CERTIFYING COMPUTATION

PROOF THAT ANSWER IS CORRECT

COUNTING GRAPH COLORINGS

3-COLORING = \{R, G, B\}^3
VALID IF ALL EDGE ENDPOINTS HAVE DISTINCT COLORS

Alice \[ \rightarrow \] 3"HOW MANY 3-COLORINGS?" \[ \rightarrow \] Bob

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 poly(n)

IDEA: REPRESENT THE NUMBER OF COLORINGS AS A POLYNOMIAL

\[ P(x_1, \ldots, x_n) = \begin{cases} \text{1} & \text{if coloring is valid} \\ \text{0} & \text{if not} \end{cases} \]

\[ P(r, g, b) = 1 \quad P(2, b, r) = 0 \]

AGREE TO REPRESENT \( R \mapsto 1 \), \( B \mapsto 0 \), \( G \mapsto -1 \)

\[ P(x_1, \ldots, x_n) = \prod_{(u, v) \text{ edges}} P_{uv}(x_u, x_v) \]

WHERE

\[ P_{uv}(x_u, x_v) = \begin{cases} \text{1} & \text{if } x_u \neq x_v \\ \text{0} & \text{if NOT} \end{cases} = \begin{cases} \text{1} & \text{if } x_u - x_v \in \{1, 3\} \\ \text{0} & \text{if NOT} \end{cases} \]

\[ = 1 - \frac{(x_u - x_v)^2 - 1}{(x_u - x_v)^2 - 4} \]

KEY: \( \deg P = 4m \) which is low
V WANT TO KNOW \[ S = \sum_{x_1, \ldots, x_6 \in \{-1,1\}} P(x_1, \ldots, x_6) \]
\[(\text{NUMBER OF 3 COLORINGS OF 6})\]
\[ S = 3751019125 \]

SUM-CHECK PROTOCOL: GIVEN P s.t. P, V CAN EVALUATE P (degP = d), PROVE \[ \sum_{x_1, \ldots, x_6 \in \{-1,1\}} P(x_1, \ldots, x_6) = S. \]

\[ P(1,0,-1) = 0 \text{ or } 1 \]
\[ P(3,7,11) = 751 \]

ABILITY TO COMPUTE ON INPUTS THAT DO NOT REPRESENT COLORS IS IMPORTANT
DESCRIPTION OF $r$ BY ITS DH COEFFICIENTS

PROVE THAT

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

FOR A RANDOM $a_i$ MODULO $q$.

BASE CLAIM $v = P(a_1, \ldots, a_n)$

NUMBERS MODULO $q$.

$V$ CAN CHECK ON HIS OWN.
**Soundness Claim.** If \( S \neq \sum p(x_i) \) then

VERIFIER REJECT with high probability.

\[
p(x_i) = \sum_{x_2, \ldots, x_n} p(x_1, \ldots, x_n)
\]

**Assumption**

\[
p(-1) + p(0) + p(1) \neq S
\]

\[
r(-1) + r(0) + r(1) = S
\]

\[
r \text{ and } p \text{ are not the same polynomial but both have degree } \leq d
\]

\[
l \left( x_i \right) = p(x_i) \text{ for at most } d \text{ values of } x_i,
\]

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

**Union Bound**

**Wrong except with prob** \( \frac{dn}{q} \)
Ex. (2 colors) $P$ \[
P(0,0) + P(0,1) + P(1,0) + P(1,1) = 3
\]
\[
P(7,0) + P(7,1) = 11
\]
\[
P(7,9) = 3
\]

**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 ∈ \{0,1\}
INTERNAL GATE COLORS REPRESENT ASSIGNMENTS TO INPUT AND OUTPUT WIRES

COLORS FOR INTERNAL GATES

(0, 101) NOT VALID
"CIRCUITS ACCEPTS INPUT"

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

P "THERE EXISTS V A COLORING THAT IS CONSISTENT ACROSS ALL EDGES."

G ITSELF HAS 2^" VERTICES.

V HOLDS AN IMPLICIT REPRESENTATION

"IS THERE AN EDGE BETWEEN U AND V"?

GRAPH SIZE = 2^" BUT REPRESENTED BY A CIRCUIT A(u,v) OF SIZE O(1)

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

"COMPLETE" A COMPUTATION THAT TAKES TIME & MEMORY 2^{0(1)}.
Both coloring \( C \) and graph \( G \) are exponentially large.

\[
\sum_{u,v \in f(q)} ((C(u) - C(v))^2 - 1)((C(u) - C(v))^2 - 4)^2 \cdot A(u,v) = 0 \quad (\star)
\]

\( C \) is a valid 3-coloring \( (C(u) \notin \{-1,0,1\}) \) iff \( (*) \) holds, \( A(u,v) = 1 \Rightarrow C(v) = C(u) \).

- \( C \) is a "table" of 2\( ^q \) values that verified 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 \( O(u) \) but also low depth \( \rightarrow \) as an arithmetic circuit \( A \) has degree \( O(u) \).

In contrast \( C : \{0,1\}^q \rightarrow \{-1,0,1\} \) can be an arbitrary function.
P can represent $C$ as a **multilinear polynomial** (every var has deg $\leq 1$)

$\rightarrow \deg C \leq n.$

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

Come up with

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

S.t. \hspace{1cm} $C(0, 0) = 0$ \hspace{1cm} $C(0, 1) = 1$ \hspace{1cm} $C(1, 0) = -1$ \hspace{1cm} $C(1, 1) = 1$

\[\begin{align*}
q &= 0 \\
a + c &= 1 \\
b &= -1
\end{align*}\]

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 $G$.

\[
\frac{1}{2} \sum_{u_i = 0} \left( \sum_{u_i \neq u_j} (C(u) - C(v))^2 - 1 \right)^2 \cdot A(u, v) = 0
\]

**Sum check**

$C(11, 5, 7) = ?$ \hspace{1cm} $C(3, 0, 21) = ?$

\[\begin{align*}
75 &\hspace{1cm} 33
\end{align*}\]
For soundness need two extra checks

- C is a 3-coloring when restricted to \( \{0,1,3\}^n \): \( \forall x \in \{0,1,3\}^n : C(x) \in \{-1,0,1\} \)
  \[ (A) \]

- C is some low-degree polynomial.
  \[ \rightarrow \text{low-degree test} \]

\[
\sum_{x \in \{0,1,3\}^n} r^x C(x)(C(x)^2-1) = 0 \quad (B)
\]

\( r \) random in \( \mathbb{F}_q \), \( r^x = r^{x_1 + 2x_2 + \ldots + 2^{n-1}x_n} \)

Claim: \( (A) \longrightarrow (B) \)  
\( (A) \) fails \( \rightarrow (B) \) fails with probability \( \leq 1 - \frac{2^n}{q} \)

To apply sumcheck we can write \( (B) \) as a \( \deg n \) polynomial in \( x \):

\[
r^x = r^{x_1 + 2x_2 + \ldots + 2^{n-1}x_n} = r^{x_1}(r^2)^{x_2} \ldots (r^{2^{n-1}})^{x_n} = (1-x_1+x_1r) \ldots (1-x_n+x_n r^{2^{n-1}}).
\]
PROOF THAT $C$ "IS CLOSE TO" HAS DEGREE $\leq n$.

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

$C(p(t))$ HAS DEGREE $n$ FOR EVERY LINE

$e(t) = (x_1, \ldots, x_n) + t(y_1, \ldots, y_n)$

V PICK RANDOM $P$ AND CHECK THAT $C(l(0)), \ldots, C(l(n+1))$ 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 \( CC(x) \), ask \( P \) for value + CERTIFICATE)

\[ \text{CONSISTENCY} \]

\[ \text{ACTUAL COLORS ARE USED} \]

\[ C \text{ IS A LOW-DEG POLY} \]

\[ \text{C IS A VALID 3COL OF 6.} \]