0$ we have
  $$\Pr[z \in B(A, \ell)] \geq 1 - 2 \exp\left(\frac{-(\ell - \lambda_0)^2}{2m}\right)$$

- Proof: Let $f: X \to \mathbb{R}$ measure that distance to the set $A$, i.e., $f(z) = d(z, A)$. Then $f$ satisfies the Lipschitz condition: whenever $z_1$ and $z_2$ differ only in $D_i \setminus D_{i-1}$ for some $i$, then $|f(z_1) - f(z_2)| \leq 1$
Isoperimetric inequality:
If $\Pr[W^u] \geq 1/m^3$ then $\Pr[B(W^u, t/3)] \geq 1 - 1/m^3$

- Let $A \subseteq X$ with $\Pr[z \in A] = c$, and let $\lambda_0 = \sqrt{2m \log \frac{2}{c}}$, then for $\ell \geq \lambda_0$ we have
  $$\Pr[z \in B(A, \ell)] \geq 1 - 2\exp\left(\frac{-(\ell - \lambda_0)^2}{2m}\right)$$

- So the martingale Lipschitz condition is satisfied: $|Y_i - Y_{i-1}| \leq 1$

- Azuma’s inequality gives:
  $$\Pr\left[|f(z) - E[f(z)]| > \lambda\right] < 2\exp\left(\frac{-\lambda^2}{2m}\right)$$
Isoperimetric inequality:
If $\Pr[W^u] \geq 1/m^3$ then $\Pr[B(W^u, t/3)] \geq 1 - 1/m^3$

• We now claim that $E[f(z)] \leq \lambda_0$. Assume the contrary. Since $\lambda_0 = \sqrt{2m \log \frac{2}{c}}$, we have

$$2 \exp\left(\frac{-\lambda_0^2}{2m}\right) = c$$

• For $z \in A$ we have $f(z) = 0$ and so

$$\Pr\left[|f(z) - E[f(z)]| > \lambda_0 \right] \geq \Pr[f(z) = 0] = c$$

which contradicts Azuma’s inequality
Isoperimetric inequality:
If $\Pr[W^u] \geq 1/m^3$ then $\Pr[B(W^u, t/3)] \geq 1 - 1/m^3$

• So we have

$$\Pr\left[ z \not\in B(A, \ell) \right] = \Pr[f(z) > \ell]$$

$$\leq \Pr\left[ |f(z) - E[f(z)]| > \ell - \lambda_0 \right] < 2 \exp\left( -\frac{(\ell - \lambda_0)^2}{2m} \right)$$

• Which completes the proof

$$\Pr\left[ z \in B(A, \ell) \right] \geq 1 - 2 \exp\left( -\frac{(\ell - \lambda_0)^2}{2m} \right)$$