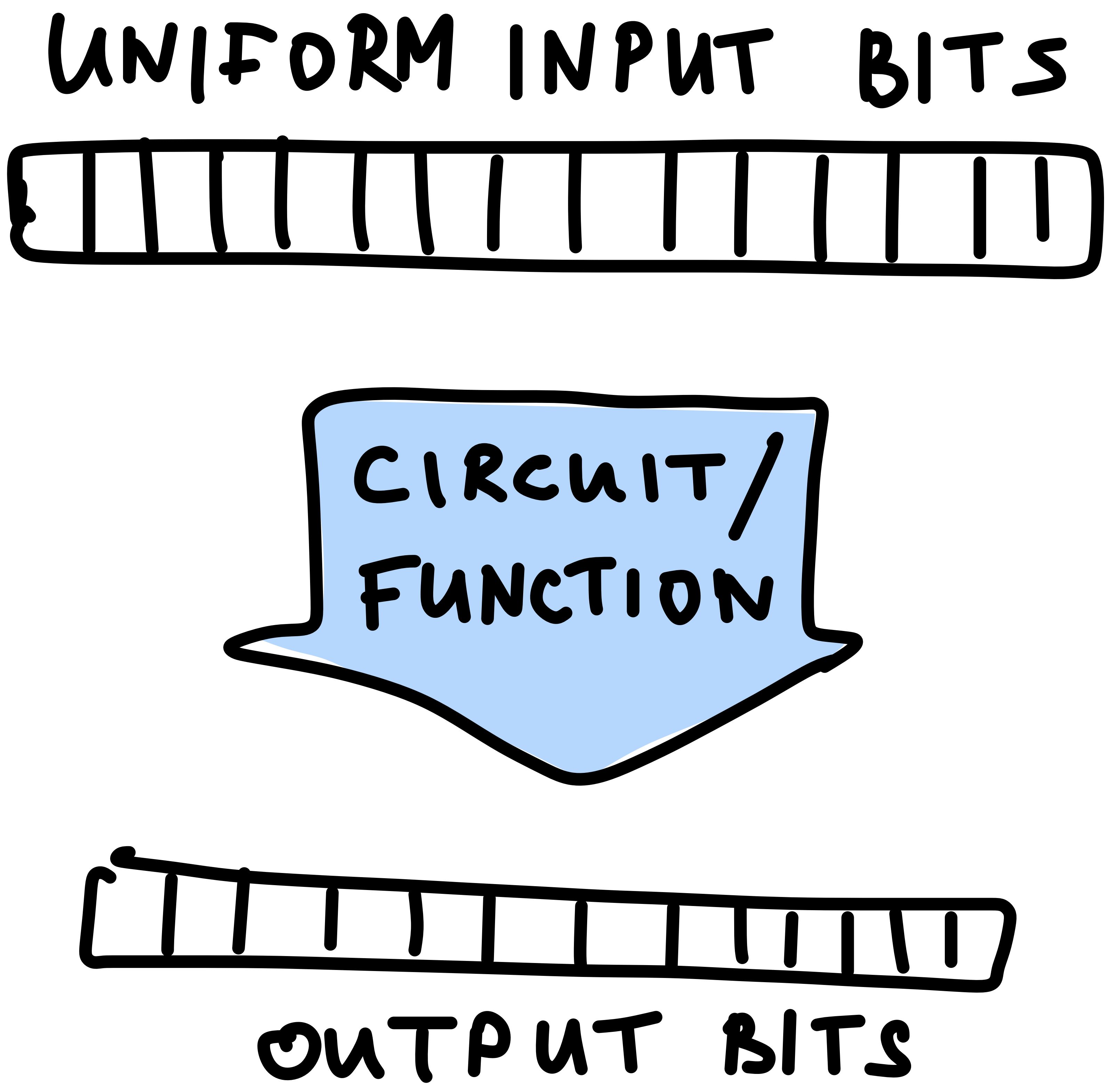
& Certifying Sampling Symmetric Functions

Yuval Filmus, Itai Leigh, Artur Riazanov, Dmitry Sokolov

Technion   Tel Aviv University   EPFL   EPFL

RANDOM 2023

Setting



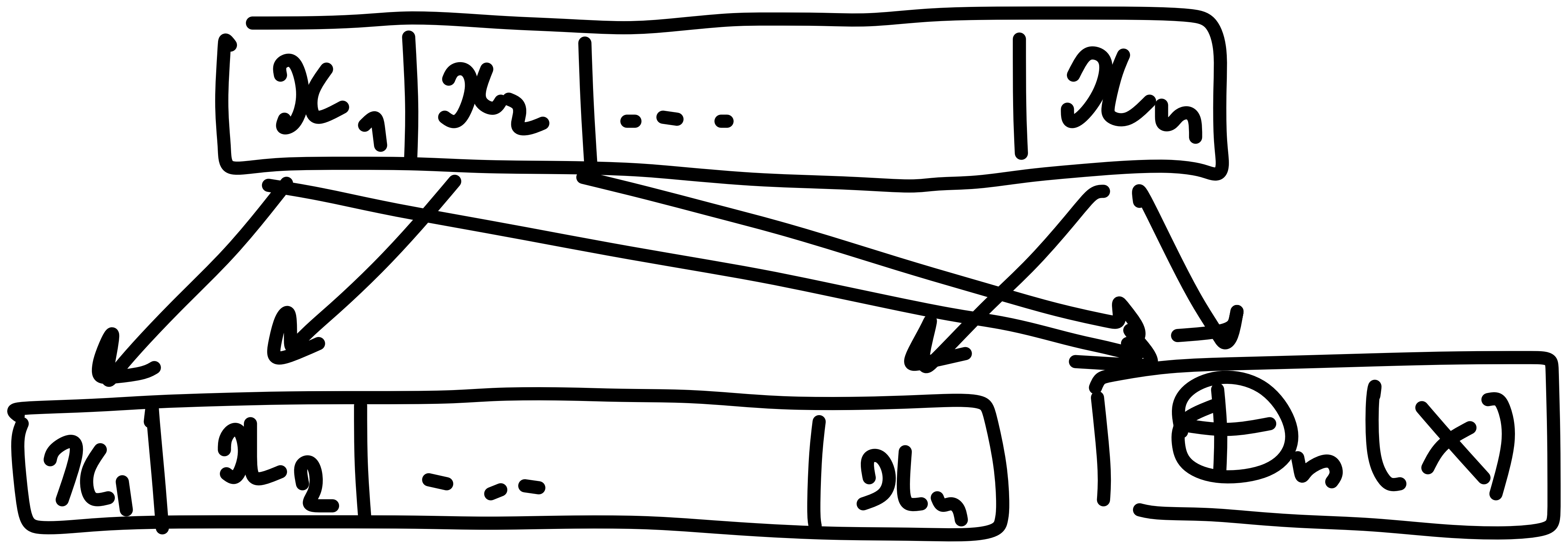
A ckt C SAMPLES A DISTRIBUTION T WITH ERROR ε

IF $\Delta(C(U_n), T) \leq \varepsilon$

WHERE

$$\Delta(P, Q) = \max_{E} \left| \Pr[P \in E] - \Pr[Q \in E] \right|$$

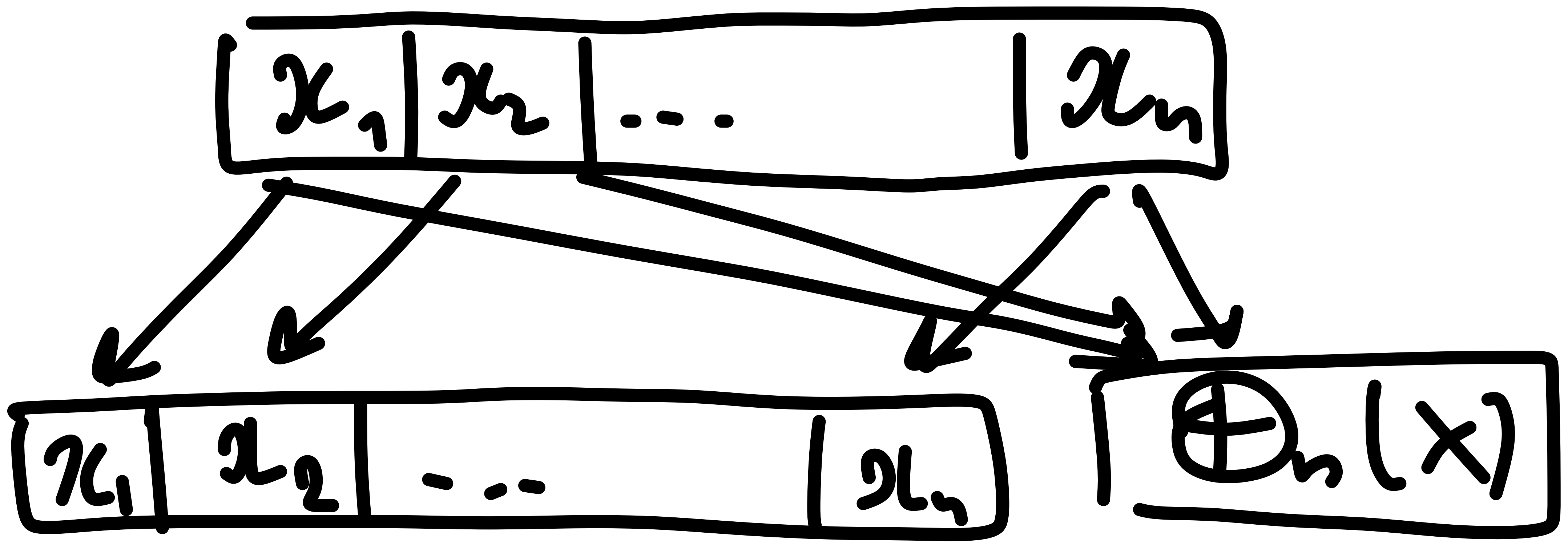
Example



$= \sum_{i \in [n]} x_i \mod 2$

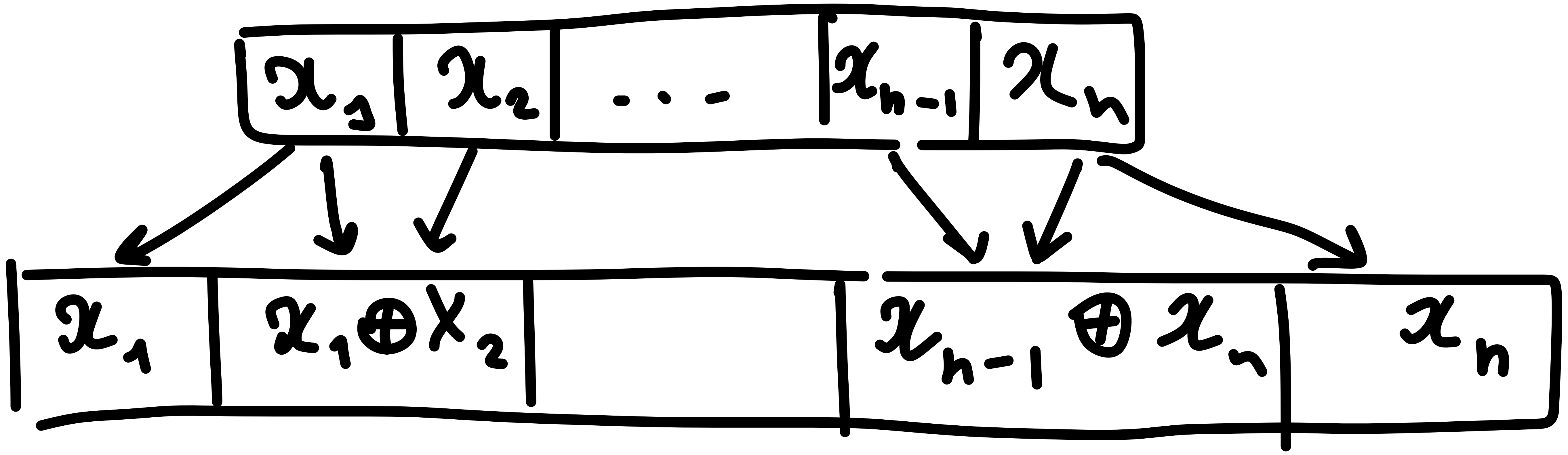
- $(U_n, \oplus_n(U_n)) =: T$
- $\oplus_n$ IS HARD FOR AC^0 CKTS. [Håstad'86]

Example



$= \sum_{i \in [n]} x_i \mod 2$

- $(U_n, \oplus_n(U_n)) =: T$
- $\oplus_n$ IS HARD FOR AC^0 CKTS. [Håstad'86]
- T IS SAMPLABLE IN NC^0.



State of the Art

[LV'11] AC^0 CAN NOT SAMPLE GOOD CODES.

[Viola'12] $\exists f : \{0,1\}^n \longrightarrow \{0,1\}$ s.t. AC^0 SAMPLES $(U_n, f(U_n))$ WITH ERROR $\geq 1/2 - o(1)$

State of the Art

[LV'11] AC^0 CAN NOT SAMPLE GOOD CODES.

[Viola'12] $\exists f : \{0,1\}^n \to \{0,1\}$ s.t. AC^0 SAMPLES $(U_n, f(U_n))$ WITH ERROR $\geq 1/2 - o(1)$

[folklore] NC^0 CAN SAMPLE $(U_n, \oplus_n(U_n))$

[IN'96] AC^0 CAN SAMPLE $(U_n, IP_{n/2}(U_n))$

[Viola'11] AC^0 CAN SAMPLE $(U_n, f(U_n))$ FOR A SYMMETRIC f.

Symmetric ~~Functions~~ Distributions

$\mathcal{U}_S$ with $S \subseteq \{0,1\}^n$ AND $\left.\begin{array}{l} x \in S \\ |x| = |y| \end{array}\right\} \Rightarrow y \in S.$

QUESTION: WHAT SYMMETRIC DISTRIBUTIONS CAN BE SAMPLED IN NC^0 ?

Symmetric ~~Functions~~ Distributions

$\mathcal{U}_S$ with $S \subseteq \{0,1\}^n$ AND $\left.\begin{array}{l} x \in S \\ |x| = |y| \end{array}\right\} \Rightarrow y \in S.$

QUESTION: WHAT SYMMETRIC DISTRIBUTIONS CAN BE SAMPLED IN NC^0 ?

Thm [Viola '12] WITH $n + n^{\varepsilon}$ INPUT BITS

slice

$$\mathcal{U}_n^{n/2} = \mathcal{U}_{\{x \in \{0,1\}^n \,:\, |x| = n/2\}}$$

REQUIRES LOCALITY $\Omega(\log n)$ TO SAMPLE.

NC^0 = LOCALITY $O(1)$.

Our result

Conj $NC^0 \cap \mathrm{SYM} = \{U_{\oplus=0}, U_{\oplus=1}, U_n, U_{\{0^n\}}, U_{\{1^n\}}\}$

Thm [BP'23] QNC^0 CAN SAMPLE $(U_n, f(U_n))$

WHERE $f \in \mathrm{SYM} \setminus \{\oplus\}$.

Our result

Conj $NC^0 \cap \mathrm{SYM} = \{ U_{\oplus=0}, U_{\oplus=1}, U_n, U_{\{0^n\}}, U_{\{1^n\}} \}$

Thm [BP'23] QNC^0 CAN SAMPLE $(U_n, f(U_n))$
WHERE $f \in \mathrm{SYM} \setminus \{\oplus\}$.

Thm ANY SYMMETRIC DISTRIBUTION $\mathcal{D}$
SUPPORTED ON $\{x \in \{0,1\}^n \mid |x| \le k\}$ REQUIRES
$\tilde{\Omega}(\log n/k)$ LOCALITY TO SAMPLE.

IN PARTICULAR, $U_n^{o(n)} \notin NC^0$. DECISION DEPTH

Proof: reduction to U_n^k

PLAN: $D \longrightarrow U_n^k \longrightarrow U_n^1$

Thm EVERY DeSym supported on $\{x \in \{0,1\}^n \mid |x| \leq k\}$ REQUIRES $\tilde{\Omega}(\log \frac{n}{k})$ decision DEPTH TO BE SAMPLED.

RECALL: $U_n^k = U_{\{x \in \{0,1\}^n : |x| = k\}}$

Fact: D FROM THE THM $\Longrightarrow \Delta(D, U_n^k) = o(1)$

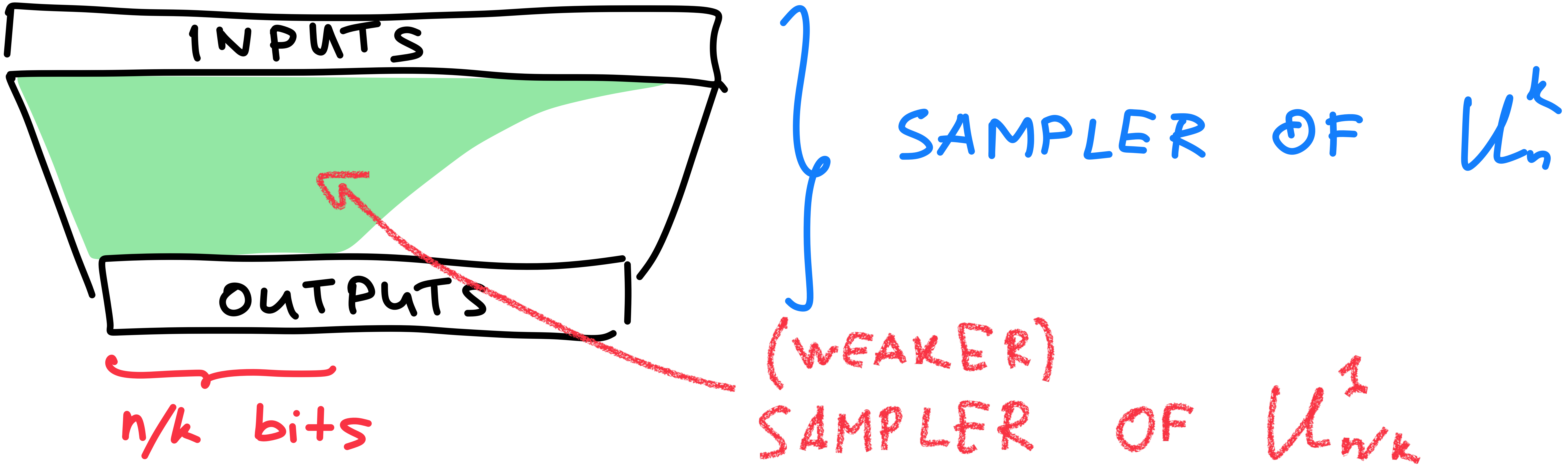
SUFFICES TO PROVE THM FOR $D = U_n^k$.

Proof: reduction to U_n^1

PLAN: $D \longrightarrow U_n^k \longrightarrow U_n^1$

Thm U_n^k REQUIRES $\tilde{\Omega}(\log \frac{n}{k})$ decision DEPTH TO BE SAMPLED.

FACT $\Delta(\text{first } \frac{n}{k} \text{ bits of } U_n^k,\ U_{n/k}^1) \leq 1 - \frac{1}{e}$



PLAN: $\mathcal{D} \longrightarrow \mathcal{U}_n^k \longrightarrow \mathcal{U}_n^1$

Thm X SAMPLABLE WITH $\tilde{O}(\log n)$ DECISION DEPTH

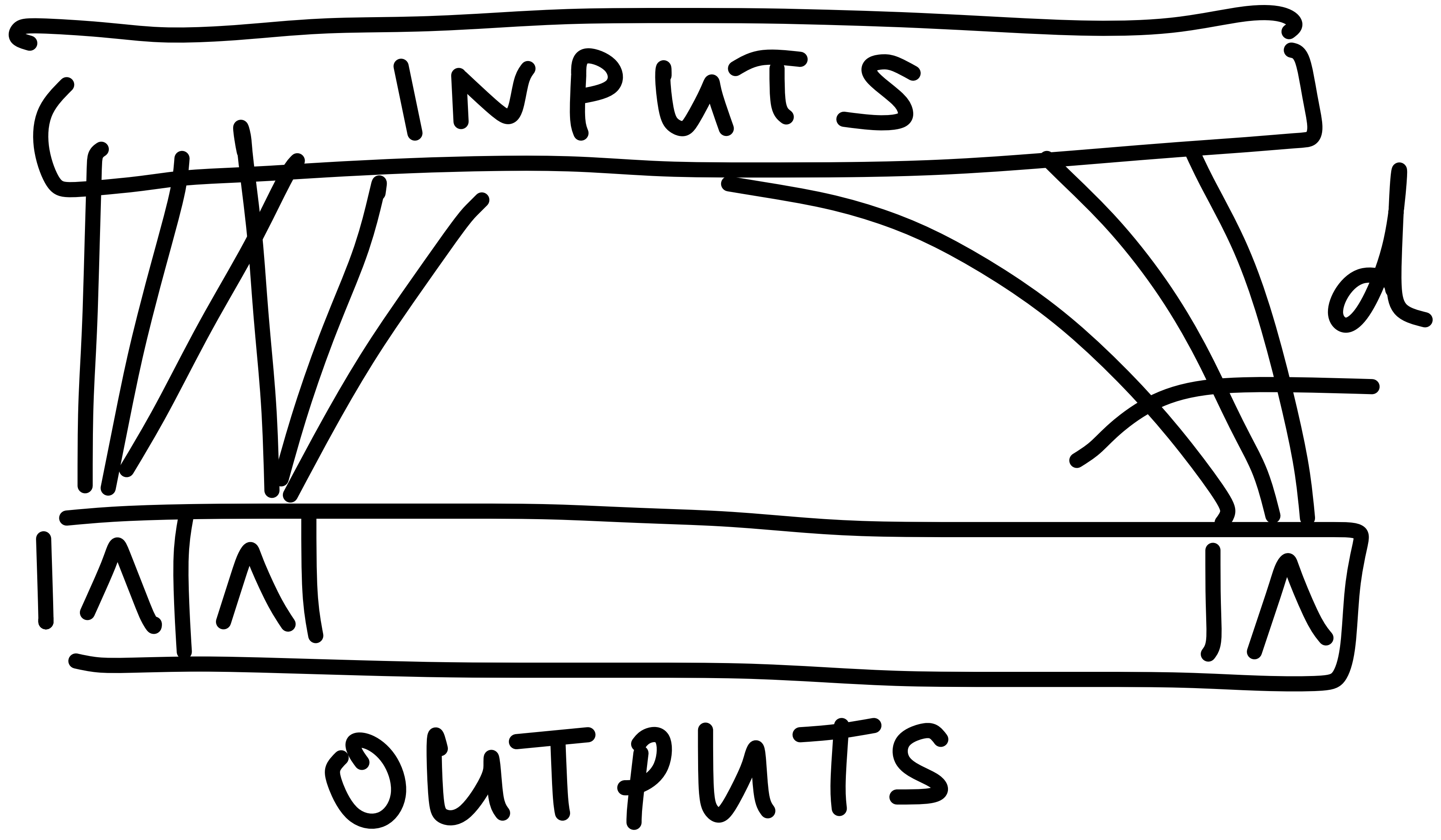
$$\Longrightarrow \Delta(X, \mathcal{U}_n^1) = 1 - o(1).$$

PLAN: $\mathcal{D} \longrightarrow U_n^k \longrightarrow U_n^1$

Thm X SAMPLABLE WITH $\tilde{O}(\log n)$ DECISION DEPTH

$$\Longrightarrow \Delta(X, U_n^1) = 1 - o(1).$$

SIMPLIFICATION: EVERY OUTPUT OF X IS MONOTONE TERM OF INPUT BITS.



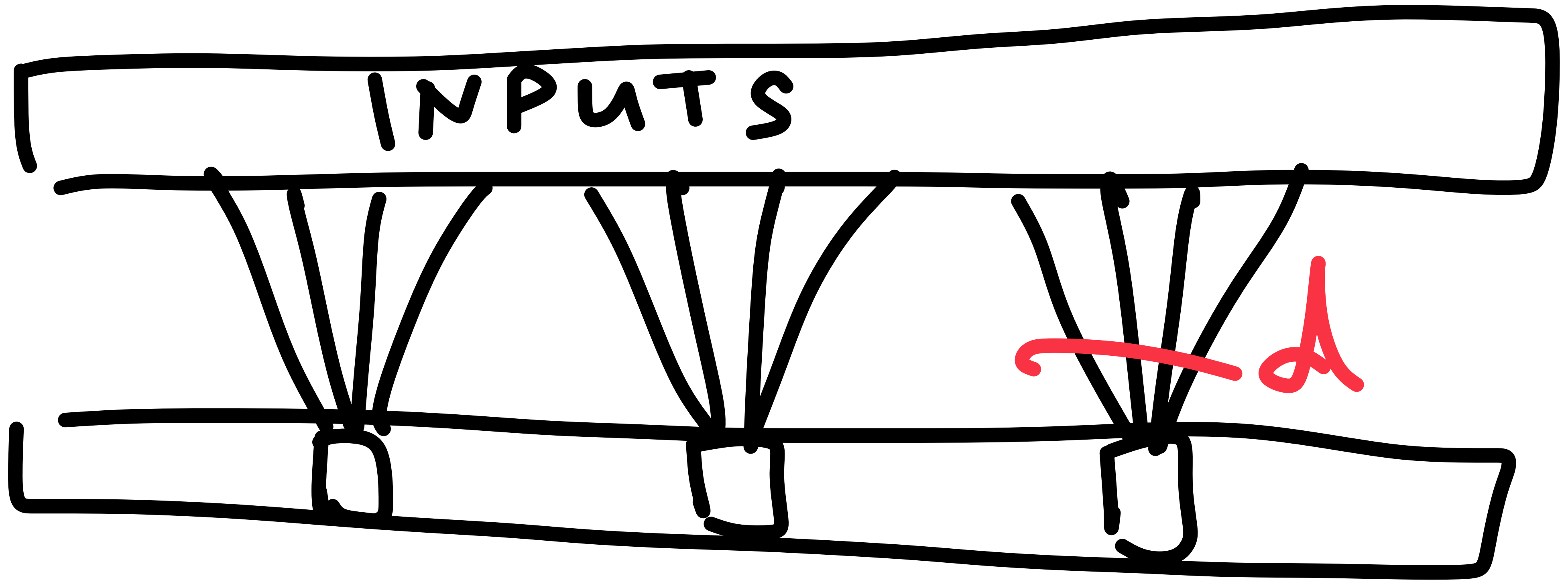
OBSERVATION

$$\mathbb{E}\Big[\sum_{i\in[n]} X_i\Big] \geq 2^{-d} n \gg 1$$

Observation:

$$\mathbb{E}\left[\sum_{i\in[n]} X_i\right] \geq 2^{-d} n \gg 1$$

Yet: $$\mathbb{E}\left[\sum_{i\in[n]} (U_n^1)_i\right] = 1$$



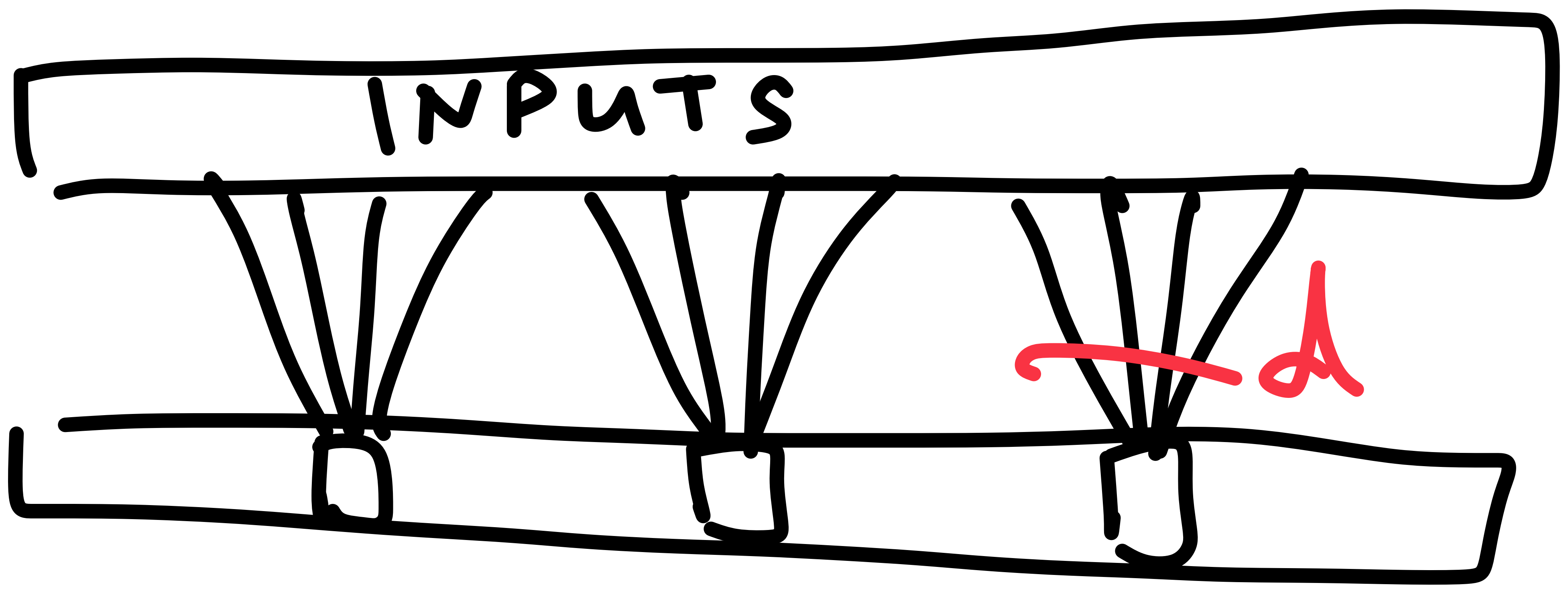
$\gg 2^d$ INDEPENDENT BITS + CONCENTRATION

$\Rightarrow$ CONTRADICTION

Observation:

$$\mathbb{E}\Big[\sum_{i\in[n]} X_i\Big] \geq 2^{-d} n \gg 1$$

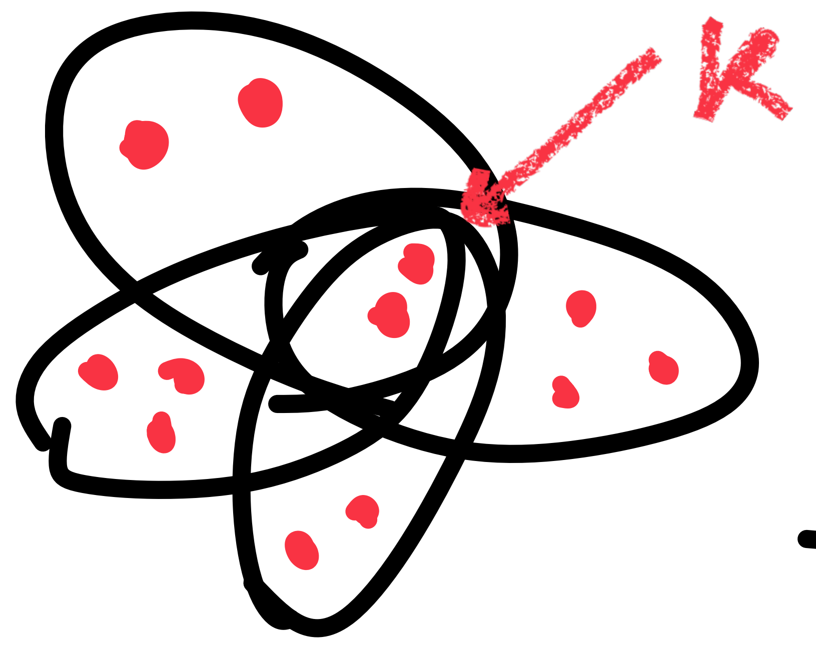
Yet: $$\mathbb{E}\Big[\sum_{i\in[n]} (U_n^1)_i\Big] = 1$$



$\gg 2^d$ INDEPENDENT BITS + CONCENTRATION

$\Rightarrow$ CONTRADICTION

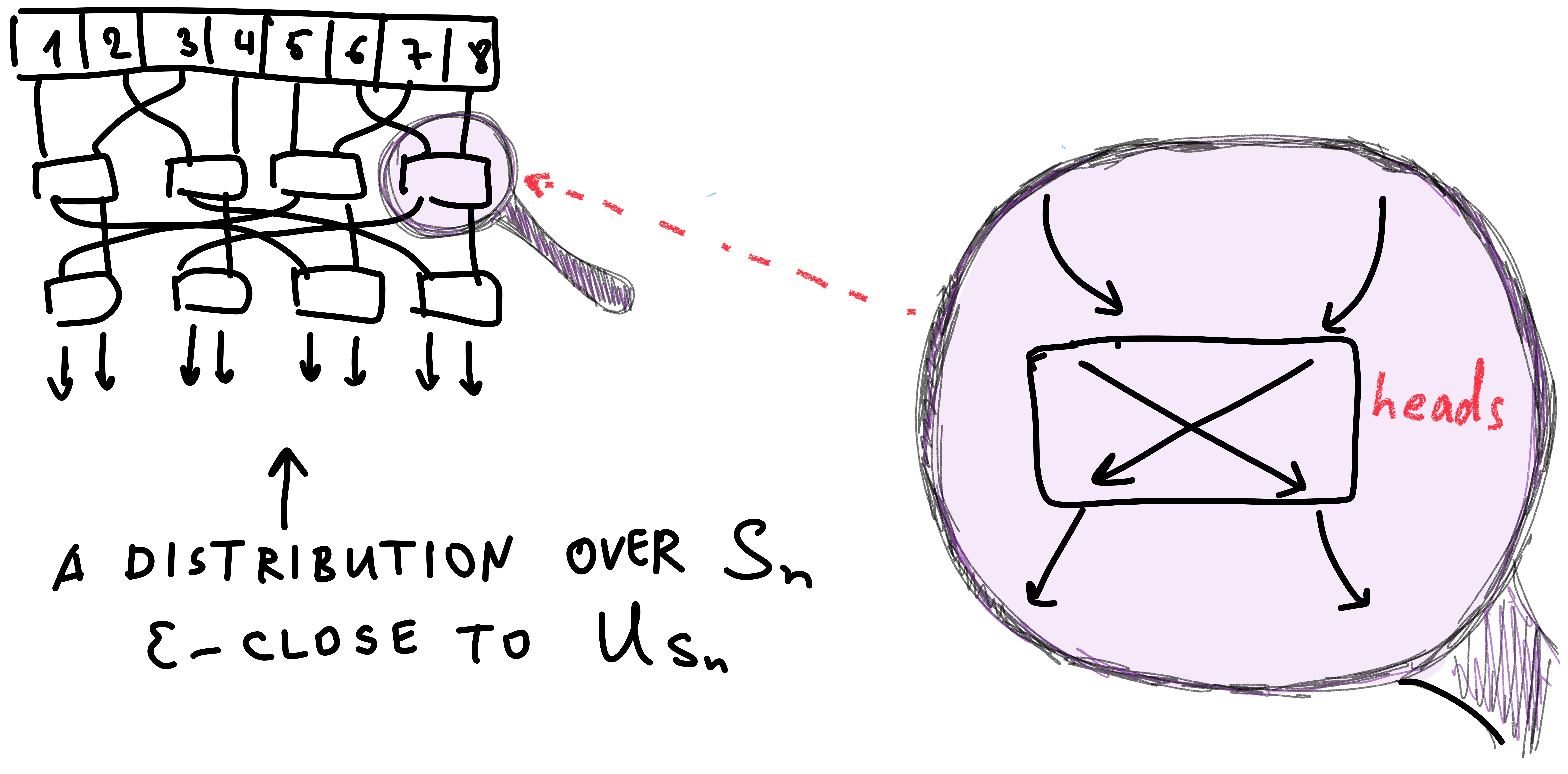
SUNFLOWERS:



SETS WITH ALL PAIRWISE INTERSECTIONS = K

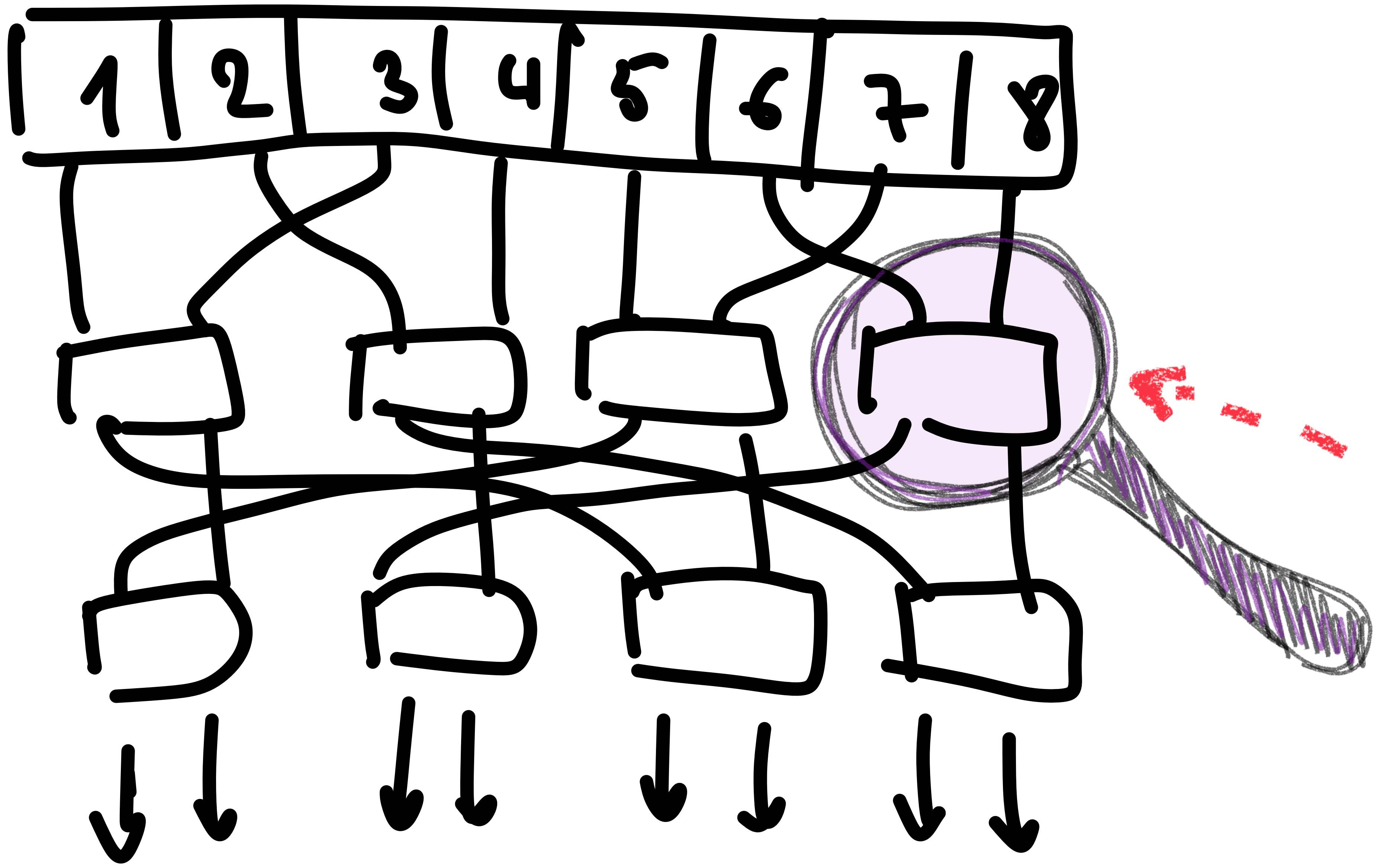
- If $X_i = 1$ FOR A PETAL $\Rightarrow$ ALL OTHER PETALS BECOME INDEPENDENT.
- LARGE SUNFLOWER ON TERMS $\Rightarrow$ CONTRADICTION.

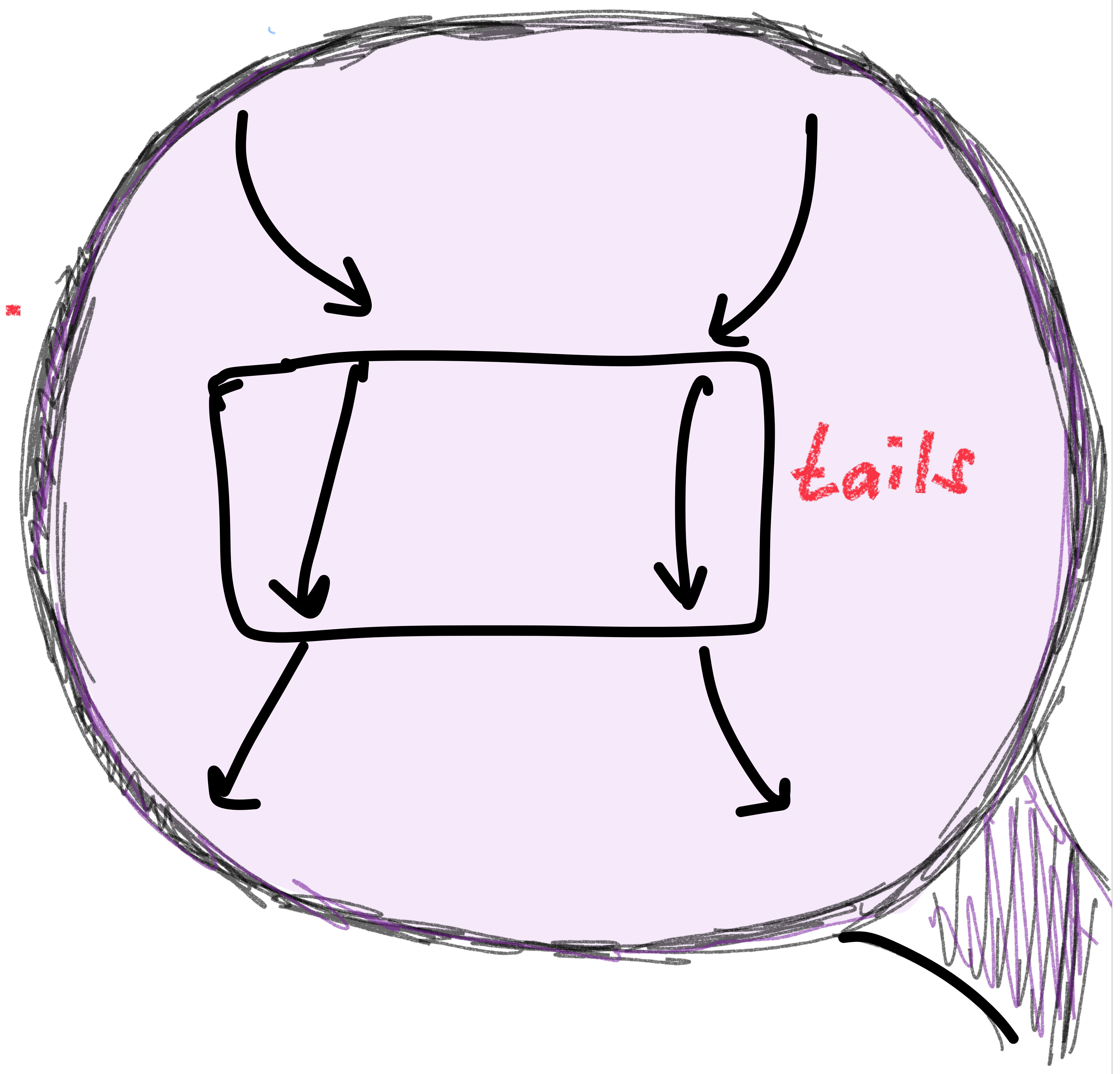
Sampling Slices: switching networks



A DISTRIBUTION OVER S_n
ε-CLOSE TO U_{S_n}

Sampling Slices: switching networks

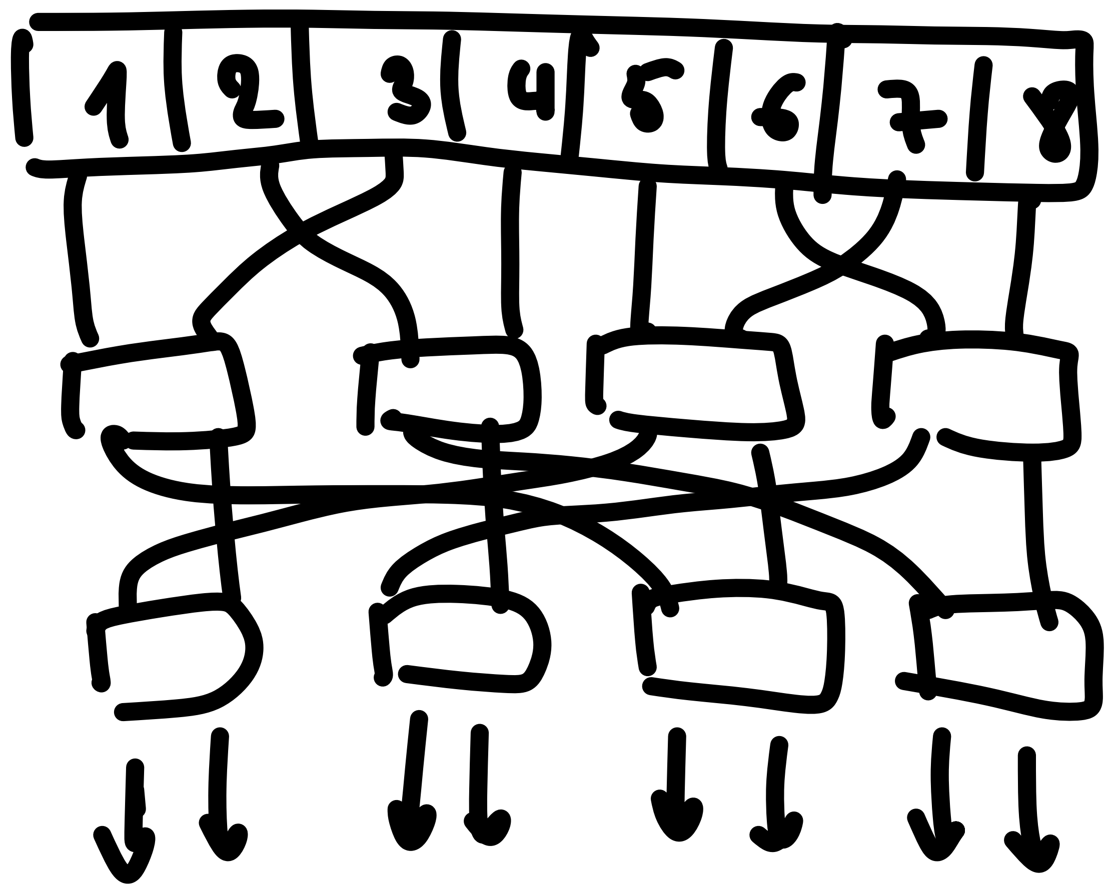




A DISTRIBUTION OVER S_n

ε-CLOSE TO U_{S_n}

Sampling Slices: switching networks



Thm [CZUMAJ '15]

$\exists$ $O(\log n)$-deep SWITCHING NETWORK THAT SHUFFLES 0-1 SEQUENCES

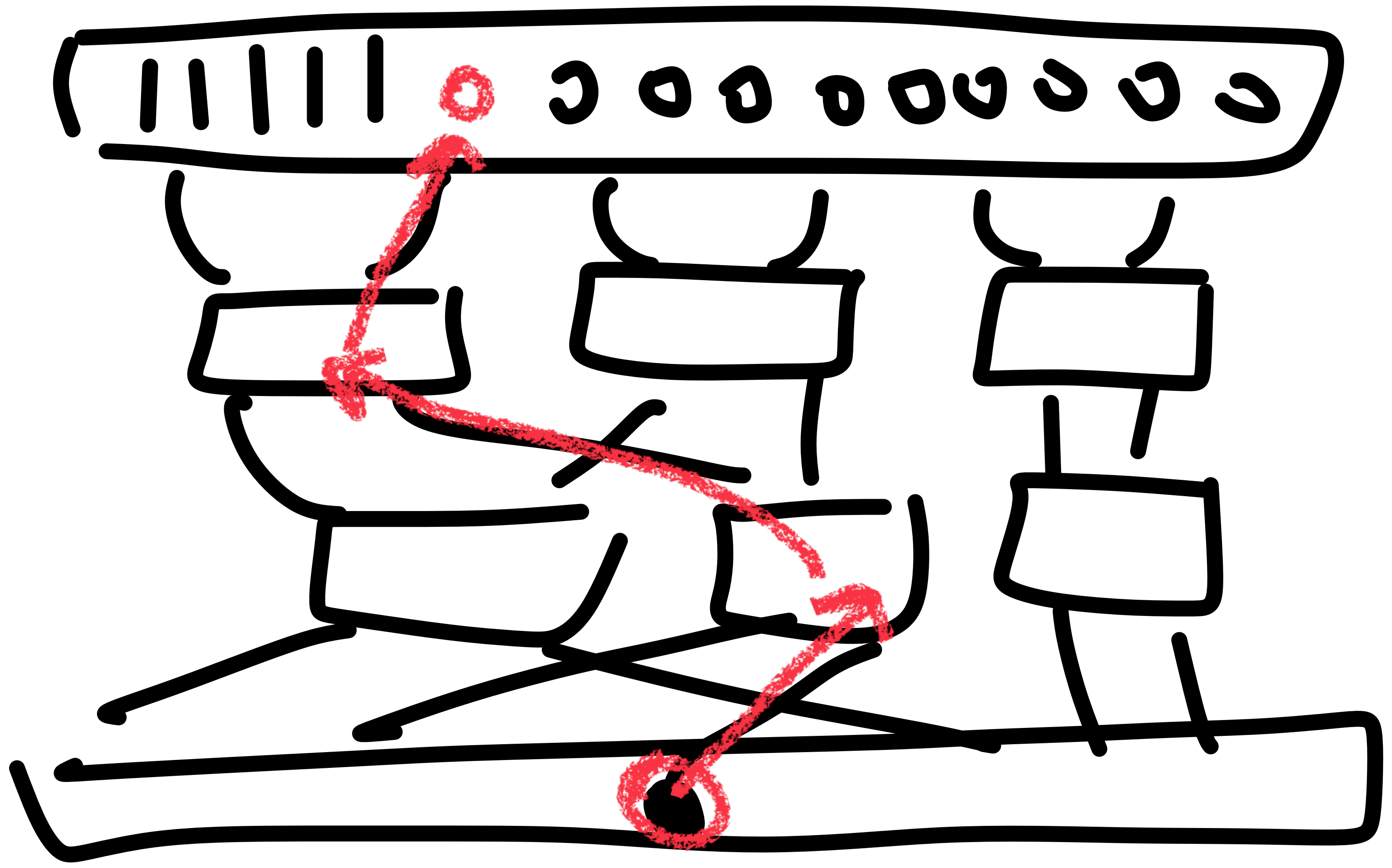
DEPTH-d SWITCHING NETWORK SAMPLING $\mathcal{D}$

[Viola '12] $\Rightarrow$

DEPTH-d DECISION FOREST SAMPLING $\mathcal{D}$

Sampling Slices: switching networks

VIOLA'S TRANSFORMATION



COIN TOSSES IN THE SWITCHING NODES

↓

INPUT BITS FOR THE SAMPLER

Conclusion

$\forall k \in [n]$ $\mathcal{U}_n^k$ IS SAMPLABLE WITH $O(\log n)$-DEPTH DECISION FOREST.

What's next?

- $\Omega(\log n)$ DEPTH LOWER BOUND FOR $\mathcal{U}_n^1$.
- ANY LOWER BOUND FOR $\mathcal{U}_n^{n/2}$.

  [VIOLA '21] IMPLIES A L.B. $\mathcal{U}_n^{n/3}$.

- ANY LOWER BOUND FOR $\mathcal{U}_{\{x \mid |x| \bmod 4 = 0\}}$
- WHAT SYMMETRIC DISTRIBUTIONS ARE IN QNC^0 ?