The Kakeya Set Conjecture over $\mathbb{Z}/N\mathbb{Z}$ for general N

Manik Dhar
Princeton University

8th Nov 2021

Introduction

Definition (Kakeya Set)

Given $N, n \in \mathbb{N}$, a set S in $(\mathbb{Z}/N\mathbb{Z})^n$ is Kakeya if for every direction $u \in (\mathbb{Z}/N\mathbb{Z})^n$ there is a line $L_u = \{x + \lambda u | \lambda \in \mathbb{Z}/N\mathbb{Z}\}$ in the direction u contained in S.

- Want to lower bound the size of Kakeya Sets.
- First proposed over finite fields [Wolff, 1999] as a simpler version of the Euclidean Kakeya conjecture (Kakeya Sets in $\mathbb{R}^n$ have Minkowski dimension n).
- Also motivated by applications in TCS for constructing randomness mergers and extractors [Dvir and Wigderson, 2011, Dvir, Kopparty, Saraf, and Sudan, 2013].

Kakeya Set bounds over finite-fields

Theorem (Finite-Field Kakeya [Dvir, 2009, Saraf and Sudan, 2008, Dvir, Kopparty, Saraf, and Sudan, 2013, Bukh and Chao, 2021])

Every Kakeya Set S in $(\mathbb{Z}/p\mathbb{Z})^n$,

$$|S| \geq \frac{p^n}{2^{n-1}}.$$

- This bound is tight and also holds for finite fields in general.
- For composite N we knew

$$|S| \gtrapprox N^{n0.59..}$$

  using work on the "Sum-Difference conjecture" (also known as the arithmetic Kakeya conjecture) [Bourgain, 1999, Katz and Tao, 1999].
- Positively resolving the Sum-Difference conjecture will also resolve the Euclidean Kakeya conjecture!

Kakeya Set Conjecture over $\mathbb{Z}/N\mathbb{Z}$

Conjecture (Kakeya Set Conjecture over $\mathbb{Z}/N\mathbb{Z}$ [Hickman and Wright, 2018])

For all $\epsilon > 0$ and $n \in \mathbb{N}$ there exists a constant $C_{n,\epsilon}$ such that any Kakeya Set $S \subset (\mathbb{Z}/N\mathbb{Z})^n$ satisfies

$$|S| \geq C_{n,\epsilon} N^{n-\epsilon}.$$

- The ϵ is not needed for prime N but is essential in general. [Hickman and Wright, 2018, D and Dvir, 2021]
- The Kakeya problem over $\mathbb{Z}/p^k\mathbb{Z}$ was suggested in [Ellenberg, Oberlin, and Tao, 2010] as another step towards the Euclidean problem as the ring has "scales".
- Kakeya Set lower bounds over $\mathbb{Z}/p^k\mathbb{Z}$ will imply the Minkowski dimension Kakeya conjecture for the p-adics [Ellenberg, Oberlin, and Tao, 2010, Hickman and Wright, 2018].

New results for composites [D and Dvir, 2021]

Theorem (Square-free N [D and Dvir, 2021])

For $N = p_1 \ldots p_r$ where p_i are distinct primes, every Kakeya Set S in $(\mathbb{Z}/N\mathbb{Z})^n$ satisfies,

$$|S| \geq \frac{N^n}{2^{nr}} \geq C_{n,\epsilon} N^{n-\epsilon}$$

- Resolves the Kakeya Set Conjecture for square-free N using well-known bounds for the number of divisors of N.
- Tight up to a factor of 2^r.Can be made tight using [Bukh and Chao, 2021].

New results for composites [D and Dvir, 2021]

Theorem ($\mathbb{Z}/p^k\mathbb{Z}$ reduction [D and Dvir, 2021])

Every Kakeya Set S in $(\mathbb{Z}/p^k\mathbb{Z})^n$ has size at least

$$|S| \geq \operatorname{rank}_{\mathbb{F}_p} W_{p^k,n}.$$

Definition (Matrix $W_{p^k,n}$)

$W_{p^k,n}$ is a matrix whose rows and columns are indexed by points in $(\mathbb{Z}/p^k\mathbb{Z})^n$ with entries,

$$W_{p^k,n}(u,v) = \mathbb{1}_{\langle u,v\rangle = 0}.$$

- $\mathbb{1}_K$ is the indicator function of the set K.

New results for composites [Arsovski, 2021a]

Theorem ($\mathbb{Z}/p^k\mathbb{Z}$ bound [Arsovski, 2021a])

Every Kakeya Set S in $(\mathbb{Z}/p^k\mathbb{Z})^n$ satisfies,

$$|S| \geq \frac{p^{kn}}{(kn)^n}.$$

Theorem ($\mathbb{Z}/p^k\mathbb{Z}$ reduction [Arsovski, 2021a])

$\exists$ a matrix $V_{p^k,n}$ (defined later) such that for every Kakeya Set S in $(\mathbb{Z}/p^k\mathbb{Z})^n$,

$$|S| \geq \operatorname{rank}_{\mathbb{F}_p} V_{p^k,n} \geq \frac{p^{kn}}{(kn)^n}.$$

- $W_{p^k,n}$ is a sub-matrix of $V_{p^k,n}$. $V_{p^k,n}$ is a sub-matrix of $W_{p^k,n+1}$.

New results for composites [Arsovski, 2021b]

- A new version of this paper [Arsovski, 2021b] gives bounds for (m, ϵ)-Kakeya Sets with a different argument.
- (m, ϵ)-Kakeya Sets have at least m points in common with lines in at least an ϵ fraction of directions.
- This proves the Hausdorff dimension Kakeya conjecture over the p-adics.
- The bound in this paper is quantitatively weaker for $(N, 1)$-Kakeya setting.

New results for composites [D, 2021]

Theorem (Stronger $\mathbb{Z}/p^k\mathbb{Z}$ bound [D, 2021])

Every Kakeya Set S in $(\mathbb{Z}/p^k\mathbb{Z})^n$ satisfies

$$|S| \geq \frac{p^{kn}}{(2(k+\log_p(n)))^n} \geq_{[\text{Arsovski, 2021a}]} \frac{p^{kn}}{(kn)^n}.$$

- Extends the techniques in [Arsovski, 2021a].
- The bound can be improved to $p^{kn}/(k+1)^n$ as $p \to \infty$ recovering [Dvir, Kopparty, Saraf, and Sudan, 2013] for prime fields.
- There exist Kakeya Sets in $(\mathbb{Z}/p^k\mathbb{Z})^n$ of size $p^{kn}(k/\log_p(k))^{-n+1}$ [Hickman and Wright, 2018].
- The proof also extends to give stronger bounds for (m, ϵ)-Kakeya Sets.

Resolution of the Kakeya Set Conjecture for general N

Theorem (General $\mathbb{Z}/N\mathbb{Z}$ bound [D, 2021])

Every Kakeya Set in $(\mathbb{Z}/N\mathbb{Z})^n$ for $N = p_1^{k_1} \dots p_r^{k_r}$ has size at least

$$\frac{N^n}{\left(\prod_{i=1}^{r} 2^n (k_i + \log_p(n))^n\right)} \geq C_{n,\epsilon} N^{n-\epsilon}.$$

- Resolves the Kakeya Set Conjecture for general N.
- As $p_i \to \infty, \forall i = \{1, \dots, r\}$ the constant can be improved to $(\prod_{i=1}^{r}(k_i + 1))^{-n}$ recovering the square-free N bound from [D and Dvir, 2021].

Talk Overview

1. The Polynomial Method over $\mathbb{Z}/p\mathbb{Z}$
2. "New" Proof for $\mathbb{Z}/p\mathbb{Z}$
3. Proof for $\mathbb{Z}/pq\mathbb{Z}$
4. Proof for $\mathbb{Z}/p^k\mathbb{Z}$

Theorem ([Dvir, 2009], improvement due to Alon, Tao.)

Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Every Kakeya Set in $\mathbb{F}_p^n$ has size at least $\binom{p+n-1}{n}$.

- **Proof:** Suppose $S < \binom{p+n-1}{n}$ = number of monomials of degree at most $p-1$.
- $\exists f \neq 0, f \in \mathbb{F}_p[x_1, \dots, x_n]$ of degree $D \leq p-1$ which vanishes on S.
- For every direction $u \in \mathbb{F}_p^n$, f vanishes on some line $L_u = \{x + \lambda u | \lambda \in \mathbb{F}_p\}$ contained in S.
- $f(x + \lambda u)$ is a uni-variate polynomial in λ of degree $D \leq p-1$ with p zeros which means it is identically 0.

Theorem ([Dvir, 2009], improvement due to Alon,Tao.)

Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Every Kakeya Set in $\mathbb{F}_p^n$ has size at least $\binom{p+n-1}{n}$.

- $f(x+\lambda u) = f_D(u)\lambda^D + O_{f,x,u}(\lambda^{D-1})$.
- As $f(x+\lambda u)$ is identically 0, $f_D(u) = 0$.
- $\forall u \in \mathbb{F}_p^n, f_D(u) = 0$.
- f_D is a non-zero homogenous polynomial of degree $D \leq p-1$ which vanishes on all of $\mathbb{F}_p^n$.
- Contradiction (due to the DeMillo-Lipton-Schwartz–Zippel lemma).

□

- The proof doesn't work for general N because small degree polynomials can vanish over all of $(\mathbb{Z}/N\mathbb{Z})^n$.
- $(x^p - x)^2$ vanishes over all of $\mathbb{Z}/p^2\mathbb{Z}$ as $a^p - a$ is divisible by p for all $a \in \mathbb{N}$.
- $(x^p - x)(x^q - x)$ vanishes over all of $\mathbb{Z}/pq\mathbb{Z}$.
- If we try to adapt the proof strategy above for $N = p^2, pq$ we will get a lower bound of $\binom{p+n-1}{n} \approx p^n \approx N^{0.5n}$.

- WLOG we assume that $S = \bigcup_{u \in (\mathbb{Z}/N\mathbb{Z})^n} L_u$ where L_u is a line in direction u.

Definition (Line matrix M_S of a Kakeya Set S)

The line matrix M_S of S is a matrix where the u'th row is the indicator vector $\mathbb{1}_{L_u}$ of L_u in direction u which is contained in S.

$$\begin{array}{cc} & \xrightarrow{\qquad x \in (\mathbb{Z}/N\mathbb{Z})^n \qquad} \\ u \in (\mathbb{Z}/N\mathbb{Z})^n \Big\downarrow & \begin{pmatrix} \cdots & \cdots & \cdots \\ \text{---} & \mathbb{1}_{L_u} & \text{---} \\ \vdots & \vdots & \ddots \end{pmatrix} \end{array} = M_S$$

Line matrix of a Kakeya Set

$$\begin{array}{cc} & \xrightarrow{x \in (\mathbb{Z}/N\mathbb{Z})^n} \\ u \in (\mathbb{Z}/N\mathbb{Z})^n \Big\downarrow & \begin{pmatrix} \cdots & \cdots & \cdots \\ \text{---} & \mathbb{1}_{L_u} & \text{---} \\ \vdots & \vdots & \ddots \end{pmatrix} = M_S \end{array}$$

Claim

For any field $\mathbb{F}$, $|S| \geq \text{rank}_{\mathbb{F}} M_S \geq |S|/N$.

Proof.

$\mathbf{|S| \geq rank_{\mathbb{F}} M_S}$**:** The non-zero columns of M_S correspond to points in S.
$\mathbf{rank_{\mathbb{F}} M_S \geq |S|/N}$**:** Iteratively pick lines in S such that every new line you pick has a point not covered by the earlier lines. These at least $|S|/N$ many lines will give linearly independent rows. □

Idea

To lower bound the rank of M_S find a matrix A such that

$$M_S \cdot A = B$$

and B is a matrix independent of S.

- $A = W_{p,n}$ works!

Claim

In the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, for a line $L = \{a + \lambda u | \lambda \in \mathbb{F}_p\}$ we have

$$\mathbb{1}_L \cdot W_{p,n} = \mathbb{1}_{\overline{H}_u},$$

where $\overline{H}_u = \{x \in \mathbb{F}_p^n | \langle x, u \rangle \neq 0\}$.

$$\mathbb{1}_L \cdot W_{p,n} = \begin{bmatrix} — & \mathbb{1}_L & — \end{bmatrix} \cdot \begin{bmatrix} \cdots & | & \cdots \\ \cdots & \mathbb{1}_{H_v} & \cdots \\ \cdots & | & \cdots \end{bmatrix}$$

$$\langle \mathbb{1}_L, \mathbb{1}_{H_v} \rangle = |L \cap H_v| = \begin{cases} 0 & \text{if } L \cap H_v = \emptyset \\ p & \text{if } L \subseteq H_v \\ 1 & \text{otherwise} \end{cases} = \begin{cases} 0 & \text{if } \langle u, v \rangle = 0 \\ 1 & \text{otherwise} \end{cases}$$

- $$M_S \cdot W_{p,n} = \mathbf{1} - W_{p,n}$$

  in the field $\mathbb{F}_p$ where $\mathbf{1}$ is the all ones matrix.
- The $\mathbb{F}_p$-rank of $W_{p,n}$ is known exactly.

Theorem ($\mathbb{F}_p$-rank of $W_{p,n}$ [Goethals and Delsarte, 1968, MacWilliams and Mann, 1968, Smith, 1969])

$$\operatorname{rank}_{\mathbb{F}_p} W_{p,n} = \binom{p+n-2}{n-1} - 1$$

- Gives us a Kakeya size lower bound of

$$|S| \geq \operatorname{rank}_{\mathbb{F}_p} W_{p,n} - 1 \geq \binom{p+n-2}{n-1} - 2 \geq \frac{p^{n-1}}{n!}.$$

“New” Proof for $\mathbb{Z}/p\mathbb{Z}$ [D and Dvir, 2021]
Why “New”?

$$\mathrm{EVAL}_{p,n} = \begin{array}{cc} & m \\ x & \begin{bmatrix} \cdots & \cdots & \cdots \\ \cdots & m(x) & \cdots \\ \cdots & \cdots & \cdots \end{bmatrix} \end{array} = \begin{bmatrix} \cdots & | & \cdots \\ \cdots & m(\mathbb{F}_p^n) & \cdots \\ \cdots & | & \cdots \end{bmatrix}$$

where $m \in \mathbb{F}_p[x_1, \dots, x_n]$ is a monomial of degree $p-1$ and $x \in \mathbb{F}_p^n$.

- $$\mathbb{1}_{L_u} \cdot \mathrm{EVAL}_{p,n} = -\mathrm{EVAL}_{p,n}(u)$$

  where $\mathrm{EVAL}_{p,n}(u)$ is the u'th row of $\mathrm{EVAL}_{p,n}$.

- $$M_S \cdot \mathrm{EVAL}_{p,n} = -\,\mathrm{EVAL}_{p,n}\,.$$
- $\mathrm{EVAL}_{p,n}$ has rank $\binom{p+n-2}{n-1} - 1$.
- $\mathrm{EVAL}_{p,n}$ equals $W_{p,n}$ after base change.
- Can also prove rank bound using DeMillo-Lipton-Schwartz–Zippel lemma.
- This proves M_S has rank at least $\binom{p+n-2}{n-1} - 1$.
- M_S acts as a "decoder".
- We can extend M_S to use the evaluation of derivatives to get stronger bounds.

- By the Chinese remainder theorem we know that $(\mathbb{Z}/pq\mathbb{Z})^n \cong \mathbb{F}_p^n \times \mathbb{F}_q^n$.
- Every element $u \in (\mathbb{Z}/pq\mathbb{Z})^n$ can be written as a tuple $(u_p, u_q) \in \mathbb{F}_p^n \times \mathbb{F}_q^n$.
- For every line in $L(u)$ with direction $u = (u_p, u_q) \in \mathbb{F}_p^n \times \mathbb{F}_q^n$,

  $$L_u = L_p(u) \times L_q(u)$$

  where $L_p(u) \subseteq \mathbb{F}_p^n$ and $L_q(u) \subseteq \mathbb{F}_q^n$ are lines with direction u_p and u_q respectively.
- $$\mathbb{1}_{L(u_p,u_q)} = \mathbb{1}_{L_p(u_p,u_q)} \otimes \mathbb{1}_{L_q(u_p,u_q)}$$
- Note, while the product $S_p \times S_q$ of two Kakeya Sets $S_p \subseteq \mathbb{F}_p^n$ and $S_q \subseteq \mathbb{F}_q^n$ is a Kakeya Set the converse is not true.

Kakeya Sets in $\mathbb{Z}/pq\mathbb{Z}$ [D and Dvir, 2021]

Theorem (Simple Kakeya Set bounds for $\mathbb{Z}/pq\mathbb{Z}$ [D and Dvir, 2021])

Every Kakeya Set S in $(\mathbb{Z}/pq\mathbb{Z})^n$ has size at least,

$$C_n p^{n-1} q^{n-1}.$$

- Let $S = \bigcup_{(u_p,u_q)\in\mathbb{F}_p^n\times\mathbb{F}_q^n} L(u_p, u_q)$ be a Kakeya Set.
- $L(u_p, u_q) = L_p(u_p, u_q) \times L_q(u_p, u_q)$
-

$$M_S = \begin{bmatrix} \dots & \dots & \ddots \\ \text{---} & \mathbb{1}_{L(u_p,u_q)} & \text{---} \\ \dots & \dots & \ddots \end{bmatrix} = \begin{bmatrix} \dots & \dots & \ddots \\ \mathbb{1}_{L_p(u_p,u_q)} & \otimes & \mathbb{1}_{L_q(u_p,u_q)} \\ \dots & \dots & \ddots \end{bmatrix}$$

Kakeya Sets in $\mathbb{Z}/pq\mathbb{Z}$ [D and Dvir, 2021]

- $$M_S \cdot (W_{p,n} \otimes I_{q^n}) = \begin{bmatrix} \cdots & \cdots & \ddots \\ \mathbb{1}_{L_p(u_p,u_q)} \cdot W_{p,n} & \otimes & \mathbb{1}_{L_q(u_p,u_q)} \\ \cdots & \cdots & \ddots \end{bmatrix}$$

Claim (Proven Earlier)

In the field $\mathbb{F}_p$, for a line $L \subseteq \mathbb{F}_p^n$ in direction u_p we have $\mathbb{1}_L \cdot W_{p,n} = \mathbb{1}_{\overline{H}_{u_p}}$.

- $$M_S \cdot (W_{p,n} \otimes I_{q^n}) = \begin{bmatrix} \cdots & \cdots & \ddots \\ \mathbb{1}_{\overline{H}_{u_p}} & \otimes & \mathbb{1}_{L_q(u_p,u_q)} \\ \cdots & \cdots & \ddots \end{bmatrix}$$

Kakeya Sets in $\mathbb{Z}/pq\mathbb{Z}$ [D and Dvir, 2021]

- **For a fixed $\mathbf{u_p}$**, the indicator vectors $\mathbb{1}_{L_q(\mathbf{u_p},u_q)}$ form the line matrix $M_{S_q(\mathbf{u_p})}$ of the Kakeya Set $S_q(\mathbf{u_p}) = \bigcup_{u_q \in \mathbb{F}_q^n} L_q(\mathbf{u_p}, u_q)$ in $\mathbb{F}_q^n$.
- $$M_S \cdot (W_{p,n} \otimes I_{q^n}) = \begin{bmatrix} \dots & \dots & \ddots \\ \mathbb{1}_{\overline{H}_{\mathbf{u_p}}} & \otimes & M_{S_q(\mathbf{u_p})} \\ \dots & \dots & \ddots \end{bmatrix} \cong \begin{bmatrix} \dots & \dots & \ddots \\ e_i & \otimes & M_{S_q(\mathbf{u_p})} \\ \dots & \dots & \ddots \end{bmatrix}$$

  where $1 \leq i \leq p^{n-1}/n!$
- We saw earlier that $\mathbb{1}_{\overline{H}_{u_p}}$ for $u_p \in \mathbb{F}_p^n$ has rank at least $p^{n-1}/n!$.
- Pick r linearly independent $\mathbb{1}_{\overline{H}_{u_p}}$ and base change to them.
- "By induction":
  $$\operatorname{rank}_{\mathbb{F}_p} M_{S_q(u_p)} \geq |S_q(u_p)| q^{-1} \geq q^{n-1}/2^{n-1}.$$
- $$|S| \geq \frac{1}{2^{n-1} n!} p^{n-1} q^{n-1}$$

□

Proof Strategy

- Let ζ be a complex primitive p^k'th root of unity. $\mathbb{Z}(\zeta)$ is the ring generated by $\mathbb{Z}$ and ζ.
- $x \in (\mathbb{Z}/p^k\mathbb{Z})^n$ is mapped to $\zeta^x = (\zeta^{x_1}, \ldots, \zeta^{x_n}) \in \mathbb{Z}(\zeta)^n$.

$$E_{p^k,n} = \begin{array}{cc} & m_v \\ x & \begin{bmatrix} \cdots & \cdots & \cdots \\ \cdots & m_v(\zeta^x) & \cdots \\ \cdots & \cdots & \cdots \end{bmatrix} \end{array} = \begin{bmatrix} \cdots & | & \cdots \\ \cdots & m_v(\zeta^{(\mathbb{Z}/p^k\mathbb{Z})^n}) & \cdots \\ \cdots & | & \cdots \end{bmatrix}$$

$m_v(y) = y_1^{v_1} \ldots y_n^{v_n}, 0 \leq v_i \leq p^k - 1$ and $x \in (\mathbb{Z}/p^k\mathbb{Z})^n$.

- **Initial Idea:** Find a “decoder” C_S with support S such that

$$C_S \cdot E_{p^k,n} = B$$

is a matrix independent of S.

- **Actual Idea:**

$$C_S \cdot E_{p^k,n} \text{“}(\text{mod } p)\text{”} = V_{p^k,n}$$

- “(mod p)” map doesn't increase rank.

The rings T_k and $\overline{T}_k$

Definition (The rings T_k and $\overline{T}_k$)

$$T_k = \frac{\mathbb{Z}(\zeta)[z]}{\langle z^{p^k} - 1\rangle} \text{ and } \overline{T}_k = \frac{\mathbb{F}_p[z]}{\langle z^{p^k} - 1\rangle}.$$

- T_k "(mod p)" $= \overline{T}_k$

Claim ("(mod p)" map ψ)

The map ψ which maps ζ to 1, $\mathbb{Z}$ to $\mathbb{F}_p$ (via the mod p map) and z to z is a ring homomorphism from T_k onto $\overline{T}_k$.

- ζ is a root of the p^k'th cyclotomic polynomial

$$\phi(x) = \frac{(x^{p^k} - 1)}{x^{p^{k-1}} - 1} = \sum_{i=0}^{p-1} x^{p^{k-1} i}.$$

- Note, $\phi(1) = 0 \pmod p$,equivalently $x - 1$ divides $\phi(x)$ in $\mathbb{F}_p$.

Vandermonde Matrix

Definition (Matrix $V_{p^k,n}$)

$V_{p^k,n}$ is a $p^{kn} \times p^{kn}$ matrix with entries in $\overline{T}_k = \mathbb{F}_p[z]/\langle z^{p^k} - 1\rangle$ whose entries are,

$$V_{p^k,n}(u,v) = z^{\langle u,v\rangle},$$

where $u, v \in (\mathbb{Z}/p^k\mathbb{Z})^n$

Theorem (Rank Bound [Arsovski, 2021a, D, 2021])

$V_{p^k,n}$ has $\mathbb{F}_p$-rank at least $\binom{p/k+n-1}{n}$.

- Rank of $V_{p^k,n}$ is defined as the largest number of $\mathbb{F}_p$-linearly independent columns of $V_{p^k,n}$
- Can write $V_{p^k,n} = LU$ where L is a lower triangular matrix and U is an upper triangular matrix with explicit formulas.
- Lower bounding the number of non-zero diagonal elements of U gives the rank bound.

Decoding evaluations on the complex torus [D, 2021]

- For $f \in \mathbb{Z}[y_1, \ldots, y_n]$ the $f(z^u) \in \overline{T}_k$ is in $\psi(\text{span}\{f(\zeta^{L_u})\})$ where L_u is a line in direction u.

Lemma (Decoding evaluations along lines on the $\mathbb{C}$ torus [D, 2021])

Given $L_u = \{a + \lambda u | \lambda \in \mathbb{Z}/p^k\mathbb{Z}\}$ there exists $c_x \in \frac{\mathbb{Q}(\zeta)[z]}{\langle z^{p^k} - 1\rangle}, x \in L_u$ such that,

$$\psi\left(\sum_{x \in L_u} c_x f(\zeta^x)\right) = f(z^u),$$

for all polynomials $f \in \mathbb{Z}[y_1, \ldots, y_n]$.

- To apply ψ, $\sum_{x \in L_u} c_x f(\zeta^x)$ must be a polynomial in z with coefficients in $\mathbb{Z}(\zeta)$.
- By linearity (over $\mathbb{Z}$) it suffices to prove the statement for monomials.

Proof of decoding lemma

- Let $m_v(x) = x_1^{v_1} \dots x_n^{v_n}$.
- $m_v(\zeta^{0*u}) = m_v(1), m_v(\zeta^u) = \zeta^{\langle v,u \rangle}, \dots, m_v(\zeta^{\lambda u}) = \zeta^{\lambda \langle v,u \rangle}, \dots$ are the evaluations of the monomial $z^{\langle u,v \rangle}$ on $z = 1, \zeta, \dots, \zeta^{p^k-1}$.
- As

$$\frac{\mathbb{Q}(\zeta)[z]}{\langle (z-1) \rangle} \oplus \dots \oplus \frac{\mathbb{Q}(\zeta)[z]}{\langle (z-\zeta^{p^k-1}) \rangle} = \frac{\mathbb{Q}(\zeta)[z]}{\langle (z-1)\dots(z-\zeta^{p^k-1}) \rangle} = \frac{\mathbb{Q}(\zeta)[z]}{\langle z^{p^k}-1 \rangle}.$$

  There exists constants $c_\lambda \in \mathbb{Q}(\zeta)[z]/\langle z^{p^k}-1 \rangle$ for $\lambda = 1, \dots, p^k$ such that

$$\sum_{\lambda=1}^{p^k} c_\lambda m_v(\zeta^{\lambda u}) = z^{\langle u,v \rangle} = m_v(z^u) \in \frac{\mathbb{Z}(\zeta)[z]}{\langle z^{p^k}-1 \rangle} = T_k.$$

Proof of decoding lemma

- As $m_v(\zeta^{a+\lambda u}) = \zeta^{\langle v,a \rangle} m_v(\zeta^{\lambda u})$,
- $$\sum_{\lambda=1}^{p^k} c_\lambda m_v(\zeta^{a+\lambda u}) = \zeta^{\langle v,a \rangle} z^{\langle u,v \rangle} = \zeta^{\langle v,a \rangle} m_v(z^u)$$
- Applying ψ gives us,

$$\psi\left(\sum_{\lambda=1}^{p^k} c_\lambda m_v(\zeta^{a+\lambda u})\right) = m_v(z^u) \in \overline{T}_k.$$

$\square$

- Can be extended to decode with derivatives at fewer points.

Decoding evaluations on the complex torus

Corollary (Decode $V_{p^k,n}(u)$ from $E_{p^k,n}(\zeta^{L_u})$)

For a line $L_u = \{a + \lambda u | \lambda \in \mathbb{Z}/p^k\mathbb{Z}\}$ we can find a row vector C_u indexed by points in $(\mathbb{Z}/p^k\mathbb{Z})^n$ such that,

$$\psi(C_u \cdot E_{p^k}) = (z^{\langle v,u\rangle})_{v\in(\mathbb{Z}/p^k\mathbb{Z})^n} = V_{p^k,n}(u).$$

- C_u has support L_u.
- First proven in [Arsovski, 2021a]. Generalized with new proof in [D, 2021].
- The matrix C with rows C_u for each line L_u in S is the required decoder matrix.

Questions?