Interactive proof

Verifiable Computation (VC)

server

client

function f

result = f(data) + 

digest δ

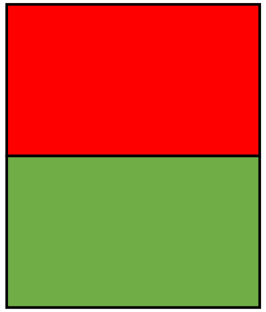
Verification: ✔ **or** ☐

data

Correctness/completeness: Pr[result = f(data) and proof is honest and verification is ✓] = 1

Soundness/security: Pr [result ≠ f (data) and verification is ✓] ≤ $\frac{1}{2^{100}}$

Power of randomness



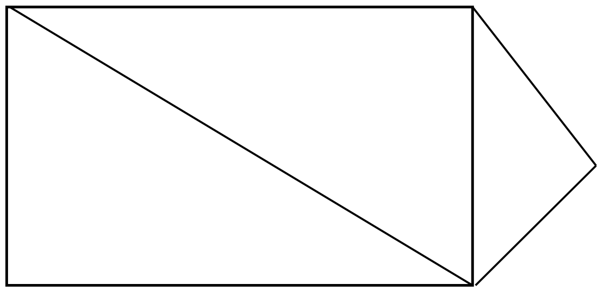
Same or different?

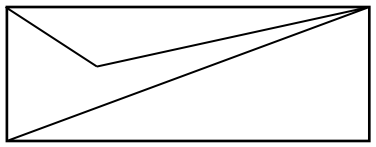
Different colors

1. Pick a random bit b
2. If b=0, flip the paper; otherwise, do nothing
3. Ask if the paper is flipped or not

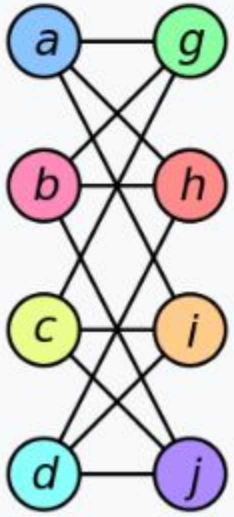
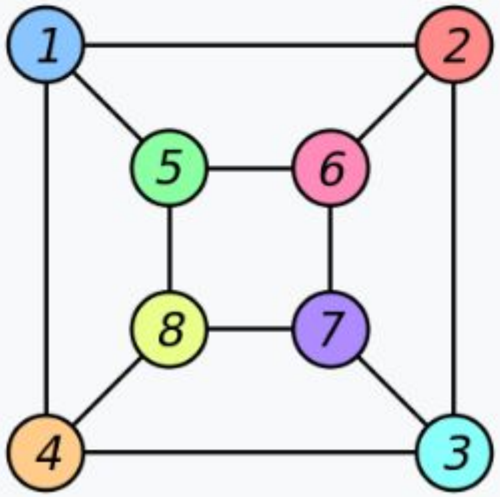
Correctness: 1
Soundness: 1/2

Graph isomorphism



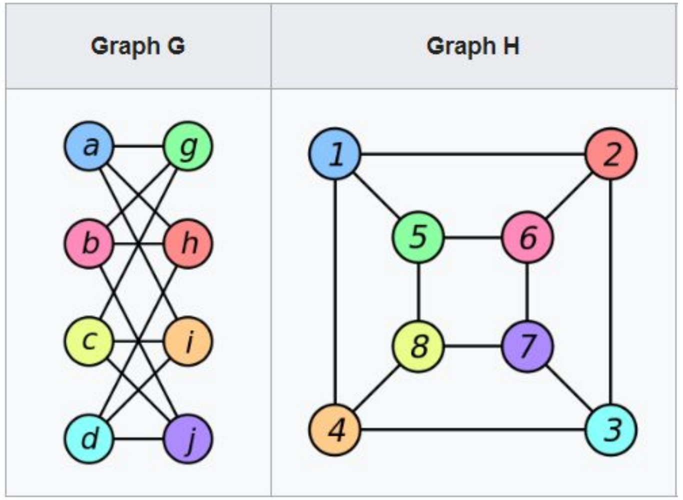


- NP problem
  - Hard to find π
  - Easy to verify

Graph G	Graph H	An isomorphism between G and H
		$f(a) = 1$ $f(b) = 6$ $f(c) = 8$ $f(d) = 3$ $f(g) = 5$ $f(h) = 2$ $f(i) = 4$ $f(j) = 7$

Isomorphic or not

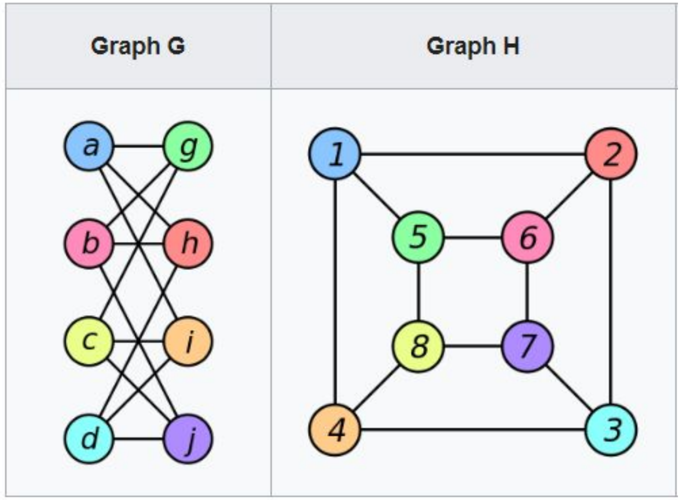
Yes, proof is π



Graph non-isomorphism

Isomorphic or not

No, proof?

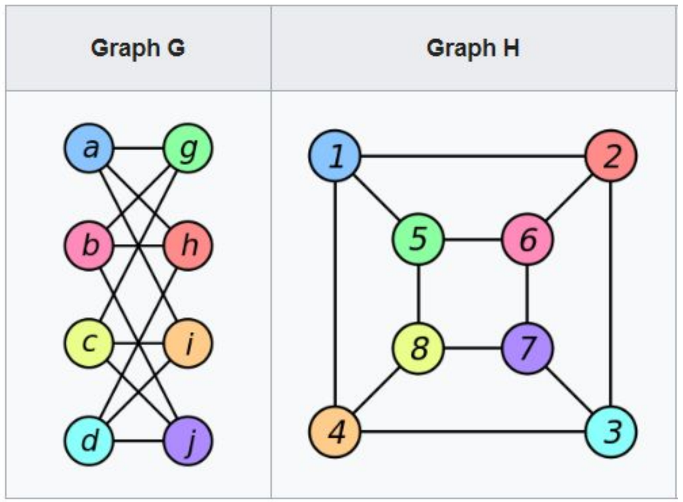


Power of randomness

Isomorphic or not

No, proof?

1. Pick a random bit b
2. If b=0, pick a random permutation π, generate graph I = π(G);
3. If b=1, pick a random permutation π, generate graph I = π(H);
4. Send graph I, ask what is bit b



Correctness: 1
Soundness: 1/2

Polynomial expansion

Expand $f(x)$ for me $\longrightarrow$

$\longleftarrow$

$g(x) = 6x^3+49x^2+128x+105$

Polynomial expansion

$f(x) = (x+3)(3x+5)(2x+7)$

Verification: pick a random value r

test $f(r) - g(r) = 0$

Schwartz–Zippel lemma

If $f(x) - g(x) \neq 0$, but $f(r) - g(r) = 0$,

$\rightarrow r$ is a root of $f(x) - g(x)$,

$\rightarrow \Pr[r \text{ is a root}] = \frac{3}{|\text{random space}|}$

Interactive proof (IP)

- Not based on cryptographic assumptions, information-theoretic secure
- IP = PSPACE
- Doubly efficient IP for bounded depth uniform circuits
  - Prover O(C)
  - Proof size O(depth log C)
  - Verifier O(depth log C+n)

Sumcheck protocol

$$H = \sum_{b_1,\dots,b_k \in \{0,1\}} f(b_1, \dots, b_k)$$

- Multivariate polynomial $f(x_1, \dots, x_k)$

Multivariate polynomials

$f(x_1, \ldots, x_k): \mathbb{F}^k \to \mathbb{F}$

E.g., $f(x_1, x_2) = 1724 + 761253x_1 + 232x_1x_2 + 14x_2 + 2321x_1x_2^3$

Degree d of $f(x_1, \ldots, x_k)$: maximum degree of $x_1, \ldots, x_k$

Number of monomials/coefficients?
$(d+1)^k$

Sumcheck protocol

$$H = \sum_{b_1,\ldots,b_k \in \{0,1\}} f(b_1, \ldots, b_k)$$

- Multivariate polynomial $f(x_1, \ldots, x_k)$

Number of evaluations in the sum: 2^k

Time to compute each evaluation: $\mathrm{T} = (d+1)^k \cdot k$

Total time to compute the sum: $2^k \cdot T$

Sumcheck protocol

$$H = \sum_{b_1,\dots,b_k \in \{0,1\}} f(b_1, \dots, b_k)$$

$f(x_1, \dots, x_k)$

$$f_1(x_1) = \sum_{b_2,\dots,b_k \in \{0,1\}} f(x_1, b_2 \dots, b_k)$$

Check:

$$H = f_1(0) + f_1(1)$$

E.g., $f(x_1, x_2) = 1724 + 761253x_1 + 232x_1x_2 + 14x_2 + 2321x_1x_2^3$

Sumcheck protocol

$$H = \sum_{b_1,\dots,b_k \in \{0,1\}} f(b_1, \dots, b_k)$$

$f(x_1, \dots, x_k)$

$$f_1(x_1) = \sum_{b_2,\dots,b_k \in \{0,1\}} f(x_1, b_2 \dots, b_k)$$

r_1

$$f_2(x_2) = \sum_{b_3,\dots,b_k \in \{0,1\}} f(r_1, x_2, b_3 \dots, b_k)$$

Check:

$$H = f_1(0) + f_1(1)$$

$$f_1(r_1) = f_2(0) + f_2(1)$$

E.g., $f(x_1, x_2) = 1724 + 761253x_1 + 232x_1x_2 + 14x_2 + 2321x_1x_2^3$

Sumcheck protocol

$$H = \sum_{b_1,\ldots,b_k \in \{0,1\}} f(b_1, \ldots, b_k)$$

$f(x_1, \ldots, x_k)$

$$f_1(x_1) = \sum_{b_2,\ldots,b_k \in \{0,1\}} f(x_1, b_2 \ldots, b_k)$$

$\longleftarrow$

$\xrightarrow{r_1}$

$$f_2(x_2) = \sum_{b_3,\ldots,b_k \in \{0,1\}} f(r_1, x_2, b_3 \ldots, b_k)$$

$\longleftarrow$

$\xrightarrow{r_2}$

$$f_3(x_3) = \sum_{b_4,\ldots,b_k \in \{0,1\}} f(r_1, r_2, x_3, b_4 \ldots, b_k)$$

$\longleftarrow$

Check:

$$H = f_1(0) + f_1(1)$$

$$f_1(r_1) = f_2(0) + f_2(1)$$

$$f_2(r_2) = f_3(0) + f_3(1)$$

Sumcheck protocol

$$H = \sum_{b_1,\dots,b_k \in \{0,1\}} f(b_1, \dots, b_k)$$

$f(x_1, \dots, x_k)$

$$f_1(x_1) = \sum_{b_2,\dots,b_k \in \{0,1\}} f(x_1, b_2 \dots, b_k)$$

r_1

$$f_2(x_2) = \sum_{b_3,\dots,b_k \in \{0,1\}} f(r_1, x_2, b_3 \dots, b_k)$$

....

r_i

$$f_{i+1}(x_{i+1}) = \sum_{b_{i+2},\dots,b_k \in \{0,1\}} f(r_1, \dots, r_i, x_{i+1}, b_{i+2} \dots, b_k)$$

Check:

$$H = f_1(0) + f_1(1)$$

$$f_1(r_1) = f_2(0) + f_2(1)$$

....

$$f_i(r_i) = f_{i+1}(0) + f_{i+1}(1)$$

Sumcheck protocol

$f(x_1, \dots, x_k)$

$$H = \sum_{b_1,\dots,b_k \in \{0,1\}} f(b_1, \dots, b_k)$$

$$f_1(x_1) = \sum_{b_2,\dots,b_k \in \{0,1\}} f(x_1, b_2 \dots, b_k)$$

r_1

$$f_2(x_2) = \sum_{b_3,\dots,b_k \in \{0,1\}} f(r_1, x_2, b_3 \dots, b_k)$$

....

r_i

$$f_{i+1}(x_{i+1}) = \sum_{b_{i+2},\dots,b_k \in \{0,1\}} f(r_1, \dots, r_i, x_{i+1}, b_{i+2} \dots, b_k)$$

....

r_{k-1}

$$f_k(x_k) = f(r_1, \dots, r_{k-1}, x_k)$$

Check:

$$H = f_1(0) + f_1(1)$$

$$f_1(r_1) = f_2(0) + f_2(1)$$

....

$$f_i(r_i) = f_{i+1}(0) + f_{i+1}(1)$$

....

$$f_{k-1}(r_{k-1}) = f_k(0) + f_k(1)$$

$$f_k(r_k) = f(r_1, \dots r_k)$$

Correctness and soundness

- Correctness: 1
- Soundness: $\frac{dk}{|\mathbb{F}|}$

Sumcheck protocol

$f(x_1, \dots, x_k)$

Check:

$H = f_1(0) + f_1(1)$

$f_1(r_1) = f_2(0) + f_2(1)$

....

$f_i(r_i) = f_{i+1}(0) + f_{i+1}(1)$

....

$f_{k-1}(r_{k-1}) = f_k(0) + f_k(1)$

$f_k(r_k) = f(r_1, \dots r_k)$

$$H = \sum_{b_1,\dots,b_k \in \{0,1\}} f(b_1, \dots, b_k)$$

$$f_1(x_1) = \sum_{b_2,\dots,b_k \in \{0,1\}} f(x_1, b_2 \dots, b_k)$$

$\longleftarrow$

$\xrightarrow{r_1}$

$$f_2(x_2) = \sum_{b_3,\dots,b_k \in \{0,1\}} f(r_1, x_2, b_3 \dots, b_k)$$

$\longleftarrow$

....

$\xrightarrow{r_i}$

$$f_{i+1}(x_{i+1}) = \sum_{b_{i+2},\dots,b_k \in \{0,1\}} f(r_1, \dots, r_i, x_{i+1}, b_{i+2} \dots, b_k)$$

$\longleftarrow$

....

$\xrightarrow{r_{k-1}}$

$$f_k(x_k) = f(r_1, \dots, r_{k-1}, x_k)$$

$\longleftarrow$

Complexity

- Prover time: $O(2^k)$ if d=1
- Proof size: $O(dk)$
- Verification time: $O(dk) + T$

Total time to compute the sum: $2^k \cdot T$

- If k = log n and d is constant:

linear prover, logarithmic proof and verifier