CERTIFYING COMPUTATION

x

Alice
Verifier

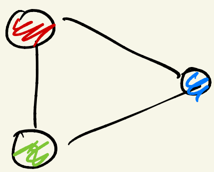
$x \longrightarrow$

$f(x) \longleftarrow$

PROOF THAT
ANSWER IS CORRECT

Bob
Prover

COUNTING GRAPH COLORINGS



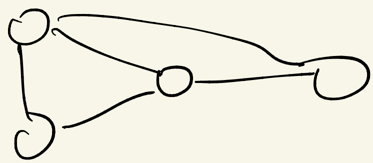
G

3 COLORING $= \{R, G, B\}^3$

VALID IF ALL EDGE ENDPOINTS HAVE DISTINCT COLORS

Alice $\xrightarrow{G \quad \text{"HOW MANY 3 COLS?"}}$ Bob

$\xleftarrow{6}$



n VERTEX GRAPH, 3-COLORINGS CAN BE COUNTED IN TIME 3^n.

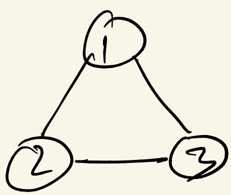
EX. $n \approx 30$ OR 40 FEASIBLE FOR Bob BUT NOT FOR Alice

LFKN PROTOCOL

PROVER HAS COMPLEXITY EXPONENTIAL IN n
VERIFIER HAS COMPLEXITY $\mathrm{poly}(n)$

<u>IDEA</u>: REPRESENT THE NUMBER OF COLORINGS AS A <u>POLYNOMIAL</u>

$$P(\underset{\substack{\uparrow \\ \text{COLOR } 1}}{x_1}, \ldots, \underset{\substack{\uparrow \\ \text{COLOR } n}}{x_n}) = \begin{cases} 1 & \text{IF COLORING IS VALID} \\ 0 & \text{IF NOT} \end{cases}$$



$$P(R, G, B) = 1$$
$$P(R, B, R) = 0$$

AGREE TO REPRESENT $\begin{cases} R \to 1 \\ B \to 0 \\ G \to -1 \end{cases}$

$$P(x_1, \ldots, x_n) = \prod_{(u,v) \text{ EDGES}} P_{uv}(x_u, x_v)$$

WHERE

$$P_{uv}(x_u, x_v) = \begin{cases} 1 & \text{IF } x_u \neq x_v \\ 0 & \text{IF NOT.} \end{cases} = \begin{cases} 1 & \text{IF } x_u - x_v \in \{-2, -1, 1, 2\} \\ 0 & \text{IF NOT} \end{cases}$$

$$= 1 - \frac{\left((x_u - x_v)^2 - 1\right)\left((x_u - x_v)^2 - 4\right)}{4}$$

<u>KEY</u>: $\deg P = 4m$ WHICH IS LOW

V   WANT TO KNOW $S = \sum_{x_1,\dots,x_4 \in \{-1,0,1\}} P(x_1,\dots,x_4)$ P

(NUMBER OF 3 COLORINGS OF G)

$S = 3751019125$

SUM-CHECK PROTOCOL: GIVEN P S.T.

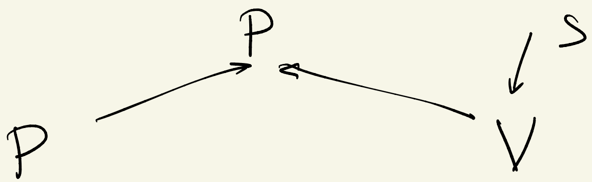
P, V CAN EVALUATE P $(\deg P = d)$,

PROVE $\sum_{x_1,\dots,x_4 \in \{-1,0,1\}} P(x_1,\dots,x_4) = S.$

$P(1,0,-1) = 0$ OR 1

$P(3,7,11) = 751$

ABILITY TO COMPUTE ON INPUTS THAT DO NOT REPRESENT COLORS IS IMPORTANT



Claim $S = \sum_{x_1,\dots,x_n \in \{-1,0,1\}} P(x_1,\dots,x_n)$

MODULO $q > 3^n$.

$$r(x_1) = \sum_{x_2,\dots,x_n \in \{-1,0,1\}} P(x_1,\dots,x_n)$$

DESCRIPTION OF r
BY ITS $d+1$ COEFFICIENTS

$\longrightarrow$

CHECK $r(-1)+r(0)+r(1) = S$

PROVE THAT

$$r(a_1) = \sum_{x_2,\dots,x_n \in \{-1,0,1\}} P(a_1, x_2, \dots, x_n)$$

FOR A RANDOM a_1 MODULO q.

$\longleftarrow$

$\vdots$

BASE Claim $v \neq P(a_1,\dots,a_n)$

NUMBERS MODULO q.

V CAN CHECK ON HIS OWN.

SOUNDNESS Claim. IF $S \neq \sum P(x_1, \dots, x_n)$ THEN VERIFIER REJECT WITH HIGH PROBABILITY.

$$p(x_1) = \sum_{x_2, \dots, x_n} P(x_1, \dots, x_n)$$

ASSUMPTION $\quad p(-1) + p(0) + p(1) \neq S$

BUT $\quad r(-1) + r(0) + r(1) = S$

r AND p ARE NOT THE SAME POLYNOMIAL BUT BOTH HAVE DEGREE $\leq d$

$\downarrow$

$r(x_1) = p(x_1)$ FOR AT MOST d VALUES OF x_1

$\downarrow$

$$P[r(a_1) \neq p(a_1)] \geq 1 - \frac{d}{q} \geq 1 - \frac{d}{3^n}.$$

UNION BOUND ALL PROVER CLAIMS ARE WRONG EXCEPT WITH PROB $\frac{dn}{q}$

Ex. (2 COLORS) P $\xrightarrow{P(0,0)+P(0,1)+P(1,0)+P(1,1)=3}$ V

$\xrightarrow{P(7,0)+P(7,1)\ =11}$

$\xrightarrow{P(7,9)\ =3}$

EFFICIENCY: VERIFIER $O(d\cdot n) = O(m\cdot n)$

PROVER $O(3^n)$ - COMPARABLE TO WORK IT TAKES JUST TO COMPUTE ANSWER

SHAMIR'S PROTOCOL: CAN CERTIFY ANY COMPUTATION THAT USES m BITS OF MEMORY & RUNS IN TIME T

VERIFIER COMPLEXITY $= O(m\cdot \log T)$

PROVER COMPLEXITY COULD BE $2^{O(m)}$

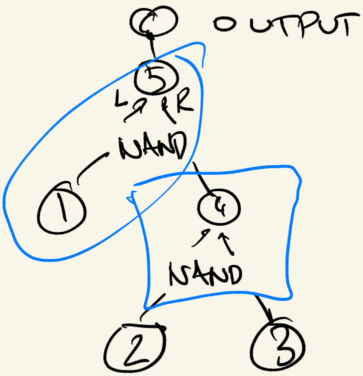
DRAWBACK 1: INEFFICIENT PROVER

DRAWBACK 2: m ITSELF COULD BE VERY LARGE

PROTOCOL FOR GENERAL COMPUTATION (LARGE TIME, LARGE MEMORY)

IDEA: USE SUMCHECK-LIKE PROTOCOL, NOT CLEAR HOW TO REPRESENT AS A POLYNOMIAL.

MODELING GENERAL COMPUTATION



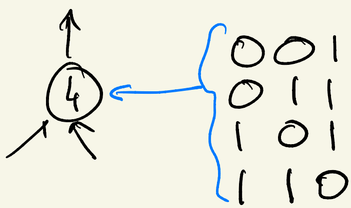
AS A COLORING PROBLEM

VERTICES = GATES

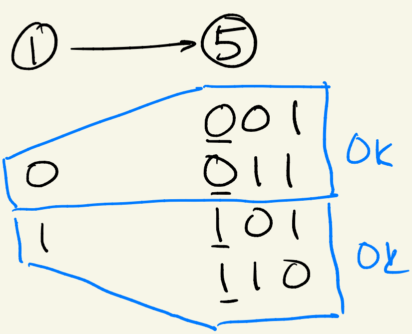
EDGES = WIRES

COLORS : INPUTS $\in \{0,1\}$

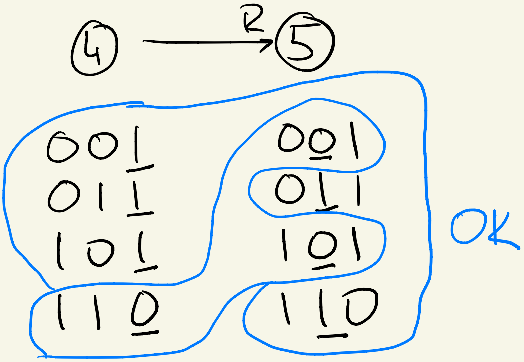
INTERNAL GATE COLORS REPRESENT ASSIGNMENTS TO INPUT AND OUTPUT WIRES



COLORS FOR INTERNAL GATES



(0, 101) NOT VALID



"CIRCUITS ACCEPT INPUT"

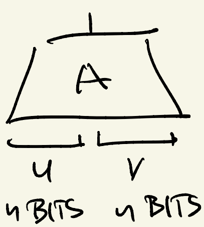
"THERE EXIST A COLORING WHICH SATISFIES ALL THE CONSTRAINTS".

$P \xrightarrow{\text{"THERE EXISTS}} V$

A COLORING THAT IS CONSISTENT ACROSS ALL EDGES"

G ITSELF HAS 2^n VERTICES.

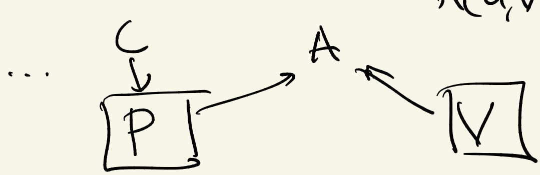
V HOLDS AN <u>IMPLICIT REPRESENTATION</u>



" IS THERE AN EDGE BETWEEN u AND v" ?

GRAPH SIZE $= 2^n$

BUT REPRESENTED BY A CIRCUIT $A(u,v)$ OF SIZE $O(n)$



"G REPRESENTED BY A HAS A VALID 3-COLORING".

"COMPLETE" A COMPUTATION THAT TAKES TIME & MEMORY $2^{O(n)}$.

BOTH COLORING C AND GRAPH G ARE EXPONENTIALLY LARGE.

$$\sum_{u,v\in\{0,1\}^n} ((C(u)-C(v))^2-1)^2((C(u)-C(v))^2-4)^2 \cdot A(u,v) = 0 \quad (*)$$

C IS A VALID 3-COLORING $(C(u)\in\{-1,0,1\})$ IFF $(*)$ HOLDS. $A(u,v)=1 \to C(u)\neq C(v)$.

- C IS A "TABLE" OF 2^n VALUES THAT VERIFIER HAS NO CAPACITY TO STORE
- IF WE WANT TO USE SUMCHECK IT BETTER BE THAT

$$((C(u)-C(v))^2-1)((C(u)-C(v))^2-4)\cdot A(u,v)$$

IS A LOW-DEGREE POLYNOMIAL IN u,v.
ENOUGH THAT A, C HAVE LOW DEGREE

TURNS OUT A HAS SMALL SIZE $(O(n))$ BUT ALSO LOW DEPTH $\to$ AS AN ARITHMETIC CIRCUIT A HAS DEGREE $O(n)$.

IN CONTRAST $C:\{0,1\}^n\to\{-1,0,1\}$ CAN BE AN ARBITRARY FUNCTION

P CAN REPRESENT C AS A MULTILINEAR POLYNOMIAL (EVERY VAR HAS DEG ≤ 1)

$\rightarrow \deg C \leq n.$

Ex. $n=2$ $\quad V = \{0,1\}^2$

00: 0	01: 1
10: -1	11: 1

COME UP WITH

$$C(x,y) = a + bx + cy + dxy$$

S.T.

$C(0,0)=0$	$C(0,1)=1$	$C(1,0)=-1$	$C(1,1)=1$
$a=0$	$a+c=1$, $c=1$	$a+b=-1$, $b=-1$	SOLVE FOR d

IN GENERAL CAN SOLVE FOR 2^n COEFFICIENTS IN TIME $O(n \cdot 2^n)$

EXPECTED BEHAVIOR OF HONEST PROVER

- CREATE C OF TOTAL DEGREE $\leq n$ THAT REPRESENTS A VALID 3-COLORING OF G.

$$\sum_{u_1=0}^{1}\left(\sum_{u_2 \ldots u_n, V} \left((C(u)-C(v))^2-1\right)^2 \left((C(u)-C(v))^2-4\right)^2 \cdot A(u,v)\right) = 0$$

SUMCHECK

$\vdots$

$C(11,5,7) = ?$ $\quad C(3,0,21) = ?$

75 $\quad$ 33

FOR SOUNDNESS NEED TWO EXTRA CHECKS

- C IS A 3-COLORING WHEN RESTRICTED TO $\{0,1\}^n$: $\underbrace{\forall x \in \{0,1\}^n : C(x) \in \{-1,0,1\}}_{(A)}$
- C IS SOME LOW-DEGREE POLYNOMIAL.
  $\longrightarrow$ LOW-DEGREE TEST

ANOTHER SUMCHECK

$$\sum_{x \in \{0,1\}^n} r^x \, C(x)\left(C(x)^2 - 1\right) = 0 \qquad (B)$$

r RANDOM IN $\mathbb{F}_q$, $r^x = r^{x_1 + 2x_2 + \dots + 2^{n-1}x_n}$

Claim: $(A) \longrightarrow (B)$

(A) FAILS $\longrightarrow (B)$ FAILS W/P $\geq 1 - \frac{2^n}{q}$

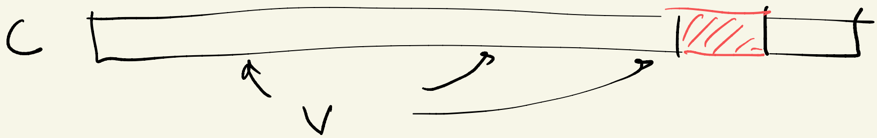
TO APPLY SUMCHECK WE CAN WRITE (B) AS A deg-n POLYNOMIAL IN x:

$$\begin{aligned} r^x &= r^{x_1 + 2x_2 + \dots + 2^{n-1}x_n} \\ &= r^{x_1} \cdot (r^2)^{x_2} \cdots \left(r^{2^{n-1}}\right)^{x_n} \\ &= (1 - x_1 + x_1 r) \cdots \left(1 - x_n + x_n r^{2^{n-1}}\right). \end{aligned}$$

LOW-DEGREE TEST Rubinfeld-Sudan

$$P \xrightarrow{\text{description of } C} V$$

PROOF THAT C "IS CLOSE TO" HAS DEGREE $\leq n$.



IDEA. $C(x_1, \dots, x_n)$ HAS DEGREE n

$C(\ell(t))$ HAS DEGREE n FOR EVERY LINE

$$\ell(t) = (x_1, \dots, x_n) + t(y_1, \dots, y_n)$$

V PICK RANDOM ℓ AND CHECK THAT $C(\ell(0)), \dots, C(\ell(n+1))$ ARE CONSISTENT WITH VALUES OF SOME DEGREE-n POLYNOMIAL IN t (LAGRANGE INTERPOLATION).

Kilian's IMPLEMENTATION OF BFL PROTOCOL

$P \xrightarrow{\text{SUCCINCT COMMITMENT OF } C} V$

(IF V WANTS TO KNOW $C(x)$
ASK P FOR VALUE + CERTIFICATE)

CONSISTENCY

$\xleftrightarrow{\text{SUMCHECK } \sum r^x C(x)(C(x)^2-1)=0}$

ACTUAL COLORS ARE USED

$\xleftrightarrow{\text{LOW-DEGREE TEST}}$

C IS A LOW-DEG POLY

$\xleftrightarrow{\text{SUMCHECK } \sum (C(u)^2-1)^2(C(v)^2-4)^2 A(u,v)=0}$

C IS A VALID 3COL OF G.