CSE 575: Advanced Cryptography
Fall 2024
Lecture 24

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Product check PIOP
- Permutation check PIOP
- “Prescribed” permutation check PIOP
- Compiling (P)IOPs to arguments

Agenda for this lecture

- Announcements
- Product check PIOP
- Permutation check PIOP
- “Prescribed” permutation check PIOP
- Compiling (P)IOPs to arguments

Announcements

- HW4 is out, due 12/6
- Final: will be assigned tonight 11:59pm, due 12/14 11:59pm.
  - Take **at most** one week, but you choose when to start.
- Rest of class: no typeset lecture notes.
  - Can get extra credit for typesetting
- Luke will prove evaluation binding of KZG in discussion

Agenda for this lecture

- Announcements
- Product check PIOP
- Permutation check PIOP
- “Prescribed” permutation check PIOP
- Compiling (P)IOPs to arguments

Zooming out a bit

Plonk PIOP

$P(S, P, X, W, pp)$:

compute trace T,
interpolate it
$\sum = \langle \omega \rangle$

ℓ_T ⟶ build PI poly v

1	2	3

$T(\omega^0) = 1$

$T(\omega^1) = 2$

$T(\omega^2) = 3$

$V(\ell_S, \ell_P, X)$:

⟵ PIOPs of ℓ_T for checks:
1. pub input
2. gate
3. wiring
4. output

Product check

$f : \prod_{a \in \Omega} f(a) = 1$

Define $t(1) = f(1)$

$t(\omega^s) = \prod_{i=0}^{s} f(\omega^i)$ for $i = 1$ to $k-1$

$t(\omega x) = t(x) f(\omega x) \quad \forall x \in \Omega$

Even at ω^{k-1}: (if $\prod_a f(a) = 1$):

$t(\omega \cdot \omega^{k-1}) = t(\omega^k) = t(1)$

$t(\omega^{k-1}) f(\omega^k) = t(\omega^{k-1}) f(1)$

$t(1) = f(1)$

Lemma: if $t(\omega^{k-1}) \overset{(1)}{=} 1$ and

(2) $t(\omega x) - t(x) f(\omega x) = 0 \quad \forall x \in \Omega$

then $\prod_a f(a) = 1$

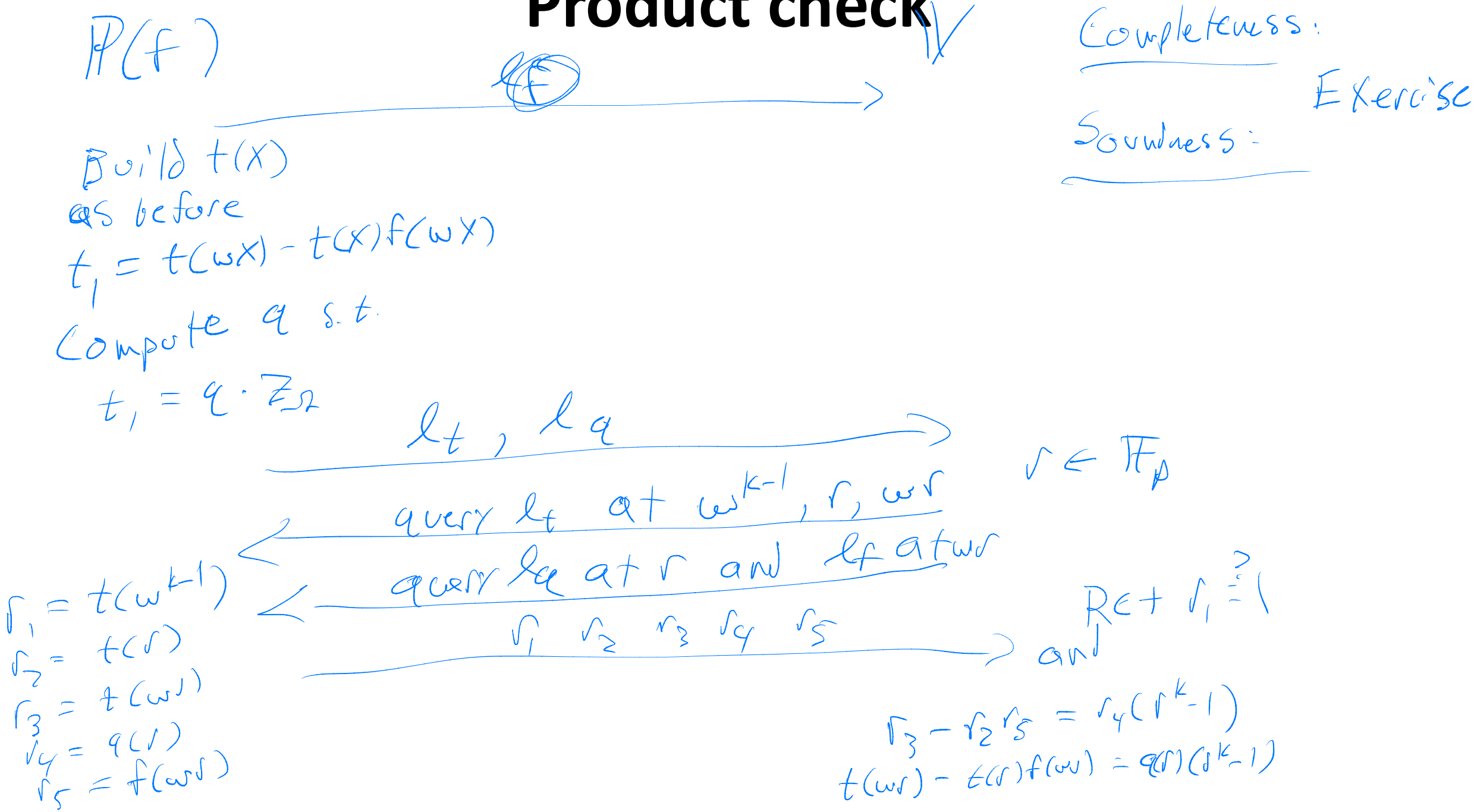
Proof:

$1 = t(\omega^{k-1}) = t(\omega \cdot \omega^{k-2})$ By 2)

$= t(\omega^{k-2}) f(\omega^{k-1})$

Recursively apply to $t(\omega^{k-2})$

Product check



Completeness:

Exercise

Soundness:

Product check

$$\prod_{a \in \Omega} \left(\frac{f}{g}\right)(a) = 1$$

Define t as

$$t(1) = f(1)/g(1)$$

$$t(\omega^s) = \prod_{i=0}^{s} \frac{f(\omega^i)}{g(\omega^i)} \qquad \text{for } s = 1, \ldots, k-1$$

Lemma: If $t(\omega^{k-1}) = 1$ and $t(\omega x) g(\omega x) = t(x) f(\omega x) \quad \forall x \in \Omega$

then $\prod_{a \in \Omega} \frac{f(a)}{g(a)} = 1$

Agenda for this lecture

- Announcements
- Product check PIOP
- Permutation check PIOP
- “Prescribed” permutation check PIOP
- Compiling (P)IOPs to arguments

Permutation check

Two polys f, g Prove $f(\Omega) = \{f(1), f(\omega), \ldots, f(\omega^{k-1})\}$

$g(\Omega) = \{g(1), g(\omega), \ldots, g(\omega^{k-1})\}$

are equal up to permutation σ

For $\hat{f} = \prod_{a \in \Omega} (X - f(a))$

$\hat{g} = \prod_{a \in \Omega} (X - g(a))$

Lemma: $\hat{f} = \hat{g}$ iff $f(\Omega)$ is a permutation of $g(\Omega)$

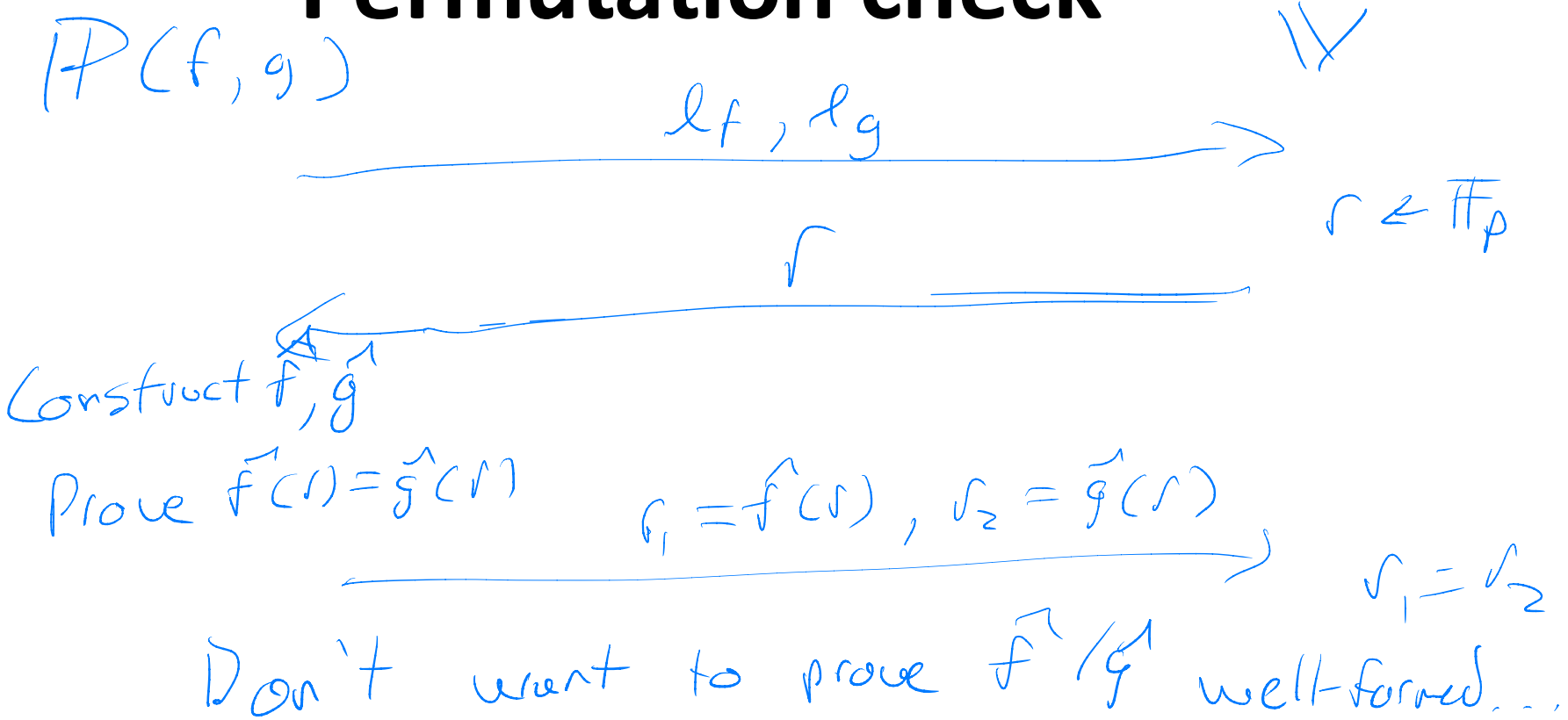
Proof:

($\Rightarrow$) use factorization of $\hat{f}/\hat{g}$ to construct σ

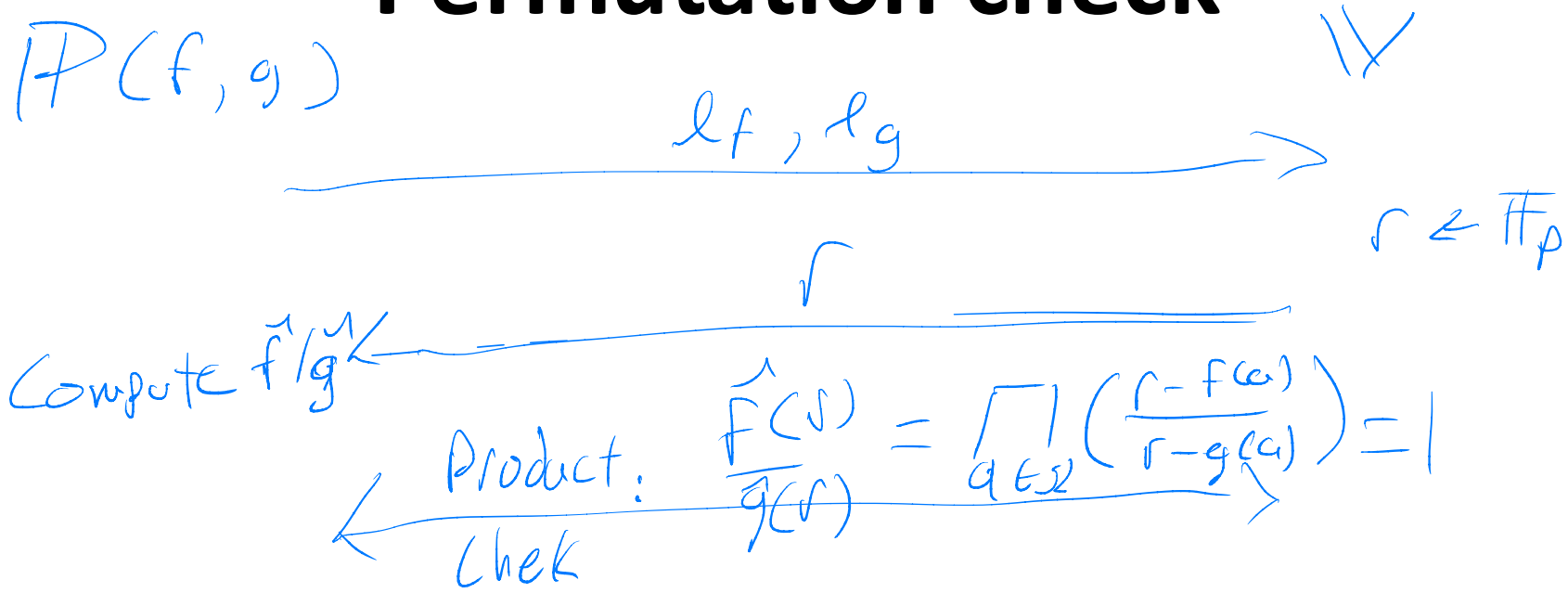
($\Leftarrow$) roots of $\hat{f}/\hat{g}$ are same, so $\hat{f} = \hat{g}$

(and $\deg \hat{f} = \deg \hat{g}$)

Permutation check



Permutation check



Agenda for this lecture

- Announcements
- Product check PIOP
- Permutation check PIOP
- “Prescribed” permutation check PIOP
- Compiling (P)IOPs to arguments

Checking a *specific* permutation

Let $W: \Omega \to \Omega$ be poly that permutes Ω according to $\sigma: [k] \to [k]$

$$W(\omega^i) = \omega^{\sigma(i)} \text{ for } i \in k$$

Prove f, g are the same on Ω;

up to W: $f(a) = g(W(a))$ $\forall a$

Observe: if $(W(a), f(a))$ is a perm of $(a, g(a))$

then $f(a) = g(W(a)) \quad \forall a \in \Omega$

Agenda for this lecture

- Announcements
- Product check PIOP
- Permutation check PIOP
- “Prescribed” permutation check PIOP
- Compiling (P)IOPs to arguments

Compiling (P)IOPs to arguments