CSE 312

Randomized Algorithms

Primality testing: Given a number $n \geq 2$, is it prime?

If $n > 2$ and prime, $n - 1 = 2^s \cdot d$ where d is odd.

Then:

(1) $a^d \not\equiv 1 \pmod{n}$ $\forall a \not\equiv 1 \pmod{n}$

(2) $a^{2^r \cdot d} \not\equiv -1 \pmod{n}$ $\forall a$ $r = 1, 2, \ldots, \log_2 n$

Choose $a \in \{2, 3, \ldots, n-1\}$ uniformly at random and test that (1) and (2) hold.

If n is <u>not</u> prime: $\mathbb{P}_a[\text{(1) or (2) is violated}] \geq \frac{1}{4}$

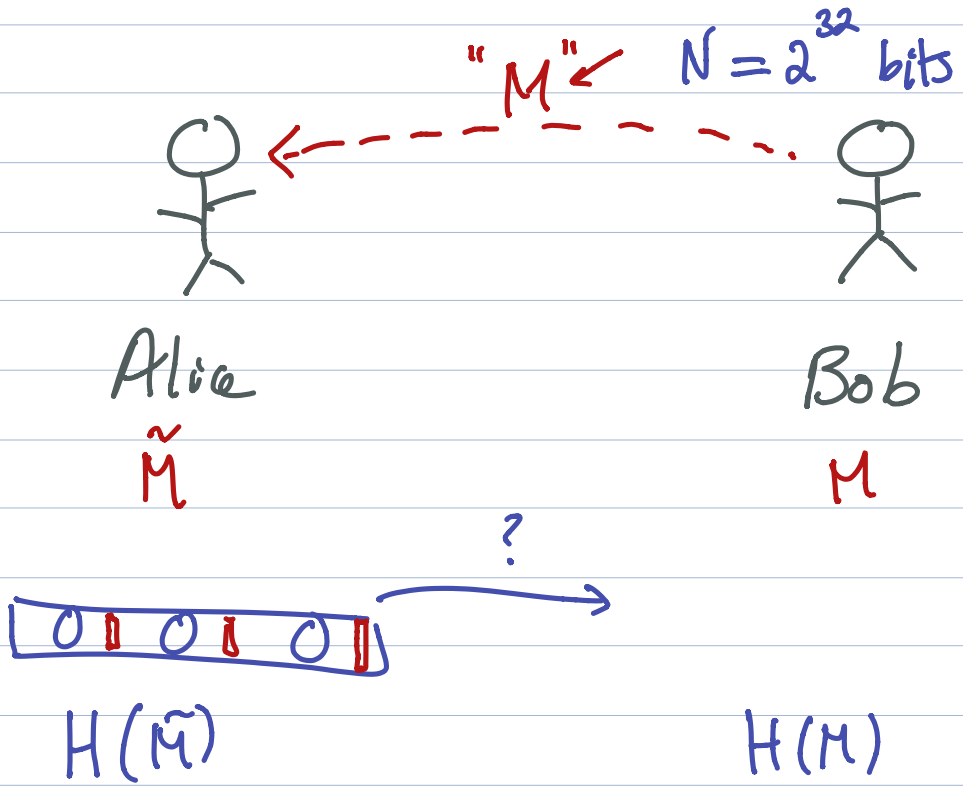
n not prime $\Rightarrow \mathbb{P}[\text{some } a_i \text{ violates (1) or (2)}]$

$a_1, a_2, \ldots, a_k \in \{0, 1, \ldots, n-1\}$

indep.

$$\mathbb{P}[\text{don't find a violation}] \leq \left(\frac{3}{4}\right)^k \qquad k = 20$$

"correctness amplification"



Have Alice generate a random prime p on $\approx c \log_2 N$ bits

$$H(x) = x \bmod p$$

$$H(x) = H(x') \iff p \mid x - x'$$

So if $X \neq X'$, then

$$\mathbb{P}[H(X) \neq H(X')]$$

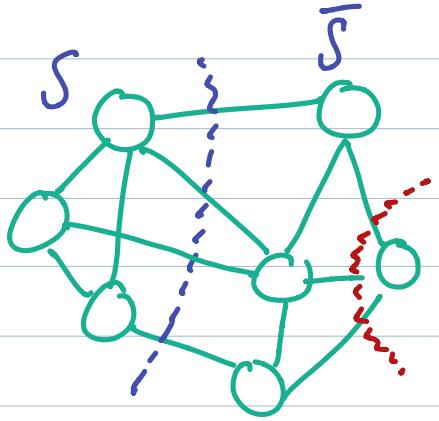
$$\leq \frac{\#\text{ primes that divide } X - X'}{\#\text{ } c \log_2 N\text{-bit primes}}$$

$$\lesssim \frac{\log_2 N}{c \log_2 N / \log\log N}$$

Choosing $c \approx \log\log N$ (< 10 in practice)

gives small error probability.

Min-cut problem:



Input: G undirected graph
Output: Minimum cut in G

Algorithm:
- Choose an edge e uniformly at random in G.
- $G \leftarrow G/e$

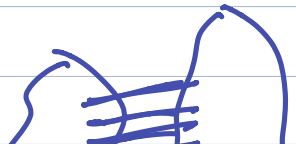
Do this until the graph has two vertices left.
Return the unique cut remaining.

Claim: Let S^* be a minimum cut in G.

$$\mathbb{P}[\text{output } S^*] \geq \frac{2}{n(n-1)}$$

where $n = \#$ vertices in G.

Suppose S^* has k edges



$$\mathbb{P}\left[\begin{array}{c}\text{contract an edge} \\ \text{of } S^* \\ \text{in one step}\end{array}\right] = \frac{k}{\text{total \#edges}}$$

$$\#\text{edges} \geq \frac{kn}{2} \qquad \leq \frac{k}{\frac{kn}{2}} = \frac{2}{n}$$

$$\mathbb{P}\left[\begin{array}{c}\text{don't contract} \\ \text{an edge of } S^* \\ \text{at any step}\end{array}\right]$$

$$\geq \left(1-\frac{2}{n}\right)\left(1-\frac{2}{n-1}\right)\left(1-\frac{2}{n-2}\right) \cdots \left(1-\frac{2}{3}\right)$$

$$= \frac{n-2}{n}\,\frac{n-3}{n-1}\,\frac{n-4}{n-2} \cdots \frac{2}{4}\,\frac{1}{3}$$

$$= \frac{2}{n(n-1)}$$