CSE 575: Advanced Cryptography
Fall 2024
Lecture 21

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Background: interpolating polynomials on subgroups
- Arithmetizing Plonkish constraints
- Gate check
- Wiring check

Agenda for this lecture

- Announcements
- Background: interpolating polynomials on subgroups
- Arithmetizing Plonkish constraints
- Gate check
- Wiring check

Announcements

- HW4 will be assigned this week
- Rest of class: no typeset lecture notes.
  - Can get extra credit for typesetting

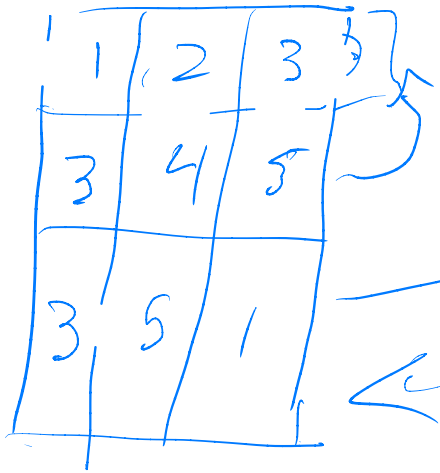
Agenda for this lecture

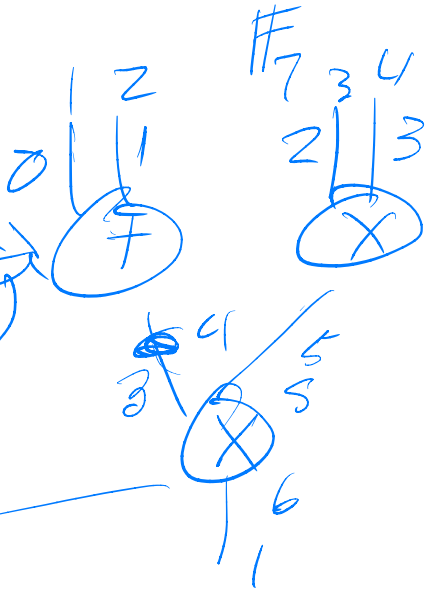
- Announcements
- Background: interpolating polynomials on subgroups
- Arithmetizing Plonkish constraints
- Gate check
- Wiring check

Polynomial interpolation

Copy constraints

$$T[\sigma[i]] = T[i]$$





Checks copy constraints

How to compute?

- $\vec{w} = \vec{a} \| \vec{b} \| \vec{c}$
- For each $i \in [m]$, compute indices of $\vec{w}$ where $\vec{w}[j] = i$

  Let B_i be the indices
- Define σ: B_i's are cycles

$\vec{a} = [0\ 2\ 4]$

$\vec{b} = [1\ 3\ 5]$

$\vec{c} = [4\ 5\ 6]$

$\vec{w} = [0\ 2\ 4\ 1\ 3\ 5\ 4\ 5\ 6]$

$\sigma = (2\ 6)(5\ 7)(0)(1)(3)(4)(8)$

Note: row vs. column major flattening (?)

Polynomial interpolation

Multiplicative subgroup of field $\mathbb{F}_p$

$\{1, \omega, \omega^2, \omega^3, \omega^4, \ldots, \omega^{k-1}\}$

k is order of ω in $\mathbb{F}_p$

Thm: $a^{p-1} \equiv 1 \bmod p$

Corollary: order of every elt. divides $p-1$

E.g. $\mathbb{F}_{17}$. 3 has order 16

$3^{16} \equiv 1$

$(3^4)^4 = 1$

Key Idea

Given list of values in $\mathbb{F}_p$, $1 = \omega^0$

can "encode" it as polynomial

$\vec{a} = (1, 2, 3, 4)$

$\vec{a}[0] = 1$

$\vec{a}[1] = 2$

$\vec{a}[2] = 3$

$\vec{a}[3] = 4$

$P_{\vec{a}}(1) = 1$

$P_{\vec{a}}(\omega) = 2$

$P_{\vec{a}}(\omega^2) = 3$

$P_{\vec{a}}(\omega^3) = 4$

(In general, $P_{\vec{a}}(\omega^i) = \vec{a}[i]$)

Polynomial interpolation

$\vec{a} = (1, 2, 3, 4)$ FFT

13

$P_{\vec{a}}(1) = 1$

$P_{\vec{a}}(13) = 2$

$P_{\vec{a}}(13^2) = 3$

$P_{\vec{a}}(13^3) = 4$

Lagrange interpolation $O(d^2)$

NTT/FFT: smooth field in $O(d \log d)$

$P_{\vec{a}}(x) = 10x^3 + 8x^2 + 6x + 11$

$P_{\vec{a}}(1) = \underbrace{10 \cdot 1 + 8 \cdot 1}_{1} \quad \underbrace{6 + 11}_{0}$

$= 1$

Agenda for this lecture

- Announcements
- Background: interpolating polynomials on subgroups
- Arithmetizing Plonkish constraints
- Gate check
- Wiring check

Arithmetizing constraints

$C = (\gamma, \$)$ $\quad \vec{X} \in \mathbb{F}^m$ $\quad \forall c \in [n]$

$\$[i](X[a[i]] \cdot X[b[i]]) + (1-\$[i])(X[a[i]] + X[b[i]]) - X[c[i]] = 0$

Need to transform into statement about polys

Trace T: $n \times 3$ table where ith row is left/right/output

"Public inputs": subset of wire indices for inputs known to both parties

I = set of public inputs

Take ω order $3n + |I|$.

$T(\omega^{-j-1}) =$ pub input j

Encode T as:

$T(\omega^{3i}) =$ left input of gate i

$T(\omega^{3i+1}) =$ right " " " "

$T(\omega^{3i+2}) =$ output of gate i

Arithmetizing constraints

Check T satisfies ϕ via:

(1) T encodes pub inputs correctly

(2) all gates correct

(3) all wiring correct

(4) check that output wire has value 1

(4) Check $T(\omega^{3n-1}) = 1$

(1) – (3) next time

Agenda for this lecture

- Announcements
- Background: interpolating polynomials on subgroups
- Arithmetizing Plonkish constraints
- Gate check
- Wiring check

Gate check

Agenda for this lecture

- Announcements
- Background: interpolating polynomials on subgroups
- Arithmetizing Plonkish constraints
- Gate check
- Wiring check

Wiring check (check copies via permutation)