EECS 498/CSE 598: Zero-Knowledge Proofs
Winter 2026
Lecture 5

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Multilinear extensions
- Relations, languages, the class NP
- Cryptography background
- Interactive proofs

Agenda for this lecture

- Announcements
- Multilinear extensions
- Relations, languages, the class NP
- Cryptography background
- Interactive proofs

Announcements

- Project 1 is online
- Autograder is working
- I saw a good movie this weekend =>

Agenda for this lecture

- Announcements
- Multilinear extensions
- Relations, languages, the class NP
- Cryptography background
- Interactive proofs

Multilinear extensions

Let $\{0,1\}^v$ be bit strings.

Any $f \in \mathbb{F}_p^{2^v}$ is a f'n $\{0,1\}^v \to \mathbb{F}_p$

Def: A v-variate poly g extends $f : \{0,1\}^v \to \mathbb{F}_p$ if $\forall i \in \{0,1\}^v$, $g(i) = f(i)$

$g : \mathbb{F}_p^v \to \mathbb{F}_p$ (where $g(i) = g(i_0, i_1, \ldots, i_{v-1})$ where $i = \sum_j 2^j i_j$)

Multilinear extensions (MLE)

Thm: Any function $f : \{0,1\}^v \to \mathbb{F}_p$ has a unique MLE.

Proof: Define

$$\chi_w(x_1, \dots, x_v) := \prod_{i=1}^{v} (x_i w_i + (1-x_i)(1-w_i))$$

$$\chi_w(x) := \begin{cases} 1 & \text{if } \vec{x} = \vec{w} \\ 0 & \text{o/w} \end{cases}$$

$$\tilde{f}(x_1, \dots, x_v) := \sum_{w \in \{0,1\}^v} f(w) \cdot \chi_w(x_1, \dots, x_v)$$

Claim: $\tilde{f}$ extends f

Claim: $\tilde{f}$ is ML

χ_w is ML

$\tilde{f}$ is lin comb of ML

Claim: $\tilde{f}$ is unique!

Multilinear extensions

$$\chi_w(x_1, \ldots, x_n) = \prod_i (x_i w_i + (1-x_i)(1-w_i))$$

$$= \chi_{w_1 \ldots w_{n/2-1}}(x_1 \ldots x_{n/2-1}) \chi_{w_{n/2} \ldots w_n}(x_{n/2} \ldots x_n)$$

$\tilde{f}$ extends f

break $\tilde{f}$ into 'chunks'

Multilinear extensions

Agenda for this lecture

- Announcements
- Multilinear extensions
- Relations, languages, the class NP
- Cryptography background
- Interactive proofs

Relations and languages, the class NP

A language L is subset of $\{0,1\}^*$

$L \Rightarrow$ set of objects sharing a property

$L_{3CNFSAT}$ L_{3COL} $x \in L$

A relation R is a subset of $\{0,1\}^* \times \{0,1\}^*$

Associate R_L to L via "witness"

$x \in L$ iff $\exists w$ s.t $(x,w) \in R_L$

A "checker"/"verifier" V for R_L is algorithm

takes (x,w), outputs 1 if $(x,w) \in R_L$,

0 o/w

Relations and languages, the class NP

NP :

class of languages

with deterministic PT

verifiers

$V_{3CNFSAT}(x, w)$

An NP-complete language:

rank-one constraint systems (R1CS)

Field $\mathbb{F}$, numbers $m, n \in \mathbb{N}$

An NP-complete language:

rank-one constraint systems (R1CS)

Field $\mathbb{F}$, numbers $m, n \in \mathbb{N}$

R1CS is defined by three matrices $A, B, C \in \mathbb{F}^{m \times n}$.

Say that $z \in \mathbb{F}^n$ satisfies the R1CS if:

$$(A \cdot z) \circ (B \cdot z) = C \cdot z$$

Notation: operator $\circ$ just means element-wise multiplication of vectors. Also called "Hadamard product"

An NP-complete language:

rank-one constraint systems (R1CS)

Field $\mathbb{F}$, numbers $m, n \in \mathbb{N}$

R1CS is defined by three matrices $A, B, C \in \mathbb{F}^{m \times n}$.

Say that $z \in \mathbb{F}^n$ satisfies the R1CS if:

$$(A \cdot z) \circ (B \cdot z) = C \cdot z$$

Can split z into a "public" part $x \in \mathbb{F}^{\ell}$ and "private" part $w \in \mathbb{F}^{n-\ell}$ ....

s.t.

$z = (x, w)$ satisfies

Notation: operator $\circ$ just means element-wise multiplication of vectors. Also called "Hadamard product"

Agenda for this lecture

- Announcements
- Multilinear extensions
- Relations, languages, the class NP
- Cryptography background
- Interactive proofs

Security definitions and adversaries

↳ Formal statement about a testable ability of an adversary to "do something"

→ break a protocol

Sec defs: a few important parts

- setup (parameters)
- generate challenge instance
- run some adversary, gets its output
  - give it oracles
- success condition

Crypto: adversaries "efficient"

Example security definition:
the discrete logarithm problem

$\log_G A$
x s.t. $xG = A$

$\mathsf{DL}^{\mathbb{G},G,p}(\mathcal{A})$:

$x \leftarrow\$ \mathbb{Z}_p$

$x' \leftarrow\$ \mathcal{A}(xG, \mathbb{G}, G, p)$

Return $x = x'$

$Adv^{DL}(\mathcal{A}) = Pr[DL^{\mathbb{G},G,p}(\mathcal{A}) = 1]$

DL hard in $\mathbb{G}$ if $\forall$ nuPPT $\mathcal{A}$, $Adv^{DL}(\mathcal{A}) = negl(n)$

Agenda for this lecture

- Announcements
- Multilinear extensions
- Relations, languages, the class NP
- Cryptography background
- Interactive proofs

Interactive proofs

Properties of interactive proofs

(If time) Finishing up Schwartz-Zippel