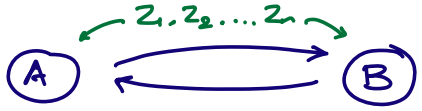
⊙ Randomness & Algebra :

Consider the following communication problem.

Two parties A & B. EQUALITY



string $x \in \{0,1\}^n$ $y \in \{0,1\}^n$

Determine if $x = y$.

→ At least n bits are needed in any deterministic protocol.

With randomness ?

→ With shared randomness.

$z_1, z_2, \ldots, z_n \underset{U}{\in} \{0,1\}^n$

A sends $b = \overline{z} \cdot \overline{x} \pmod 2$

B checks if $b = \overline{z} \cdot \overline{y} \pmod 2$

- If $x = y$ then $\mathbb{P}[\text{Error}] = 0$.

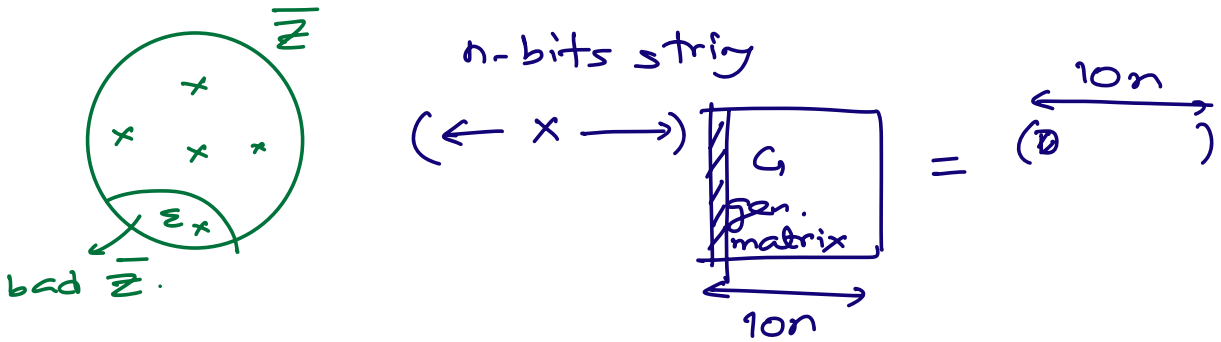
  If $x \neq y$ then $\mathbb{P}[\text{Error}] \leq \frac{1}{2}$

If $w \neq 0$, $\underset{z}{\mathbb{P}}[wz = 0 \pmod 2] \leq \frac{1}{2}$.

- Theorem (Newman):

$$f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$$

If there is a protocol w. shared randomness, error ε, communication C, then there is a protocol with private randomness, communication $C + O(\log n)$ and error $\leq \varepsilon + 1/n$.



If $w \neq 0$ then $w \cdot G$ has Hamming weight at least n.

- Example of generator matrix.

generator for Reed-Solomon code

(Vandermond matrix)

$$(\leftarrow w \rightarrow) \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 2 & \cdots & \ell \\ 0 & 1 & 2^2 & \cdots & \ell^2 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 1 & 2^{n-1} & \cdots & \ell^{n-1} \end{bmatrix} = (\checkmark \ \checkmark \ \checkmark \ \ldots \ \checkmark)$$

$j \quad \sum w_i j^i$

$$P_w(x) = \sum_{i=0}^{n-1} w_i \cdot x^i \quad \text{mod prime } p$$

$$2\ell \geq p > \ell + 1$$

A picks $j \in \{0, \ldots, \ell-1\}$ at random.

Sends j, $P_x(j)$.

⊙ $\mathbb{P}[\text{Error}] \leq \frac{n-1}{\ell+1}$.

Communication: $\log \ell$ bits of randomness.

$O(\log \ell)$ " " $P_x(j)$.

- Freivald's matrix product verification:

Claim: $AB = C$

($n \times n$ matrices)

→ With randomness, $A\left[B\left(w_1^1\right)\right] = C\left(w_1^1\right)$

Union bound: $\mathbb{P}(\text{Error}) \leq \frac{1}{|S|}$.

mult: $O(n^2)$.

- Randomized Algorithm (8th March):

Last time:

$w \in \{0,1\}^n$

$w \neq 0 \Rightarrow \mathbb{P}_{z \in \{0,1\}^n}[w \cdot z = 0 \pmod 2] \leq \frac{1}{2}$.

Application:

(1) A common protocol with public randomness.
where A & B can determine if their strings $x, y \in \{0,1\}^n$ are equal w communication $= k$ bits, $\mathbb{P}[\text{Error}] \leq \frac{1}{2^k}$.

(2) Protocol with private randomness for the equality problem.

Communication $= O(\log n)$ bits. Error $\leq \frac{1}{n}$.

(3) Freivald's algorithm for verifying matrix multiplication.

- To verify if $AB = C$ ($n \times n$ matrices), check $ABz = Cz$ for $z \in \{0,1\}^n$.

$AB = C \Rightarrow \mathbb{P}[\text{Error}] = 0$

$AB \neq C \Rightarrow \mathbb{P}[\text{Error}] \leq \frac{1}{2}$.

- Another communication problem:

A	B
$x \in \{0,1\}^n$	$y \in \{0,1\}^n$

Assume $x \neq y$.

Goal: Determine if $x < y$ or $y < x$, where x & y are treated as integers in $\{0, 1, 2, \ldots, 2^n - 1\}$.

Naive approach:

Check equality & do "divide-and-conquer": (DnC).

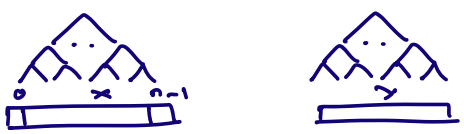
DnC: $\log n$ rounds of communication.

Need $K = \log \log n$ bits of communication per round to get $1/2^K \approx \frac{1}{\log n}$ error prob to use union bound over all rounds.

Total = $O(\log n) \times \log \log n$.

Interesting: We can do it using $O(\log n)$ bits.

- An $O(\log n)$-bit protocol.



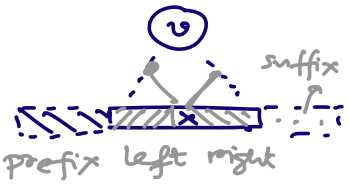
Assume w.l.o.g. n is power of 2

DnC can be thought of a walk along the tree.

- For a node v of the tree

  $prefix_v(x)$, $left_v(x)$, $right_v(x)$

  $prefix_v(y)$, $left_v(y)$, $right_v(y)$



- Initially, v = root.

  If $prefix_v(x) \overset{?}{\neq} prefix_v(y)$ (can be checked using EQUALITY protocol, 10 bits)

  $v = v.parent$

  If $left_v(x) \neq left_v(y)$,

  $v = v.leftchild$

  Else

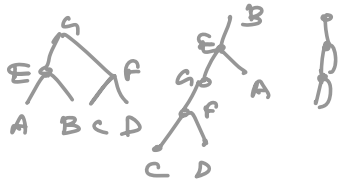
  $v = v.rightchild$.

  Repeat $20 \log n$ times.

If v is a leaf (at ith position), then determine if $x_i < y_i$ or $y_i < x_i$.

- Analysis: Let l be the left most leaf where x & y differ.

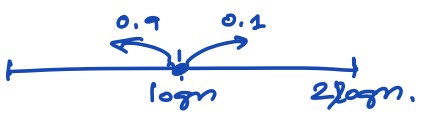
Track $dist(v, l)$.



<u>Claim:</u> If $dist(v_t, l) > 0$, then

$$\mathbb{P}[dist(v_{t+1}, l) = dist(v_t, l) - 1] \geq 1 - \frac{1}{2^k}$$

$$\geq 0.9$$



$T = 20 \log n$.

$\mathbb{P}[\text{dist}(v_t, \ell) > 0] \leq \frac{1}{n}$. (Chernoff)

– Expecting $18 \log n$ net movement, we want only $\log n$.

- $W \cdot Z$ is a polynomial of degree 1 in $Z_1, Z_2, \ldots, Z_n$.
- Polynomial Identity Lemma: (Schwartz-Zippel, DeMillo, Lipton, Ore, ..]

Let $p(Z_1, Z_2, \ldots, Z_n)$ be a nonzero polynomial over a field $\mathbb{F}$ of total degree $\leq d$

[Every monomial $Z_1^{e_1} Z_2^{e_2} \cdots Z_n^{e_n}$ with nonzero coefficient satisfies $\sum_{i=1}^{n} e_i \leq d$].

Then $\mathbb{P}_{(z_1, \ldots z_n) \in S^n} [p(z_1, \ldots, z_n) = 0] \leq \frac{d}{|S|}$.

($S \subseteq \mathbb{F}$)

Proof: by induction of #variables (n).

$$p(\bar{z}) = p_k(z_2, \ldots, z_n) z_1^k + p_{k-1}(z_2, \ldots, z_n) z_1^{k-1} + \ldots + p_0(z_2, \ldots, z_n).$$

event $p(\bar{z}) = 0 \subseteq \{(p_k(z_2, \ldots, z_n) = 0)\}$ or $\{[(p_k(z_2, \ldots, z_n) \neq 0) \text{ and } p(\bar{z}) = 0]\}$.

$$\mathbb{P}[p(\bar{z})=0] \le \mathbb{P}[p_k(z_2,\dots,z_n)=0] + \mathbb{P}[\cdots]$$

$$\le \frac{d-k}{|S|} + \mathbb{P}[p(\bar{z})=0 \mid p_k(z_2,\dots,z_n) \neq 0]$$

$$\le \frac{d-k}{|S|} + \frac{k}{|S|}$$ [univariate nonzero polynomial of degree k]

$$= \frac{d}{|S|}.$$ ∎

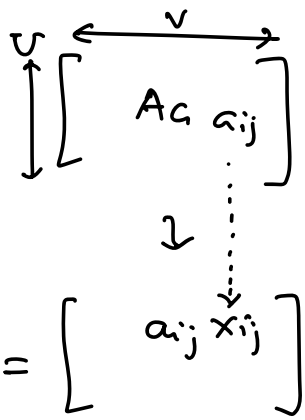
⊙ Applications:

- Bipartite Matching:

Given: A bipartite graph $G = (U \cup V, E)$

Goal: Does G have a perfect matching?

Consider adjacency matrix:



$$M = \begin{bmatrix} & a_{ij}x_{ij} & \\ & & \end{bmatrix}.$$

$\det(M)$ = polynomial in $\{x_{ij}\}$ of total degree $\le n$.

- G has a matching iff $\det(M)$ is a nonzero polynomial.

Substitute for x_{ij} random values from $\{1, 2, \ldots, n^2\}$, then from polynomial identity lemma;

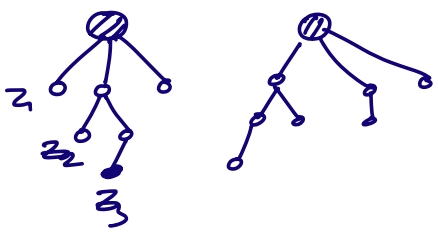
$$\mathbb{P}[\text{Error}] \leq \frac{n}{n^2} = \frac{1}{n}.$$

- Note: $\det(M)$ can be computed efficiently in parallel.

MATCHING $\in$ RNC.

⊙ Application: Tree isomorphism.

T_1 & T_2 are unordered rooted trees.

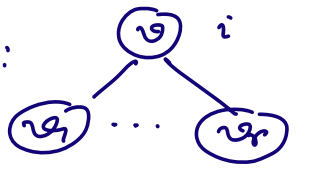


keep one variable for each level.

$z_0, z_1, \ldots, z_l$ (l = length of longest root to leaf path)

If v is a leaf then $p_v = z_i$.
at level i

For a node :



$(z_i - p_{v_1})$
$(z_i - p_{v_2})$
...
$(z_i - p_{v_i})$.

- Unique factorization of polynomials implies $p_{T_1} = p_{T_2}$ iff $T_1 \cong T_2$.

Degree $(p_T) \leq$ #nodes $= n$.

Pick $z_1, z_2, \ldots, z_k \in \{0, \ldots, n^2\}$.

[We don't need to open the polynomial & compute. We do it efficiently like a circuit].

$O(1)$ amount comm. with shared randomness. ✓.

° Randomized Algo:

• Algebra & Randomization:

Input: A positive integer N (n bits)

Output: 1 if N is prime
0 if N is composite

- If $N = 2$, output 1.
- If N is even or $N = 1$, then output 0.
- If $N = a^b$ $(a, b \geq 2)$ then output 0.

Fermat's little theorem:

If N is prime then

$a^{N-1} \equiv 1 \pmod N$

for all $a \in [N-1]$

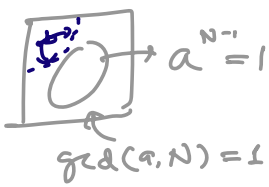
- Flag = 0.
- Repeat 5 times:
  - Pick $a \in \{1, 2, .., N-1\}$ uniformly
  - if $a^{N-1} \neq 1$ then output 0.
  - if $a^{(N-1)/2} \neq \pm 1$ then output 0.
  - if $a^{(N-1)/2} = -1$ then Flag = 1.

$b = a^{(N-1)/2}$

If N is prime then

$b^2 = 1 \pmod N$

$\Rightarrow (b+1)(b-1) = 0 \pmod N$

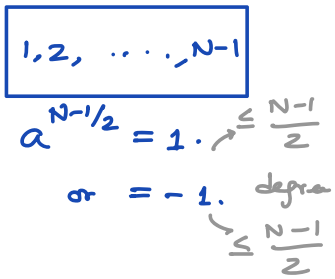


- If (Flag == 1), then output 1.
  else output 0.

- **Proof of correctness:**

Claim: If N is prime then $\mathbb{P}[\text{Error}] \leq 1/2^5$.

→ we can only make error in the third step w.p. $= \frac{1}{2}$



Claim: If N is composite then

$$\mathbb{P}[\text{Error}] \leq \frac{1}{2^5}.$$

Suppose $\exists\, a \in \{1, 2, \ldots, N-1\}$ s.t. $a^{\frac{N-1}{2}} = -1 \pmod N$ [otherwise, there is no error].

This implies that for at least half of b s.t. $b^{N-1} = 1 \pmod N$, $b^{(N-1)/2} \neq \pm 1 \pmod N$.

Let $N = N_1 \times N_2$ s.t. $\gcd(N_1, N_2) = 1$.

$\mathbb{Z}_N = \mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2}$. this is actually isomorphism between two rings.

$a \longmapsto (a \bmod N_1,\ a \bmod N_2)$.

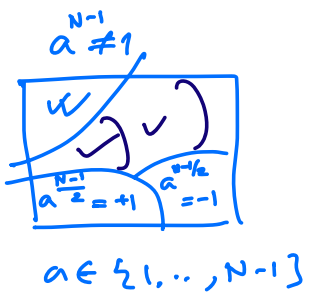
$1 \longmapsto (1, 1)$

$-1 \longmapsto (-1, -1)$.

$\alpha \longleftarrow (1, -1)$

$\beta \longleftarrow (-1, 1)$

} Squares are 1, but they are neither $+1$ nor -1.



$a = (a_1, a_2)$

$a^{(N-1)/2} = (a_1^{(N-1)/2},\ a_2^{(N-1)/2}) = (-1, -1)$.

$(a_1, 1) \xrightarrow{u}$ raise to power $\frac{N-1}{2}$ will give $(-1, 1)$.

Similarly, $(1, a_2) \xrightarrow{v}$.

$u^{\frac{N-1}{2}} = (-1, 1)$.

$v^{\frac{N-1}{2}} = (1, -1)$.

$a_1 \longmapsto (\alpha, \beta)$

$a_2 \longmapsto (\alpha, \beta)$

$\Downarrow$

$a_1 = a_2$.

$N_1 \mid a_1 - a_2$.

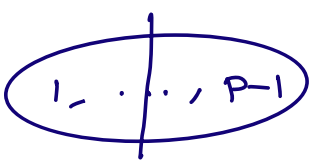
$N_2 \mid a_1 - a_2$

$\Rightarrow N_1 N_2 \mid a_1 - a_2$ $(\because \gcd(N_1, N_2) = 1)$.

(Chinese remainder theorem).

⊙ Solving quadratic equations (mod p):

$x^2 + bx + c = 0$.



$a^2, (-a)^2$

quadratic residues & nonresidues mod p.

- There is no known deterministic polytime algorithm.

$$\frac{-b \pm \sqrt{b^2 - 4c}}{2}$$ ← Need to find root of $b^2 - 4c$.

- Q. How to solve $x^2 - c \stackrel{?}{=} 0$.

$x^2 - c = (x - \alpha)(x - \beta)$

$\{0, 1, 2, \ldots, p-1\}$

$A(x) = x^{(p-1)/2} - 1.$

$B(x) = x^{(p-1)/2} + 1.$

Compute $\gcd(x-\alpha,\ x^{(p-1)/2} - 1)$

$= (x-\alpha)$ if β is not a root of $A(x)$ & α is not a root of $A(x)$.

$x \leftarrow rx + s. \quad r, x \sim [p-1].$

⊙ $Q(x) = (x-\alpha)(x-\beta).$

unknown

Pick $(r, s) \in \{1, \ldots, p-1\} \times \{0, \ldots, p-1\}.$

Consider $Q(rx+s) = \underbrace{a(x^2 + b'x + c')}_{\hat{Q}}.$

Suppose $\gcd(\hat{Q}, A)$

$= x - \gamma.$

$\hat{Q}(x)$

$(x-\alpha)(x-\beta) \mapsto (rx+s-\alpha)(rx+s-\beta).$

$= r^2\left(x - \left(\frac{\alpha-s}{r}\right)\right)\left(x + \left(\frac{\beta-s}{r}\right)\right).$

$r\gamma + s = \alpha$ or $\beta.$ ← this is one root.

We are finding, $\frac{\alpha-s}{r} = l_1, \ \frac{\beta-s}{r} = l_2$

i.e., $\alpha = rl_1 + s, \quad \beta = rl_2 + s.$

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} l_1 & 1 \\ l_2 & 1 \end{pmatrix} \begin{pmatrix} r \\ s \end{pmatrix}.$$

M.

As $l_1 \neq l_2$, M is non-singular.

• Randomized Algorithms :

$x_S : \{0,1\}^n \longrightarrow \{0,1\}$, $S \subseteq [n]$.

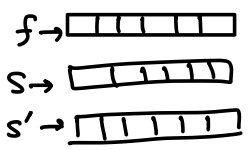
$$x \longmapsto \sum_{i \in S} x_i \pmod 2$$

Given: Access to $f : \{0,1\}^n \longrightarrow \{0,1\}$

$$\mathbb{P}[f(x) = x_S(x)] \geq \frac{1}{2} + \varepsilon, \quad \varepsilon > 0.$$

Goal: Determine S.

(2^n values)
Truth table



- If $\varepsilon > 1/4$, then S is unique.
  - If both S & S' agree w. $f > 3/4$, then S & S' agree with each other is $> 1/2$.

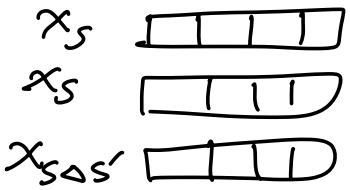
To compute $x_S(x)$: $f(r) + f(r+x)$ (where $f(r) = x_S(r)$, $f(r+x) = x_S(r+x)$)

where $r \in_U \{0,1\}^n$.

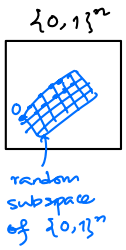
Then we get success w.p. $\frac{1}{2}+\delta$. → independently + Chernoff

Repeat say $10 \log n$ times, w.h.p. majority of the value will give you the correct input.

Compute $x_S(e_1), x_S(e_2), \ldots, x_S(e_n)$.



Any two parities agree & disagree at exactly half of the places.

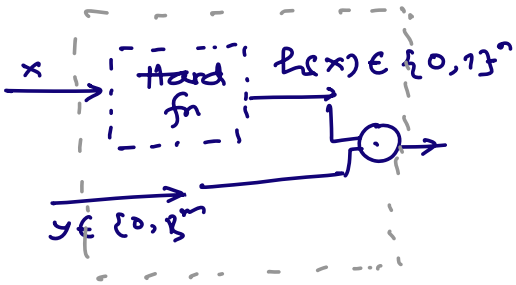


Suppose $0 < \varepsilon \leq 1/4$.

$$\left|\{S \text{ s.t. } \mathbb{P}_x[f(x) = \chi_S(x)] \geq \tfrac{1}{2} + \varepsilon\}\right| \leq O\left(\tfrac{1}{\varepsilon^2}\right)$$

Goal: Given access to f, list all such S in time poly$(n, 1/\varepsilon)$.

Goldreich-Levin Theorem.



- **Algorithm:** $(t \approx \log(\frac{n}{\varepsilon^2}))$.

  Pick $v_1, v_2, \ldots, v_t$ uniformly at random from $\{0,1\}^n$.

  for $T \subseteq [t]$, define $v_T = \sum_{i \in T} v_i$. (2^t vectors are produced)

- Guess bits $\bar{a} = (a_1, a_2, \ldots, a_t) \in \{0,1\}^t$

  Define $a_T = \sum_{i \in T} a_i$

- To compute $x_S(e_i)$: ($2^t - 1 = N$.)

majority $\{ a_T + f(v_T + e_i) : T \subseteq [t], T \neq \phi \}$.

(a_T: $T \subseteq [1,2,3]$; v_T: $T \subseteq [1,4,7]$.)

Claim: If $T \neq \phi$, then $v_T \in_U \{0,1\}^n$.

Claim: If $T \neq T'$, then $v_T, v_{T'}$ are independent (pairwise).

[Note they are not mutually independent.

$v_{\{1\}}, v_{\{2\}}, v_{\{1,2\}}$ → are not pairwise indep but not mutually indep.].

- If $\bar{a} = (x_S(v_1), x_S(v_2), \ldots, x_S(v_t))$

then $b_T = a_T + f(v_T + e_i)$

are pairwise independent.

& $\mathbb{P}[b_T = x_S(e_i)] \geq \frac{1}{2} + \varepsilon$.

- $\mathbb{P}$[Majority is incorrect, i.e. $maj(b_T) \neq x_S(e_i)$]

By Chebyshev. $\leq \frac{Var}{Dev^2} \leq \frac{N}{(\varepsilon N)^2} = \frac{1}{\varepsilon^2 N}$.

Set $t = \log\left(\frac{10n}{\varepsilon^4} + 1\right)$.

$\mathbb{E}$[# number of b_T's] $\geq \frac{N}{2} + \varepsilon N$.

$Var \leq n$.

[∵ There are $\{0,1\}$ variables & there are n variables]

So $N = \frac{10n}{\varepsilon^4} \Rightarrow \mathbb{P}[\text{Error}] = \frac{1}{\varepsilon^2 N} = \frac{\varepsilon^2}{10n}$.

By union bound if

$$a = (x_S(v_1), x_S(v_2), \ldots, x_S(v_t)).$$

$\mathbb{P}[\text{Maj decodes each } x_S(e_i) \text{ correctly}]$

$$\geq 1 - \varepsilon^2/10.$$

$\bar{a} :=$

Cycle through all choices of $(a_1, \ldots, a_t)$.

For each compute Majority (b_f) & determine an S.

Let $P = \{S : S \text{ is generated for some choice } \bar{a}\}$.

<u>Claim</u>: S good if $\mathbb{P}[x_S(x) = f(x)] \geq \frac{1}{2} + \varepsilon$,

$\mathbb{P}[\forall \text{ good } S,\ S \in P] \geq 9/10$.