On The Hardness of Approximate and Exact (Bichromatic) Maximum Inner Product

$$Max_{(a,b)\in A\times B}\ a \cdot b$$

Lijie Chen (Massachusetts Institute of Technology)

Max-IP and Z-Max-IP

- **(Boolean) Max-IP**:
  - Given sets A and B of Boolean vectors (each of size n) find a in A and b in B with maximum inner product:
    - For sets A and B, set $MaxIP(A,B) \coloneqq \max_{(a,b)\in A\times B} \langle a,b\rangle$.
  - Approx. version: find a r-multiplicative approximation to the answer:
    - Want an ALG s.t. $MaxIP(A,B) \leq ALG(A,B) \leq MaxIP(A,B)\cdot r$.

- **Z-Max-IP**:
  - Two sets of n Integer vectors.

Max-IP and Z-Max-IP

- Basic problems, relevant in practice.
- Important theoretical implications as well.
- Approx. Boolean Max-IP:
  - [ARW'17]: basis of the recent breakthrough result in Hardness for Approximation in P, implies hardness for many other problems.
- Z-Max-IP:
  - [Wil'18]: Hardness for Z-Max-IP implies hardness for finding furthest pair in low dimension Euclidean space.

- Bichromatic LCS Closest Pair over permutations,
- Approximate Regular Expression Matching,
- Diameter in Product Metric,
- Approximate Closest Pair in Euclidian Space [Rub'18]

New Hardness for Z-Max-IP (under SETH)

- Z-Max-IP for n vectors of $2^{O(\log^* n)}$ dimensions requires $n^{2-o(1)}$ time under SETH.
  - Z-Max-IP for n vectors of $2^{O(\log^* n)}$ in $n^{1.99}$ time.
  - ⇒Max-IP for n vectors of $O(\log n)$ dim. in $n^{1.99}$ time.
  - ⇒CNF-SAT for n variables and $O(n)$ clauses in $2^{0.995n}$ time.
  - ⇔SETH is false. [CIP'06]

Z-Max-IP:
Given sets A and B of Integer vectors (each of size n) find a in A and b in B with maximum inner product:

- *Closer to the upper bound*
  - [Mat'92] : Z-Max-IP in $n^{2-1/O(d)}$ time.

$$\log^*(n) := \begin{cases} 0 & n \le 1; \\ \log^*(\log n) + 1 & n > 1. \end{cases}$$

Upper Bound	?	Lower Bound	⟸	Lower Bound
$n^{2-\epsilon}$ when $d = O(1)$ [Mat'92]		$n^{2-o(1)}$ when $d = 2^{O(\log^* n)}$ [This work]		$n^{2-o(1)}$ when $d = \omega(\log^2 \log n)$ Implicit in [Wil'18]

New Hardness for Z-Max-IP (under SETH)

1. New Hardness for Z-Max-IP (under SETH):
   - Z-Max-IP for n vectors of $2^{O(\log^* n)}$ dimensions requires $n^{2-o(1)}$ time.

Z-Max-IP:
Given sets A and B of Integer vectors (each of size n) find a in A and b in B with maximum inner product:

- *Separation for Boolean Max-IP / Z-Max-IP:*
  - Z-Max-IP is **much harder** than Boolean Max-IP.
  - Progress on Open Problem 23 in Dagstuhl workshop on *Structure and Hardness in P*

$$\log^*(n) := \begin{cases} 0 & n \le 1; \\ \log^*(\log n) + 1 & n > 1. \end{cases}$$

Z-Max-IP	Boolean Max-IP
$n^{2-o(1)}$ when $d = 2^{O(\log^* n)}$ [This work]	$n^{2-\epsilon}$ when $d = c \log n$. [AW15, ACW16]
HARD	EASY

New Hardness for Z-Max-IP (under SETH)

1. New Hardness for Z-Max-IP (under SETH):
   - Z-Max-IP for n vectors of $2^{O(\log^* n)}$ dimensions require $n^{2-o(1)}$ time.

Z-Max-IP:
Given sets A and B of Integer vectors (each of size n) find a in A and b in B with maximum inner product.

- *New Hardness for ℓ_2-Furthest Pair in R^d. (reductions from [Wil18])*
  - Finding *ℓ_2-Furthest Pair in R^d among n points for $d = 2^{O(\log^* n)}$ requires $n^{2-o(1)}$ time.*
  - *Stronger separation between furthest and closest pair.*

$$\log^*(n) := \begin{cases} 0 & n \le 1; \\ \log^*(\log n) + 1 & n > 1. \end{cases}$$

ℓ_2-Furthest Pair		ℓ_2-Furthest Pair		ℓ_2-Closest Pair
$n^{2-o(1)}$ when $d = 2^{O(\log^* n)}$	⟸	$n^{2-o(1)}$ when $d = \omega(\log^2 \log n)$		$2^{O(d)} \cdot n\ polylog(n)$
[This work]		[Wil'18]		[BS76, KM95, DHKP97]
HARD				EASY

Characterization of Boolean Approx. Max-IP

2. Characterization of Approx. Max-IP:

- [ARW'17]: Finding $2^{(\log^{1-o(1)} n)}$ approximation to Max-IP with $n^{o(1)}$ dimensions, requires $n^{2-o(1)}\ time$.

- A more refined question:
  - *For each vector dimension $d = d(n)$, what is the smallest r such that Max-IP can be r-approximated in truly sub-quadratic time?*

- **Boolean Max-IP**:
  - For sets A and B with n Boolean vectors, find $MaxIP(A,B) := \max_{(a,b)\in A\times B} \langle a,b\rangle$.
  - Approx. version: find a r-multiplicative approximation to the answer: $MaxIP(A,B) \le ALG(A,B) \le MaxIP(A,B)\cdot r$.
  - d = d(n) : vector dimensions
  - r = r(n) : approx. ratio

Characterization of Boolean Approx. Max-IP

2. Characterization of Approx. Max-IP:

- A more refined question:
  - *For each vector dimension $d = d(n)$, what is the smallest r such that Max-IP can be r-approximated in truly sub-quadratic time?*

- We obtain a characterization (under SETH)!
  - For all d satisfying $\omega(\log n) < d < n^{o(1)}$
  - Truly sub-quadratic time for $r = \left(\frac{d}{\log n}\right)^{\Omega(1)}$ EASY!
  - Requires $n^{2-o(1)}$ time for $r = \left(\frac{d}{\log n}\right)^{o(1)}$ HARD!

- **Boolean Max-IP**:
  - For sets A and B with n Boolean vectors, find $MaxIP(A,B) := \max_{(a,b)\in A\times B} \langle a, b\rangle$.
  - Approx. version: find a r-multiplicative approximation to the answer: $MaxIP(A,B) \le ALG(A,B) \le MaxIP(A,B)\cdot r$.
  - d = d(n) : vector dimensions
  - r = r(n) : approx. ratio

Characterization of Boolean Approx. Max-IP

2. Characterization of Approx. Max-IP:
   - We obtain a characterization!
     - $r = \left(\frac{d}{\log n}\right)^{\Omega(1)}$ $n^{2-\epsilon}$ time. EASY!
     - $r = \left(\frac{d}{\log n}\right)^{o(1)}$ $n^{2-o(1)}$ time. HARD!
   - Example:
     - $d = c \log n$, $O(1)$-approximation is EASY.
     - $d = \log^2 n$, $O(\log^{0.1} n)$–approximation is EASY.
     - $d = \log^2 n$, $(\log^{o(1)} n)$-approximation is HARD.
   - Upper Bound via *polynomial method*.
   - Lower Bound follows from [Rub'18].

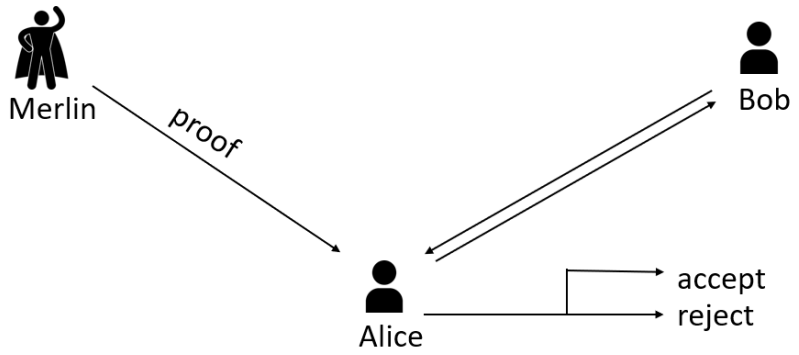
- **Boolean Max-IP**:
  - For sets A and B with n Boolean vectors, find $MaxIP(A,B) := \max_{(a,b)\in A\times B} \langle a, b\rangle$.
  - Approx. version: find a r-multiplicative approximation to the answer: $MaxIP(A,B) \le ALG(A,B) \le MaxIP(A,B)\cdot r$.
  - d = d(n) : vector dimensions
  - r = r(n) : approx. ratio

New Merlin-Arthur Protocol for Set-Disjointness

3. A new MA Protocol for Set-Disjointness

- [AW'09]: An $O(\sqrt{n}\log n)$ MA protocol.
- [Kla'03]: $\Omega(\sqrt{n})$ Lower Bound.
- This work: an $O(\sqrt{n\log n\log\log n})$ protocol.

- **MA Communication Protocol**:
  - Alice holds x, Bob holds y, want to compute F(x,y).



- F(x,y) = 1 ⇒ exists a proof, $\Pr[acc] \geq \frac{2}{3}$.
- F(x,y) = 0 ⇒ for all proofs, $\Pr[acc] \leq \frac{1}{3}$.
- Complexity = Proof Length + Communication

$\Omega(\sqrt{n})$ [Lower Bound] [Kla'03] **?** $O(\sqrt{n\log n\log\log n})$ [Upper Bound] [This work] ⟸ $O(\sqrt{n}\log n)$ [Upper Bound] [AW'09]

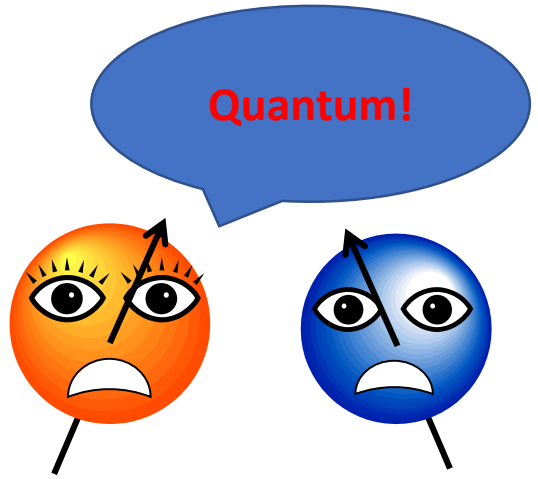
New Connection with Communication Complexity

4. New Connection with Communication Complexity

- [ARW'17]:
  - $\sqrt{n}\log n$ MA protocol for Set-Disjointness
  - $\Rightarrow$ SETH-Hardness for Approx. Boolean Max-IP.

- Open Question from [ARW'17]:
  - There is a $\sqrt{n}$ BQP protocol for Set-Disjointness. Does it also imply some hardness results?

- [This work]: YES!
  - $\sqrt{n}$ BQP protocol for Set-Disjointness
  - $\Rightarrow$ SETH-Hardness for Approx. $\{-1,1\}$-Max-IP



$\{-1, 1\}$-Max-IP:
Given sets A and B of vectors with $\{-1,1\}$ entries (each of size n) find a in A and b in B with maximum inner product.

Proof Overview: SETH-Hardness of Z-Max-IP

- Starting Point： SETH implies OV Conjecture.

- Orthogonal Vectors (OV) Problem:
  - Given two sets A,B of Boolean vectors, find an orthogonal pair between them.

OV Conjecture: OV with sets of n vectors, $\omega(\log n)$ dimensions requires $n^{2-o(1)}$ time.

Our Goal: A “dimensionality” reduction
from $\omega(\log n)$ dimensional OV to $2^{O(\log^* n)}$ dimensional Z-Max-IP

Reduction RoadMap

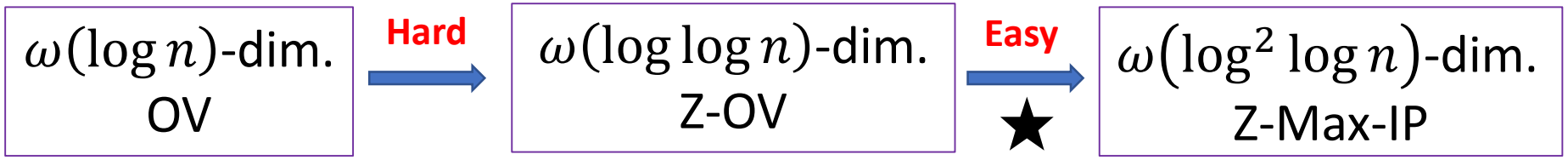
- First cover a baby version which shows $\omega(\log^2 \log n)$ dimensional Z-Max-IP is hard. (same as [Wil'18])
  - Then outline the key ideas to get the $2^{O(\log^* n)}$ dimensional hardness.

- An intermediate problem:
  - **Z-OV**: Given two sets A,B of Integer vectors, find an orthogonal pair between them.

Orthogonal Vectors (OV) Problem:
Two sets A,B of Boolean vectors, find an orthogonal pair between them.

Z-Max-IP:
Two sets of n Integer vectors. find a pair between them which maximize their inner product.

$\omega(\log n)$-dim. OV → **Hard** → $\omega(\log \log n)$-dim. Z-OV → **Easy** → $\omega(\log^2 \log n)$-dim. Z-Max-IP

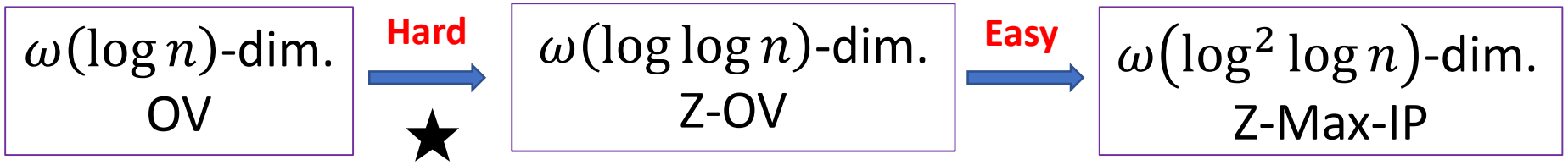


Easy Part: Z-OV ⇒Z-Max-IP

- Implicit in [Wil'18].
- $a, b \in Z^d$. (Squaring trick)
  - $a \cdot b = 0 \Rightarrow -(a \cdot b)^2 = 0$
  - $a \cdot b \neq 0 \Rightarrow -(a \cdot b)^2 < 0$
- To solve Z-OV, it suffices to calculate the maximum value of $-(a \cdot b)^2$ for $(a, b) \in A \times B$.
- $-(a \cdot b)^2 = -(\sum_i a_i \cdot b_i)^2 = -\sum_{i,j} a_i a_j b_i b_j$
- $\bar{a}_{i,j} = a_i \cdot a_j$, $\bar{b}_{i,j} = -b_i \cdot b_j$.
- Maximize $\bar{a} \cdot \bar{b}$, Z-Max-IP with d^2 dim.

Z-OV:
Two sets A,B of Integer vectors, find an orthogonal pair between them.

Z-Max-IP:
Given sets A and B of Integer vectors (each of size n) find a in A and b in B with maximum inner product.



Hard Part: OV ⇒Z-OV

- Want to reduce the dimension:
  - E.g. use *few integers* to represent a *long Boolean vector*
- Key Idea: Chinese Remainder Theorem (CRT)!
- t primes $q_1, q_2, \cdots, q_t$.
- t remainders $r_1, r_2, \cdots, r_t$.
- CRT: exists a unique integer $0 \leq x < \prod_i q_i$, s.t.
  - $x \equiv r_i \ (mod\ q_i)$.

Use a number to represent a vector

x

$r_1, r_2, \cdots, r_t$

OV:
Two sets A,B of Boolean vectors, find an orthogonal pair between them.

Z-OV:
Two sets A,B of Integer vectors, find an orthogonal pair between them.

$\omega(\log n)$-dim. OV

Hard ★

$\omega(\log\log n)$-dim. Z-OV

Easy

$\omega(\log^2 \log n)$-dim. Z-Max-IP

Chinese Remainder Theorem

- Fix t primes $q_1, q_2, \cdots, q_t$.
- $a = crr(x_1, x_2, \cdots, x_t)$, i.e. $a \equiv x_i (mod\ q_i)$.
- $b = crr(y_1, y_2, \cdots, y_t)$, i.e. $b \equiv y_i (mod\ q_i)$.

$crr(r_1, r_2, \cdots, r_t) :=$
the unique integer $0 \leq x < \prod_i q_i$, s.t.
$x \equiv r_i\ (mod\ q_i)$.

crr: *Chinese Remainder Representation*

$$a \cdot b \equiv x_i \cdot y_i (mod\ q_i) \text{ for } 1 \leq i \leq t.$$

Multiplication between Two integers

simulate

Multiplication between Two vectors

Exactly what we want!

$\omega(\log n)$-dim. OV → (Hard ★) $\omega(\log\log n)$-dim. Z-OV → (Easy) $\omega(\log^2 \log n)$-dim. Z-Max-IP

Hard Part: OV ⇒Z-OV

- The reduction:
  - d : vector dimension ($d = \omega(\log n)$).
  - $\ell \cdot b = d$
  - represent a vector x in $\{0,1\}^{\mathrm{d}}$ by a $\ell \times b$ table.
  - Map each row into a single number using Chinese Remainder Theorem

$crr(r_1, r_2, \cdots, r_t) :=$
the unique integer $0 \le x < \prod_i q_i$, s.t.
$x \equiv r_i \ (mod\ q_i)$.

crr: *Chinese Remainder Representation*

b columns

ℓ rows

$x_{1,1}$	$x_{1,2}$	$\cdots$	$x_{1,b}$
$\vdots$	$\ddots$	$\ddots$	$\vdots$
$x_{\ell,1}$	$x_{\ell,2}$	$\cdots$	$x_{\ell,b}$

$x \in \{0,1\}^d$

→

$crr(x_{1,1}, x_{1,2}, \cdots, x_{1,b})$
$\vdots$
$crr(x_{\ell,1}, x_{\ell,2}, \cdots, x_{\ell,b})$

$\varphi(x) \in Z^{\ell}$

Want ℓ to be as small as possible

$\omega(\log n)$-dim. OV → (Hard ★) $\omega(\log\log n)$-dim. Z-OV → (Easy) $\omega(\log^2 \log n)$-dim. Z-Max-IP

Hard Part: OV ⇒Z-OV

b columns

ℓ rows

$x_{1,1}$	$x_{1,2}$	$\cdots$	$x_{1,b}$
$\vdots$	$\ddots$	$\ddots$	$\vdots$
$x_{\ell,1}$	$x_{\ell,2}$	$\cdots$	$x_{\ell,b}$

$x \in \{0,1\}^d$

→

$crr(x_{1,1}, x_{1,2}, \cdots, x_{1,b})$
$\vdots$
$crr(x_{\ell,1}, x_{\ell,2}, \cdots, x_{\ell,b})$

$\varphi(x) \in Z^{\ell}$

- The reduction:
  - d : vector dimension
  - $\ell \cdot b = d$
  - represent a vector x in $\{0,1\}^{\mathrm{d}}$ by a $\ell \times b$ table.
  - Map each row into a single number using Chinese Remainder Theorem

For $i \in [\ell]$ and $j \in [b]$, $\varphi(x)_i \equiv x_{i,j} \ (mod\ q_j)$

$$\varphi(x) \cdot \varphi(y) \ (mod\ q_j)$$
$$= \sum_{i=1}^{\ell} (\varphi(x)_i \cdot \varphi(y)_i)(mod\ q_j)$$
$$= \sum_{i=1}^{\ell} (x_{i,j} \cdot y_{i,j})(mod\ q_j)$$

→ The inner product of j-th column of x and j-th column of y.

→ Set all $q_j > \ell$.
$x \cdot y = 0 \Leftrightarrow \varphi(x) \cdot \varphi(y) \equiv 0 \ (mod\ q_j)$ for all j.

$\omega(\log n)$-dim. OV → (Hard ★) $\omega(\log\log n)$-dim. Z-OV → (Easy) $\omega(\log^2 \log n)$-dim. Z-Max-IP

Hard Part: OV ⇒Z-OV

- $V \coloneqq$ all multiples of $\prod_j q_j$ between 0 and $\ell \cdot \left(\prod_j q_j\right)^2$.
- Given an OV instance with sets A and B.
- $x \cdot y = 0 \Leftrightarrow \varphi(x) \cdot \varphi(y) \equiv 0 \ (mod\ q_j)$ for all $j \Leftrightarrow \varphi(x) \cdot \varphi(y) \in V$.
- Let $v \in V$,
  - $\varphi(x) \cdot \varphi(y) = v \Leftrightarrow [\varphi(x), -1] \cdot [\varphi(y), v] = 0$.
  - $A_v \coloneqq \{[\varphi(x), -1] : x \in A\}$.
  - $B_v \coloneqq \{[\varphi(y), v] : y \in B\}$.

- Therefore,
  - There is an orthogonal pair between A and $B \Leftrightarrow$
  - There exists v s.t. there is an orthogonal pair between A_v and B_v.

- In summary:
  - One d-dim. OV instance ⇒ $|V|$ instances of $(\ell + 1)$-dim. Z-OV

$$\varphi(x) \cdot \varphi(y) \ (mod\ q_j)$$
$$= \sum_{i=1}^{\ell} (\varphi(x)_i \cdot \varphi(y)_i)(mod\ q_j)$$
$$= \sum_{i=1}^{\ell} (x_{i,j} \cdot y_{i,j})(mod\ q_j)$$

The inner product of j-th column of x and j-th column of y.

Set all $q_j > \ell$.
$x \cdot y = 0 \Leftrightarrow \varphi(x) \cdot \varphi(y) \equiv 0 \ (mod\ q_j)$ for all j.

Hard Part: OV ⇒Z-OV Informal Analysis

- Recall what we have: $\omega(\log n)$-dim. OV requires $n^{2-o(1)}$ time.
- To preserve hardness, want $|V| = n^{o(1)}$.
  - $|V| = \left(\prod_j q_j\right)^{O(1)} = b^{O(b)}$.
  - Have to set $b = o\left(\frac{\log n}{\log\log n}\right)$.
  - Therefore, $\ell = \frac{\omega(\log n)}{b} = \omega(\log\log n)$.
- Q.E.D.

- $V \coloneqq$ all multiplier of $\prod_j q_j$ between 0 and $\ell \cdot \left(\prod_j q_j\right)^2$.
  - $A_v \coloneqq \{[\varphi(x), -1] : x \in A\}$.
  - $B_v \coloneqq \{[\varphi(y), v] : y \in B\}$.
- Therefore,
  - There is an orthogonal pair between A and $B \Leftrightarrow$
  - There exists v s.t. there is an orthogonal pair between A_v and B_v.
- In summary:
  - One d-dim. OV instance ⇒ $|V|$ instances of $(\ell+1)$-dim. Z-OV

$\omega(\log n)$-dim. OV ✓→ $\omega(\log\log n)$-dim. Z-OV **Easy**→ $\omega\left(\log^2\log n\right)$-dim. Z-Max-IP

$2^{O(\log^* n)}$dim. Hardness: Sketch

- What is the bottleneck?
- Not enough small primes!
  - $q_i's$ are b distinct primes, most of them $\gg b$, even if we only need them to be $> \ell$.
- Idea: Use another CRT to *embed small primes inside big primes*.
- Recursive: Then pack even smaller primes inside small primes, and recurse.
  - *Pretend we have many small primes, even though we don't'.*

- Recall what we have: $\omega(\log n)$-dim. OV requires $n^{2-o(1)}$ time.
- To preserve hardness, want $|V| = n^{o(1)}$.
  - $|V| = \left(\prod_j q_j\right)^{O(1)} = b^{O(b)}$.
  - Have to set $b = o\left(\frac{\log n}{\log\log n}\right)$.
  - Therefore, $\ell = \frac{\omega(\log n)}{b} = \omega(\log\log n)$.
- Q.E.D.

One Step of Recursion

- Pick w primes $p_1, p_2, \cdots, p_w$, such that $\left(\prod_j p_j\right)^2 \cdot \ell < b$.
  - d : vector dimension ($d = \omega(\log n)$)
  - $\ell \cdot b = d$ (want ℓ as small as possible)
  - represent a vector x in $\{0,1\}^{\mathrm{d}}$ by a $\ell \times (b/w)$ table, each entry is a vector in $\{0,1\}^w$.

inner crr_m: CRT w.r.t small primes $p_i's$
outer crr: CRT w.r.t. big primes q_i's, $q_i > b$.

b/w columns

ℓ rows

$\vec{x}_{1,1}$	$\vec{x}_{1,2}$	$\cdots$	$\vec{x}_{1,b/w}$
$\vdots$	$\ddots$	$\ddots$	$\vdots$
$\vec{x}_{\ell,1}$	$\vec{x}_{\ell,2}$	$\cdots$	$\vec{x}_{\ell,b/w}$

$crr(crr_m(\vec{x}_{1,1}), crr_m(\vec{x}_{1,2}), \cdots, crr_m(\vec{x}_{1,b/w}))$
$\vdots$
$crr(crr_m(\vec{x}_{\ell,1}), crr_m(\vec{x}_{\ell,2}), \cdots, crr_m(\vec{x}_{\ell,b/w}))$

$x \in \{0,1\}^d$

$\varphi(x) \in Z^\ell$

One Step of Recursion

inner crr_m: CRT w.r.t small primes $p_i's$
outer crr: CRT w.r.t. big primes q_i's, $q_i > b$.

b/w columns

ℓ rows

$\vec{x}_{1,1}$	$\vec{x}_{1,2}$	$\cdots$	$\vec{x}_{1,b/w}$
$\vdots$	$\ddots$	$\ddots$	$\vdots$
$\vec{x}_{\ell,1}$	$\vec{x}_{\ell,2}$	$\cdots$	$\vec{x}_{\ell,b/w}$

$crr(crr_m(\vec{x}_{1,1}), crr_m(\vec{x}_{1,2}), \cdots, crr_m(\vec{x}_{1,b/w}))$
$\vdots$
$crr(crr_m(\vec{x}_{\ell,1}), crr_m(\vec{x}_{\ell,2}), \cdots, crr_m(\vec{x}_{\ell,b/w}))$

$x \in \{0,1\}^d$

$\varphi(x) \in Z^\ell$

For $i \in [\ell]$ and $j \in [b/w]$, $\varphi(x)_i \equiv crr_m(\vec{x}_{i,j}) \ (mod\ q_j)$

$$\varphi(x) \cdot \varphi(y) \ (mod\ q_j)$$
$$= \sum_{i=1}^{\ell} (\varphi(x)_i \cdot \varphi(y)_i)(mod\ q_j)$$
$$= \sum_{i=1}^{\ell} \left(crr_m(\vec{x}_{i,j}) \cdot crr_m(\vec{y}_{i,j})\right)(mod\ q_j)$$

Get to know:

$$\sum_{i=1}^{\ell} \left(crr_m(\vec{x}_{i,j}) \cdot crr_m(\vec{y}_{i,j})\right)$$

and whether for all i,

$$\vec{x}_{i,j} \cdot \vec{y}_{i,j} = 0.$$

$\left(\prod_j p_j\right)^2 \cdot \ell < b \Rightarrow \sum_{i=1}^{\ell} \left(crr_m(\vec{x}_{i,j}) \cdot crr_m(\vec{y}_{i,j})\right) < q_j.$

One Step of Recursion: Informal Analysis

$$\varphi(x)\cdot\varphi(y)\ (mod\ q_j)$$
$$=\sum_{i=1}^{\ell}(\varphi(x)_i\cdot\varphi(y)_i)(mod\ q_j)$$
$$=\sum_{i=1}^{\ell}\left(crr_m(\vec{x}_{i,j})\cdot crr_m(\vec{y}_{i,j})\right)(mod\ q_j)$$

Get to know:

$$\sum_{i=1}^{\ell}\left(crr_m(\vec{x}_{i,j})\cdot crr_m(\vec{y}_{i,j})\right)$$

and whether for all i,

$$\vec{x}_{i,j}\cdot\vec{y}_{i,j}=0.$$

$\left(\prod_j p_j\right)^2\cdot\ell<b\Rightarrow\sum_{i=1}^{\ell}\left(crr_m(\vec{x}_{i,j})\cdot crr_m(\vec{y}_{i,j})\right)<q_j.$

- Set $\left(\prod_j p_j\right)^2\cdot\ell=w^{O(w)}=b$
  $\Rightarrow \mathrm{w}=\Theta(\log b/\log\log b).$
- $|V|=\left(\prod_j q_j\right)^{O(1)}=b^{\mathrm{O}(b/w)}=(\log b)^{O(b)}.$
- Want $|V|=n^{o(1)}$, set $b=o(\log n/\log\log\log n).$
- Therefore, $\ell=\frac{\omega(\log n)}{b}=\omega(\log\log\log n).$
- Improvement!

- A recursive construction leads to the final $2^{O(\log^* n)}$ dim. hardness.

Open Questions

- Construct an $O(\sqrt{n})$-bit MA protocol for Set-Disjointness.

- Show that Z-Max-IP for ***any*** $\omega(1)$ dimensions requires $n^{2-o(1)}$ time under some plausible hypothesis.
  - Implies same hardness for $\omega(1)$ dimensions ℓ_2-Furthest Pair

- **NP·UPP** communication protocol: *a potential approach*
  - NP·UPP: a *relaxation* of MA, *where Arthur's error can be arbitrary close to* 0.5.
  - Our results can be interpreted as a sub-linear proof length, $O(\log^* n)$ communication NP·UPP protocol for Set-Disjointness.
  - $O(\log^* n)$ to $\alpha(n) \Rightarrow$ Z-Max-IP for $2^{\alpha(n)}$ dim. requires $n^{2-o(1)}$ under SETH.

Thanks

Any Questions?