July 15, 2024

Introduction to Zerocheck

Outline:

1. Mathematical Preliminaries
   - Multilinear Polynomials
   - Lagrange vs Monomial Basis
   - equality indicator
   - Multilinear Extensions + Evaluation Formula
   - Polynomial Identity Testing
2. Why zerocheck matters
3. The zerocheck to sumcheck reduction

Today (7/15/24)

4. The interactive sumcheck protocol
5. Completeness and Soundness

Next time (7/22/24)

6. Notes on Performance
7. Simple performance optimizations
8. Section 3 performance optimizations
9. Zerocheck Batching

Final Part (7/29/24)

Goal: To teach concepts behind zero-check and jargon bust the mathematical language behind Binius

(1) Math Prelims

Defn: A multilinear polynomial is linear in each variable

ex// $f(x_0, x_1, x_2) = x_0 + x_1x_2 + X_0X_1 + X_0X_1X_2$ ✓

ex// $f(x_0, x_1, x_2) = x_0 + x_0^2x_1 + X_1X_2$ ✗ non-linear in x_0

Defn: A monomial is a product of powers of indeterminates and a coefficient ← also: polynomial with one term

ex// $M(x_0,x_1,x_2) = a_0 x_0 x_1^3 x_2^9$ (where $a_0 \in \mathbb{F}$) ✓

ex// $P(x_0,x_1,x_2) = x_0x_1 + x_0^2x_2^9$ ✗ this is a polynomial but not a monomial

Notation: read $a \mid b$ as "a divides b" so $3 \mid 9$ but $3 \nmid 10$

Defn: Individual degree of x_i in monomial M is the power of x_i in the expression. Formally $\max\{k \in \mathbb{N} \text{ where } x_i^k \mid M\}$ ← divides
$\deg_{x_i}(M)$

Defn: Total degree in monomial M is sum of all powers (or equivalently sum of individual degrees)
$\deg(M)$

Defn: Individual degree of x_i in polynomial P is the max of monomial individual degrees.
$\deg_{x_i}(P)$

Defn: Total degree in polynomial P is the max of monomial total degrees.
$\deg(P)$

ex// $f(x_0, x_1, x_2) = \underbrace{x_0x_1^3}_{M_1} + \underbrace{x_0^2x_1^2x_2^2}_{M_2}$ (P)

- $\deg_{x_0}(M_1) = 1$, $\deg_{x_0}(M_2) = 2 \Rightarrow \deg_{x_0}(P) = \max\{1,2\} = 2$
- $\deg(M_1) = 4$, $\deg(M_2) = 6 \Rightarrow \deg(P) = \max\{4,6\} = 6$

Defn: An $\mathbb{F}$-basis for vector space V is a minimal set of vectors that "span" V.

ex// Consider the vector space $V = \mathbb{Q}[X]^{\leq 3}$ ← notation alert: $\mathbb{F}[x]^{\leq d}$, or the set of degree ≤ 3 univariate (single variable) polynomials with coefficients from $\mathbb{Q}$

Then the set $\{1, X, X^2, X^3\}$ is a $\mathbb{Q}$-basis

why? ① Every elt of V can be written as a linear combination of basis vectors with $\mathbb{Q}$-coefficients (spanning)

② You cannot continue to satisfy ① by removing any basis vector (minimality)

ex// Let $W = T_2[X_0, X_1, X_2]^{\leq 1}$ (multilinear polys on 3 vars with T_2 coeffs)

then the set $B = \{1, X_0, X_1, X_2, X_0X_1, X_0X_2, X_1X_2, X_0X_1X_2\}$

is a T_2-basis for W (of dimension $2^3 = 8$)

$T_2 \cong \mathbb{F}_{2^2}$.

Nerd Note: "B is an $\mathbb{F}$-basis for a vector space V" roughly means

- V is a vector space over the field $\mathbb{F}$
- Every $\vec{x} \in V$ can be uniquely written as an $\mathbb{F}$-linear combination of basis vectors in B

this means coeffs live in $\mathbb{F}$

Fact: A vector space V can have multiple $\mathbb{F}$-basis sets, but these will all have the same cardinality (size).

These most recent examples are called **Monomial Bases** because each basis elt is a monomial.

Why is this useful? We can represent elements of a vector space by their coeffs with respect to a specific basis // coordinate vector

ex// I could write $f(x_0, \dots, x_{n-1}) = b_0 + b_1 x_0 + \cdots + b_{2^n-1} x_0 \cdots x_{n-1}$

or I could represent f as $[b_0, b_1, \dots, b_{2^n-1}]$

where these are monomial basis coefficients

✡✡ to evaluate a poly @ $\vec{r} = (r_0, \dots, r_{n-1})$, eval basis polys @ r, dot product with coefficients

$[1, r_0, r_1, \dots, r_0 r_1 \cdots r_{n-1}] \cdot [b_0, \dots, b_{2^n-1}] = f(r_0, \dots, r_{n-1})$

Fact: A multilinear polynomial can be uniquely defined by its "boolean hypercube" evaluations.

given: $f: \{0,1\}^n \to \mathbb{F}$
$\exists!$ multilinear poly whose evals agree with f

ex// Knowing
- f is multilinear on 2 vars
- $f(0,0) = a_0$
- $f(1,0) = a_1$
- $f(0,1) = a_2$
- $f(1,1) = a_3$

By Fact there is exactly one polynomial that f can be

$$f(x_0,x_1) = a_0(1-x_0)(1-x_1) + a_1 x_0(1-x_1) + a_2(1-x_0)x_1 + a_3 x_0 x_1$$

$$= a_0 \cdot 1 + (a_1-a_0)\cdot x_0 + (a_2-a_0)\cdot x_1 + (a_0+a_3-a_2-a_1)\cdot x_0 x_1$$

Let $b_0 = a_0$, $b_1 = a_1 - a_0$, $b_2 = a_2 - a_0$, $b_3 = a_0 + a_3 - a_2 - a_1$

Then $f(x_0,x_1)$ can be represented as $[b_0, b_1, b_2, b_3]$ in monomial basis

... or as $[a_0, a_1, a_2, a_3]$ in the (standard) Lagrange basis

Defn For input domain D, a Lagrange Polynomial $L_{\vec{v}}(x_0, \dots, x_{n-1})$ is an indicator polynomial s.t.

$$L_{\vec{v}}(\vec{x}) = \begin{cases} 1, & \vec{x} = \vec{v} \\ 0, & \vec{x} \neq \vec{v} \end{cases} \quad \text{and } \vec{x} \in D$$

$L_{(0,0)}(x_0,x_1)$ $L_{(1,0)}(x_0,x_1)$ $L_{(1,1)}(x_0,x_1)$

Defn $\{(1-x_0)(1-x_1), x_0(1-x_1), (1-x_0)x_1, x_0 x_1\}$ is the Lagrange basis over the 2-dimensional boolean hypercube input domain (read: $\{0,1\}^2$) for the vector space of 2-variate multilinear polynomials

$$[1-x_0, x_0] \otimes [1-x_1, x_1] = \begin{bmatrix} (1-x_0)(1-x_1) \\ (1-x_0)x_1 \\ x_0(1-x_1) \\ x_0 x_1 \end{bmatrix}$$

Sometimes this is written as $\bigotimes_{i=0}^{n-1} [1-x_i, x_i]$

which we call a tensor product

$$\begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix}$$

Note: Lagrange Basis coefficients are exactly the evaluations of the polynomial over the input domain for which the L.B. is defined

→ in our case, the n-dimensional boolean hypercube $\{0,1\}^n$

Defn The equality indicator is a multilinear polynomial on $2n$ variables

$$eq(X_0,\dots,X_{n-1},Y_0,\dots,Y_{n-1}) = \begin{cases} 1, & X_i = Y_i \ \forall i \\ 0, & X_i \neq Y_i \ \exists i \end{cases}$$

$eq(X_0,Y_0) = (1-X_0)(1-Y_0) + X_0Y_0$

$eq(\vec{X},\vec{Y}) = \prod_{i=0}^{n-1}(1-X_i)(1-Y_i) + X_iY_i$

like all polynomials, this can be partially evaluated, or specialized.

Evaluating a multilinear polynomial at the point $r_0,\dots,r_{n-1}$

Defn: The multilinear extension of f is denoted as $\tilde{f}$, $f:\{0,1\}^n \to \mathbb{F}$, $\tilde{f}:\mathbb{F}^n \to \mathbb{F}$

eq 1
$$\tilde{f}(Y_0,\dots,Y_{n-1}) = \sum_{\vec{v}\in\{0,1\}^n} \tilde{eq}(\vec{v},\vec{Y}) \cdot \underbrace{f(v)}_{\text{constant}}$$

Key: Two multilinears are equal iff their evaluations agree over the boolean hypercube input domain

- Let $\vec{Y}$ be a hypercube point $\vec{v}$
- Then $\tilde{eq}(X,\vec{v})$ is literally the Lagrange Basis poly at $\vec{v}$

$L.B. = [\tilde{eq}(X_0,X_1,0,0), \tilde{eq}(X_0,X_1,1,0), \dots, \tilde{eq}(X_0,X_1,1,1)]$

$f: \{0,1\}^2 \to \mathbb{F}$

$f(0,0) = a_0$
$f(1,0) = a_1$
$f(0,1) = a_2$
$f(1,1) = a_3$

$$\tilde{f}(Y_0,Y_1) = \tilde{eq}(0,0,Y_0,Y_1)\cdot a_0 + \tilde{eq}(1,0,Y_0,Y_1)\cdot a_1 + \tilde{eq}(0,1,Y_0,Y_1)\cdot a_2 + \tilde{eq}(1,1,Y_0,Y_1)\cdot a_3$$

eff // set $Y_0 = 0,\ Y_1 = 1$

$f(Y_0,Y_1) = f(0,1) = a_2$

$\tilde{f}(Y_0,Y_1) = \tilde{f}(0,1) =$

$0\cdot a_0$
$+ 0\cdot a_1$
$+ 1\cdot a_2$
$+ 0\cdot a_3$

---

2 vars $\tilde{eq}(X_0,Y_0) = (1-X_0)(1-Y_0) + X_0Y_0$

4 vars $\tilde{eq}(X_0,X_1,Y_0,Y_1) = [(1-X_0)(1-Y_0) + X_0Y_0]\cdot [(1-X_1)(1-Y_1) + X_1Y_1]$

so $f(y) = f(v) = 0 \cdot f(0,\cdots,0) + 0 \cdot f(1,0,\cdots,0) + \cdots + 1 \cdot f(v) + \cdots + 0 \cdot f(1,1,\cdots,1) = f(v)$

This shows us that eq 1 is a proper way to evaluate $\tilde{f}$ anywhere, not just at points inside the hypercube domain.

Note: Let $\vec{r} = (r_0, \cdots, r_{n-1})$ be a point not necessarily in the hypercube. Then

$$\left[\tilde{eq}(0,\cdots,0,\vec{r}), \tilde{eq}(1,0,\cdots,0,\vec{r}), \cdots, \tilde{eq}(1,\cdots,1,\vec{r})\right]$$

is exactly the evaluations of the standard L.B. polynomials (for n-variate multilinear polynomial vector space) @ $\vec{r}$

Polynomial Identity Testing (for multilinears and univariates)

- zero testing (univariate) $f(x) \stackrel{?}{=} 0$

Q: Is the multilinear polynomial $f(x_0, x_1, x_2) = 0$? (identically 0?)

A: Yes iff $f(0,0,0) = f(1,0,0) = f(0,1,0) = \cdots = f(1,1,1) = 0$ iff $f(0) = f(1) = \cdots = f(d) = 0$ // any d+1 points

A_2: Yes w.h.p (w/ high probability) if $f(\vec{r}) = 0$ where $\vec{r}$ is sampled from a large domain. if $f(r) = 0$

Why? If f is **not** zero then it cannot have too many roots. Defn: r is a root of f if $f(r) = 0$

So? if f is 0 at random point, and $f \neq 0$ what is the chance you picked a root? (Low)

- **equality testing**

Q: Are the multilinear polynomials $f(x_0, x_1, x_2)$ and $g(x_0, x_1, x_2)$ the same?

A_1: Yes if $f(0,0,0) = g(0,0,0) \wedge \cdots \wedge f(1,1,1) = g(1,1,1)$ ← logical and

A_2: Yes if $h(x_0, x_1, x_2) := f(x_0, x_1, x_2) - g(x_0, x_1, x_2) = 0$

Note: h is multilinear too ☺

(Can ignore this)

Math Detour

Schwartz-Zippel (univariate)

(F is a field, K is an extension field)

Let $f(x) \in \mathbb{F}[x]^{\leq d}$, if $r \leftarrow_R K$, then $f(r) = 0$ with prob
$= 1$ if $f(x) = 0$
$\leq \frac{d}{|K|}$ if $f(x) \neq 0$

Schwartz-Zippel (multilinear)

Let $g(x_0, \ldots, x_{n-1}) \in \mathbb{F}[x_0, \ldots, x_{n-1}]^{\leq 1}$

- $\vec{r} \leftarrow_R K^n$, $g(\vec{r}) = 0$ with prob $= 1$ if $g(\vec{x}) = 0$
$\leq \frac{d}{|K|}$ if $g(\vec{x}) \neq 0$

(where d is total degree) $d \leq n$

(2) Why Zerocheck matters?

Setting: I want to prove to you that I know the value of the 10th fibonacci number.

row #	A	B	C
0	0	1	1
1	1	1	2
2	1	2	3
3	2	3	5
4	3	5	8
5	5	8	13
6	8	13	21
7	13	21	34

← let's say I create an 8×3 matrix of values, let's call this a (computation) **trace**

IF I can show the following properties are true about my trace

inputs • $A[0] = 0,\ A[1] = 1$

outputs • $C[7] = 34$

copy • $B[i] = A[i+1] \quad \forall i \in \{0, \dots, 6\}$

$C[i] = B[i+1] \quad \forall i \in \{0, \dots, 6\}$

gate • $\forall i \in \{0, \dots, 7\} \quad A[i] + B[i] - C[i] = 0$

then the verifier will be convinced that

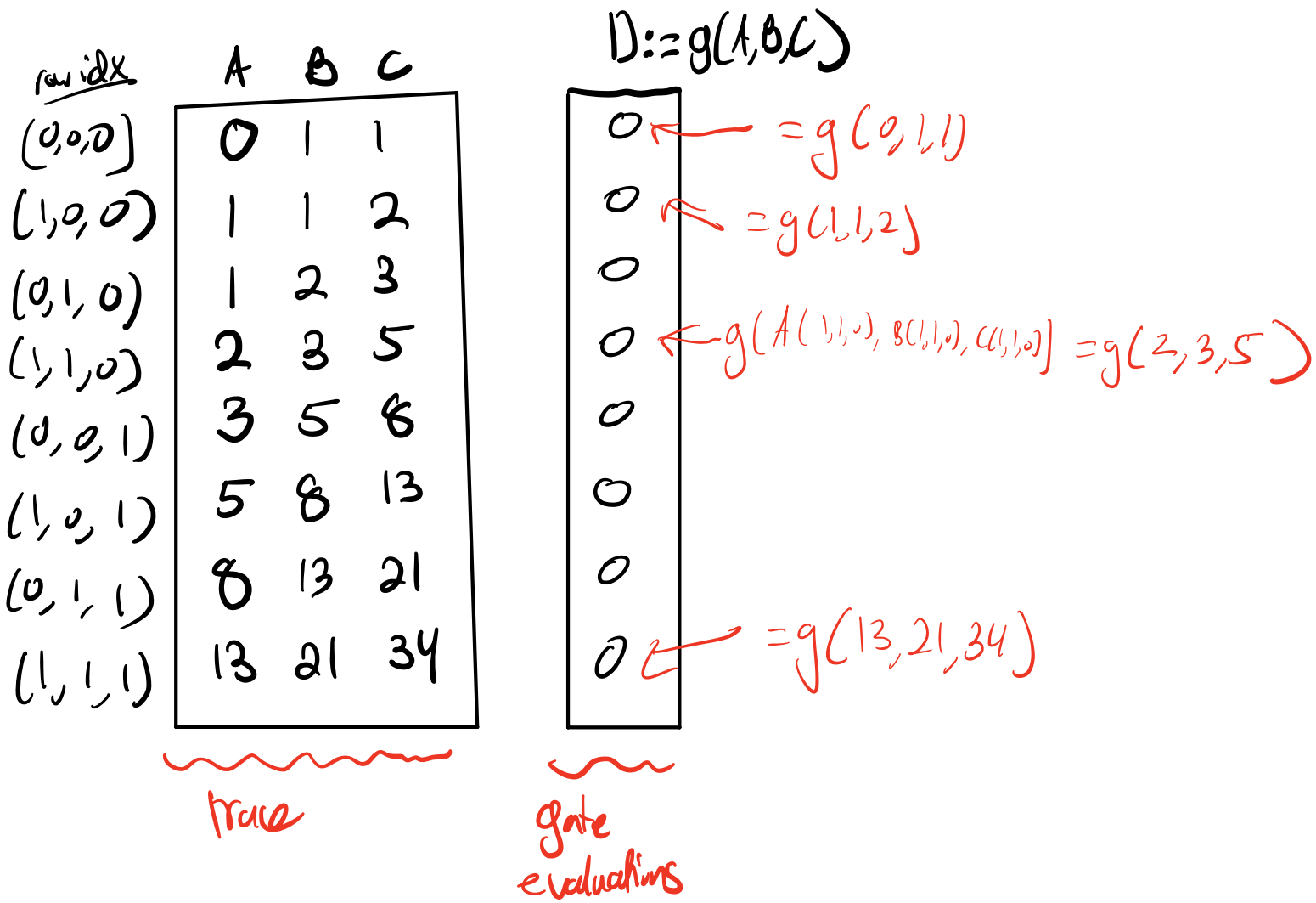
$f(0) = 0,\ f(1) = 1$ and $f(9) = 34$

Let's focus on "gate" properties,

Let $g(A, B, C) = A + B - C$

called the "gate polynomial" or "constraint"

Note: (this is typically a bottleneck in proving speed)



Goal: Show that this vector D is all zeros.

This would require the verifier to know the full trace and evaluate $g(A(\vec{v}), B(\vec{v}), C(\vec{v}))$ at every raw idx $\vec{v}$

defeating purpose of succinct proof

(or is there another way to test if a vector of length 2^n is all zeros?)

Idea: Pretend like $\widetilde{D}$ is actually a multilinear polynomial on n-vars where the v^{th} entry $D[v]$ is evaluation of $\widetilde{D}(\vec{v})$

Then zero test $\widetilde{D}(x_0, \cdots, x_{n-1})$ at a random point $\vec{r} = (r_0, \cdots, r_{n-1})$. If $\widetilde{D}(\vec{r}) = 0$, then verifier would agree w.h.p. that gate constraints are valid for every row

Defn **Zerocheck** is an interactive protocol btwn a prover and a verifier where the prover convinces the verifier that a specific multivariate polynomial evaluates to 0 over the hypercube.

Here $h(x_0, \cdots, x_{n-1}) := g(A(x_0, \cdots, x_{n-1}), B(x_0, \cdots, x_{n-1}), C(x_0, \cdots, x_{n-1}))$ is the polynomial in question

and P wants to show V that $h(\vec{v}) = 0 \quad \forall v \in \{0,1\}^n$

COMMON MISUNDERSTANDING

This is NOT saying $h(x_0, \cdots, x_{n-1}) = 0$

because h is not multilinear in general (e.g. $g(A,B,C) = A^3 - BC$)

However $\tilde{D}(x_0, \ldots, x_{n-1}) = \sum_{v \in \{0,1\}^n} \tilde{eq}(\vec{x}, \vec{v}) \cdot \underbrace{h(v)}_{\text{constant}}$

is a multilinear polynomial whose hypercube evaluations, by design, agree with h.

So we are checking that $\tilde{D}(x_0, \ldots, x_{n-1}) \stackrel{?}{=} 0$

(3) Zerocheck to Sumcheck Reduction:

We wish to ~~zerotest~~ the multilinear polynomial $\tilde{h}$.

So, sample $\vec{r} \leftarrow_R \mathbb{T}_L^n$ and check $\tilde{h}(\vec{r}) \stackrel{?}{=} 0$

This means WTS (want to show):

$$\tilde{h}(\vec{r}) := \sum_{\vec{v} \in \{0,1\}^n} \widetilde{eq}(\vec{v}, \vec{r}) \cdot h(v) \stackrel{?}{=} 0$$

Defn: Sumcheck is an interactive protocol where P convinces V that a multivariate polynomial $\tilde{h}(x_0, \ldots, x_{n-1})$ has hypercube evaluations that sum to a claimed total s.

i.e. P proves to V that

$$\sum_{v \in \{0,1\}^n} \tilde{h}(v) \stackrel{?}{=} s$$

$$\tilde{h}(y) = \widetilde{eq}(y, \vec{r}) \cdot h(y)$$

$$\tilde{D}(x) := \sum_{\vec{r} \in \{0,1\}^n} eq(r, x) \cdot h(r)$$

$$D(X, Y) := eq(Y, X) \cdot h(Y)$$

$$D(\vec{r}, Y) := eq(Y, \vec{r}) \cdot h(Y)$$

$$\tilde{h}(Y) := \tilde{D}(\vec{r}, Y)$$

$$\sum_{r \in \{0,1\}^n} \tilde{h}(Y) \stackrel{?}{=} 0$$

$$\Downarrow$$

$$\sum_{r \in \{0,1\}^n} eq(r, \vec{r}) \cdot h(r) \stackrel{?}{=} 0$$

$$\tilde{D}(\vec{r}) := \sum_{r \in \{0,1\}^n} eq(r, \vec{r}) \cdot h(r)$$

So, to complete the zerocheck to sumcheck reduction...

- Given: zerocheck instance $h(x_0, \ldots, x_{n-1})$
- Sample $\vec{r} \xleftarrow{R} (T_L)^n$
- Define $\overline{h}(x_0, \ldots, x_{n-1}) := eq(\vec{x}, \vec{r}) \cdot h(\vec{x})$
- Output: sumcheck instance $\left(\overline{h}(x_0, \ldots, x_{n-1}), 0\right)$

Summary:

- We reviewed some key mathematical machinery for understanding modern SNARKs
- we have motivated why zerocheck is important
- we have discussed how one reduces zerocheck to sumcheck

Next time

- we dive into how sumcheck works generally, (mostly) ignoring the context for why Binius cares about the sumcheck protocol.

It is very important to grok this material well, as we will build on these ideas in the next lecture. Please take time to review and ask many questions if you're confused. I know math is hard, but you don't have to do it alone ☺

July 22, 2024

(4) The interactive sumcheck protocol:

Recall: sumcheck is an interactive protocol between a prover and a verifier where P convinces V that a specific n-variate polynomial $f(x_0, \dots, x_{n-1})$ has hypercube evaluations that sum to a claimed value s.

i.e.

$$\sum_{\vec{x} \in \{0,1\}^n} f(\vec{x}) \stackrel{?}{=} s$$

$$\Leftrightarrow f(0,\dots,0) + f(1,0,\dots,0) + \cdots + f(1,\dots,1) \stackrel{?}{=} s$$

Instance: $f(x_0,\dots,x_{n-1})$ poly, s claimed sum

Goal: verifier should not need to evaluate f 2^n times
IN FACT, will only need to do so once

Asm: f is represented as a composition of multilinears (Multilinear Composite)

$$f(x_0,\dots,x_{n-1}) = g(h_1(x_0,\dots,x_{n-1}), \dots, h_c(x_0,\dots,x_{n-1}))$$

where
- g is a c-variate composition function of total degree d
- h_i is an n-variate multilinear polynomial $\forall i \in \{1,\dots,c\}$

then we can say
- f is an n-variate polynomial of "max individual degree" d

ex// $f(x_0,x_1,x_2) = x_0^3 x_2^3 + x_1^2 x_2 + x_1^5$ is max individual degree 5

define
$h_1(x_0,x_1,x_2) = x_0 x_2$
$h_2(x_0,x_1,x_2) = x_1$
$h_3(x_0,x_1,x_2) = x_2$

then $f(\vec{x}) = g(h_1(\vec{x}),\dots,h_3(\vec{x}))$

$g(A,B,C) = A^3 + B^2 C + B^5$