Randomized Algorithms

南京大学

尹一通

Chernoff Bound

independent $X_1, X_2, \ldots, X_n \in \{0,1\}$

let $X = \sum_{i=1}^{n} X_i$

$t > 0:$

$$\Pr[X \geq \mathbf{E}[X] + t] \leq \exp\left(-\frac{2t^2}{n}\right)$$

$$\Pr[X \leq \mathbf{E}[X] - t] \leq \exp\left(-\frac{2t^2}{n}\right)$$

The method of bounded differences

Independent random variables: $X=(X_1, X_2, \ldots, X_n)$.

$f(x_1, x_2, \ldots, x_n)$ satisfies the Lipschitz condition:

$$|f(x_1, \ldots, x_n) - f(x_1, \ldots, x_{i-1}, y_i, x_{i+1}, \ldots, x_n)| \le c_i$$

for arbitrary possible values $x_1, \ldots, x_n, y_i$.

$t > 0$:

$$\Pr[f(\boldsymbol{X}) \geq \mathbf{E}[f(\boldsymbol{X})] + t] \leq \exp\left(-\frac{2t^2}{\sum_{i=1}^n c_i^2}\right)$$

$$\Pr[f(\boldsymbol{X}) \leq \mathbf{E}[f(\boldsymbol{X})] - t] \leq \exp\left(-\frac{2t^2}{\sum_{i=1}^n c_i^2}\right)$$

Martingale

Definition:

A sequence of random variables $X_0, X_1, \ldots$ is a **martingale** if for all $i > 0$,

$$\mathbf{E}[X_i \mid X_0, \ldots, X_{i-1}] = X_{i-1}$$

What does this mean?

Azuma's Inequality:

Let $X_0, X_1, \ldots$ be a martingale such that, for all $k \geq 1$,

$$|X_k - X_{k-1}| \leq c_k,$$

Then

$$\Pr\left[|X_n - X_0| \geq t\right] \leq 2\exp\left(-\frac{t^2}{2\sum_{k=1}^{n} c_k^2}\right).$$

Generalization

Definition:

$Y_0, Y_1, \ldots$ is a martingale with respect to $X_0, X_1, \ldots$ if, for all $i \geq 0$,

- Y_i is a function of $X_0, X_1, \ldots, X_i$;
- $\mathbf{E}[Y_{i+1} \mid X_0, \ldots, X_i] = Y_i$.

Definition:

$Y_0, Y_1, \ldots$ is a martingale with respect to $X_0, X_1, \ldots$ if, for all $i \geq 0$,

- Y_i is a function of $X_0, X_1, \ldots, X_i$;
- $\mathbf{E}[Y_{i+1} \mid X_0, \ldots, X_i] = Y_i$.

- Betting on a fair game;
- X_i : win/loss of the *i*-th bet;
- Y_i : wealth after the *i*-th bet -- Martingale (fair game)

Azuma's Inequality (general version):

Let $Y_0, Y_1, \ldots$ be a martingale with respect to $X_0, X_1, \ldots$ such that, for all $k \geq 1$,

$$|Y_k - Y_{k-1}| \leq c_k,$$

Then

$$\Pr[|Y_n - Y_0| \geq t] \leq 2\exp\left(-\frac{t^2}{2\sum_{k=1}^{n} c_k^2}\right).$$

Doob Sequence

Definition (Doob sequence):

The Doob sequence of a function f with respect to a sequence $X_1, \ldots, X_n$ is

$$Y_i = \mathbf{E}[f(X_1, \ldots, X_n) \mid X_1, \ldots, X_i]$$

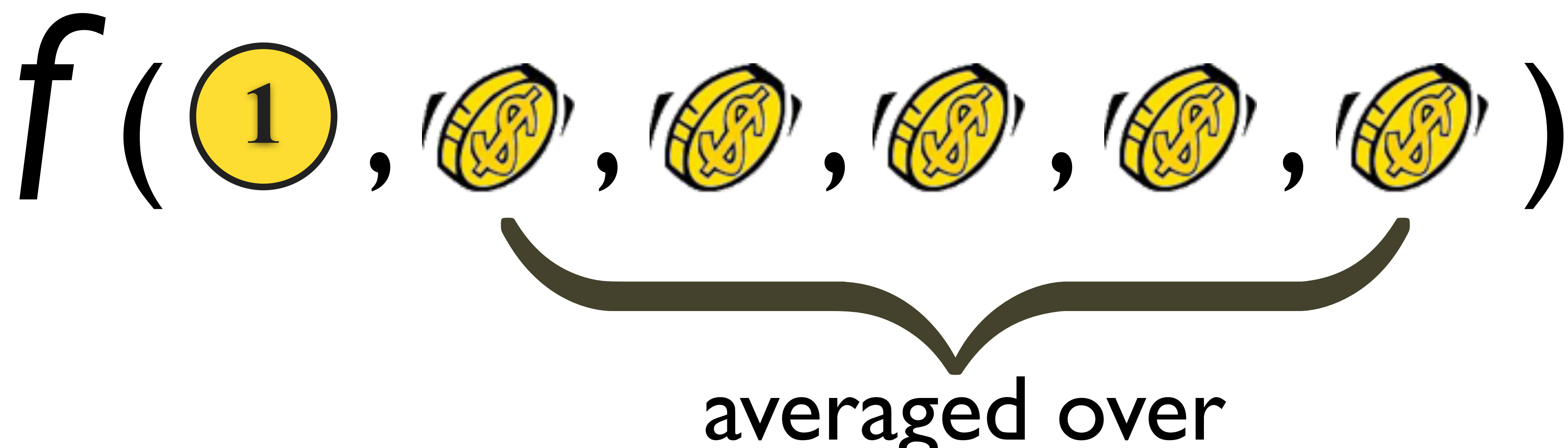
$Y_0 = \mathbf{E}[f(X_1, \ldots, X_n)]$ - - - - - - → $Y_n = f(X_1, \ldots, X_n)$

Doob Sequence

$$\mathbf{E}[f] = Y_0,$$

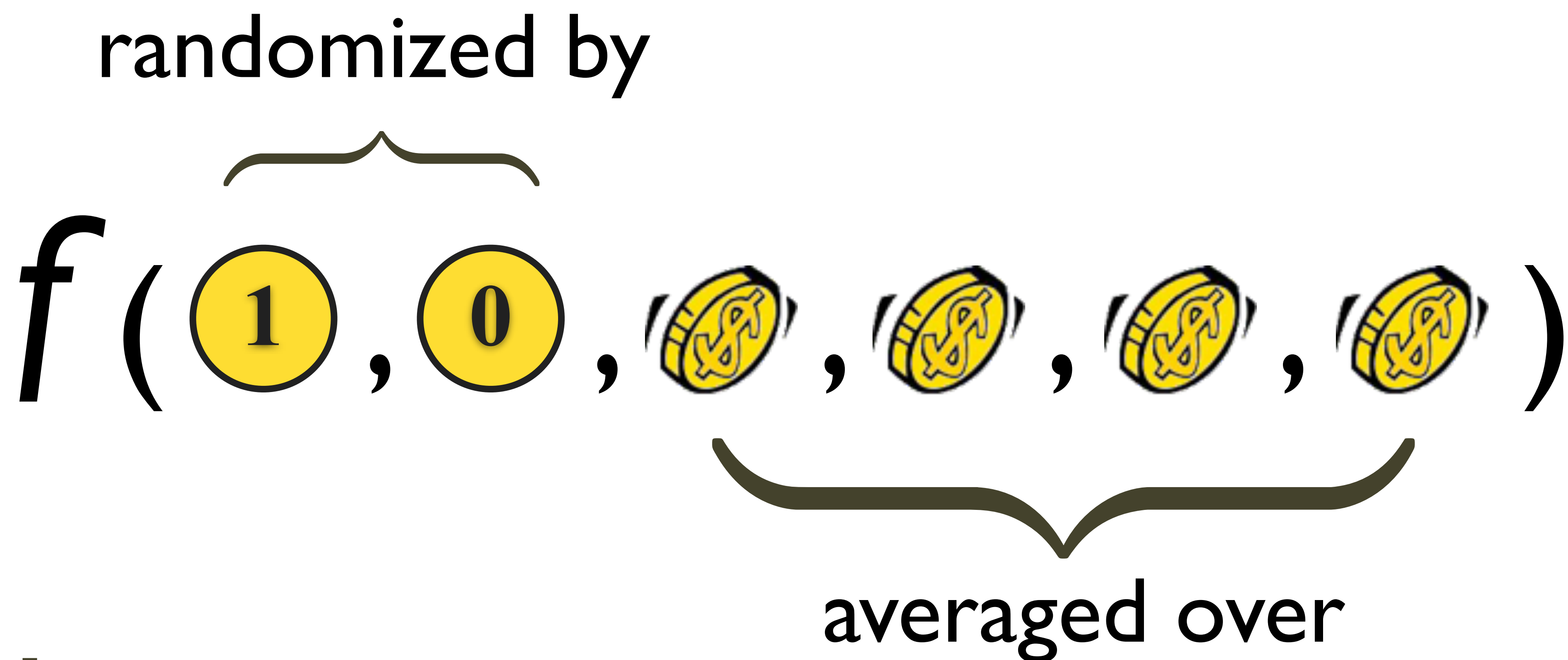
Doob Sequence

randomized by



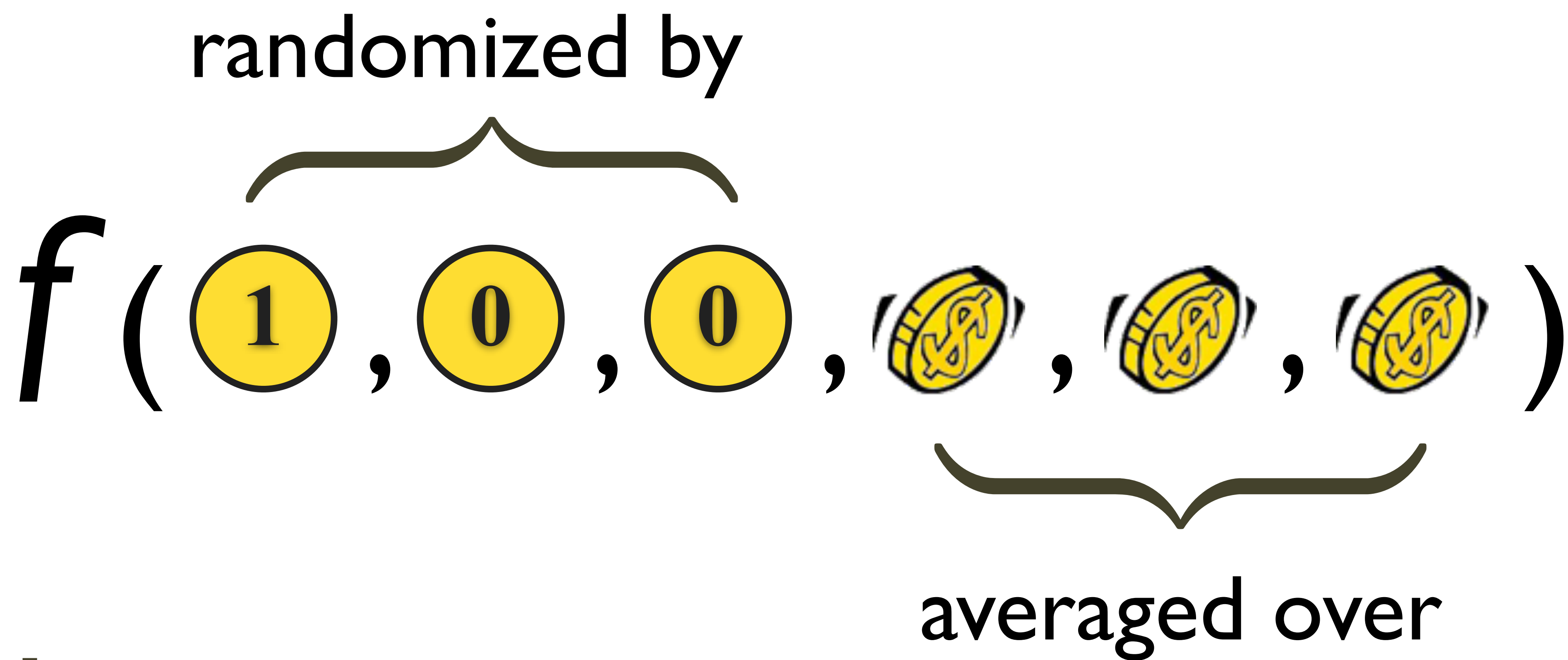
$$\mathbf{E}[f] = Y_0, \quad Y_1,$$

Doob Sequence



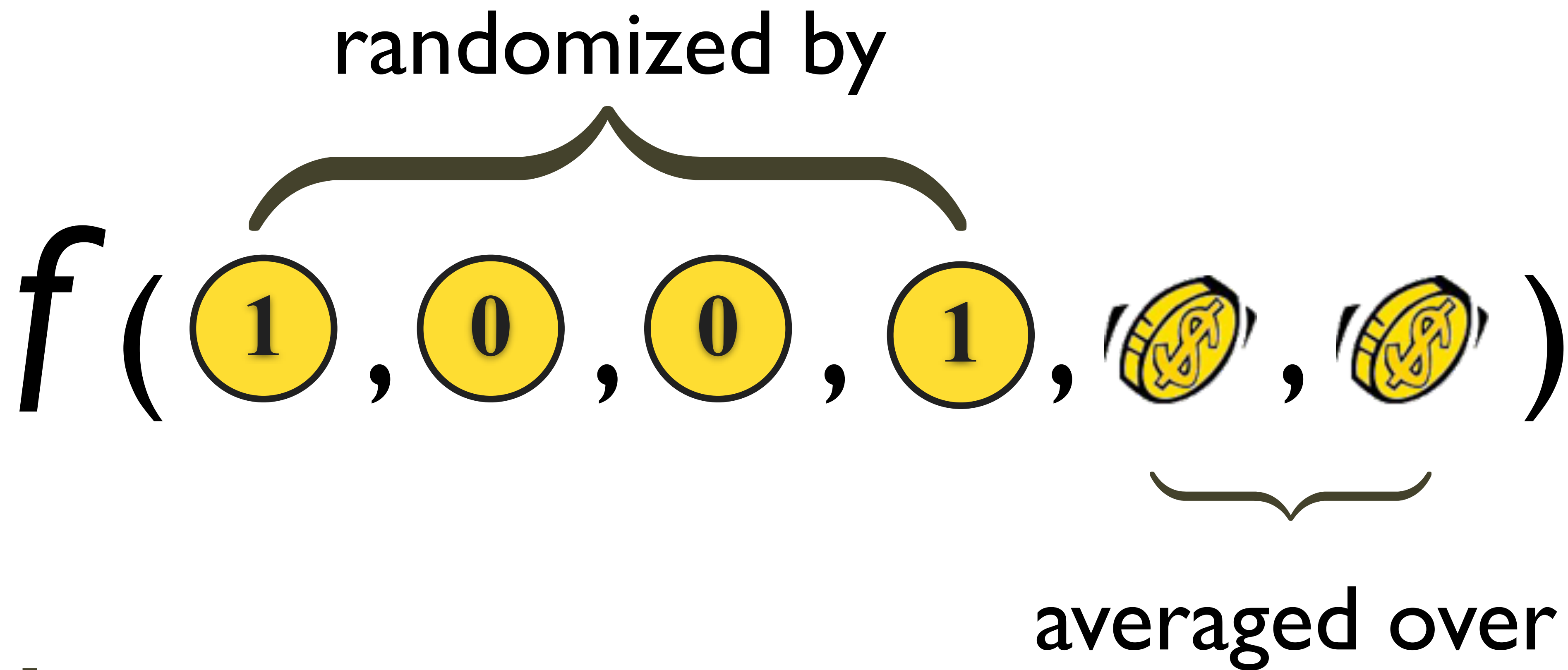
$$\mathbf{E}[f] = Y_0, \quad Y_1, \quad Y_2,$$

Doob Sequence



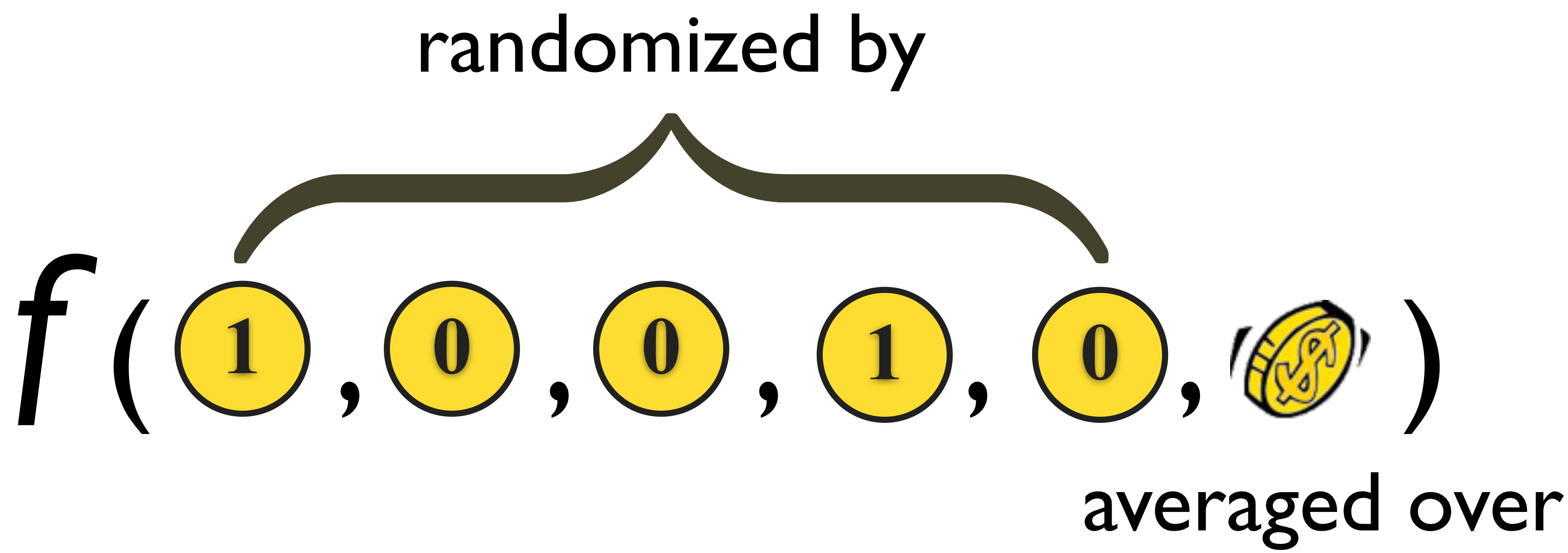
$$\mathbf{E}[f] = Y_0, \quad Y_1, \quad Y_2, \quad Y_3,$$

Doob Sequence



$$\mathbf{E}[f] = Y_0, \quad Y_1, \quad Y_2, \quad Y_3, \quad Y_4,$$

Doob Sequence



$$\mathbf{E}[f] = Y_0, \quad Y_1, \quad Y_2, \quad Y_3, \quad Y_4, \quad Y_5,$$

Doob Sequence

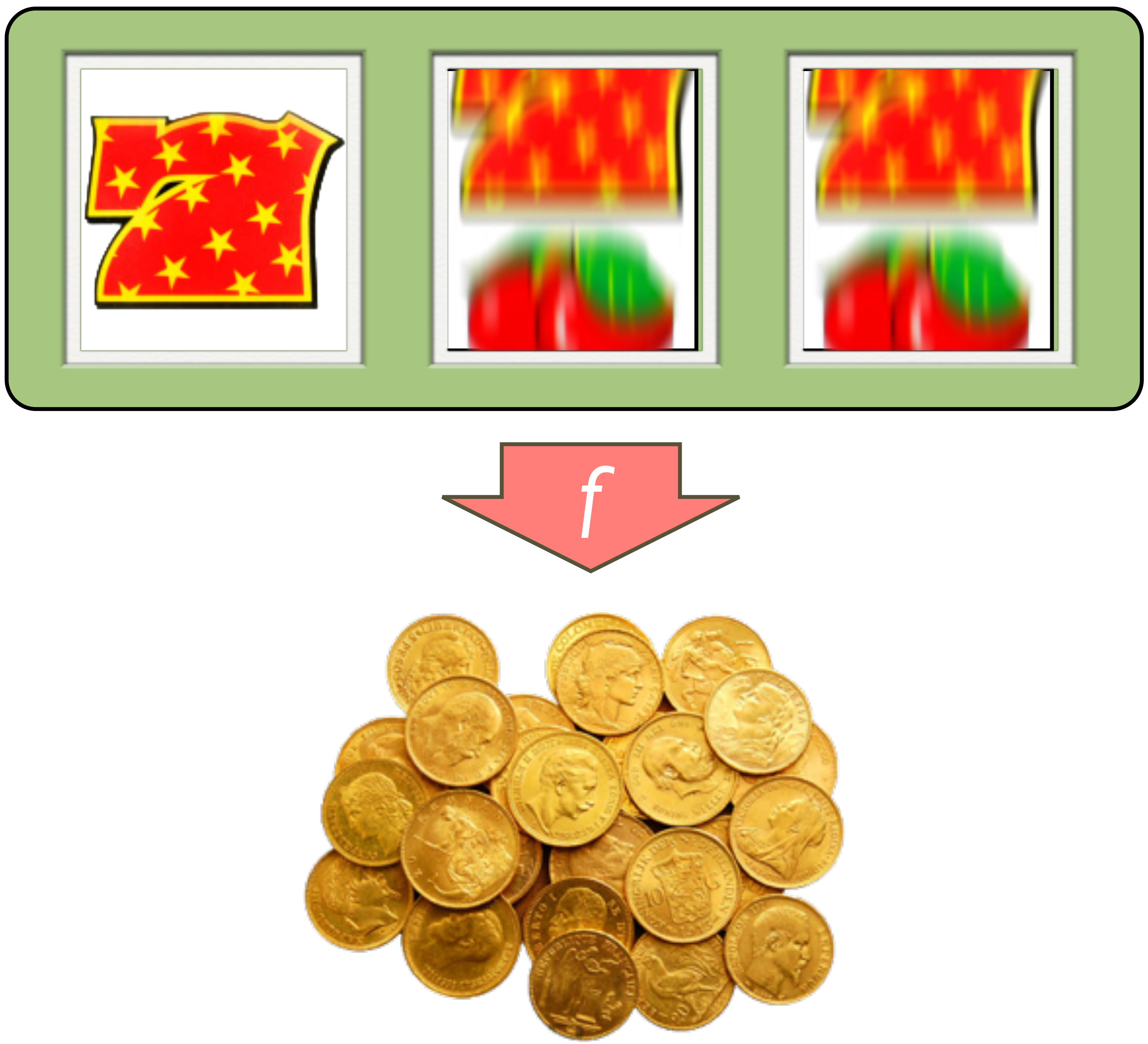
randomized by

$$f(\underbrace{1, 0, 0, 1, 0, 1}_{})$$

no information full information

$$\mathbf{E}[f] = Y_0, \quad Y_1, \quad Y_2, \quad Y_3, \quad Y_4, \quad Y_5, \quad Y_6 \quad = f$$

Doob Martingale



Doob sequence:

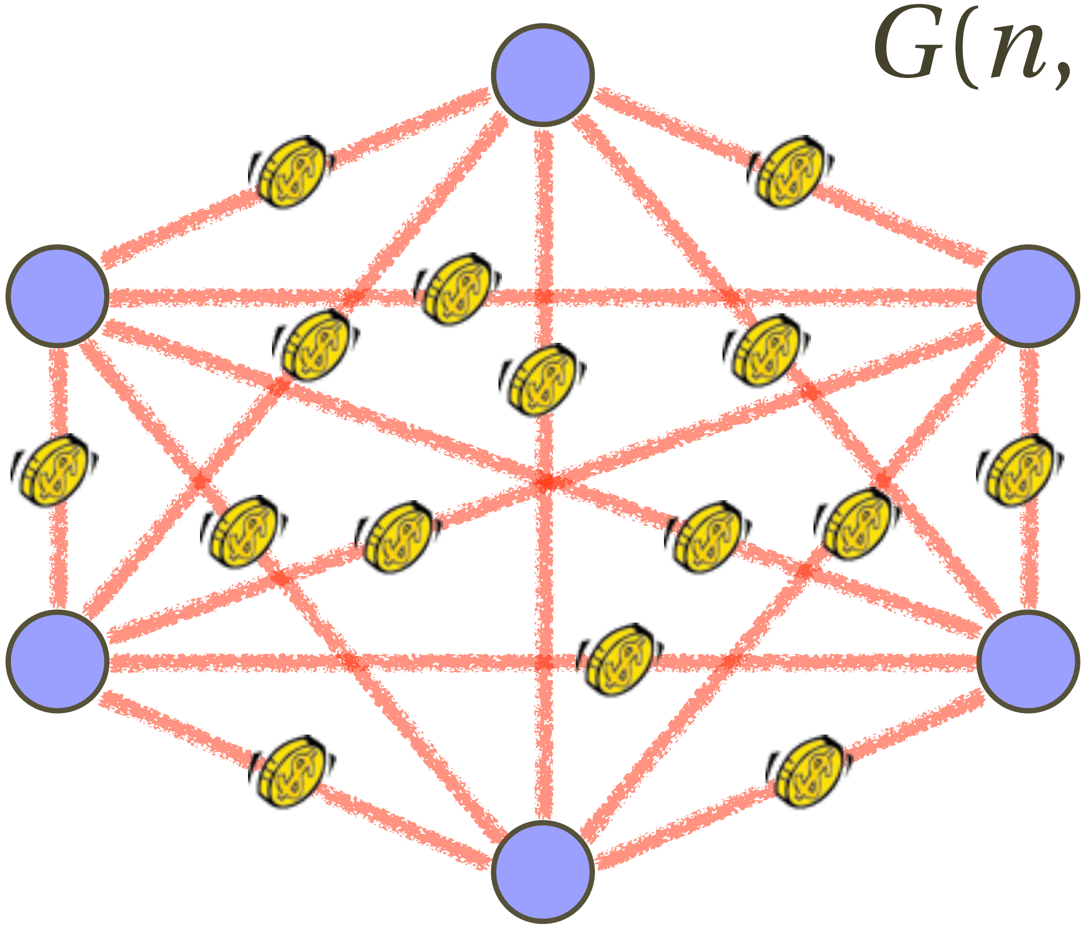
$$Y_i = \mathbf{E}[f(X_1,\ldots,X_n) \mid X_1,\ldots,X_i]$$

Doob sequence is a martingale:

$$\mathbf{E}[Y_i \mid X_1,\ldots,X_{i-1}] = Y_{i-1}$$

Proof:

$$\begin{aligned}
&\mathbf{E}[Y_i \mid X_1,\ldots,X_{i-1}] \\
&= \mathbf{E}[\mathbf{E}[f(X_1,\ldots,X_n) \mid X_1,\ldots,X_i] \mid X_1,\ldots,X_{i-1}] \\
&= \mathbf{E}[f(X_1,\ldots,X_n) \mid X_1,\ldots,X_{i-1}] \\
&= Y_{i-1}
\end{aligned}$$



$G(n, p)$

Graph parameter:

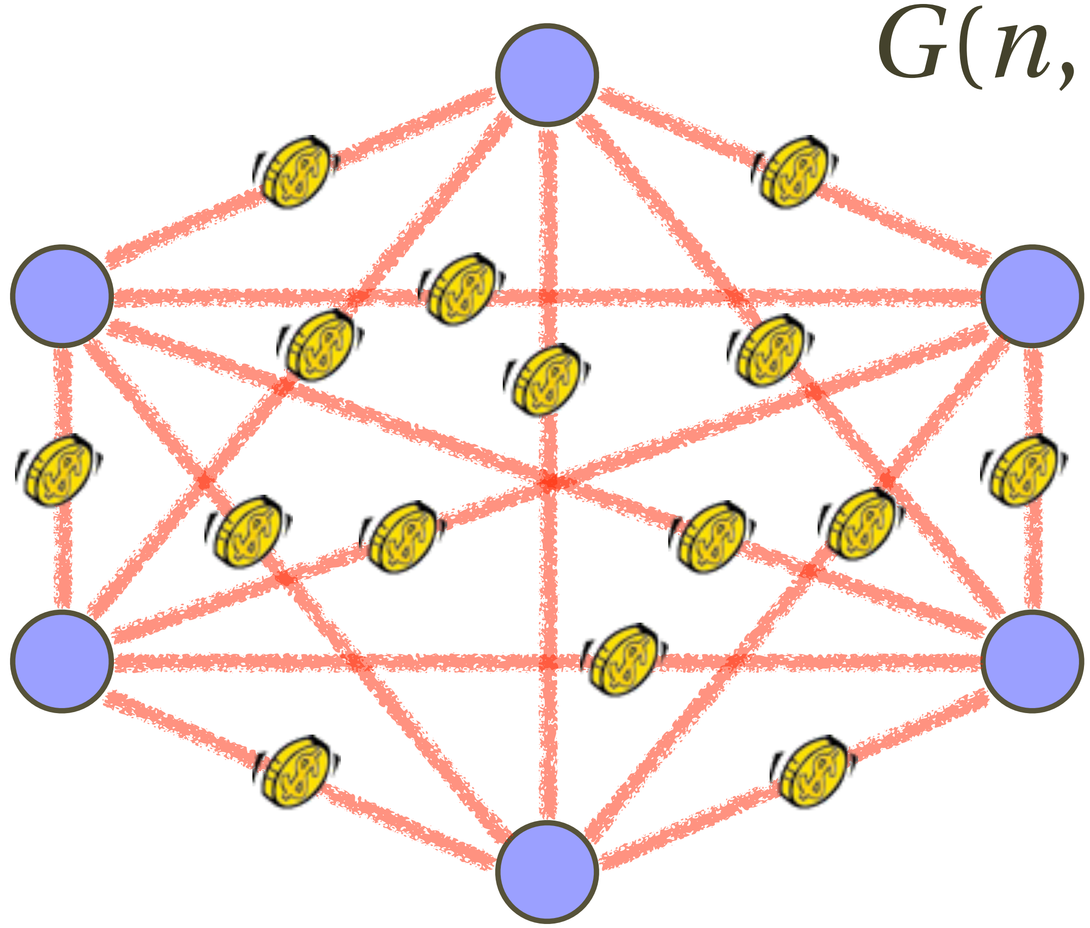
$$f(G)$$

example: chromatic #, components, diameter ...

numbering all vertex-pairs: $1, 2, 3, \ldots, \binom{n}{2}$

$$I_j = \begin{cases} 1 & \text{edge } j \in G \\ 0 & \text{edge } j \notin G \end{cases} \qquad Y_i = \mathbf{E}[f(G) \mid I_1, \ldots, I_i]$$

$$Y_0 = \mathbf{E}[f(G)] \dashrightarrow Y_{\binom{n}{2}} = f(G)$$



Graph parameter:

$$f(G)$$

example: chromatic #, components, diameter ...

numbering all vertices: $1, 2, 3, \ldots, n$

X_i : subgraph of G induced by the first i vertices

$$Y_i = \mathbf{E}[f(G) \mid X_1, \ldots, X_i]$$

$$Y_0 = \mathbf{E}[f(G)] \dashrightarrow Y_n = f(G)$$

Martingales induced by a random graph

- Edge exposure martingale:

$$I_j \text{ indicates the } j\text{th edge}$$

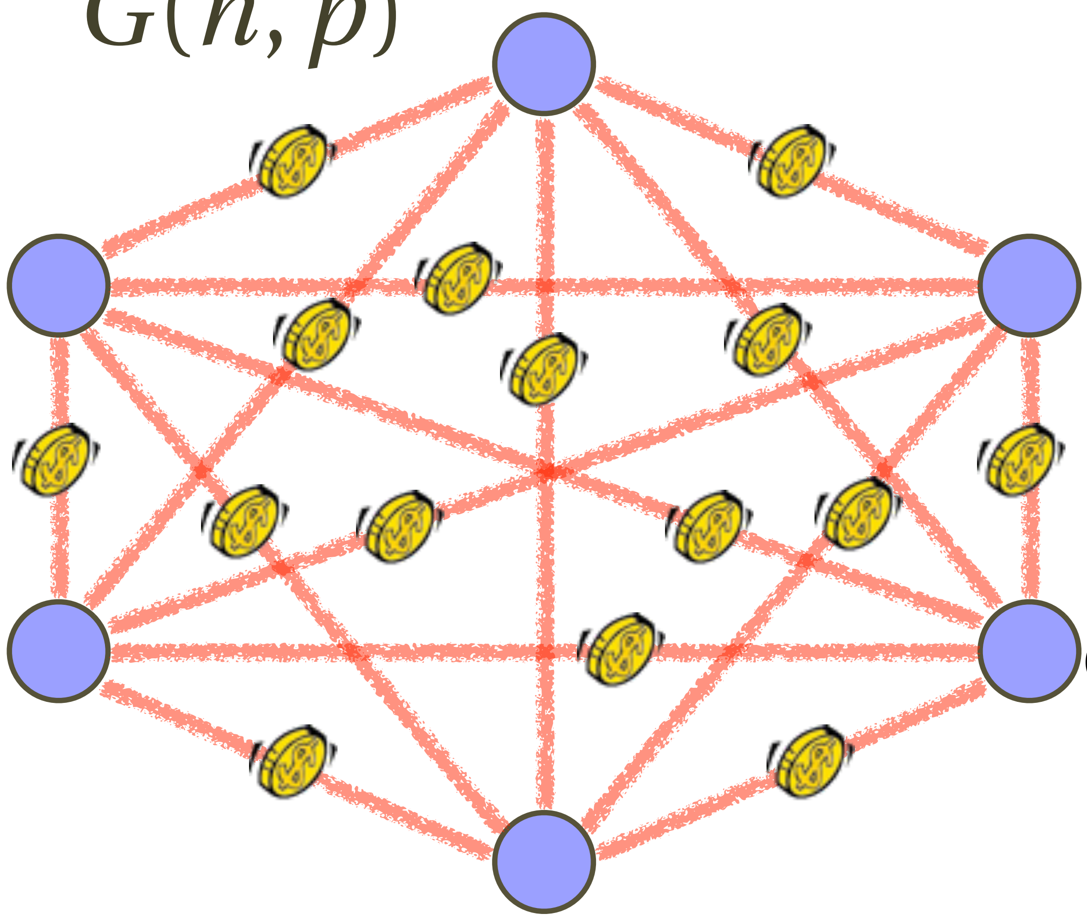
$$Y_i = \mathbf{E}[f(G) \mid I_1, \ldots, I_i]$$

- Vertex exposure martingale:

$$X_i = G([i])$$

$$Y_i = \mathbf{E}[f(G) \mid X_1, \ldots, X_i]$$

$G(n,p)$



chromatic number:

$\chi(G)$

the smallest number of colors to properly color G

X_i : subgraph of G induced by the first i vertices

$$Y_i = \mathbf{E}[\chi(G) \mid X_1, \ldots, X_i]$$

Doob martingale: $Y_0, Y_1, \ldots, Y_n$

$$Y_0 = \mathbf{E}[\chi(G)] \qquad\qquad Y_n = \chi(G)$$

chromatic number: $\chi(G)$

X_i : subgraph of G induced by the first i vertices

$$Y_i = \mathbf{E}[\chi(G) \mid X_1, \ldots, X_i]$$

Doob martingale: $Y_0, Y_1, \ldots, Y_n$

$$Y_0 = \mathbf{E}[\chi(G)] \qquad\qquad Y_n = \chi(G)$$

Observation:

a vertex can always be given a new color.

$$|Y_i - Y_{i-1}| \leq 1$$

Azuma's Inequality (general version):

Let $Y_0, Y_1, \ldots$ be a martingale with respect to $X_0, X_1, \ldots$ such that, for all $k \geq 1$,

$$|Y_k - Y_{k-1}| \leq c_k,$$

Then

$$\Pr[|Y_n - Y_0| \geq t] \leq 2\exp\left(-\frac{t^2}{2\sum_{k=1}^{n} c_k^2}\right).$$

Observation:

a vertex can always be given a new color.

$$|Y_i - Y_{i-1}| \leq 1$$

$$\Pr[|\chi(G) - \mathbf{E}[\chi(G)]| \geq t\sqrt{n}]$$

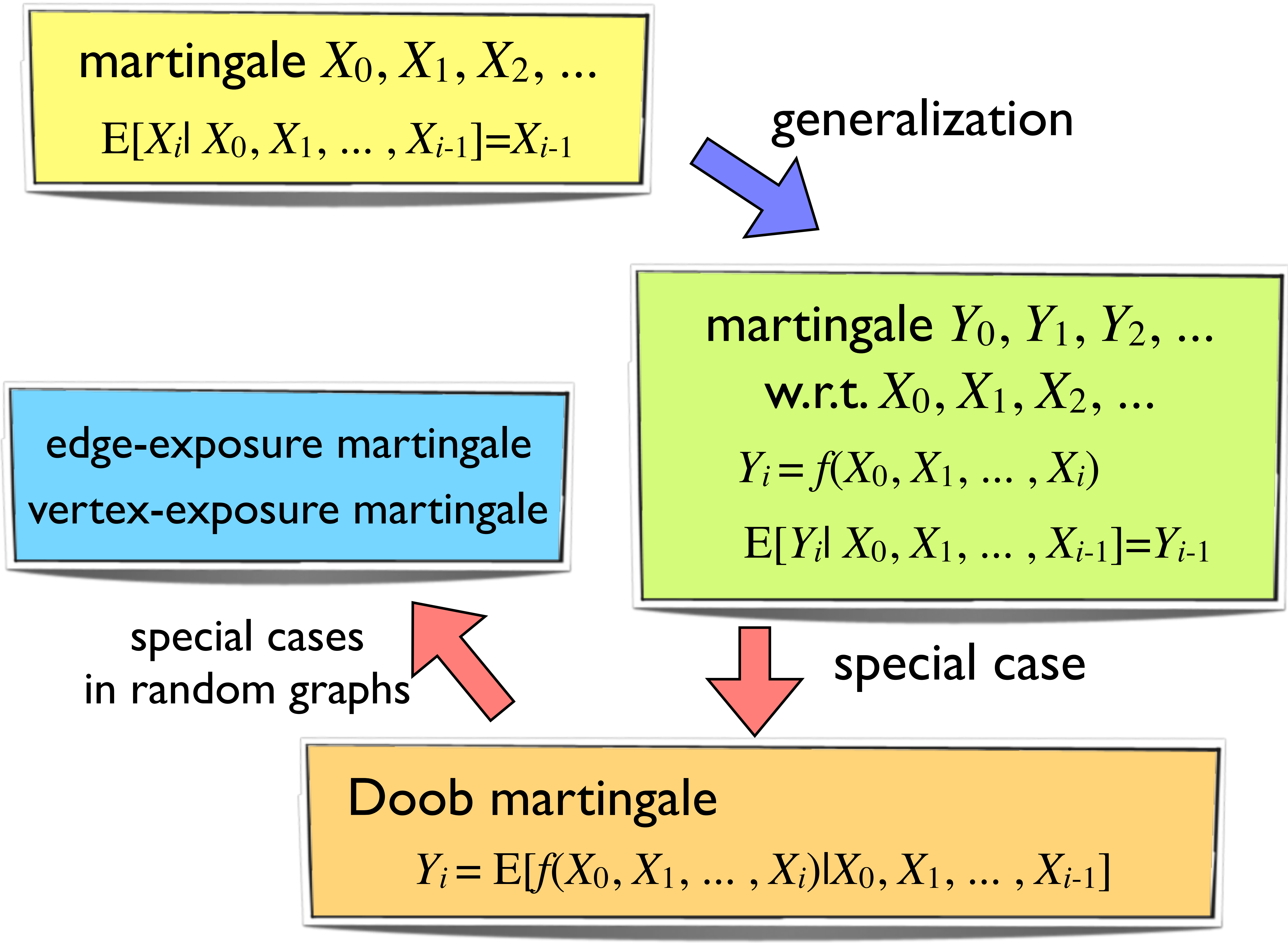
$$= \Pr[|Y_n - Y_0| \geq t\sqrt{n}] \leq 2e^{-t^2/2}$$

Tight Concentration of Chromatic Number

Theorem [Shamir & Spencer (1987)]:

Let $G \sim G(n, p)$. Then

$$\Pr\left[\left|\chi(G) - \mathbf{E}\left[\chi(G)\right]\right| \geq t\sqrt{n}\right] \leq 2e^{-t^2/2}.$$


martingale $X_0, X_1, X_2, \ldots$
$E[X_i \mid X_0, X_1, \ldots, X_{i-1}] = X_{i-1}$
generalization
martingale $Y_0, Y_1, Y_2, \ldots$
w.r.t. $X_0, X_1, X_2, \ldots$
$Y_i = f(X_0, X_1, \ldots, X_i)$
$E[Y_i \mid X_0, X_1, \ldots, X_{i-1}] = Y_{i-1}$
edge-exposure martingale
vertex-exposure martingale
special cases
in random graphs
special case
Doob martingale
$Y_i = E[f(X_0, X_1, \ldots, X_i) \mid X_0, X_1, \ldots, X_{i-1}]$

The Power of Doob + Azuma

- For a function of (dependent) random variables: $f(X_1, \ldots, X_n)$
- Doob martingale:

$$Y_i = \mathbf{E}[f(X_1, \ldots, X_n) \mid X_1, \ldots, X_i]$$

$$Y_0 = \mathbf{E}[f(X_1, \ldots, X_n)] \qquad Y_n = f(X_1, \ldots, X_n)$$

- If the differences $|Y_i - Y_{i-1}|$ are bounded,
- Azuma ⇒ $|Y_n - Y_0|$ is small whp.

$f(X_1, \ldots, X_n)$ is tightly concentrated to its mean

The method of bounded differences:

Let $\boldsymbol{X} = (X_1, \ldots, X_n)$ and let f be a function of $X_0, X_1, \ldots, X_n$ satisfying that, for all $1 \le i \le n$,

$$|\mathbf{E}[f(\boldsymbol{X}) \mid X_1, \ldots, X_i] - \mathbf{E}[f(\boldsymbol{X}) \mid X_1, \ldots, X_{i-1}]| \le c_i,$$

Then

$$\Pr\left[|f(\boldsymbol{X}) - \mathbf{E}[f(\boldsymbol{X})]| \ge t\right] \le 2\exp\left(-\frac{t^2}{2\sum_{i=1}^{n} c_i^2}\right).$$

The method of bounded differences:

Let $\boldsymbol{X} = (X_1, \ldots, X_n)$ and let f be a function of $X_0, X_1, \ldots, X_n$ satisfying that, for all $1 \le i \le n$,

$$|\underbrace{\mathbf{E}[f(\boldsymbol{X}) \mid X_1, \ldots, X_i]}_{Y_i} - \underbrace{\mathbf{E}[f(\boldsymbol{X}) \mid X_1, \ldots, X_{i-1}]}_{Y_{i-1}}| \le c_i,$$

Then

(Azuma)

$$\Pr\left[|\underbrace{f(\boldsymbol{X})}_{Y_n} - \underbrace{\mathbf{E}[f(\boldsymbol{X})]}_{Y_0}| \ge t\right] \le 2\exp\left(-\frac{t^2}{2\sum_{i=1}^n c_i^2}\right).$$

Doob martingale: $\quad Y_i = \mathbf{E}[f(\boldsymbol{X}) \mid X_1, \ldots, X_i]$

The method of bounded differences:

Let $\boldsymbol{X} = (X_1, \ldots, X_n)$ and let f be a function of $X_0, X_1, \ldots, X_n$ satisfying that, for all $1 \le i \le n$,

$$|\mathbf{E}[f(\boldsymbol{X}) \mid X_1, \ldots, X_i] - \mathbf{E}[f(\boldsymbol{X}) \mid X_1, \ldots, X_{i-1}]| \le c_i,$$

hard to check!

Then

$$\Pr\left[|f(\boldsymbol{X}) - \mathbf{E}[f(\boldsymbol{X})]| \ge t\right] \le 2\exp\left(-\frac{t^2}{2\sum_{i=1}^n c_i^2}\right).$$

$$|\mathbf{E}[f(\boldsymbol{X}) \mid X_1, \ldots, X_i] - \mathbf{E}[f(\boldsymbol{X}) \mid X_1, \ldots, X_{i-1}]| \le c_i,$$

Lipschitz Condition:

$f(x_1, \ldots, x_n)$ satisfies the **Lipschitz condition** with constants c_i, $1 \le i \le n$, if

$$\Big| f(x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n) - f(x_1, \ldots, x_{i-1}, y_i, x_{i+1}, \ldots, x_n) \Big| \le c_i.$$

Average-case:

$$|\mathbf{E}[f(\boldsymbol{X}) \mid X_1,\ldots,X_i] - \mathbf{E}[f(\boldsymbol{X}) \mid X_1,\ldots,X_{i-1}]| \le c_i,$$

Worst-case:

Lipschitz Condition:

$f(x_1,\ldots,x_n)$ satisfies the **Lipschitz condition** with constants c_i, $1 \le i \le n$, if

$$\Big| f(x_1,\ldots,x_{i-1},x_i,x_{i+1},\ldots,x_n) - f(x_1,\ldots,x_{i-1},y_i,x_{i+1},\ldots,x_n) \Big| \le c_i.$$

The method of bounded differences:

Let $\boldsymbol{X} = (X_1, \ldots, X_n)$ be n independent random variables and let f be a function satisfying the Lipschitz condition with constants c_i, $1 \leq i \leq n$. Then

$$\Pr\left[|f(\boldsymbol{X}) - \mathbf{E}[f(\boldsymbol{X})]| \geq t\right] \leq 2\exp\left(-\frac{t^2}{2\sum_{i=1}^{n} c_i^2}\right).$$

The method of bounded differences:

Let $\boldsymbol{X} = (X_1, \ldots, X_n)$ be n independent random variables and let f be a function satisfying the Lipschitz condition with constants c_i, $1 \le i \le n$. Then

$$\Pr\left[|f(\boldsymbol{X}) - \mathbf{E}[f(\boldsymbol{X})]| \ge t\right] \le 2\exp\left(-\frac{t^2}{2\sum_{i=1}^{n} c_i^2}\right).$$

Proof:

Lipschitz condition
+
independence

⇒ bounded averaged differences

Occupancy Problem

- m-balls-into-n-bins:
- number of empty bins?

$$X_i = \begin{cases} 1 & \text{bin } i \text{ is empty} \\ 0 & \text{otherwise} \end{cases}$$

\# empty bins: $X = \sum_{i=1}^{n} X_i$

$$\mathbf{E}[X] = \sum_{i=1}^{n} \mathbf{E}[X_i] = n\left(1 - \frac{1}{n}\right)^m$$

deviation: $\Pr[|X - \mathbf{E}[X]| \geq t] \leq ?$

X_i are dependent

Occupancy Problem

- m-balls-into-n-bins:
- number of empty bins?

empty bins: X

deviation:

$$\Pr[|X-\mathbf{E}[X]|\ge t]\le ?$$

Y_j : the bin of ball j (Independent!)

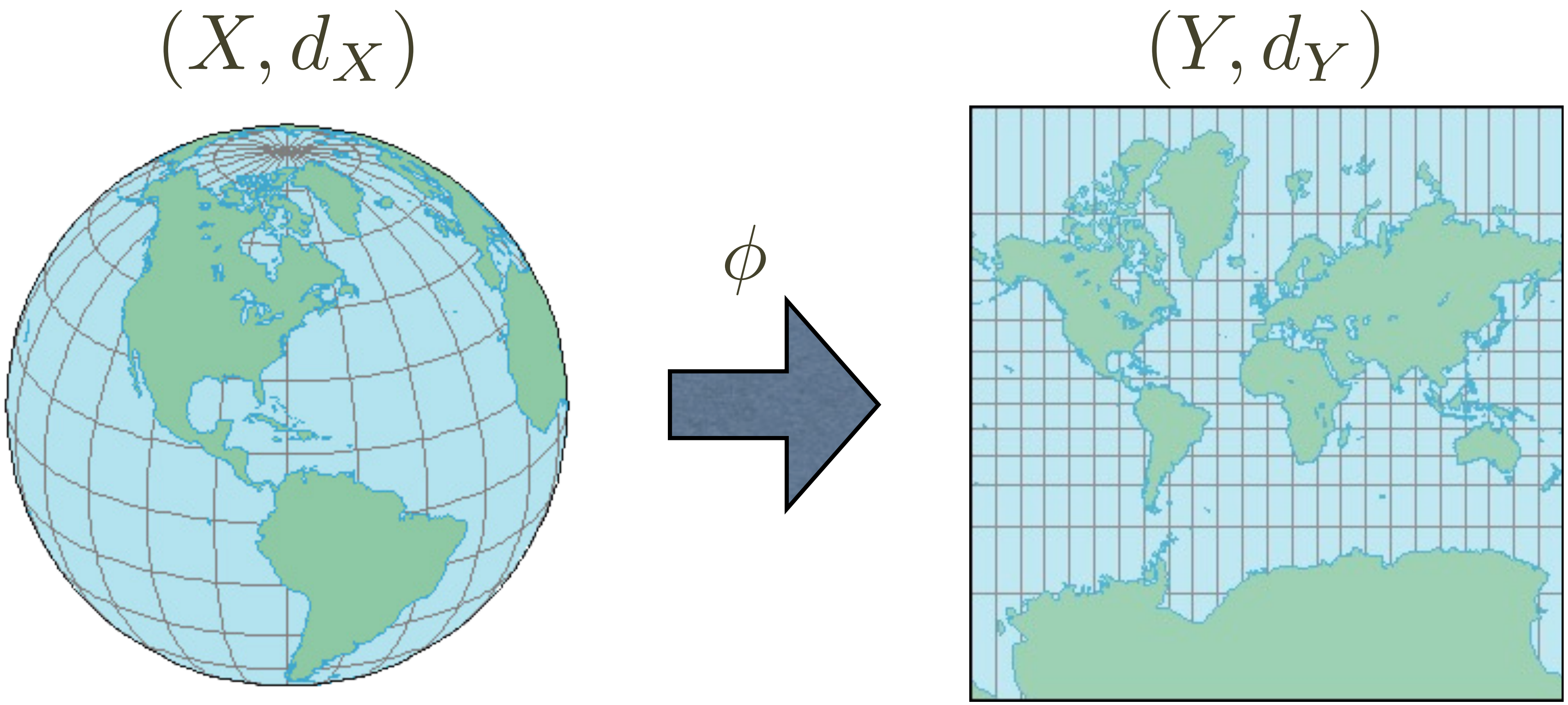
$$X=f(Y_1,\ldots,Y_m)\quad=|[n]-\{Y_1,\ldots,Y_m\}|$$

Lipschitz:

changing any Y_j can change X for at most 1

$$\Rightarrow\quad \Pr[|X-\mathbf{E}[X]|\ge t\sqrt{m}]\le 2e^{-t^2/2}$$

Metric Embedding



low-distortion: For a small $\alpha \geq 1$

$$\forall x_1, x_2 \in X, \quad \frac{1}{\alpha} d_X(x_1, x_2) \leq d_Y(\phi(x_1), \phi(x_2)) \leq \alpha d_X(x_1, x_2)$$

Dimension Reduction

In Euclidian space, it is always possible to embed a set of n points in arbitrary dimension to $O(\log n)$ dimension with constant distortion.

Johnson-Lindenstrauss Theorem:

For any $0 < \epsilon < 1$, for any set V of n points in $\mathbf{R}^d$, there is a map $\phi : \mathbf{R}^d \to \mathbf{R}^k$ with $k = O(\ln n)$, such that $\forall u, v \in V$,

$$(1-\epsilon)\|u-v\|^2 \leq \|\phi(u)-\phi(v)\|^2 \leq (1+\epsilon)\|u-v\|^2$$

Johnson-Lindenstrauss Theorem

Johnson-Lindenstrauss Theorem:

For any $0 < \epsilon < 1$, for any set V of n points in $\mathbf{R}^d$, there is a map $\phi : \mathbf{R}^d \to \mathbf{R}^k$ with $k = O(\ln n)$, such that $\forall u, v \in V$,

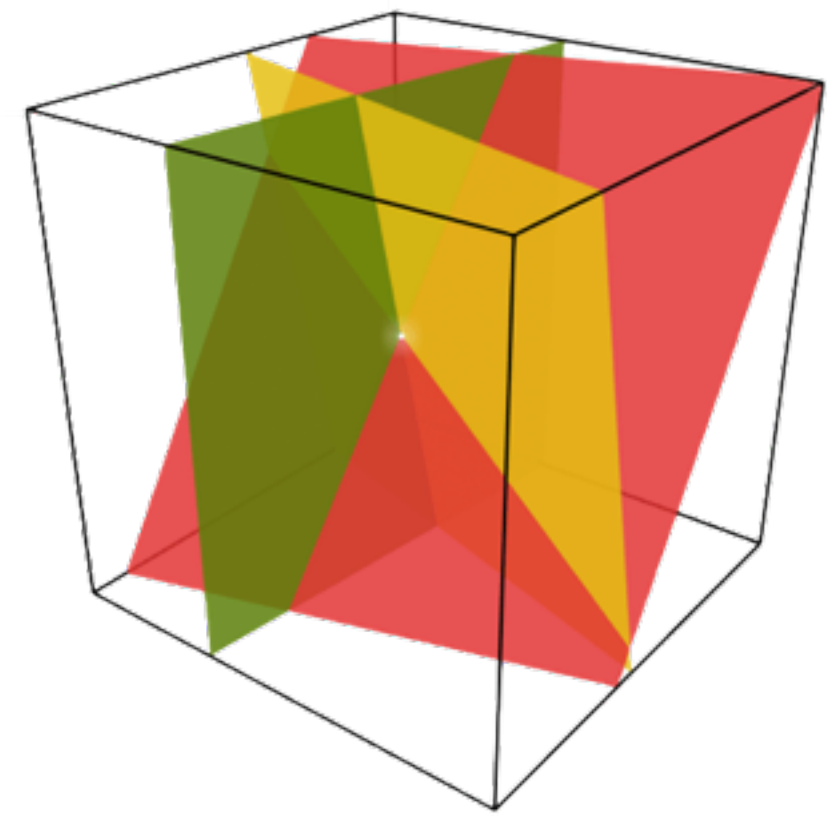
$$(1-\epsilon)\|u-v\|^2 \leq \|\phi(u)-\phi(v)\|^2 \leq (1+\epsilon)\|u-v\|^2$$

- $\phi(v) = Av$.
- A is a random projection matrix.

Random Projection

Random $k \times d$ matrix A:

- Projection onto a uniform random subspace. (Johnson-Lindenstrauss) (Dasgupta-Gupta)
- i.i.d. Gaussian entries. (Indyk-Motiwani)
- i.i.d. $-1/+1$ entries. (Achlioptas)



rows: $A_{1\cdot}, A_{2\cdot}, \ldots, A_{k\cdot}$

random orthogonal unit vectors $\in \mathbb{R}^d$

Johnson-Lindenstrauss Theorem

- Let V be a set of n points in $\mathbf{R}^d$.
- For some $k = O(\ln n)$.
- Let A be a random $k \times d$ matrix that projects onto a uniform random k-dimensional subspace.

W.h.p., $\forall u, v \in V$, (for the case ε=1/2)

$$\frac{\|u-v\|^2}{2} \le \left\| \sqrt{\frac{d}{k}} Au - \sqrt{\frac{d}{k}} Av \right\|^2 \le \frac{3\|u-v\|^2}{2}$$

the projection

A: projection onto a uniform random k-subspace

W.h.p., $\forall u, v \in V$,

$$\left\| \sqrt{\frac{d}{k}} Au - \sqrt{\frac{d}{k}} Av \right\|^2 \leq \frac{3\|u - v\|^2}{2} \qquad \left\| \sqrt{\frac{d}{k}} Au - \sqrt{\frac{d}{k}} Av \right\|^2 \geq \frac{\|u - v\|^2}{2}$$

Step I: Reduce to unit vectors

A: projection onto a uniform random k-subspace

$O(n^2)$ pairs

W.h.p., $\forall u, v \in V$,

$$\left\|\sqrt{\frac{d}{k}}Au - \sqrt{\frac{d}{k}}Av\right\|^2 \leq \frac{3\|u-v\|^2}{2} \qquad \left\|\sqrt{\frac{d}{k}}Au - \sqrt{\frac{d}{k}}Av\right\|^2 \geq \frac{\|u-v\|^2}{2}$$

$$\left\|A\frac{(u-v)}{\|u-v\|}\right\|^2 \leq \frac{3k}{2d} \qquad \left\|A\frac{(u-v)}{\|u-v\|}\right\|^2 \geq \frac{k}{2d}$$

treat $(u-v)$ as a vector, $\frac{u-v}{\|u-v\|}$ is a unit vector

New goal:

$\forall$ unit vector u, with probability $o(\frac{1}{n^2})$

$$\|Au\|^2 > \frac{3k}{2d} \quad \text{or} \quad \|Au\|^2 < \frac{k}{2d}$$

A: projection onto a uniform random k-subspace

$\forall$ unit vector u, with probability $o(\frac{1}{n^2})$

$$\|Au\|^2 > \frac{3k}{2d} \quad \text{or} \quad \|Au\|^2 < \frac{k}{2d}$$

Step II:

Random projection of fixed unit vector

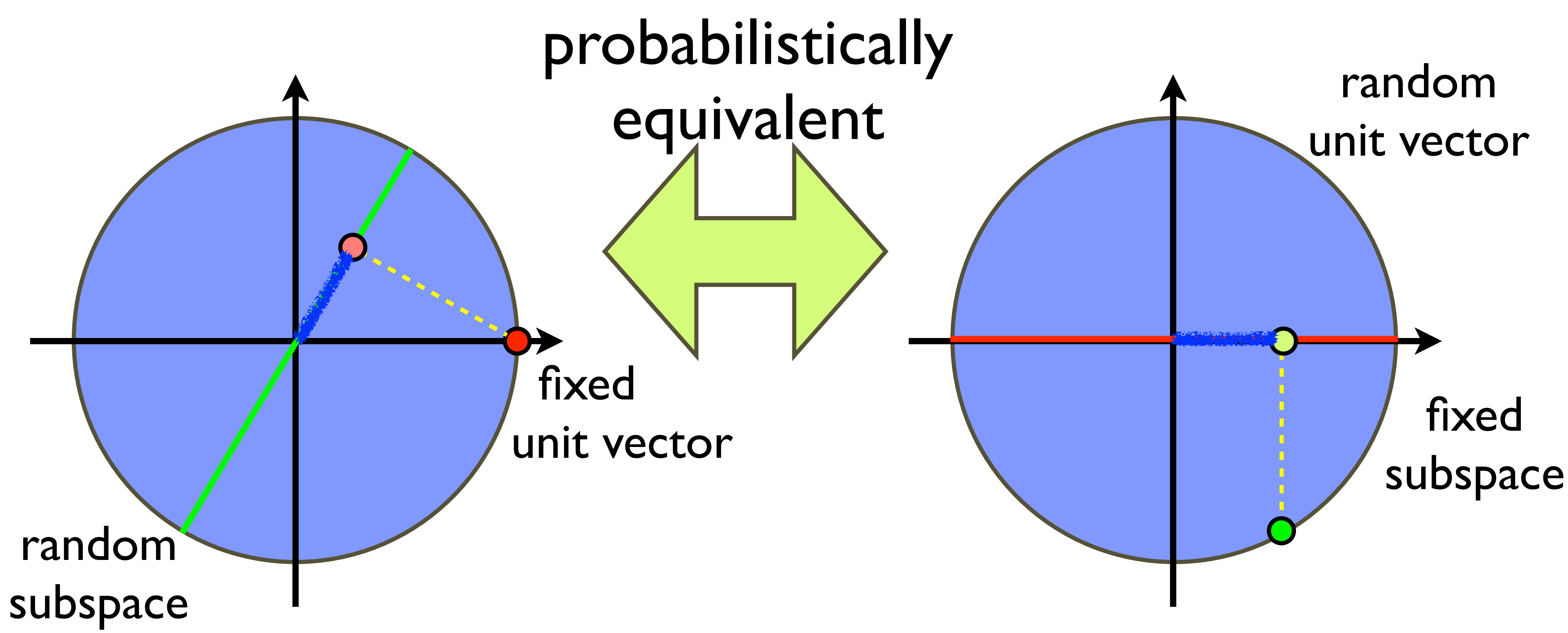
$\Updownarrow$

Fixed projection of random unit vector

A: projection onto a uniform random k-subspace

$\forall$ unit vector u, with probability $o(\frac{1}{n^2})$

$$\|Au\|^2 > \frac{3k}{2d} \quad \text{or} \quad \|Au\|^2 < \frac{k}{2d}$$



"inner-products are invariant under rotations"

A: projection onto a uniform random k-subspace

$\forall$ unit vector u, with probability $o(\frac{1}{n^2})$

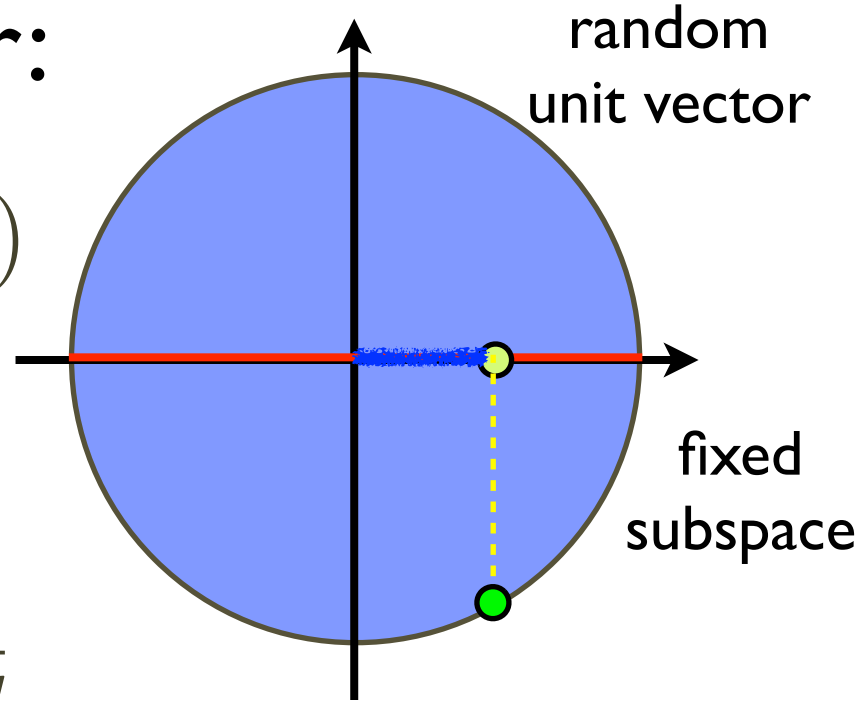
$$\|Au\|^2 > \frac{3k}{2d} \quad \text{or} \quad \|Au\|^2 < \frac{k}{2d}$$

uniform random unit vector:

$$Y = (Y_1, \ldots, Y_k, Y_{k+1}, \ldots, Y_d)$$

$$Z = (Y_1, \ldots, Y_k)$$

$$\|Z\|^2 > \frac{3k}{2d} \quad \text{or} \quad \|Z\|^2 < \frac{k}{2d}$$



uniform random unit vector:

$$Y = (Y_1, \ldots, Y_k, Y_{k+1}, \ldots, Y_d)$$

Let $Z = (Y_1, \ldots, Y_k)$ with probability $o(\frac{1}{n^2})$

$$\|Z\|^2 > \frac{3k}{2d} \quad \text{or} \quad \|Z\|^2 < \frac{k}{2d}$$

Looks clean, however . . .

- $\|Z\|^2 = Y_1^2 + Y_2^2 + \cdots + Y_k^2$
- Y_i's are dependent for uniform unit vector Y.

uniform random unit vector:

$$Y = (Y_1, \ldots, Y_k, Y_{k+1}, \ldots, Y_d)$$

Let $Z = (Y_1, \ldots, Y_k)$ with probability $o(\frac{1}{n^2})$

$$\|Z\|^2 > \frac{3k}{2d} \quad \text{or} \quad \|Z\|^2 < \frac{k}{2d}$$

Step III:

Bound $\|Z\|^2$

uniform random unit vector:

$$Y = (Y_1, \ldots, Y_k, Y_{k+1}, \ldots, Y_d)$$

Let $Z = (Y_1, \ldots, Y_k)$

Generating uniform unit vector:

$X_1, \ldots, X_d$ are i.i.d. normal distributions $N(0,1)$.

$$X = (X_1, \ldots, X_d), \qquad Y = \frac{1}{\|X\|} X$$

Y is a uniform random unit vector.

The density:

$$\Pr[(x_1, \ldots, x_d)] = \prod_{i=1}^{d} \frac{1}{\sqrt{2\pi}} e^{-x_i^2/2} = (2\pi)^{-d/2} e^{-\|x\|^2/2}$$

Spherically symmetric!

$X_1, \ldots, X_d$ are i.i.d. normal distributions $N(0,1)$.

$$X = (X_1, \ldots, X_d), \qquad Z = \frac{1}{\|X\|}(X_1, \ldots, X_k)$$

$$\|Z\|^2 = \frac{X_1^2 + \cdots + X_k^2}{X_1^2 + \cdots + X_d^2}$$

$$\|Z\|^2 < \frac{k}{2d} \iff (k - 2d)\sum_{i=1}^{k} X_i^2 + k \sum_{i=k+1}^{d} X_i^2 > 0$$

$$\|Z\|^2 > \frac{3k}{2d} \iff (3k - 2d)\sum_{i=1}^{k} X_i^2 + 3k \sum_{i=k+1}^{d} X_i^2 < 0$$

Sum of independent random variables! Chernoff?

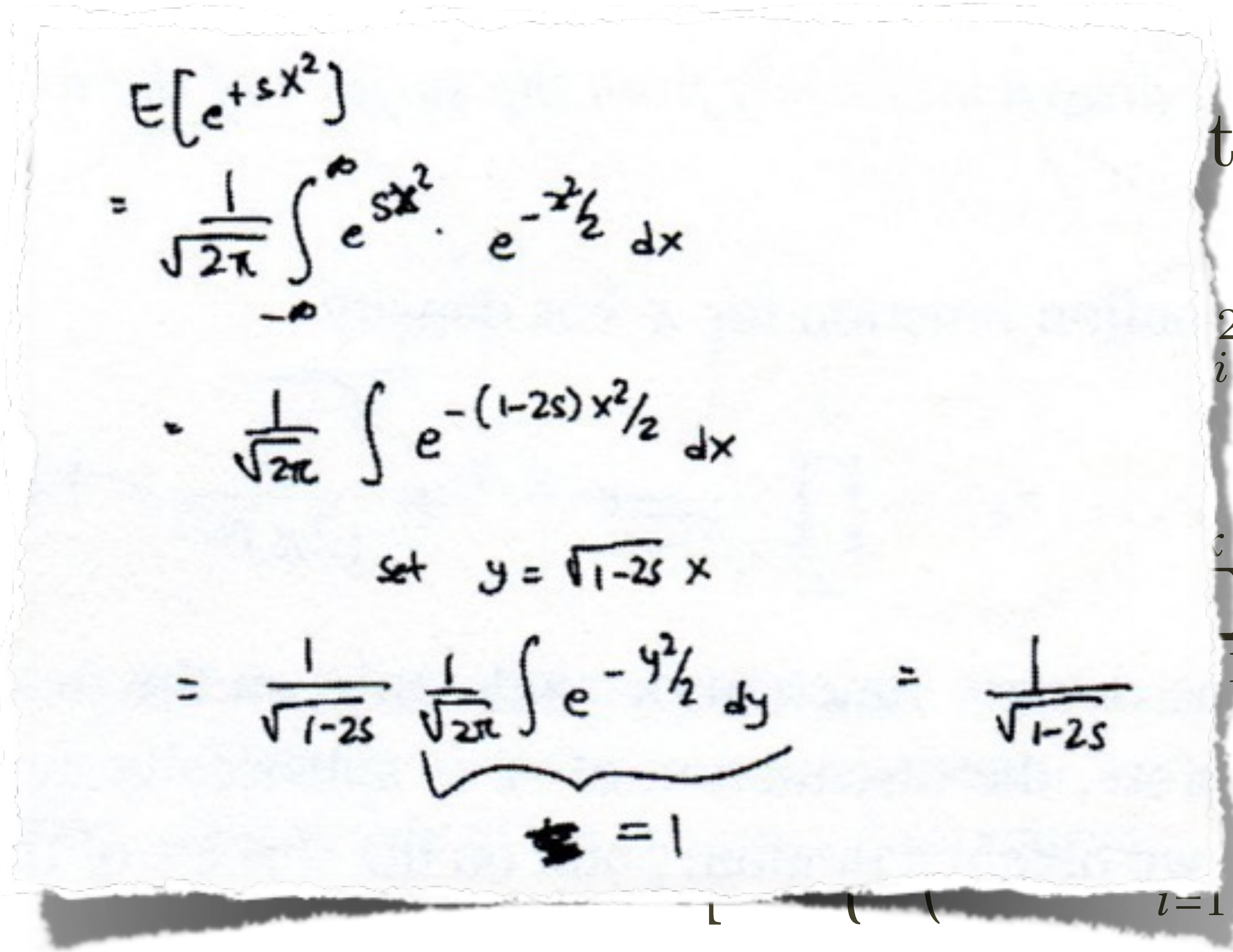
$X_1, \ldots, X_d$ are i.i.d. normal distributions $N(0,1)$.

Upper bound: $\Pr\left[(k-2d)\sum_{i=1}^{k} X_i^2 + k \sum_{i=k+1}^{d} X_i^2 > 0 \right]$

(for $\lambda > 0$) $= \Pr\left[\exp\left\{\lambda\left((k-2d)\sum_{i=1}^{k} X_i^2 + k\sum_{i=k+1}^{d} X_i^2\right)\right\} > 1\right]$

(Markov) $\leq \mathbf{E}\left[\exp\left\{\lambda\left((k-2d)\sum_{i=1}^{k} X_i^2 + k\sum_{i=k+1}^{d} X_i^2\right)\right\}\right]$

(independence) $= \prod_{i=1}^{k} \mathbf{E}\left[e^{\lambda(k-2d)X_i^2}\right] \cdot \prod_{i=k+1}^{d} \mathbf{E}\left[e^{\lambda k X_i^2}\right]$



tributions $N(0,1)$.

$$\ldots {}_i^2 + k \sum_{i=k+1}^{d} X_i^2 > 0 \Big]$$

$$\ldots X_i^2 + k \sum_{i=k+1}^{d} X_i^2 \Big)\Big\} > 1 \Big]$$

$$\ldots X_i^2 + k \sum_{i=k+1}^{d} X_i^2 \Big)\Big\} \Big]$$

(independence) $$= \prod_{i=1}^{k} \mathbf{E}\left[e^{\lambda(k-2d)X_i^2}\right] \cdot \prod_{i=k+1}^{d} \mathbf{E}\left[e^{\lambda k X_i^2}\right]$$

$$\mathbf{E}\left[e^{sX_i^2}\right] = \frac{1}{\sqrt{1-2s}}.$$

$$= (1-2\lambda(k-2d))^{-\frac{k}{2}}(1-2\lambda k)^{-\frac{d-k}{2}}$$

$X_1, \ldots, X_d$ are i.i.d. normal distributions $N(0,1)$.

$$\Pr\left[(k-2d)\sum_{i=1}^{k} X_i^2 + k \sum_{i=k+1}^{d} X_i^2 > 0 \right]$$

$$\leq \; (1-2\lambda(k-2d))^{-\frac{k}{2}}(1-2\lambda k)^{-\frac{d-k}{2}} \quad \leq e^{-k/16}$$

minimized when $\lambda = \frac{1}{2d-k}$

$$\Pr\left[(3k-2d)\sum_{i=1}^{k} X_i^2 + 3k \sum_{i=k+1}^{d} X_i^2 < 0 \right] \quad \leq e^{-k/24}$$

$Z = \frac{1}{\|X\|}(X_1, \ldots, X_k)$ for some $k = O(\ln n)$

$$\Pr\left[\|Z\|^2 > \frac{3k}{2d} \vee \|Z\|^2 < \frac{k}{2d} \right] = o(\frac{1}{n^3})$$

for some $k = O(\ln n)$

Z: fixed k-subspace of random unit vector.

$$\Pr\left[\|Z\|^2 \text{ distorted from } k/d\right] = o(\frac{1}{n^3})$$

Au: random k-subspace of fixed unit vector.

$$\Pr\left[\|Au\|^2 \text{ distorted from } k/d\right] = o(\frac{1}{n^3})$$

$\forall u, v$

$$\Pr\left[\left\|\sqrt{d/k}A(u-v)\right\|^2 \text{ distorted from } \|u-v\|^2\right] = o(\frac{1}{n^3})$$

$O(n^2)$ pairs of (u, v). Union bound ⇒ Johnson-Lindenstrauss

Johnson-Lindenstrauss Theorem

Johnson-Lindenstrauss Theorem:

For any $0 < \epsilon < 1$, for any set V of n points in $\mathbf{R}^d$, there is a map $\phi : \mathbf{R}^d \to \mathbf{R}^k$ with $k = O(\ln n)$, such that $\forall u, v \in V$,

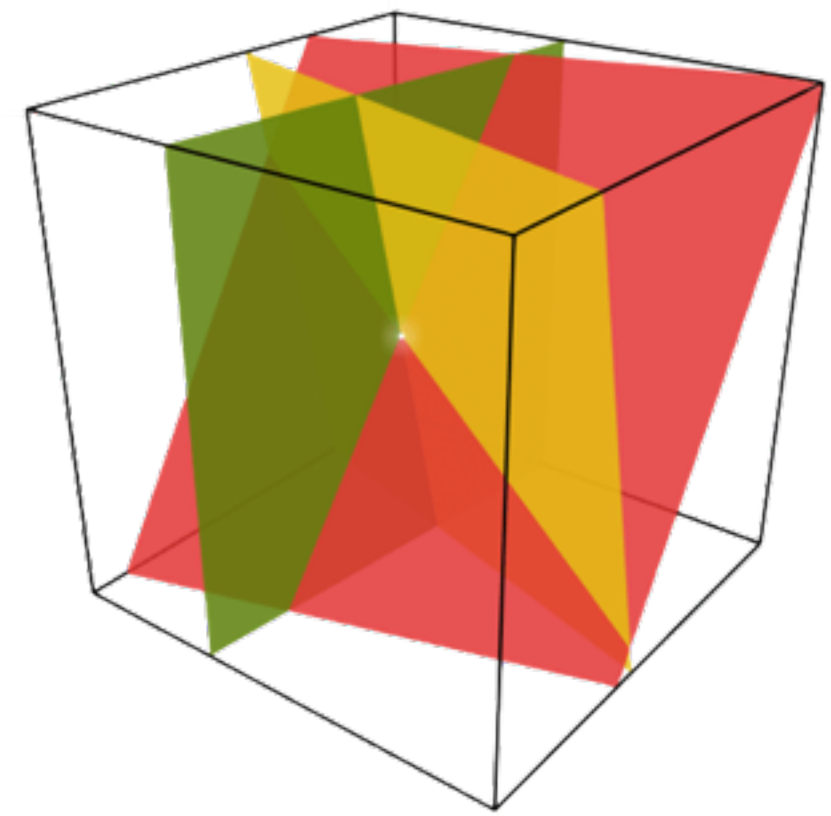
$$(1-\epsilon)\|u-v\|^2 \leq \|\phi(u)-\phi(v)\|^2 \leq (1+\epsilon)\|u-v\|^2$$

- $\phi(v) = Av$.
- A is a random projection matrix.

Random Projection

Random $k{\times}d$ matrix A:

- Projection onto a uniform random subspace. (Johnson-Lindenstrauss) (Dasgupta-Gupta)
- i.i.d. Gaussian entries. (Indyk-Motiwani)
- i.i.d. $-1/+1$ entries. (Achlioptas)



rows: $A_{1\cdot}, A_{2\cdot}, \ldots, A_{k\cdot}$

random orthogonal unit vectors $\in \mathbb{R}^d$