Class 18

Extractors and Expanders

Warm-up

- Say that X is a k-source on $\{0,1\}^n$. Let $N = 2^n$.
- Let $\sigma \in \mathbb{R}^N$ correspond to the pmf for X.

1. Why is $\|\sigma\|_\infty \leq 2^{-k}$?
2. Argue that $\|\sigma\|_2 \leq 2^{-k/2}$.
   - Hint: $\|x\|_2^2 \leq \|x\|_\infty \|x\|_1$

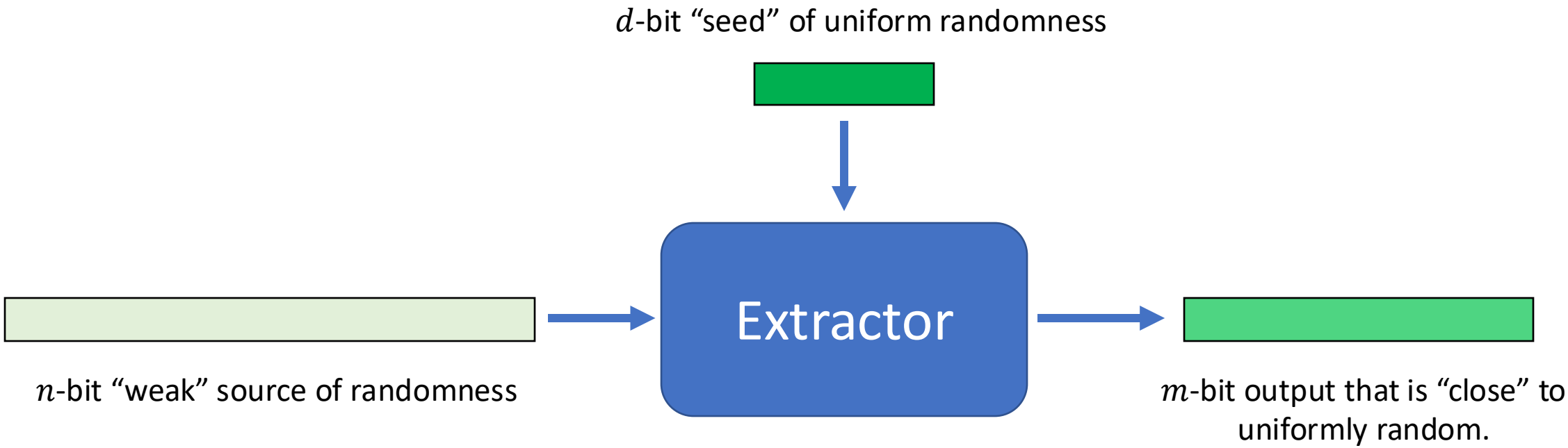
Announcements

- HW7 due Friday.
- EXAM: Friday 3/21, 8:30am-11:30am, Hewlett 201.
  - Practice exam out now

Pseudorandomness

- Deterministic (or not-so-random) objects that behave like random ones.
- Useful for derandomization.

Extractors


d-bit “seed” of uniform randomness
Extractor
n-bit “weak” source of randomness
m-bit output that is “close” to uniformly random.

Expanders

- Let $G = (V, E)$ be an unweighted, undirected, regular graph with degree D and with N vertices.
- Let A be the normalized adjacency matrix of G.
- Say that the eigenvalues of A are $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_N$

- The **expansion** of A is $\lambda(G) = \max\{\lambda_2, |\lambda_N|\}$

Theorem:

- Let $\{X_t\}$ be a random walk on $G = (V, E)$.
- The stationary distribution of $\{X_t\}$ is π = uniform on V.
- If $\lambda(G) < 0.99$, then $\tau_{mix} = O(\log N)$

Questions?

Minilectures, Warm-up?

Warm-up:

- Say that X is a k-source on $\{0,1\}^n$. Let $N = 2^n$.
- Let $\sigma \in \mathbb{R}^N$ correspond to the pmf for X.

1. Why is $\|\sigma\|_\infty \leq 2^{-k}$?
2. Argue that $\|\sigma\|_2 \leq 2^{-k/2}$.
   - Hint: $\|x\|_2^2 \leq \|x\|_\infty \|x\|_1$

$\sigma_i = \mathbb{P}[X = i]$, $\forall i \in \{0, \ldots, N-1\}$

(or, the binary expansion of i.)

Warm-Up

- Say that X is a k-source on $\{0,1\}^n$
- Let $N = 2^n$, and let σ be the "vectorized" version of the distribution of X

1. Why is $\|\sigma\|_\infty \leq 2^{-k}$?

By definition!

$$k \leq H_\infty(X) = \min_x \log\left(\frac{1}{\Pr[X = x]}\right) = \log\left(\frac{1}{\|\sigma\|_\infty}\right)$$

$\sigma_i = \mathbb{P}[X = i]$, $\forall i \in \{0, \ldots, N-1\}$

(or, the binary expansion of i.)

Warm-Up

- Say that X is a k-source on $\{0,1\}^n$
- Let $N = 2^n$, and let σ be the "vectorized" version of the distribution of X

2. Argue that $\|\sigma\|_2 \leq 2^{-k/2}$.

$$||\sigma||_2^2 = \sum_i \sigma_i^2 \leq \sum_i ||\sigma||_\infty \sigma_i = ||\sigma||_\infty \sum_i \sigma_i = ||\sigma||_\infty \leq 2^{-k}$$

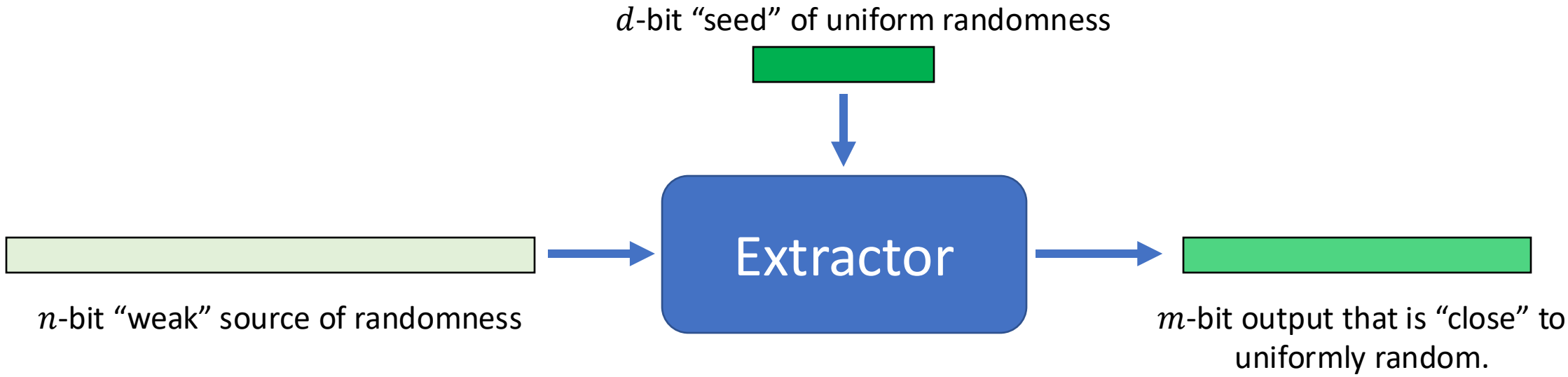
Today

- We will consider a way to make an extractor out of an expander graph.

Today

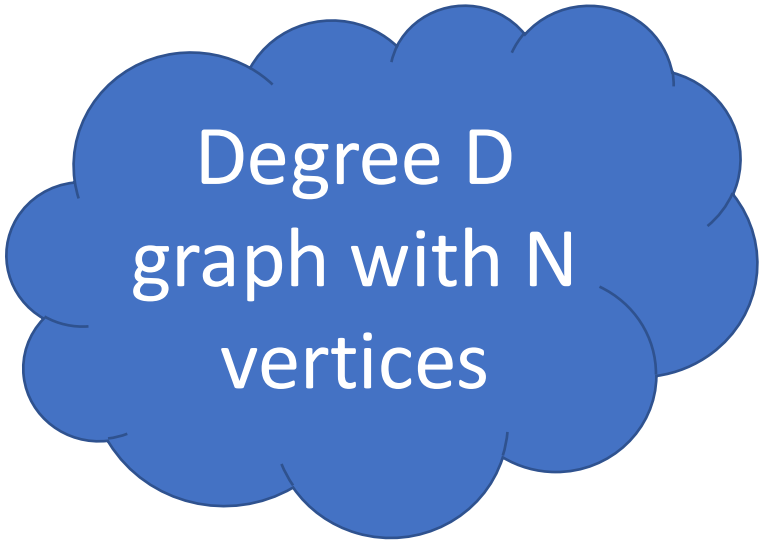
- We will consider a way to make an extractor out of an expander graph.

- Recall: An extractor looks like this:



Today

- We will consider a way to make an extractor out of an expander graph.
- Recall: An expander graph looks like this:



Normalized adjacency matrix $A \in \mathbb{R}^{N \times N}$

This is $\frac{1}{D}$ times the standard adjacency matrix.

- The eigenvalues of A are $1 = \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_N$
- The expansion is $\lambda(G) = \max\{\lambda_2, |\lambda_n|\}$
- For an expander, $\lambda(G)$ is decently less than 1.

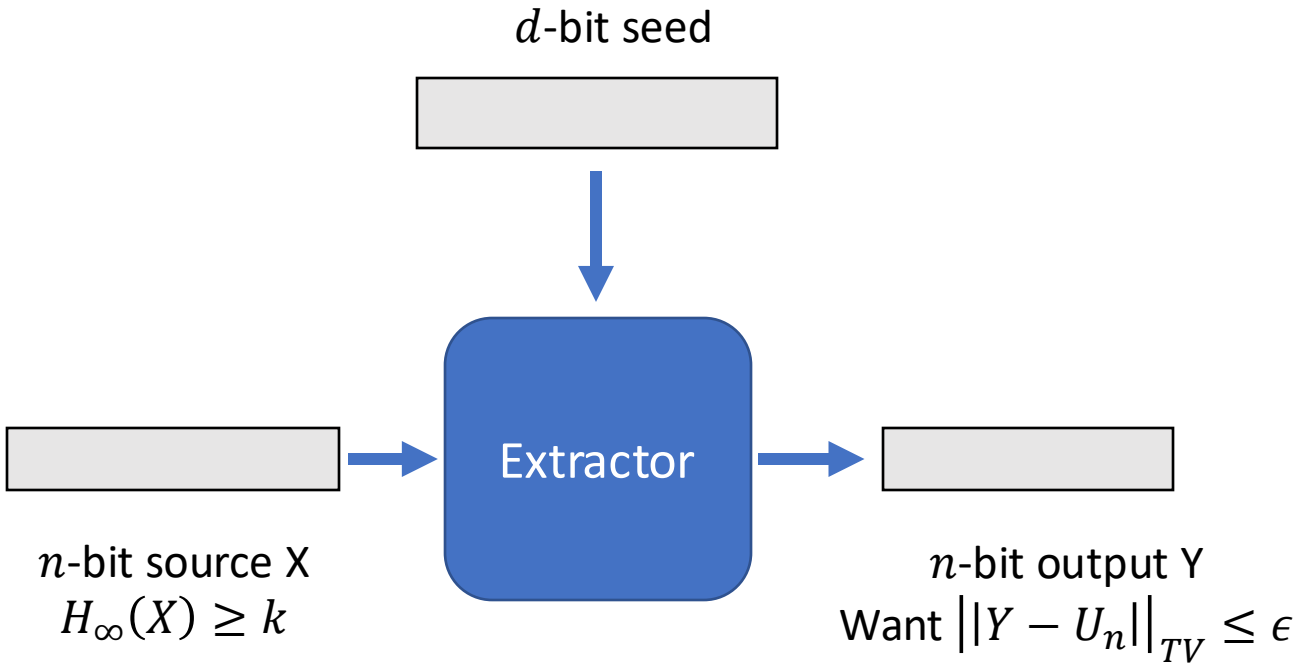
Our extractor

$N = 2^n$, and choose $k \leq n$ and $\epsilon > 0$

Let $d = \ell \cdot \log(D)$, where $\ell = \frac{n-k}{2} + \log\left(\frac{1}{\epsilon}\right)$

G =Degree D graph with N vertices

- Parameters:
  - $m = n$
  - $d = \log(D) \cdot \left(\frac{n-k}{2} + \log(1/\epsilon)\right)$



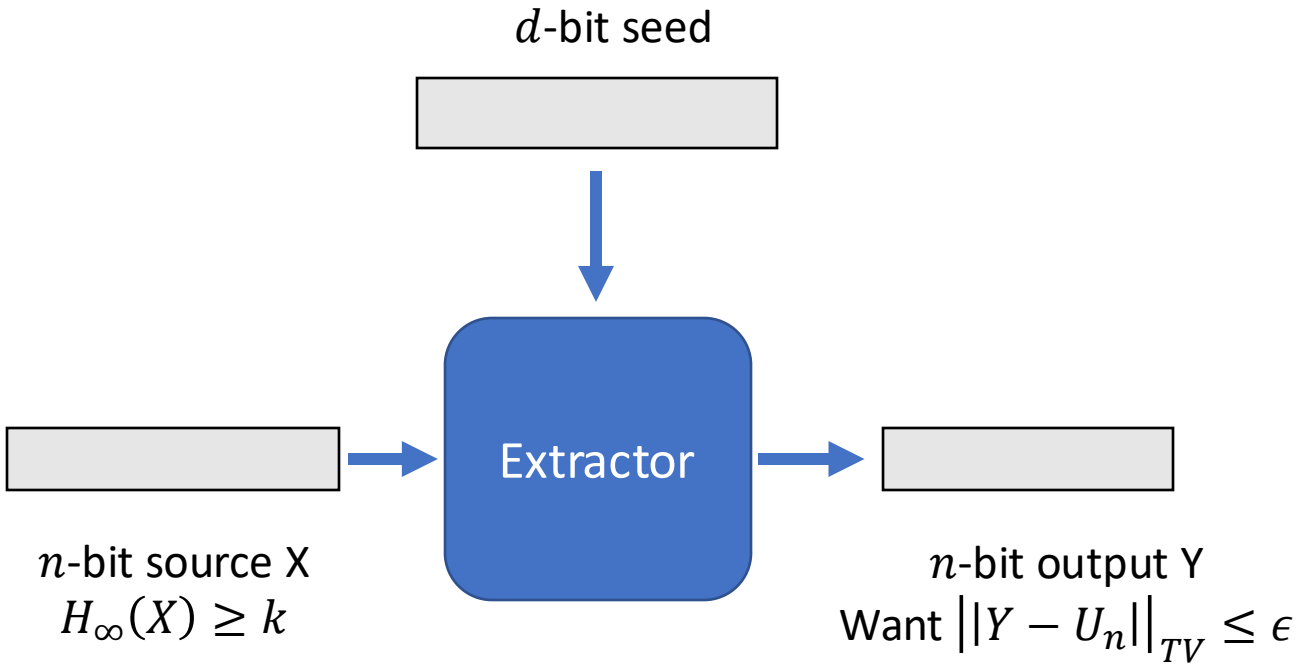
Our extractor

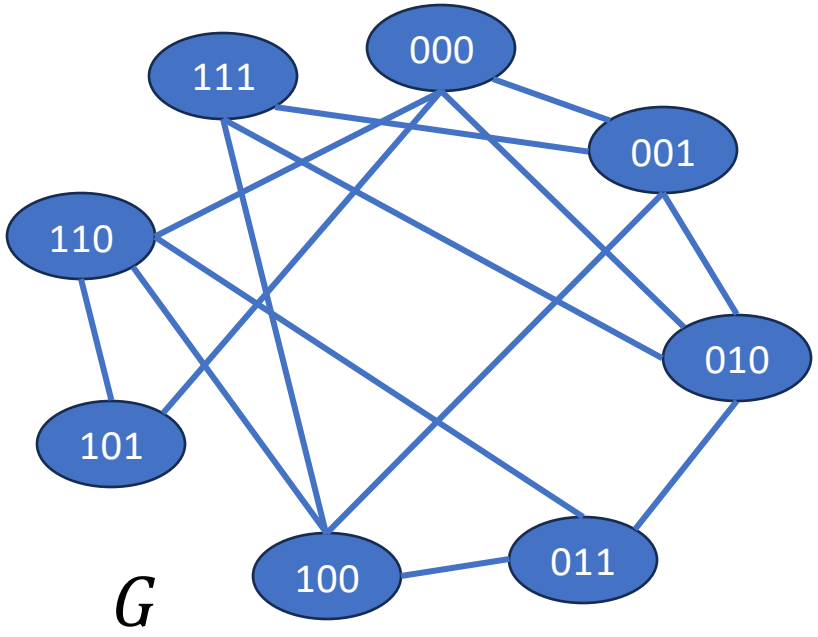
$N = 2^n$, and choose $k \leq n$ and $\epsilon > 0$

Let $d = \ell \cdot \log(D)$, where $\ell = \frac{n-k}{2} + \log\left(\frac{1}{\epsilon}\right)$

G =Degree D graph with N vertices

- Associate each vertex of G with a string in $\{0,1\}^n$
- Take a random walk on G, starting from $x \sim X$, and following a random walk given by the seed $s \sim U_d$.





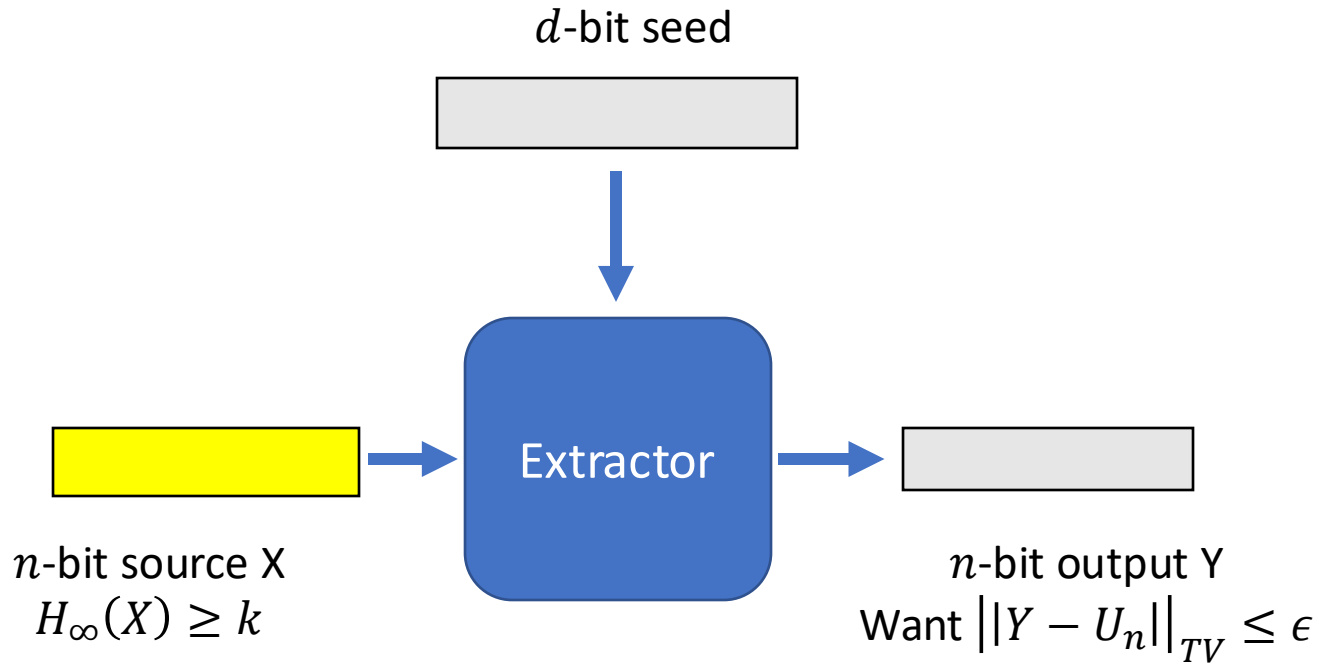
Our extractor

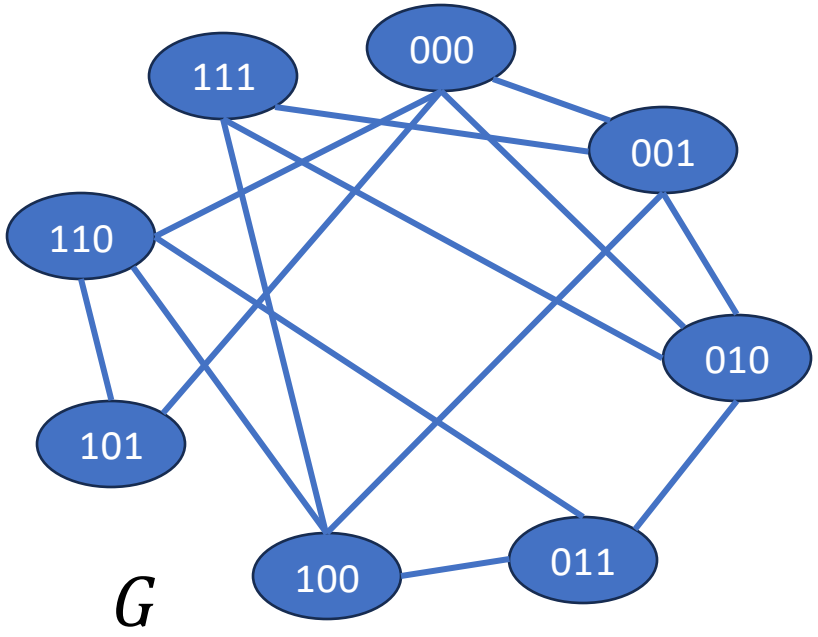
$N = 2^n$, and choose $k \leq n$ and $\epsilon > 0$

Let $d = \ell \cdot \log(D)$, where $\ell = \frac{n-k}{2} + \log\left(\frac{1}{\epsilon}\right)$

G =Degree D graph with N vertices

- Associate each vertex of G with a string in $\{0,1\}^n$
- Take a random walk on G, starting from $x \sim X$, and following a random walk given by the seed $s \sim U_d$.





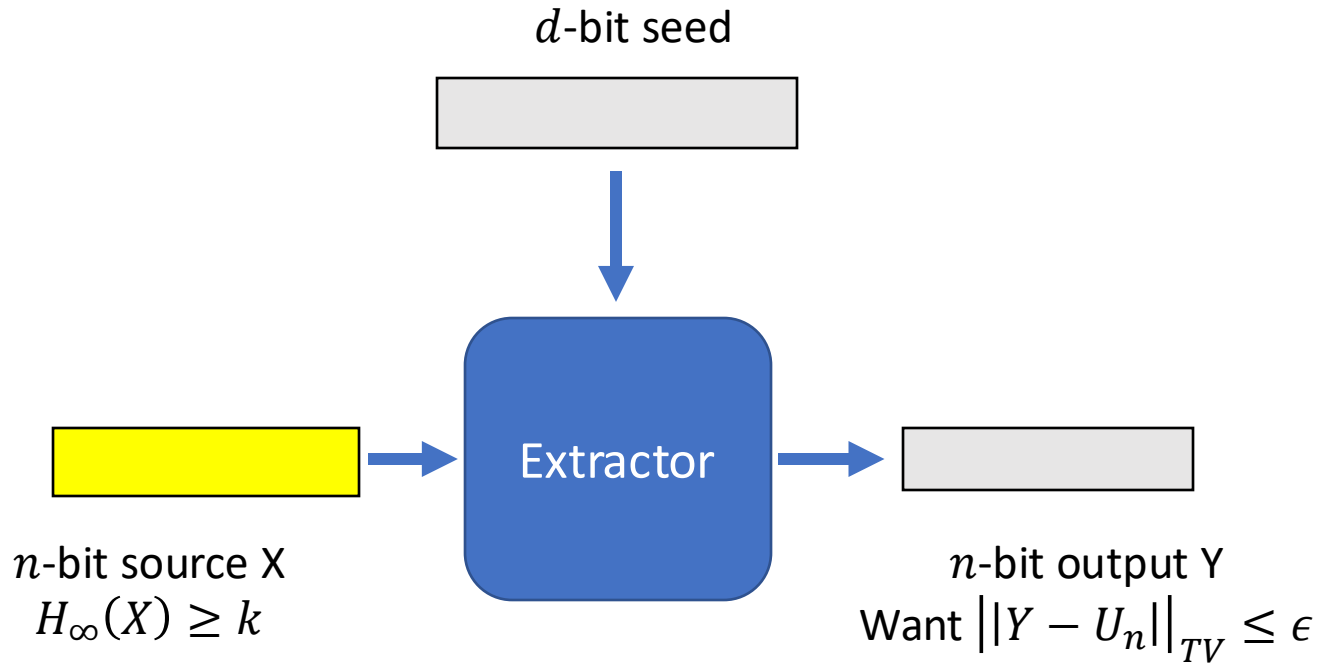
Our extractor

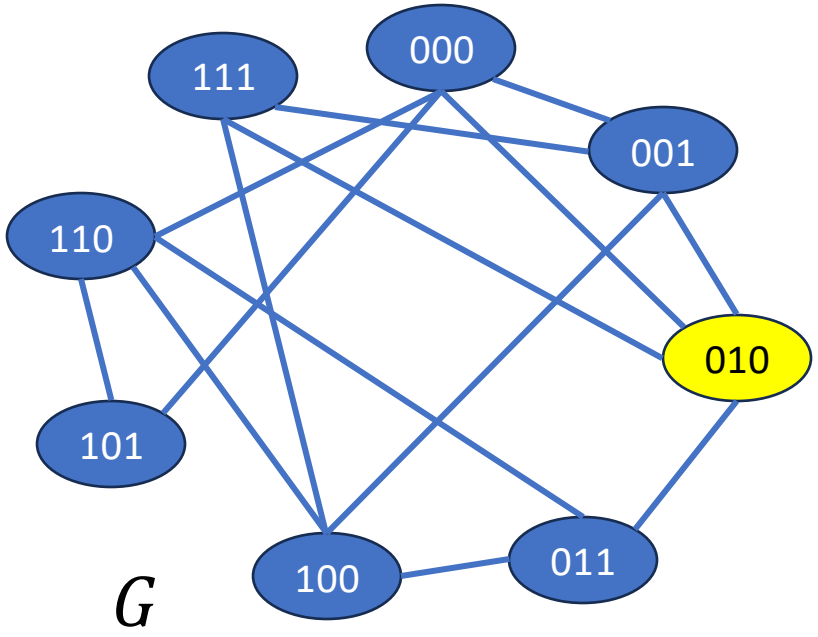
$N = 2^n$, and choose $k \leq n$ and $\epsilon > 0$

Let $d = \ell \cdot \log(D)$, where $\ell = \frac{n-k}{2} + \log\left(\frac{1}{\epsilon}\right)$

G =Degree D graph with N vertices

- Associate each vertex of G with a string in $\{0,1\}^n$
- Take a random walk on G, starting from $x \sim X$, and following a random walk given by the seed $s \sim U_d$.





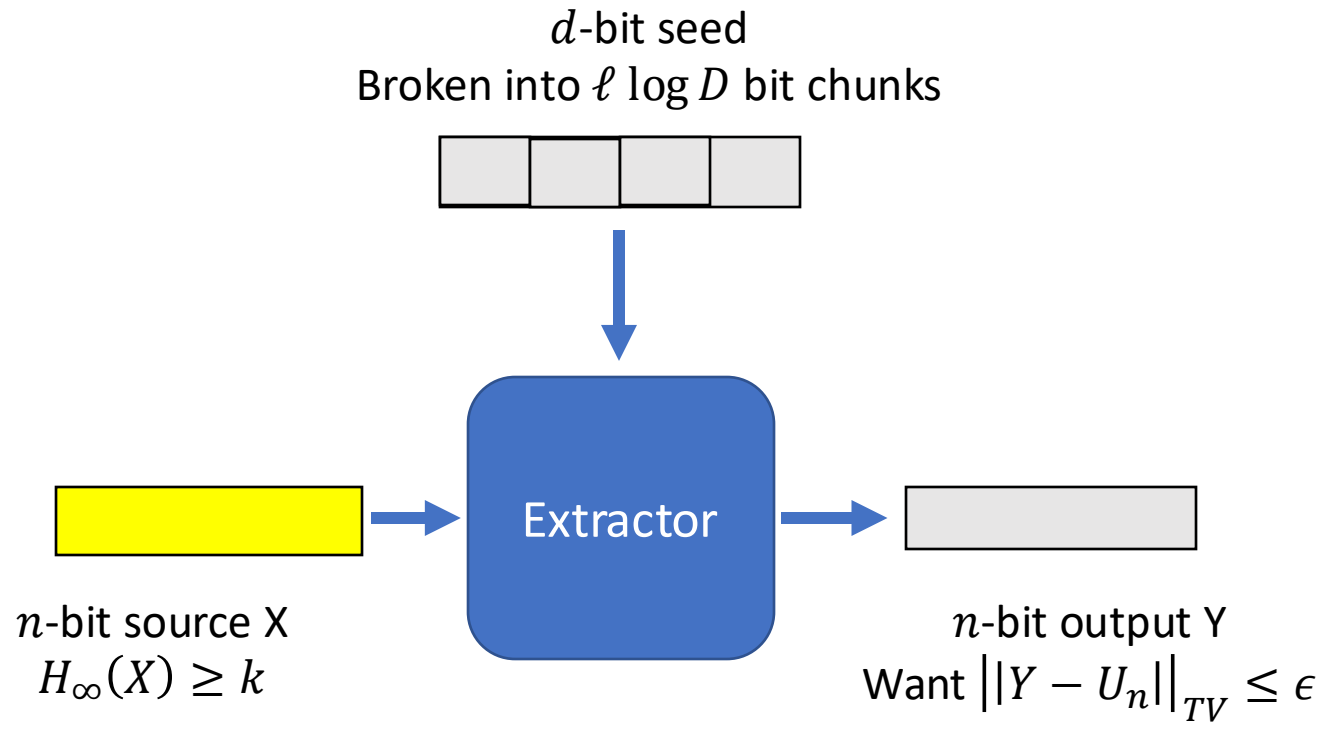
Our extractor

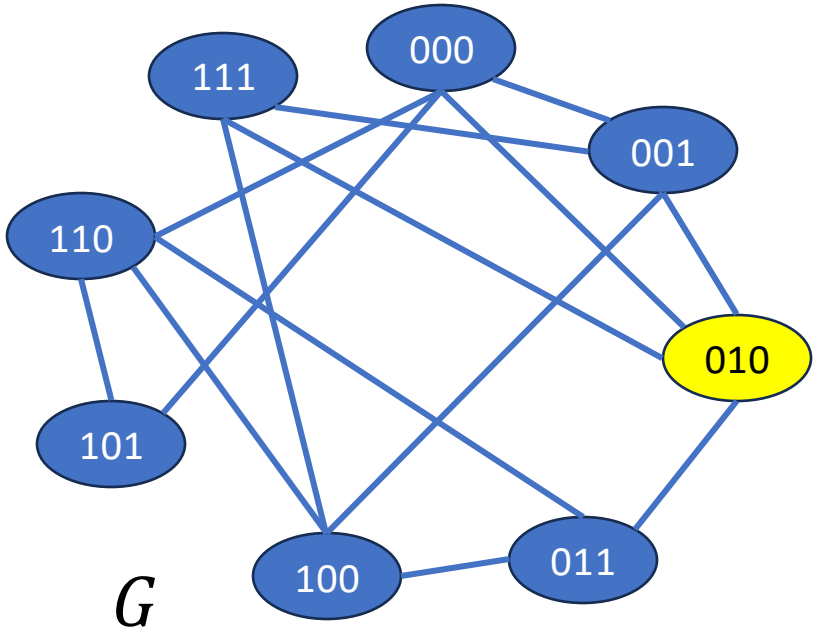
$N = 2^n$, and choose $k \leq n$ and $\epsilon > 0$

Let $d = \ell \cdot \log(D)$, where $\ell = \frac{n-k}{2} + \log\left(\frac{1}{\epsilon}\right)$

G =Degree D graph with N vertices

- Associate each vertex of G with a string in $\{0,1\}^n$
- Take a random walk on G, starting from $x \sim X$, and following a random walk given by the seed $s \sim U_d$.





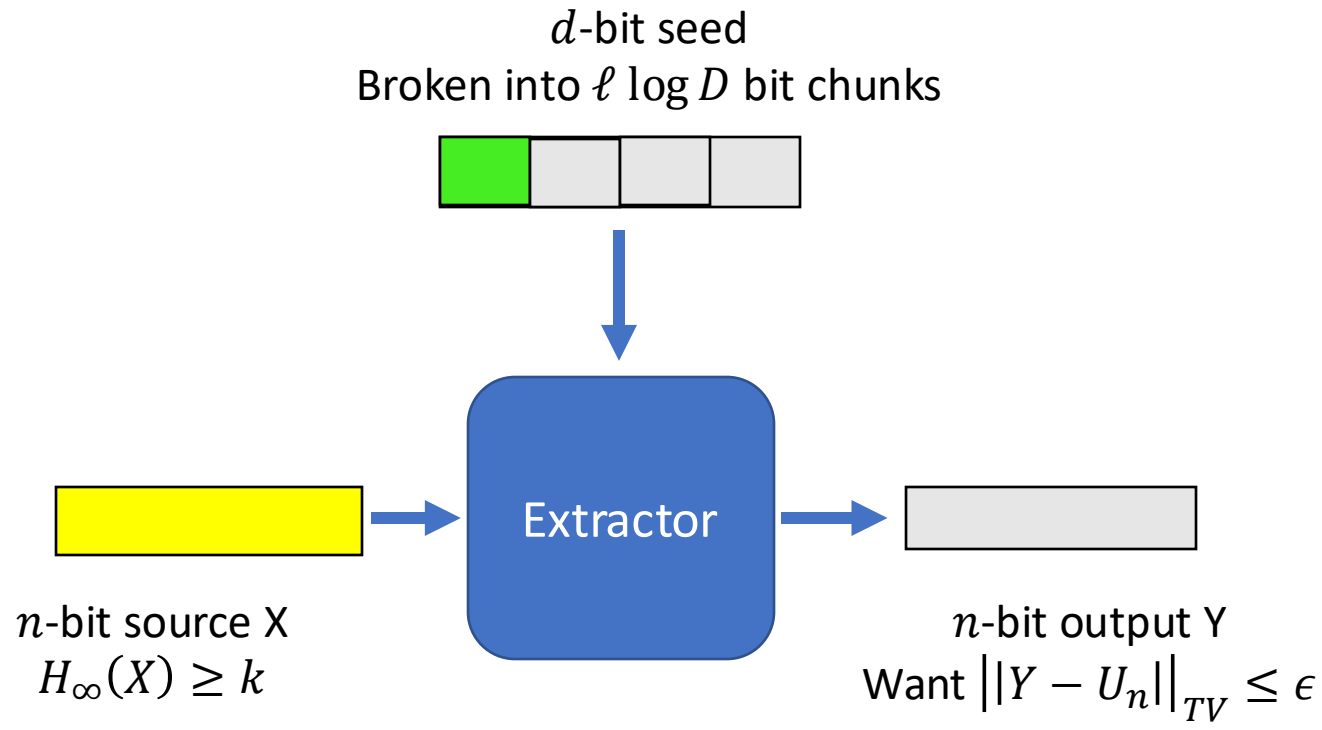
Our extractor

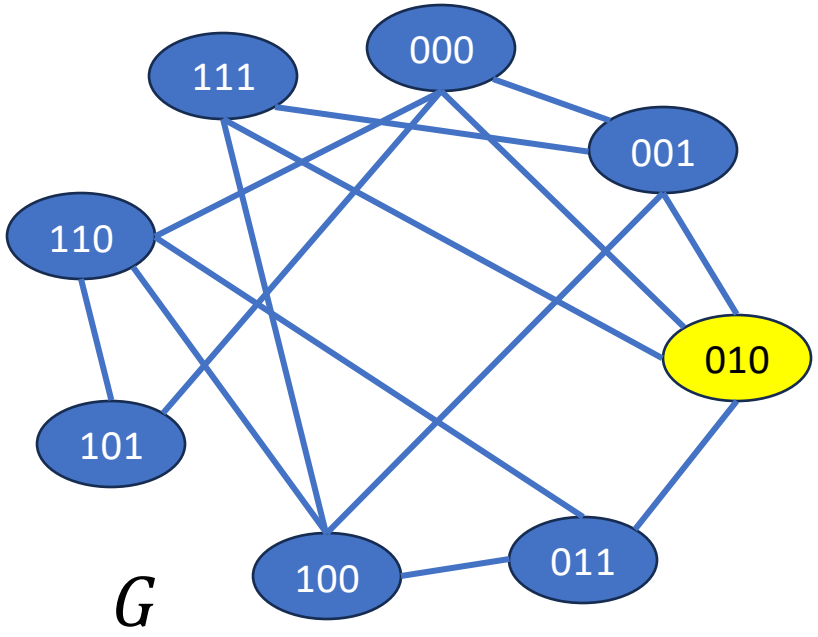
$N = 2^n$, and choose $k \leq n$ and $\epsilon > 0$

Let $d = \ell \cdot \log(D)$, where $\ell = \frac{n-k}{2} + \log\left(\frac{1}{\epsilon}\right)$

G =Degree D graph with N vertices

- Associate each vertex of G with a string in $\{0,1\}^n$
- Take a random walk on G, starting from $x \sim X$, and following a random walk given by the seed $s \sim U_d$.





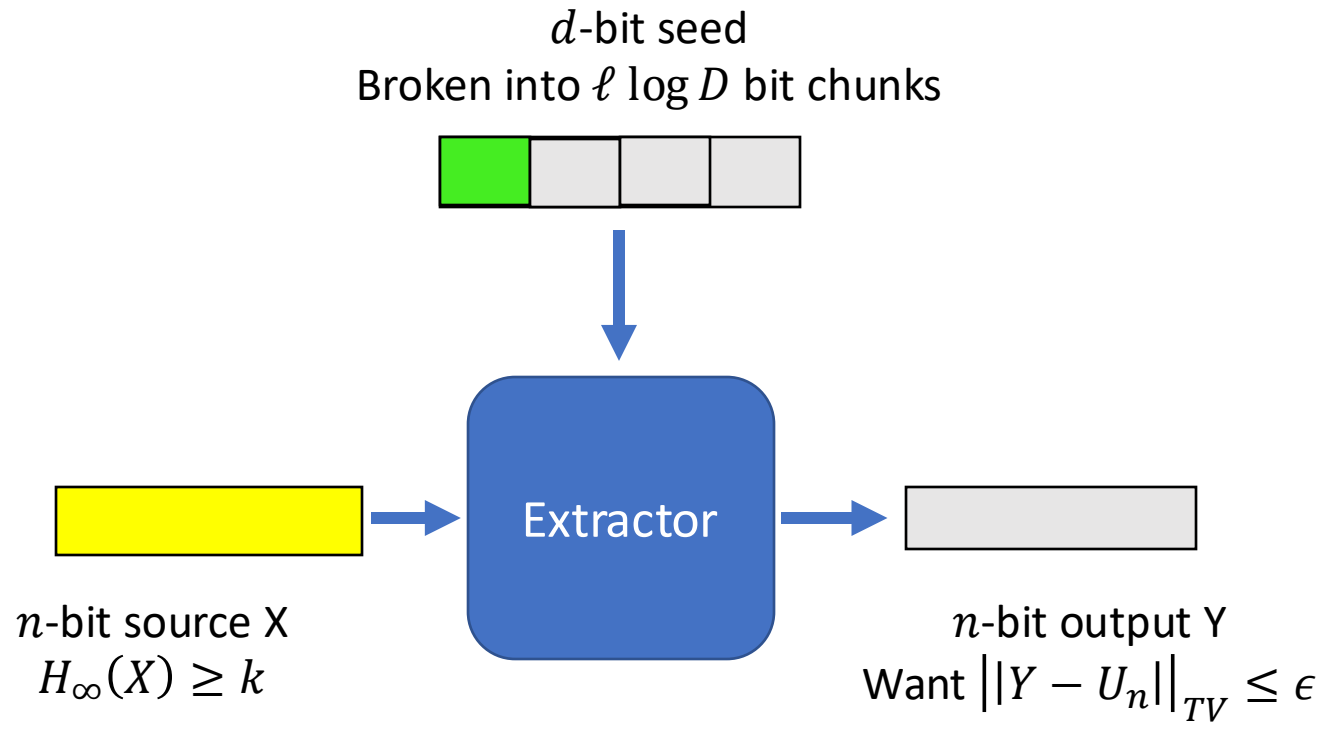
Our extractor

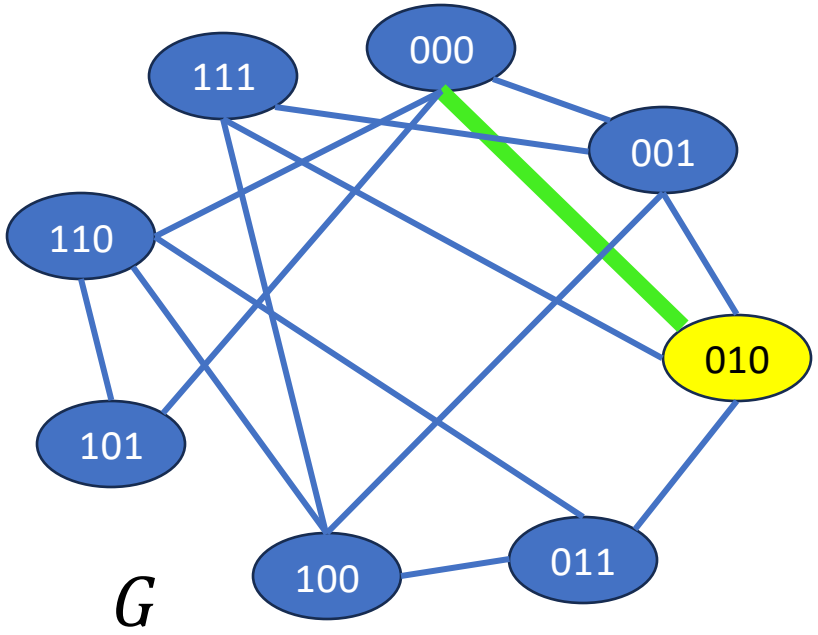
$N = 2^n$, and choose $k \leq n$ and $\epsilon > 0$

Let $d = \ell \cdot \log(D)$, where $\ell = \frac{n-k}{2} + \log\left(\frac{1}{\epsilon}\right)$

G =Degree D graph with N vertices

- Associate each vertex of G with a string in $\{0,1\}^n$
- Take a random walk on G, starting from $x \sim X$, and following a random walk given by the seed $s \sim U_d$.





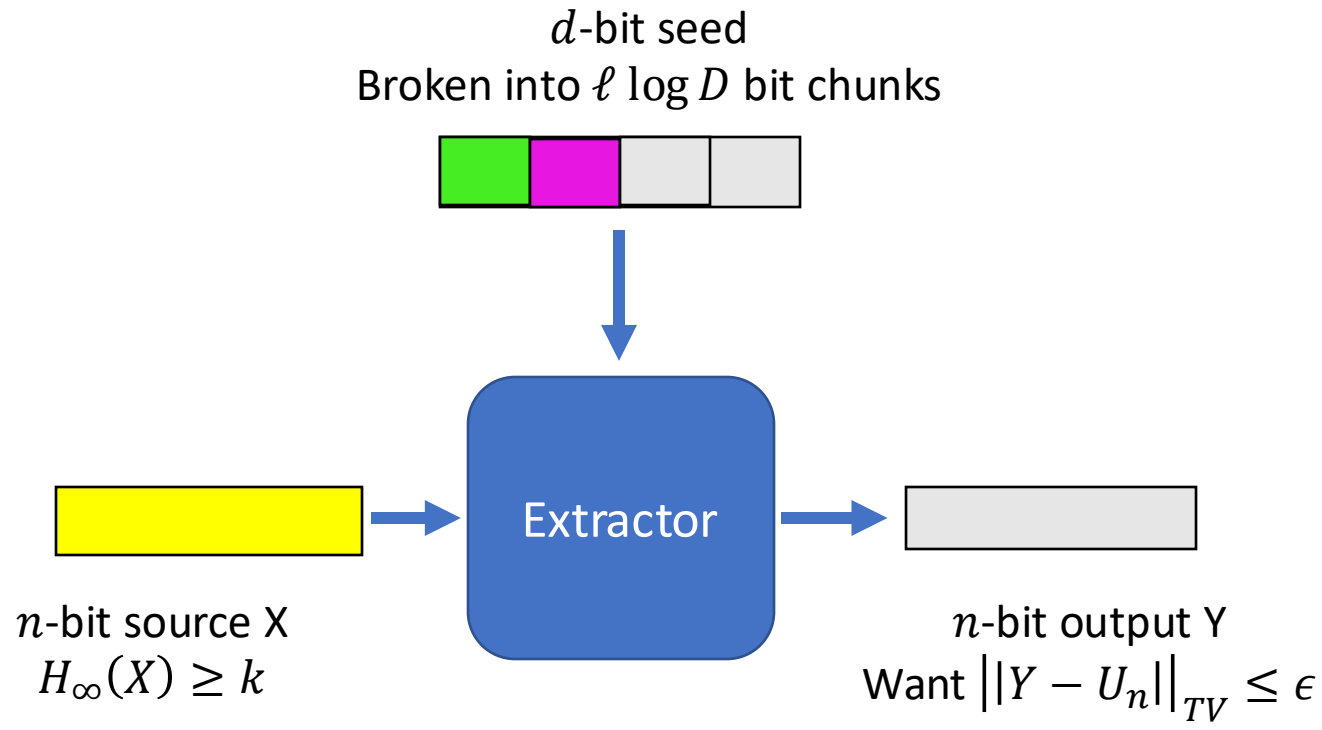
Our extractor

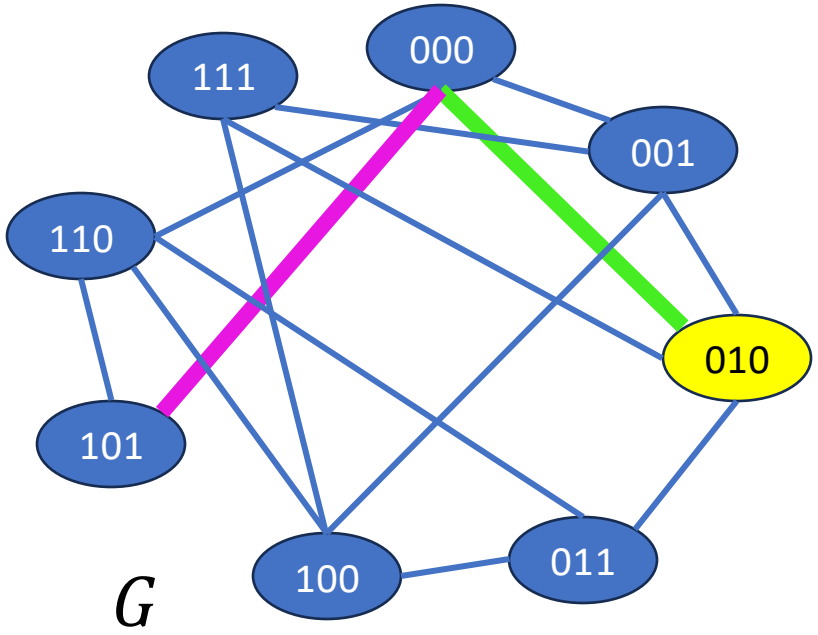
$N = 2^n$, and choose $k \leq n$ and $\epsilon > 0$

Let $d = \ell \cdot \log(D)$, where $\ell = \frac{n-k}{2} + \log\left(\frac{1}{\epsilon}\right)$

G =Degree D graph with N vertices

- Associate each vertex of G with a string in $\{0,1\}^n$
- Take a random walk on G, starting from $x \sim X$, and following a random walk given by the seed $s \sim U_d$.





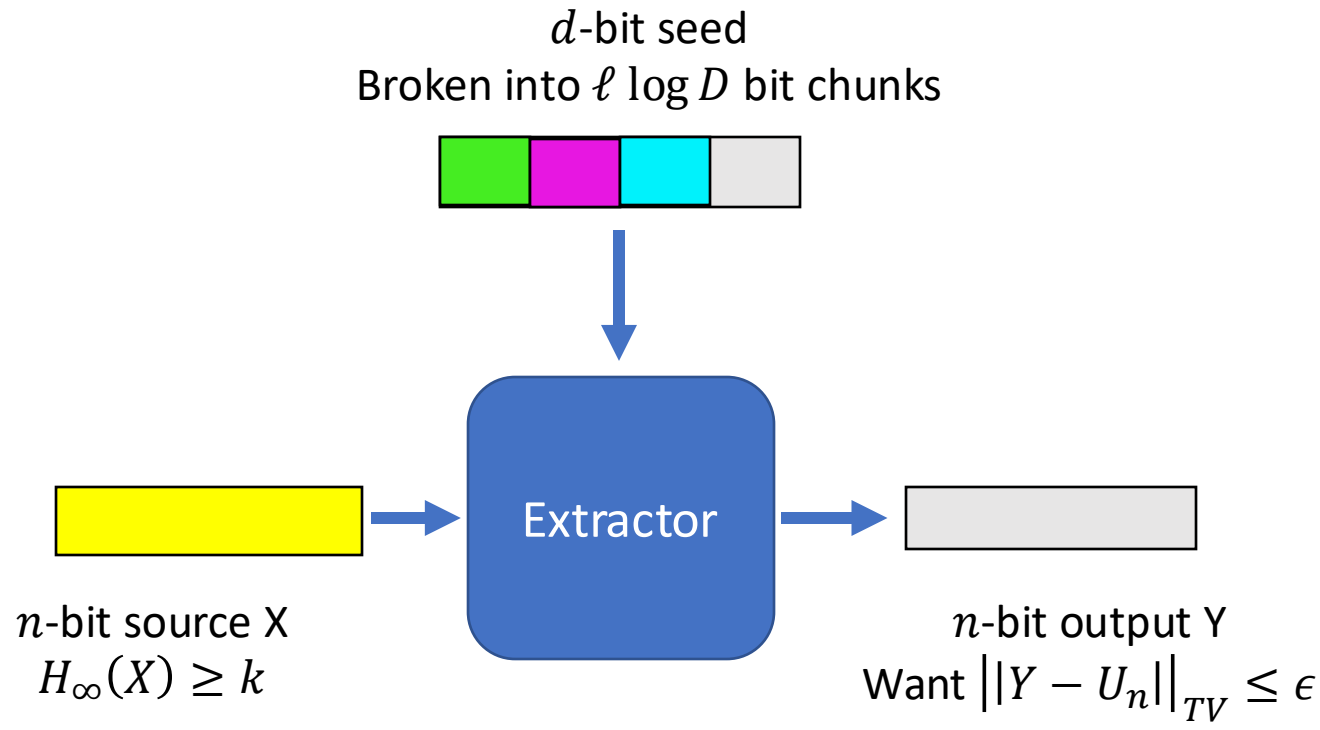
Our extractor

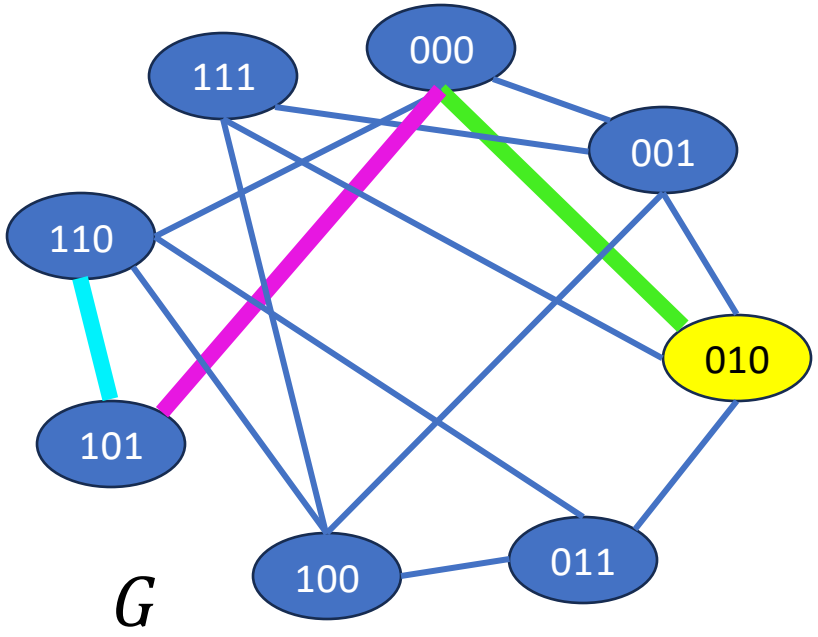
$N = 2^n$, and choose $k \leq n$ and $\epsilon > 0$

Let $d = \ell \cdot \log(D)$, where $\ell = \frac{n-k}{2} + \log\left(\frac{1}{\epsilon}\right)$

G =Degree D graph with N vertices

- Associate each vertex of G with a string in $\{0,1\}^n$
- Take a random walk on G, starting from $x \sim X$, and following a random walk given by the seed $s \sim U_d$.





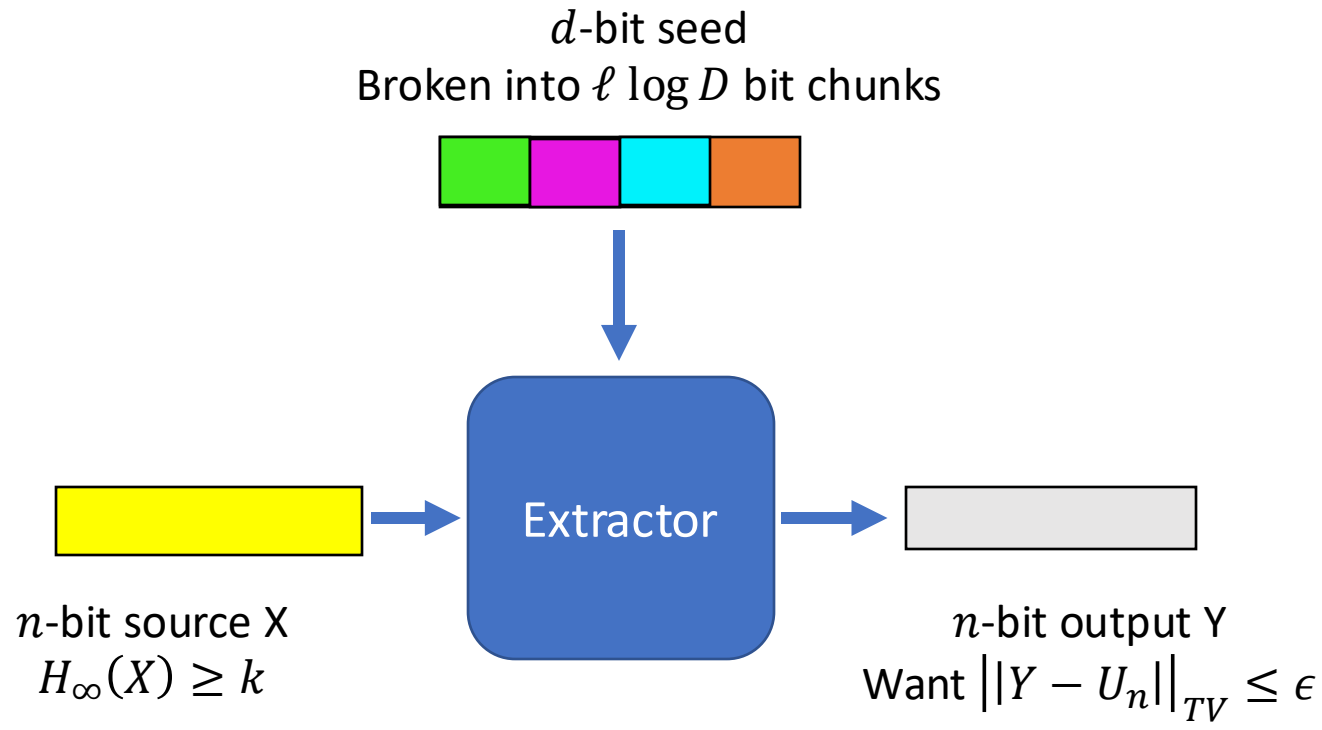
Our extractor

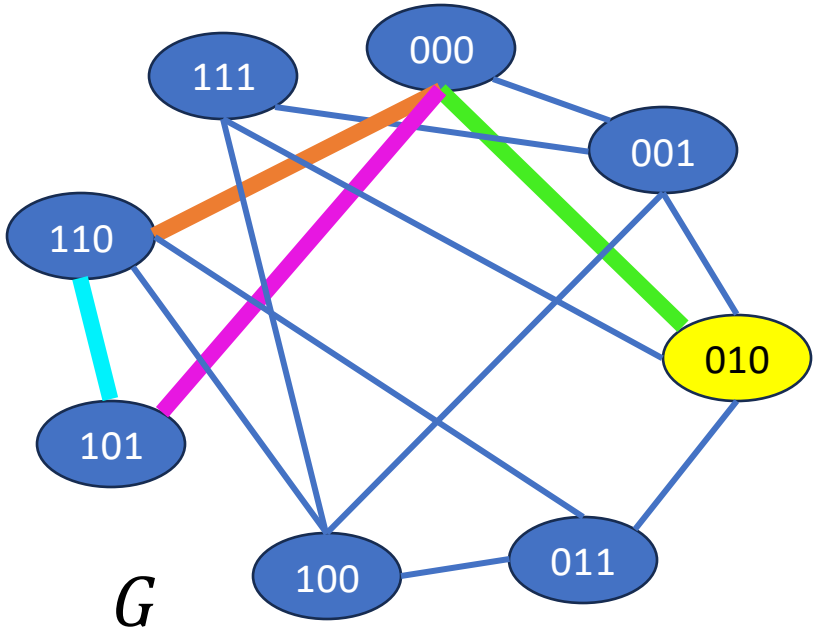
$N = 2^n$, and choose $k \leq n$ and $\epsilon > 0$

Let $d = \ell \cdot \log(D)$, where $\ell = \frac{n-k}{2} + \log\left(\frac{1}{\epsilon}\right)$

G =Degree D graph with N vertices

- Associate each vertex of G with a string in $\{0,1\}^n$
- Take a random walk on G, starting from $x \sim X$, and following a random walk given by the seed $s \sim U_d$.





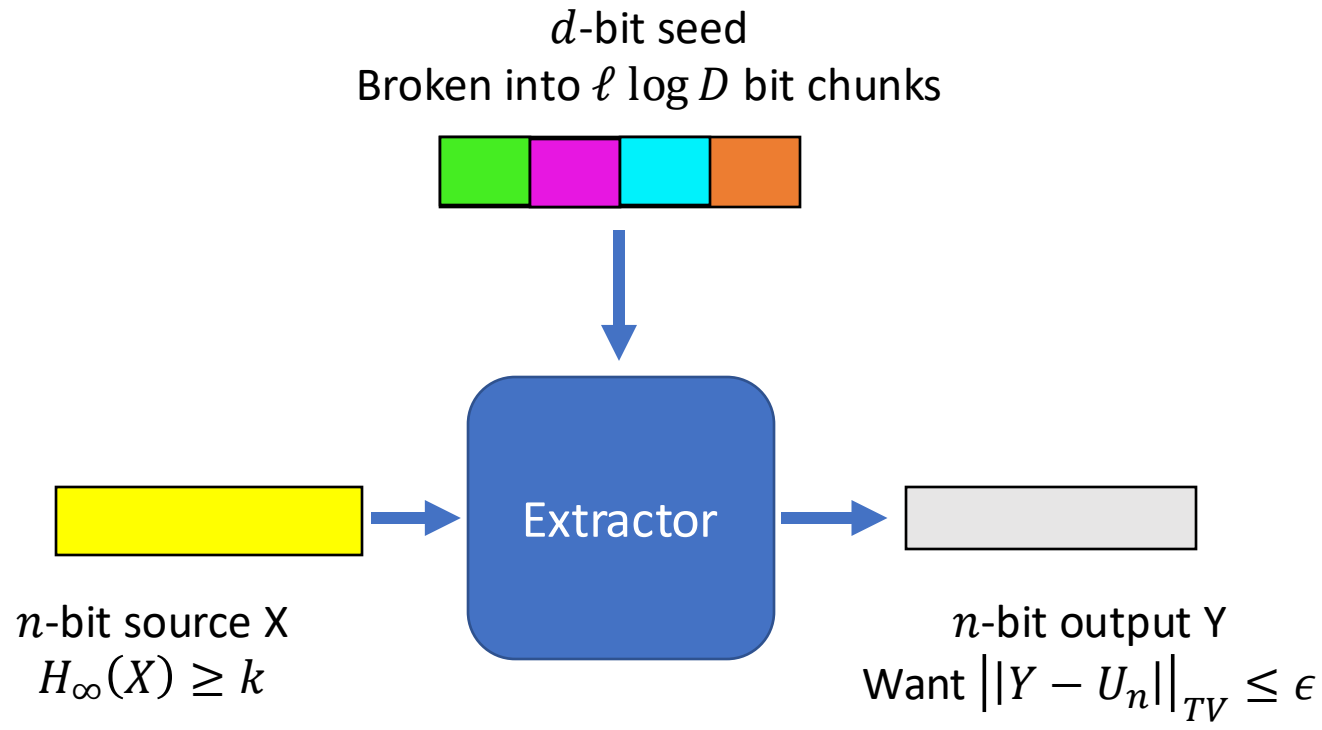
Our extractor

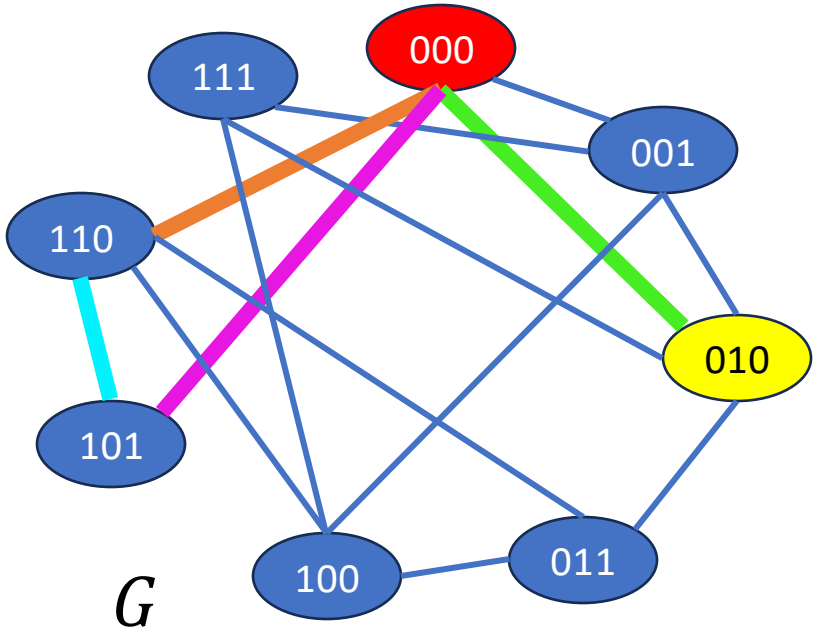
$N = 2^n$, and choose $k \leq n$ and $\epsilon > 0$

Let $d = \ell \cdot \log(D)$, where $\ell = \frac{n-k}{2} + \log\left(\frac{1}{\epsilon}\right)$

G =Degree D graph with N vertices

- Associate each vertex of G with a string in $\{0,1\}^n$
- Take a random walk on G, starting from $x \sim X$, and following a random walk given by the seed $s \sim U_d$.





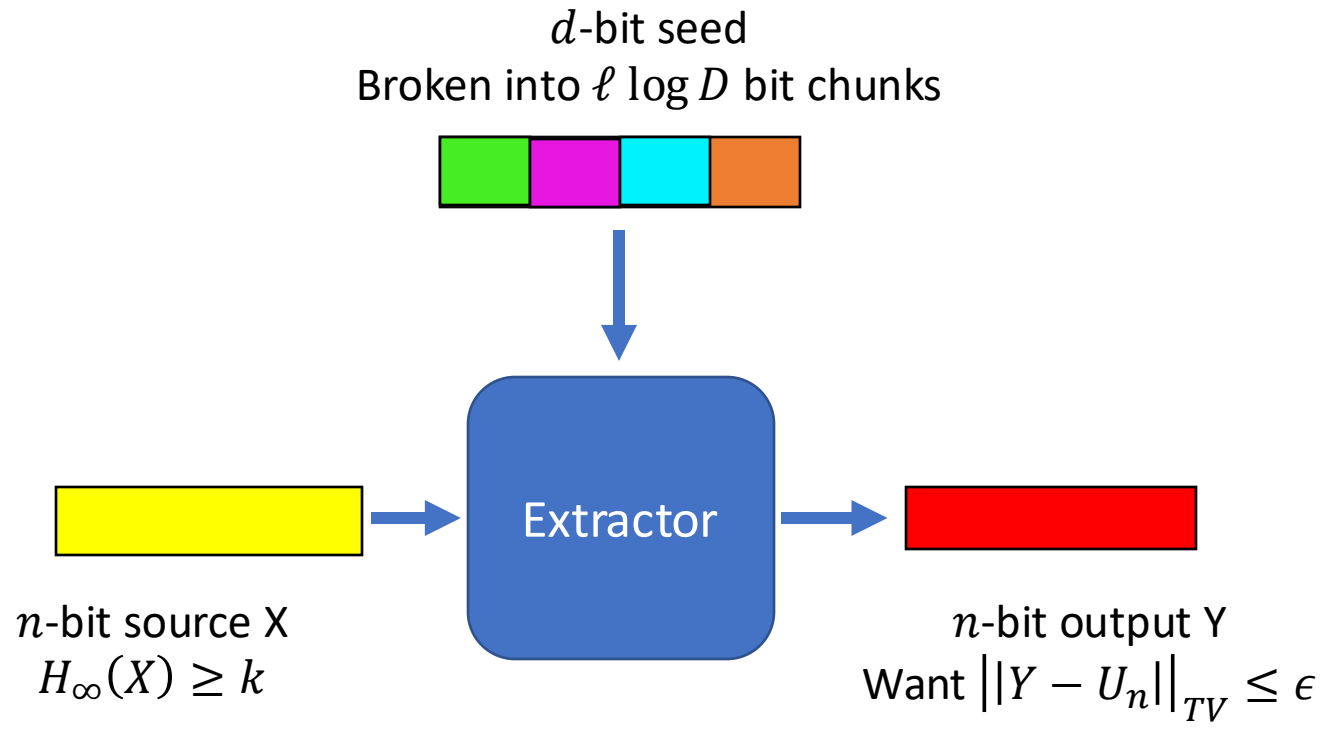
Our extractor

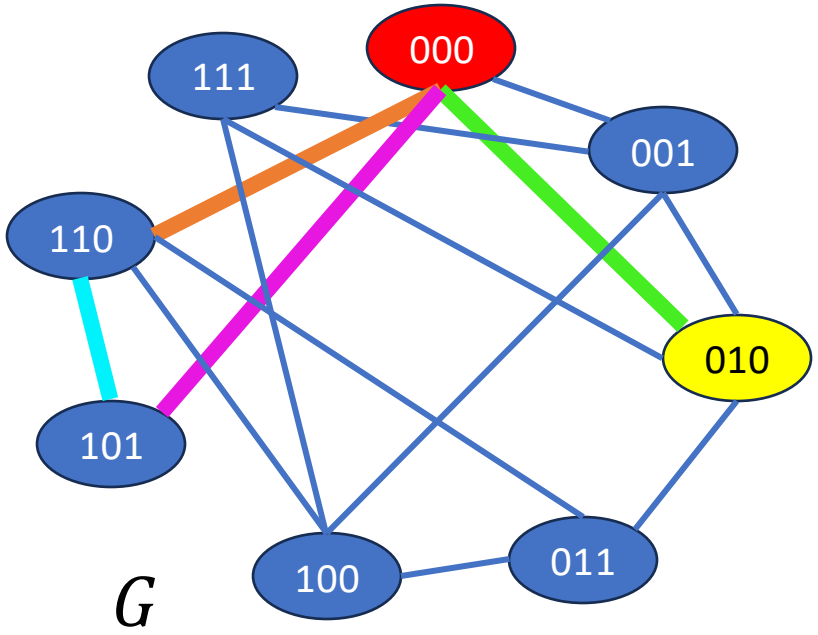
$N = 2^n$, and choose $k \leq n$ and $\epsilon > 0$

Let $d = \ell \cdot \log(D)$, where $\ell = \frac{n-k}{2} + \log\left(\frac{1}{\epsilon}\right)$

G =Degree D graph with N vertices

- Associate each vertex of G with a string in $\{0,1\}^n$
- Take a random walk on G, starting from $x \sim X$, and following a random walk given by the seed $s \sim U_d$.





Claim

- If we choose $\ell = \frac{n-k}{2} + \log\left(\frac{1}{\epsilon}\right)$, then this is a (k, ϵ)-extractor.
  - Seed length: $d = \ell \cdot \log(D) = O(\ell)$
  - Output length: n

This is not as good as our existential result, but it's still non-trivial!

Existential result: $\mathrm{d} = \log(n-k) + 2\log(1/\epsilon) + O(1)$

Group Work: prove the claim!

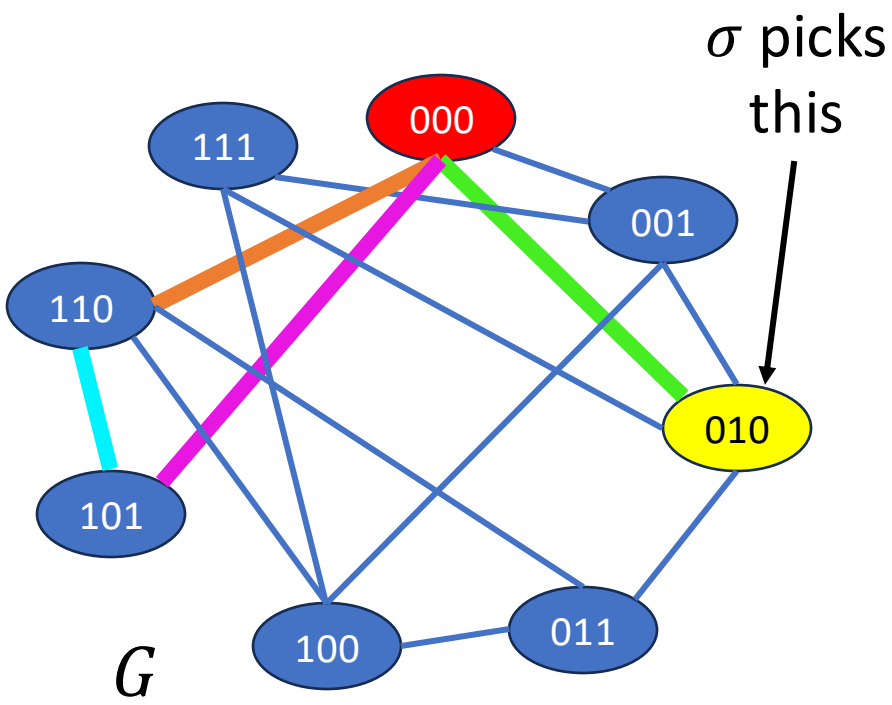
- If we choose $\ell = \frac{n-k}{2} + \log\left(\frac{1}{\epsilon}\right)$, then this is a (k, ϵ)-extractor.
  - Seed length: $d = \ell \cdot \log(D) = O(\ell)$
  - Output length: n

1. Let $\sigma \in \mathbb{R}^n$ represent the probability mass function of our input X. Explain why $Ext(X, U_d) \sim A^\ell \cdot \sigma$, where A is the normalized adjacency matrix for G.
2. Let $\pi = \frac{1}{N}\mathbf{1}$ correspond to the uniform distribution. Explain why $\|U_n - Ext(X, U_d)\|_{TV} = \|\pi - A^\ell \cdot \sigma\|_{TV} \leq \frac{\sqrt{N}}{2}\lambda(G)^\ell \|\pi - \sigma\|_2$
3. Argue that $\|\pi - \sigma\|_2 \leq 2 \cdot 2^{-k/2}$
4. Conclude that $\|U_n - Ext(X, U_d)\|_{TV} \leq \epsilon$, which means that Ext is a (k, ϵ)-extractor.

σ is pmf of X

1. Why is $Ext(X, U_d) \sim A^\ell \cdot \sigma$

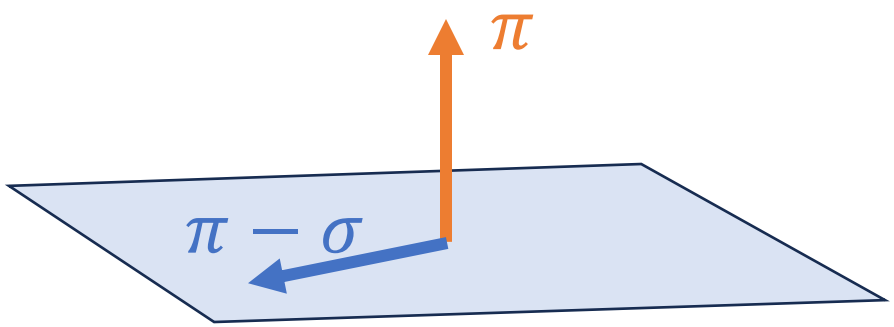
- The output of our extractor is a random walk starting from $v \sim \sigma$
- Distribution after one step is $A\sigma$
- Distribution after ℓ steps is $A^\ell\sigma$



2. Bounding $||U_n - Ext(X, U_d)||$

- Let $Y = Ext(X, U_d)$
- Let π be the uniform distribution.

$$\|\pi - A^\ell \sigma\|_{TV} = \frac{1}{2}\|\pi - A^\ell \sigma\|_1 = \frac{1}{2}\|A^\ell(\pi - \sigma)\|_1$$



Span of all the other eigenvectors
(Eigenvalues $< \lambda(G)$ in magnitude)

$$\leq \frac{\sqrt{N}}{2}\|A^\ell(\pi - \sigma)\|_2$$ Cauchy-Shwarz

$$\leq \frac{\sqrt{N}}{2}\lambda(G)^\ell\|\pi - \sigma\|_2$$ Argument from lecture notes

Every time you hit $\pi - \sigma$ with A:

- The length shrinks by a factor of at least $\lambda(G)$
- We still get something in the **blue** space

Let $\pi = \frac{1}{N}\mathbf{1}$ correspond to the uniform distribution. Explain why

$$\|U_n - Ext(X, U_d)\|_{TV} = \|\pi - A^\ell \cdot \sigma\|_{TV} \leq \frac{\sqrt{N}}{2}\lambda(G)^\ell\|\pi - \sigma\|_2$$

3. Bounding $||\pi - \sigma||_2 \leq 2 \cdot 2^{-k/2}$

$$||\pi - \sigma||_2 \leq ||\pi||_2 + ||\sigma||_2 \leq 2^{-n/2} + 2^{-k/2} \leq 2 \cdot 2^{-k/2}$$

$$||\pi||_2 = \left(\sum_{x \in \{0,1\}^n} \frac{1}{2^n} \right)^{\frac{1}{2}}$$

$||\sigma||_2 \leq 2^{-k/2}$ (Warm-up!)

4. Ext is a (k, ϵ)-extractor

- Let $Y = Ext(X, U_d)$
- Let π be the uniform distribution.

$$\|U_n - Y\|_{TV} \leq \frac{\sqrt{N}}{2} \cdot \lambda(G)^{\ell} \cdot \|\pi - \sigma\|_2$$

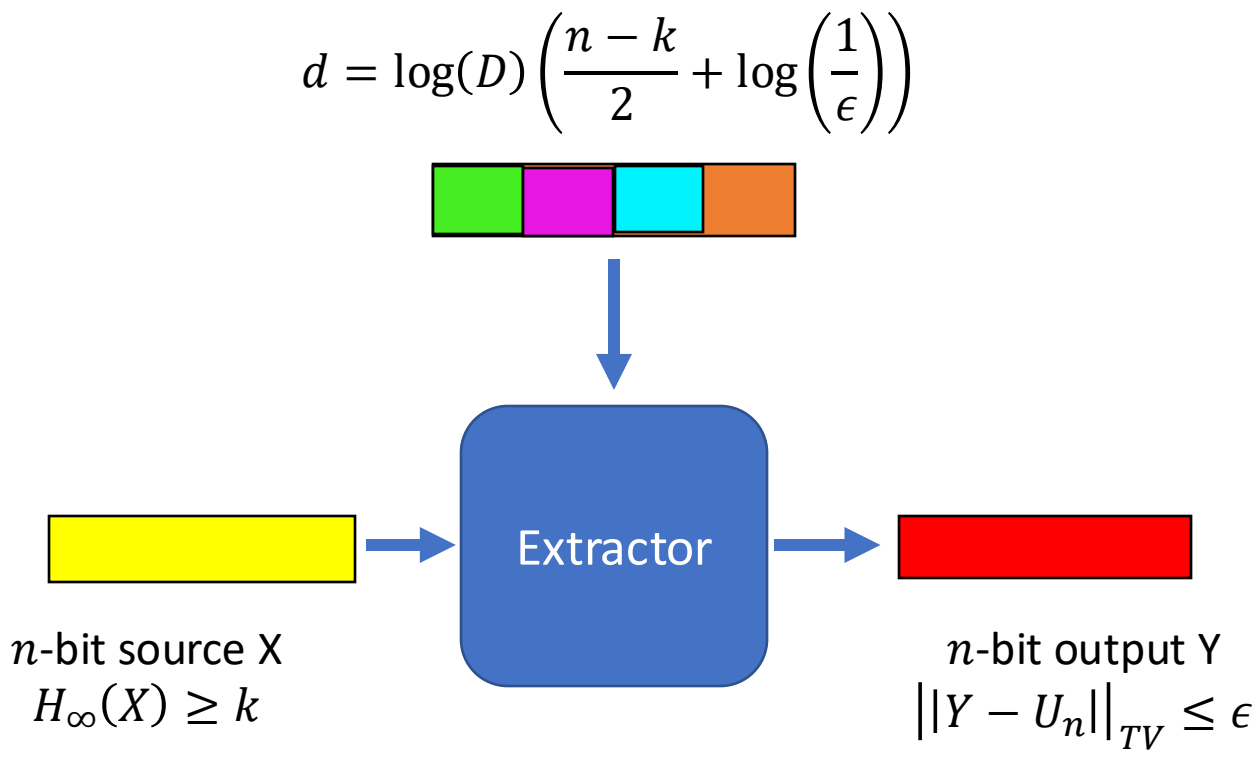
$$\leq \frac{2^{\frac{n}{2}}}{2} \cdot \left(\frac{1}{2}\right)^{\frac{n-k}{2}+\log\left(\frac{1}{\epsilon}\right)} \cdot 2 \cdot 2^{-\frac{k}{2}} = 2^{\log(1/\epsilon)} \leq \epsilon$$

We know:

- $\|U_n - Y\|_{TV} \leq \frac{\sqrt{N}}{2} \cdot \lambda(G)^{\ell} \cdot \|\pi - \sigma\|_2$
- $\|\pi - \sigma\|_2 \leq 2 \cdot 2^{-\frac{k}{2}}$
- $\ell = \frac{n-k}{2} + \log\left(\frac{1}{\epsilon}\right)$
- $\lambda(G) \leq \frac{1}{2}$

Hooray!

- So Ext is a (k, ϵ) extractor.
- It's a pretty good one when $k = n - O(\log n)$, say.
  - In that case the seed length is $O\left(\log\left(\frac{n}{\epsilon}\right)\right)$
- Why do we care? Say we want to use X in a randomized algorithm A.
  - Draw an input $x \in X$
  - Run A on Ext(x, s) for ALL possible seeds s and take majority vote.
  - Fun exercise: this works whp.



Recap

- We can use a good spectral expander to get an okay extractor.
- This extractor is pretty good when k is large!

Bigger Recap…

What just happened?

- Techniques for analyzing randomized algorithms!
  - Linearity of expectation
  - Markov and Chebyshev
  - Chernoff bounds
  - "Poissonization"
  - Metric embeddings/JL transforms
  - The probabilistic method
    - Second moment method
    - LLL
    - Derandomization via conditional expectation
  - Markov chains
    - Mixing times, coupling, spectral methods
  - Martingales
    - Azuma-Hoeffding bound
    - Martingale stopping theorem
  - Pseudorandomness

Plus homework!

And quizzes!

And in-class work!

- Algorithms!
  - Polynomial identity testing
  - Perfect matchings
  - Karger's algorithm for minimum cut
  - Primality testing
  - Sampling-based median
  - Randomized routing
  - Load balancing and the power of 2 choices
  - Bourgain's embedding, and an approximate sparsest-cut algorithm
  - Locality sensitive hashing
  - Compressed sensing
  - Count-min sketch (aka that sketching alg from HW)
  - Deterministic approximation algorithms for k-SAT, Max-Cut
  - Algorithmic LLL
  - Randomized algorithm for 2SAT
  - MCMC, sampling random colorings
  - Consensus algorithms
  - Extractors via expander walks for derandomizing randomized algorithms

Key take-aways

- Randomness is a powerful tool in computation.
- There's a lot of beautiful math that goes into analyzing it.

- I hope that now, you:
  - Are proficient with some techniques for the analysis of randomized algorithms.
  - Have seen enough examples of using these techniques that you can use them in your own work/research/life.

Thanks to the CAs!

Joey

Luna

Nevin

Thank You!!!!!

- For all your hard work, great questions, and engagement throughout the quarter!

That’s all!

…except for HW7 and the final exam