

& Certifying

Sampling Symmetric Functions

Yuval Filmus, Itai Leigh, Artur Riazanov, Dmitry Sokolov

TECHNION

Tel Aviv
University

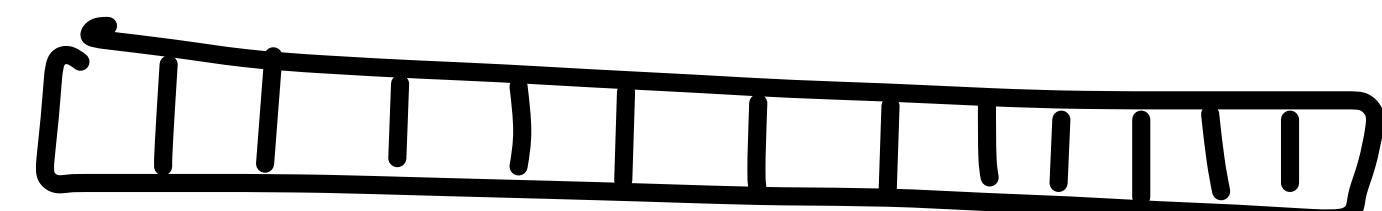
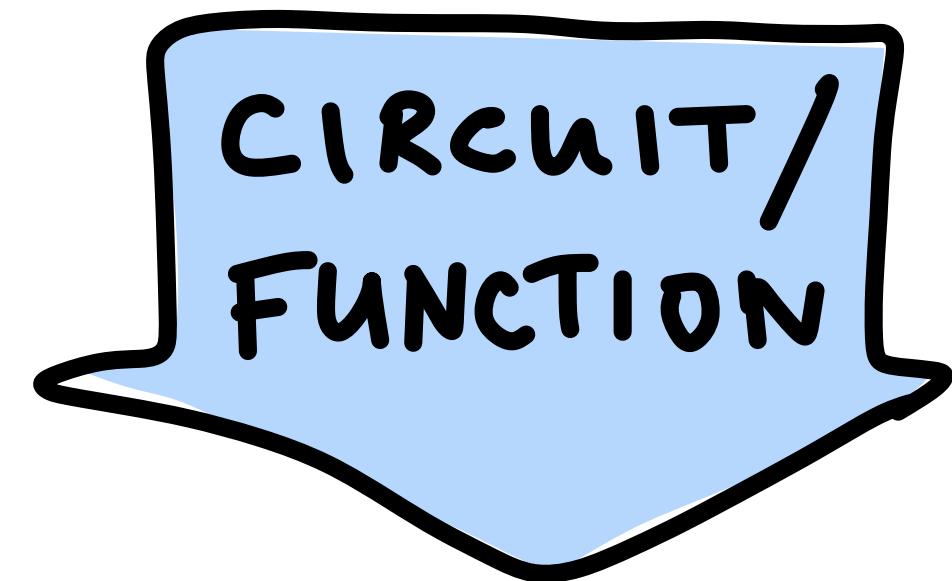
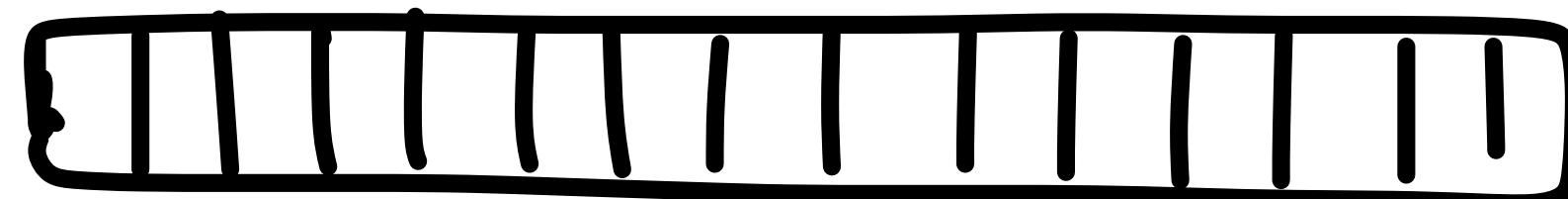
EPFL

EPFL

RANDOM 2023

Setting

UNIFORM INPUT BITS



OUTPUT BITS

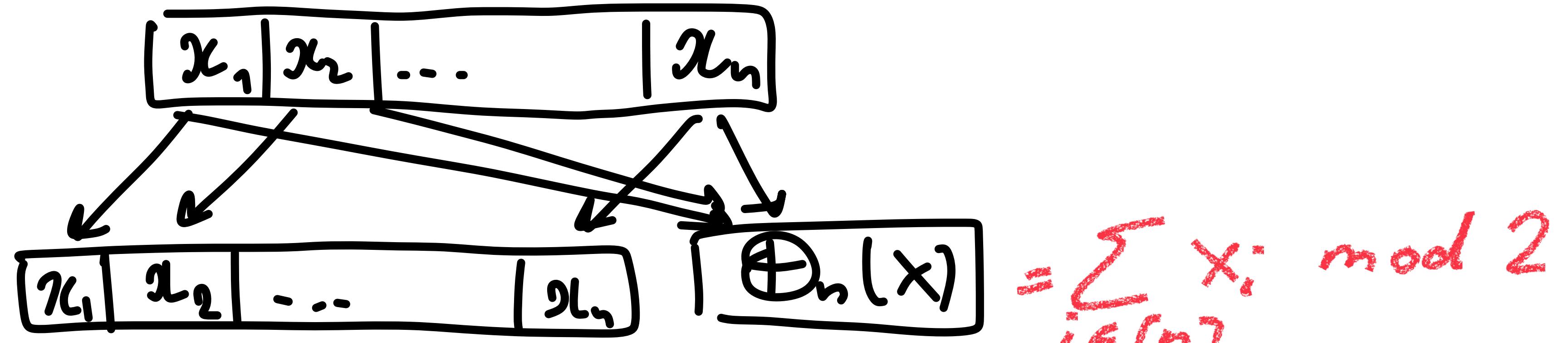
A ckt C SAMPLES A
DISTRIBUTION T WITH ERROR ϵ

IF $\Delta(c(\mu_h), T) \leq \epsilon$

WHERE

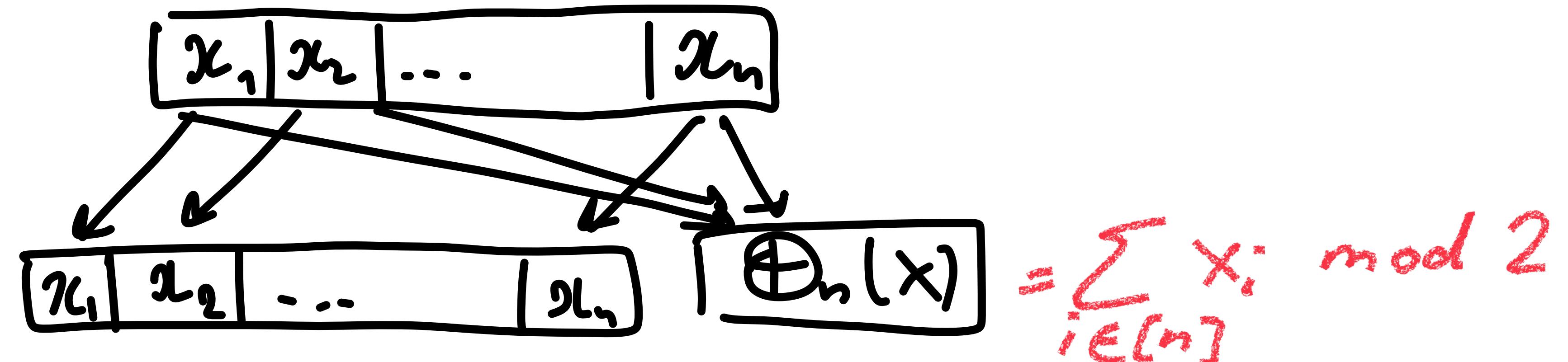
$$\Delta(P, Q) = \max_E |P_2[P \in E] - Q_2[Q \in E]|$$

Example

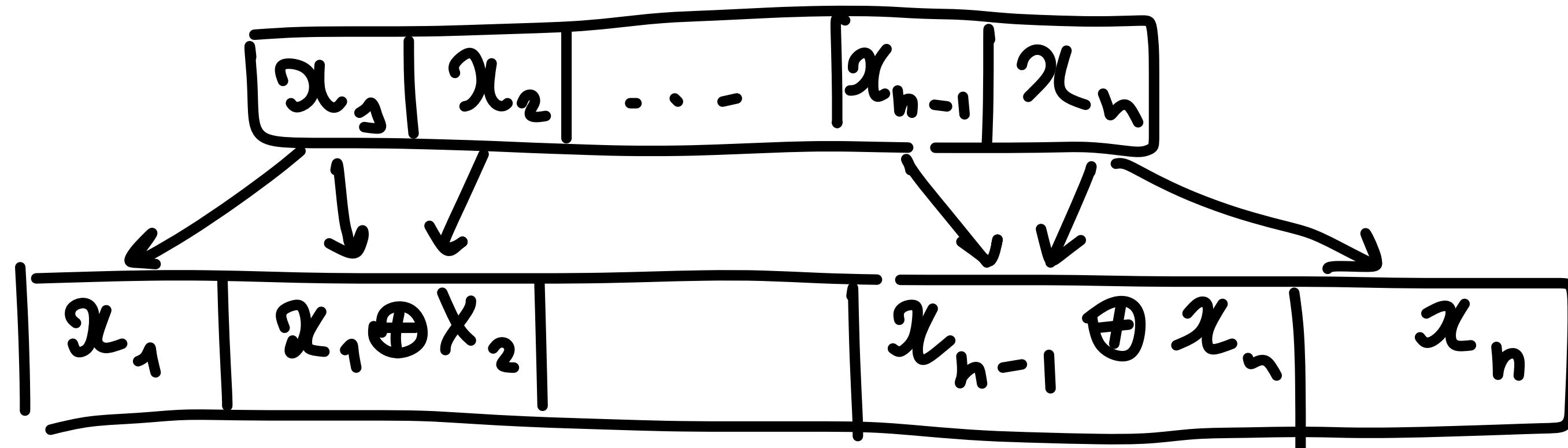


- $(U_n, \Theta_n(U_n)) =: T$
- Θ_n is HARD FOR AC^0 CKTS. [Håstad '86]

Example



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



State of the Art

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

[Viola`12] $\exists f: \{0,1\}^n \rightarrow \{0,1\}$ s.t. AC^ω SAMPLES $(U_n, f(U_n))$ WITH ERROR $\geq \gamma_2^{-o(1)}$

State of the Art

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

[Viola'12] $\exists f: \{0,1\}^n \rightarrow \{0,1\}$ s.t. AC° SAMPLES $(U_n, f(U_n))$ WITH ERROR $\geq Y_2 - o(1)$

[Folklore] NC° CAN SAMPLE $(U_n, \bigoplus_n (U_n))$

[IN'Sf] AC° CAN SAMPLE $(U_n, \text{IP}_{n/2}(U_n))$

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

Symmetric ~~Functions~~ Distributions

As with $S \subseteq \{0,1\}^n$ AND $\begin{cases} x \in S \\ |x| = |y| \end{cases} \Rightarrow y \in S.$

QUESTION: WHAT SYMMETRIC DISTRIBUTIONS
CAN BE SAMPLED IN NC⁰?

Symmetric ~~Functions~~ Distributions

U_S with $S \subseteq \{0,1\}^n$ AND $\begin{cases} x \in S \\ |x|=|y| \end{cases} \Rightarrow y \in S.$

QUESTION: WHAT SYMMETRIC DISTRIBUTIONS CAN BE SAMPLED IN NC⁰?

I_{hm} [Viola'12] WITH $n + n^\epsilon$ INPUT BITS

$U_{n/2}^{n/2} = U_{\{x \in \{0,1\}^n : |x|=n/2\}}$

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

slice

NC⁰ = LOCALITY O(1).

Our result

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

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

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

Our result

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

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

Thm ANY SYMMETRIC DISTRIBUTION \mathcal{D}
SUPPORTED ON $\{x \in \{0,1\}^n \mid |x| \leq k\}$ 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:



Thm Every $D \in \text{Sym}$ 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 $\Rightarrow \Delta(D, U_n^k) = o(1)$

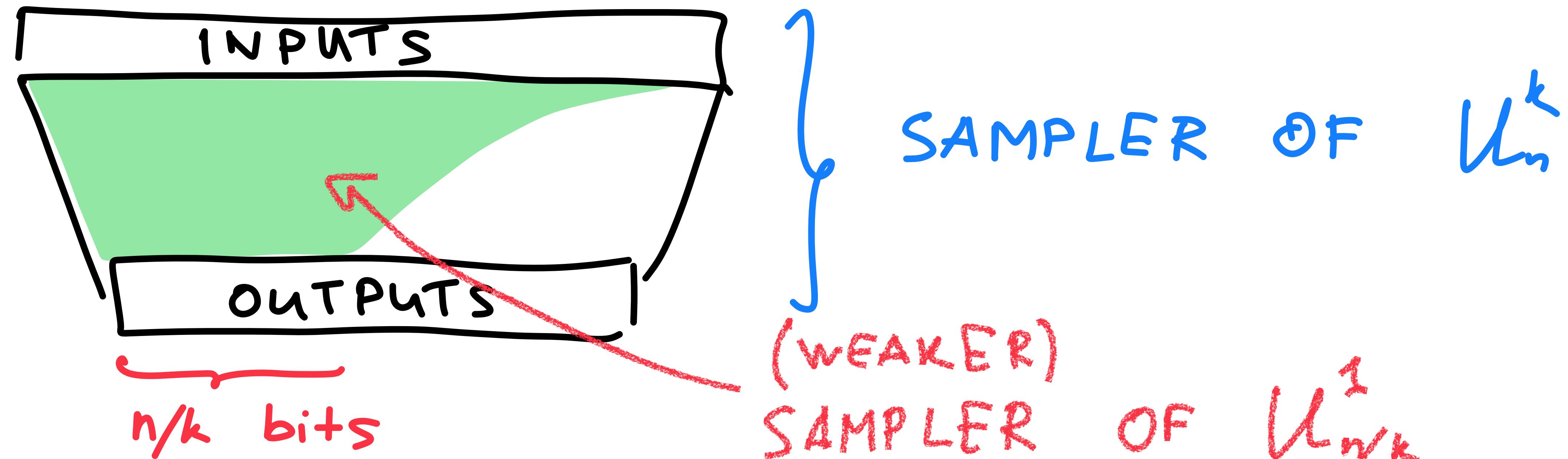
SUFFICES TO PROVE THM FOR $D = U_n^k$.

Proof: reduction to U_λ^1

A hand-drawn diagram illustrating a process flow. On the left, a yellow rectangular box contains the word "PLAN" in black, handwritten capital letters. A thick black curved arrow originates from the bottom of this box and curves upwards and to the right. This arrow points to a long, thin black horizontal arrow that also points to the right. This second arrow points to the beginning of a large, handwritten black letter "U".

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

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



PLAN:

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

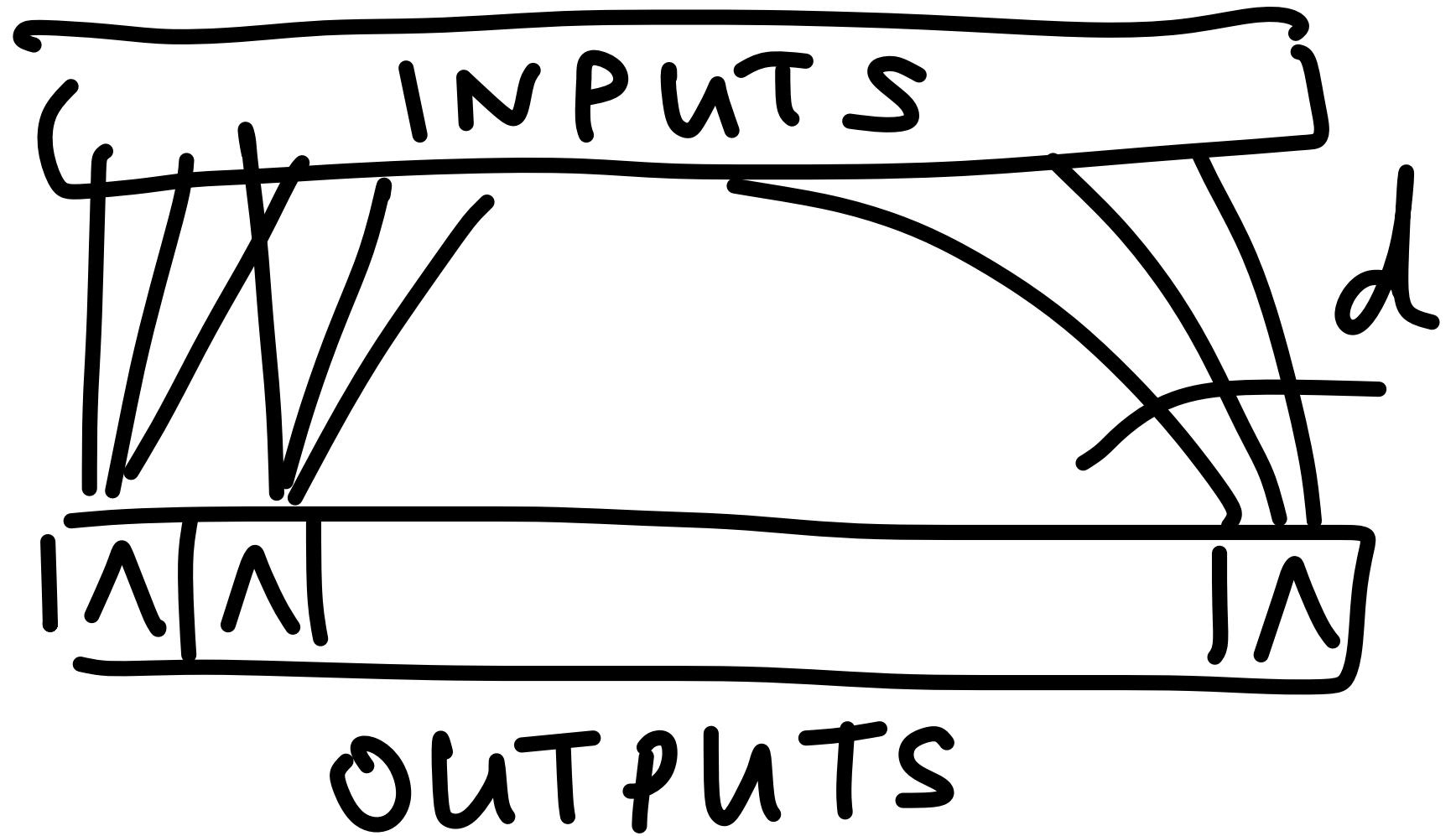
Thm. \times SAMPLABLE WITH $\tilde{O}(\log n)$ DECISION DEPTH
 $\Rightarrow \Delta(x, U_n^1) = 1 - o(1).$

PLAN:

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

Thm. X SAMPLABLE WITH $\tilde{O}(\log n)$ DECISION DEPTH
 $\Rightarrow \Delta(X, U_n^1) = 1 - o(1).$

SIMPLIFICATION TERM: Every output of X is MONOTONE OF INPUT BITS.



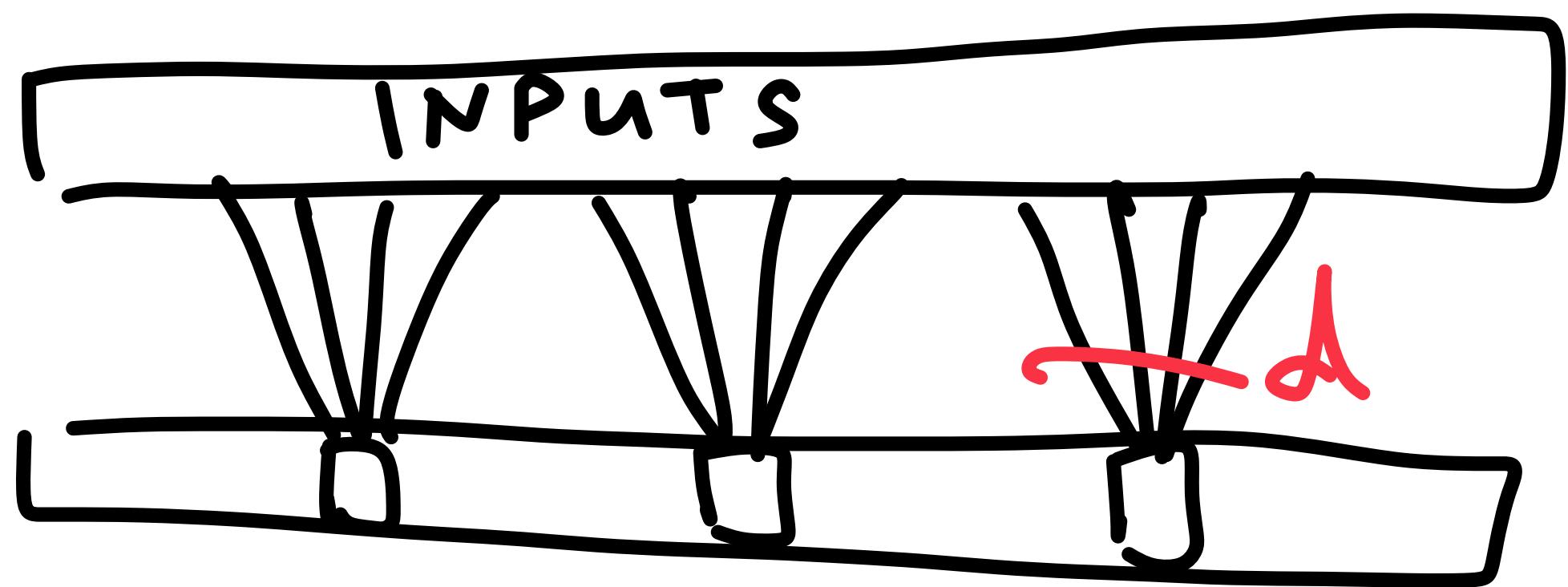
OBSERVATION

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

Observation:

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

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

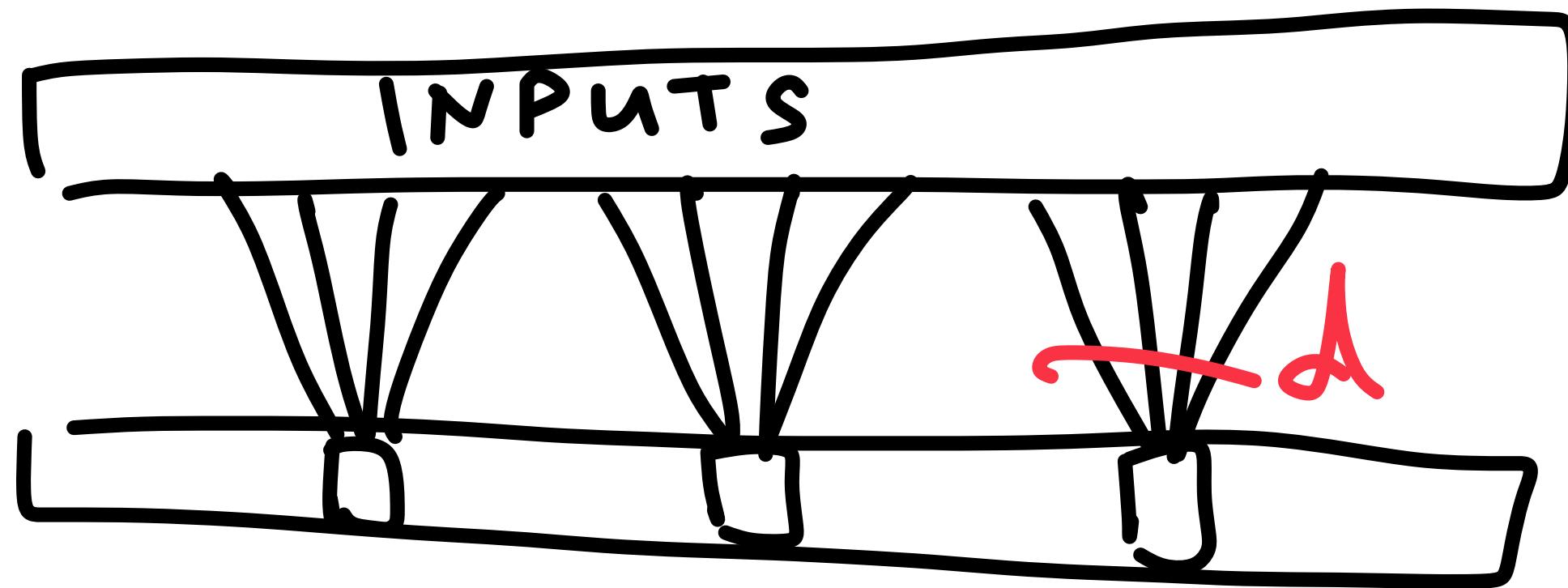


$\gg 2^d$ INDEPENDENT
BITS + CONCENTRATION
 \Rightarrow CONTRADICTION

Observation:

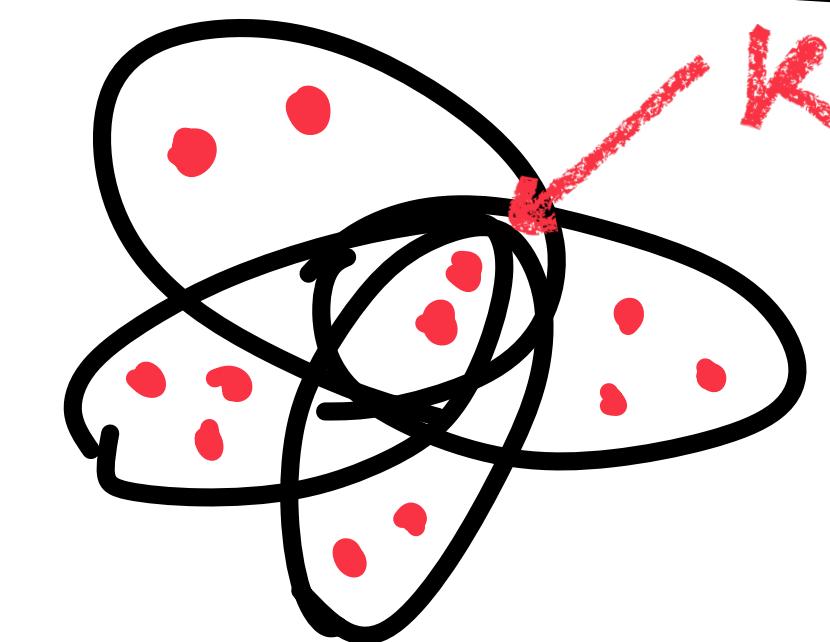
$$E\left[\sum_{i \in [n]} X_i\right] \geq 2^{-d} n \gg 1$$

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



$\gg 2^d$ INDEPENDENT
BITS + CONCENTRATION
 \Rightarrow CONTRADICTION

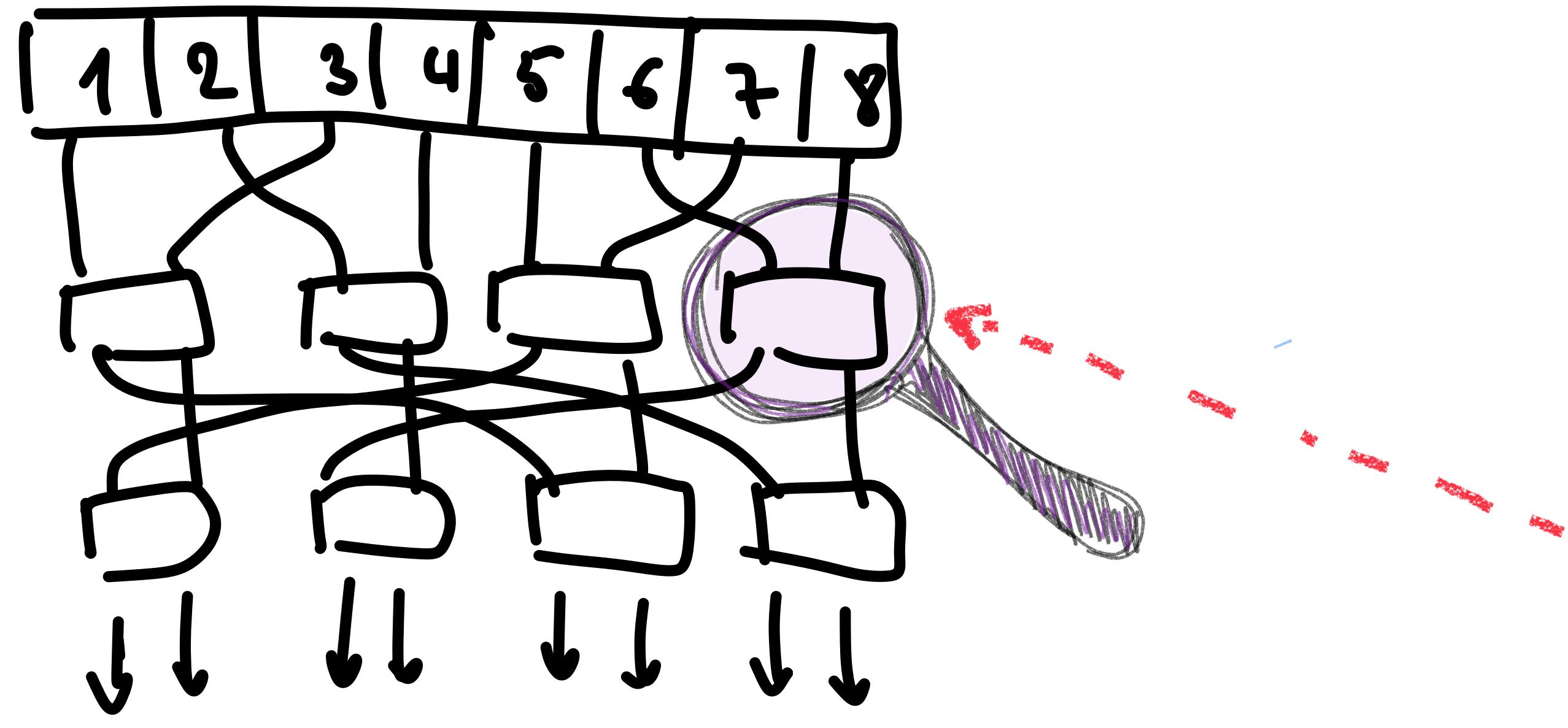
SUNFLOWERS:



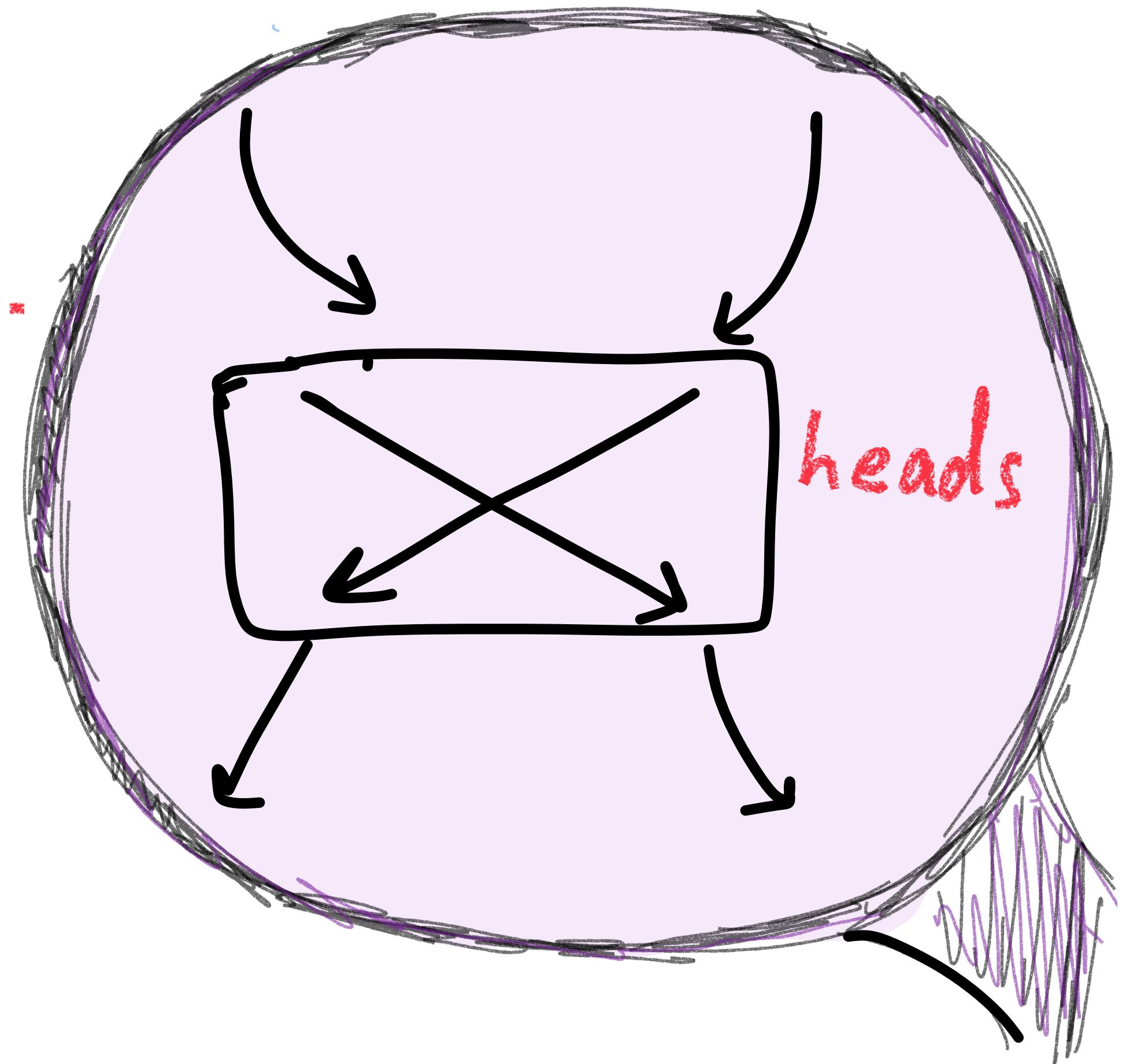
SETS WITH
ALL PAIRWISE
INTERSECTIONS = K

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

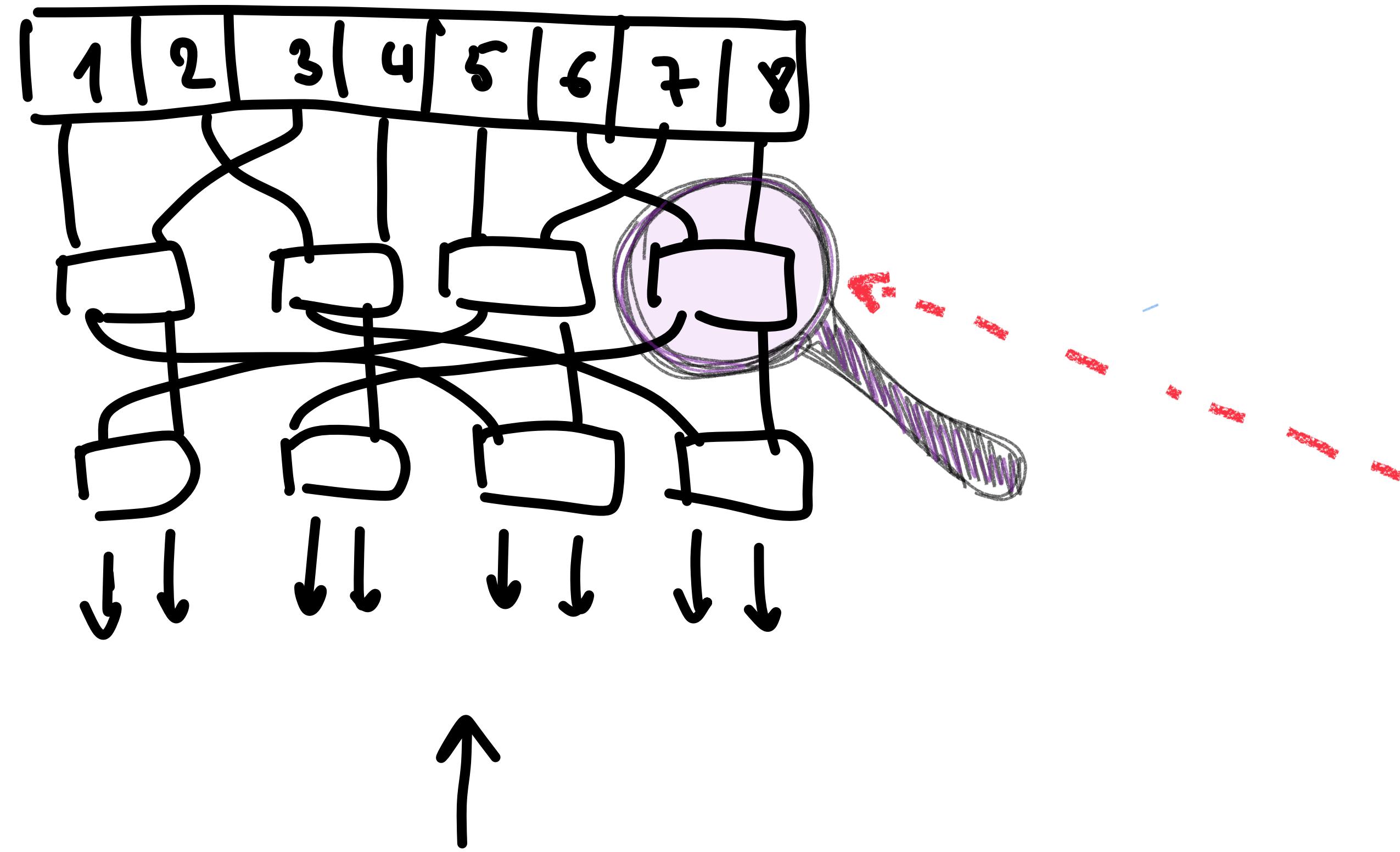
Sampling Slices: switching networks



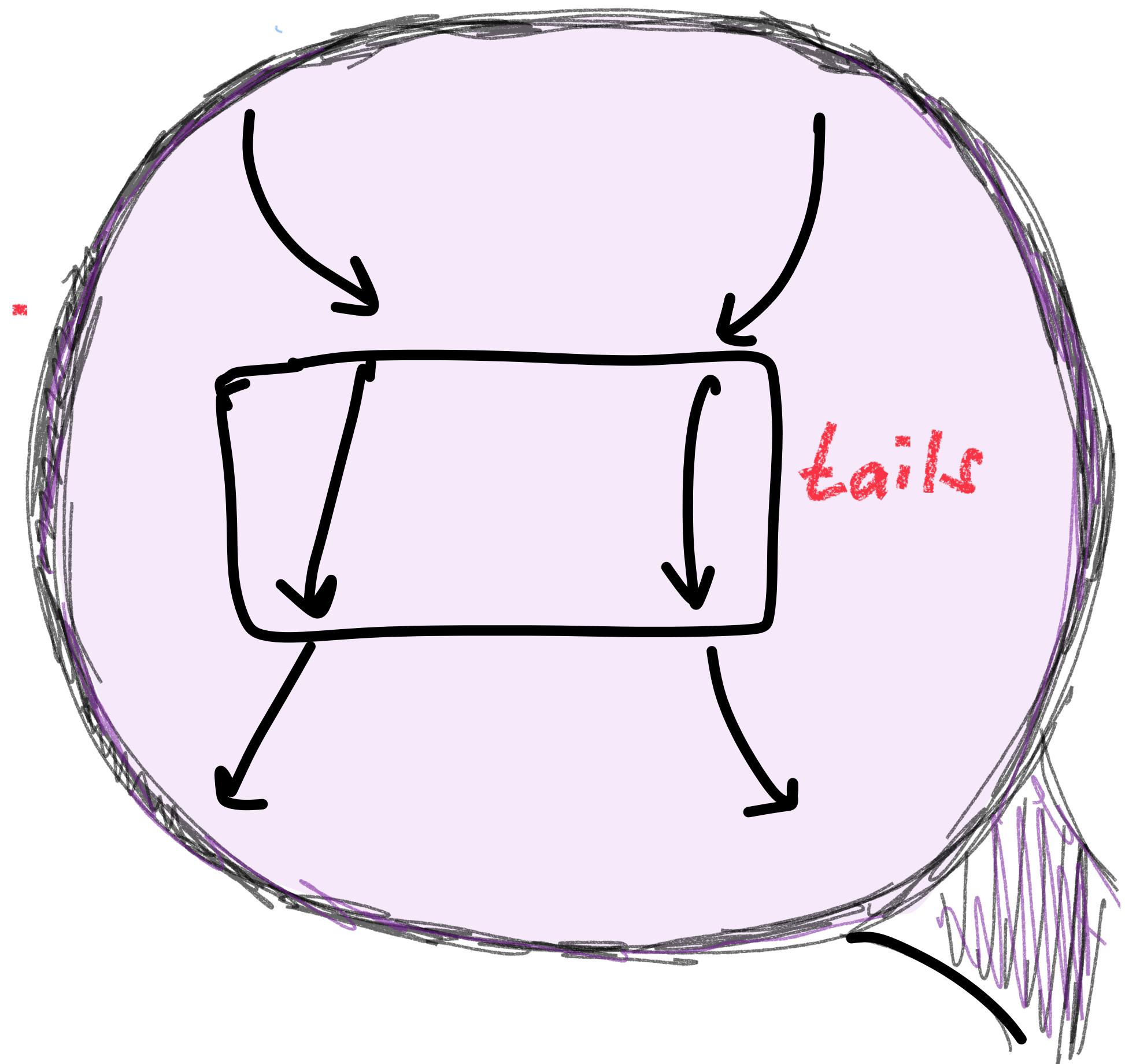
A DISTRIBUTION OVER S_n
 ϵ -CLOSE TO U_{S_n}



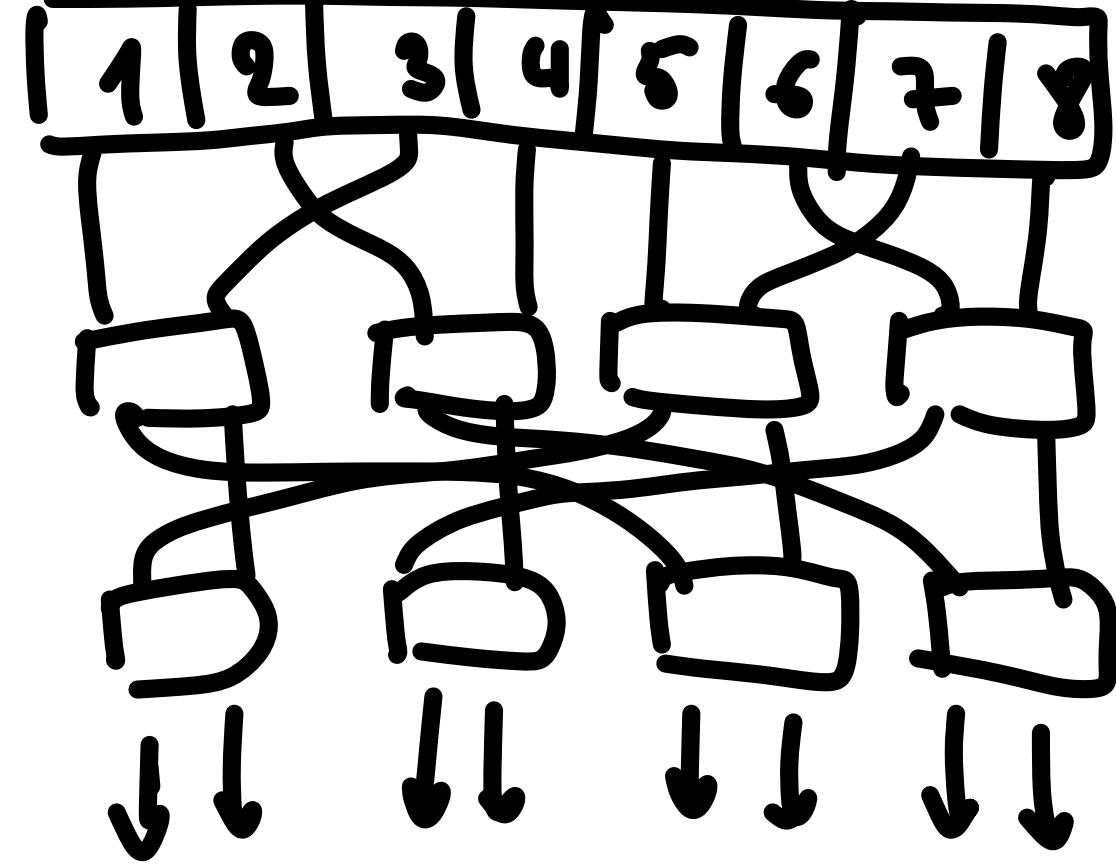
Sampling Slices: switching networks



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



Sampling Slices: switching networks



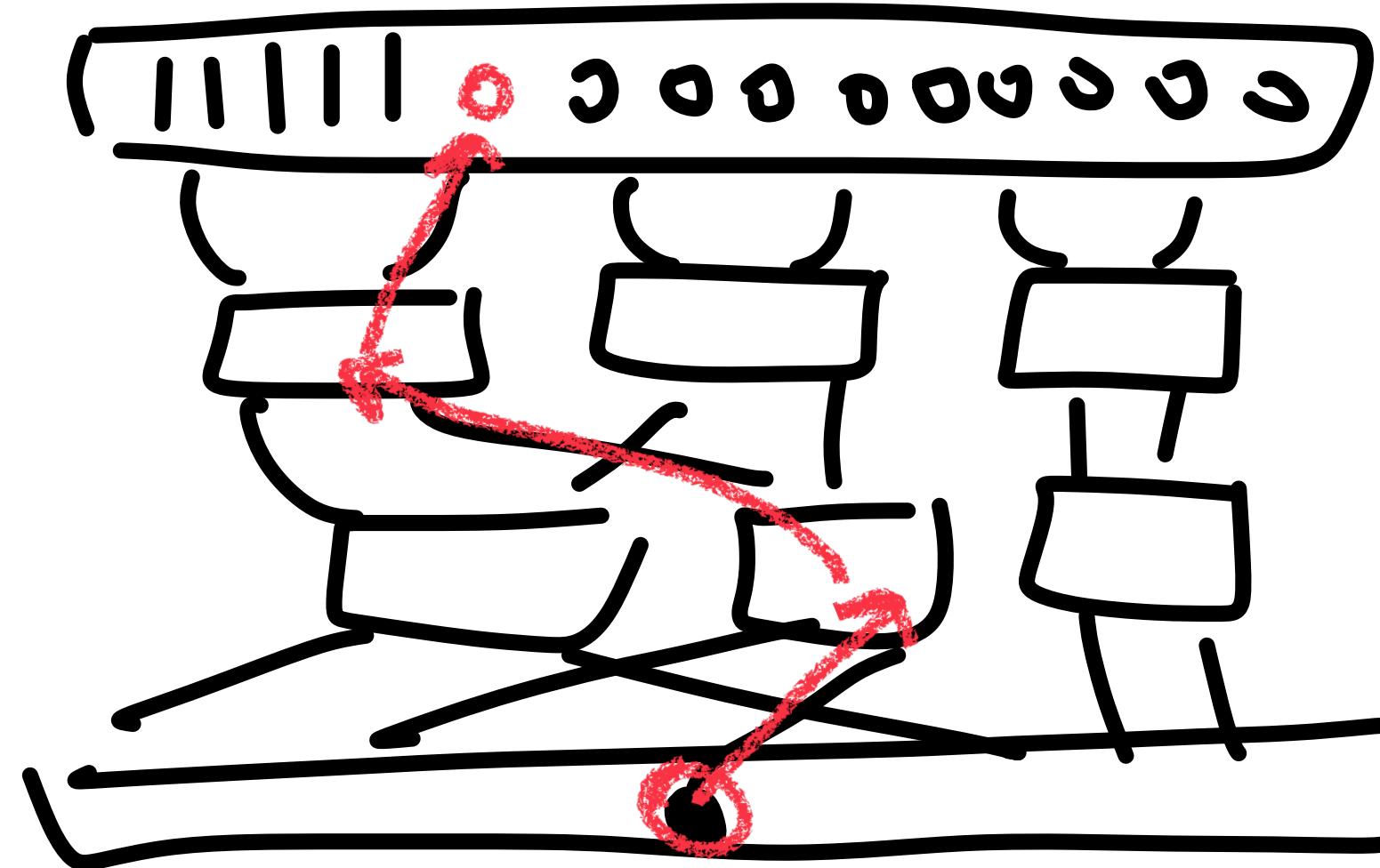
DEPTH - d
SWITCHING NETWORK
SAMPLING D

Ihm [CzumAJ '15]
↳ $O(\log n)$ - deep SWITCHING
NETWORK THAT SHUFFLES
0-1 SEQUENCES

[Viola '12] DEPTH - d
DECISION FOREST
SAMPLING D

Sampling Slices: switching networks

Viola's TRANSFORMATION



COIN TOSSES IN THE SWITCHING
NODES
↓
INPUT BITS FOR THE SAMPLER

Conclusion

$\forall k \in [n]$ U_n^k is SAMPLABLE WITH
 $O(\log n)$ -DEPTH DECISION FOREST.

What's next?

- $\Omega(\log n)$ DEPTH LOWER BOUND FOR U_n^1 .
- ANY LOWER BOUND FOR $U_n^{n/2}$.
- [VIOLA '21] IMPLIES A L.B. $U_n^{n/3}$.
- ANY LOWER BOUND FOR $U_{\{x \mid |x| \bmod 4 = 0\}}$
- WHAT SYMMETRIC DISTRIBUTIONS ARE IN QNC^0 ?