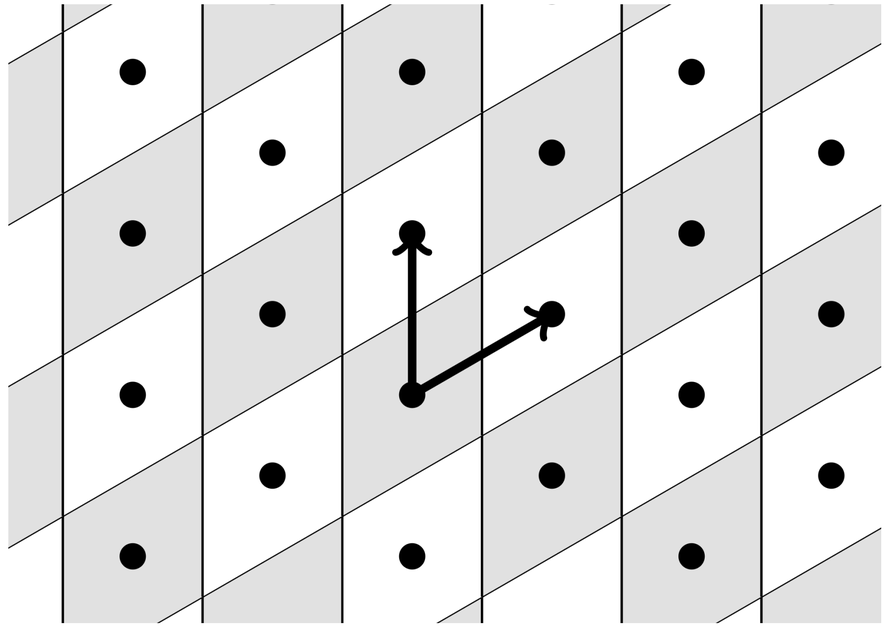
Spherical Codes from Craig's Lattices

Léo Ducas
Centrum Wiskunde & Informatica (CWI), University of Leiden
Julian Nowakowski
Centrum Wiskunde & Informatica (CWI)
Ailsa Robertson
University of Amsterdam

Lattices and Error Correction

A **lattice** is a discrete subgroup $\mathscr{L}$ of $(\mathbb{R}^n, +)$.

Every lattice is of the form $\mathscr{L} = \mathbf{B} \cdot \mathbb{Z}^d$, for some **basis** $\mathbf{B} \in \mathbb{R}^{n \times d}$ and **dimension** d.

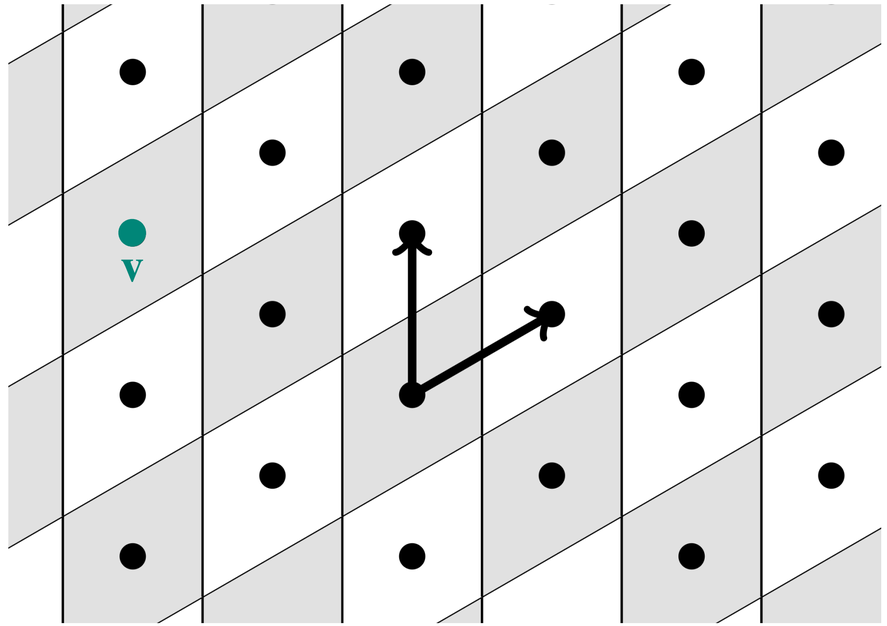


Lattices and Error Correction

A **lattice** is a discrete subgroup $\mathscr{L}$ of $(\mathbb{R}^n, +)$.

Every lattice is of the form $\mathscr{L} = \mathbf{B} \cdot \mathbb{Z}^d$, for some **basis** $\mathbf{B} \in \mathbb{R}^{n \times d}$ and **dimension** d.

- Alice wants to send a message to Bob.
- Alice encodes her message as $\mathbf{v} \in \mathscr{L}$.

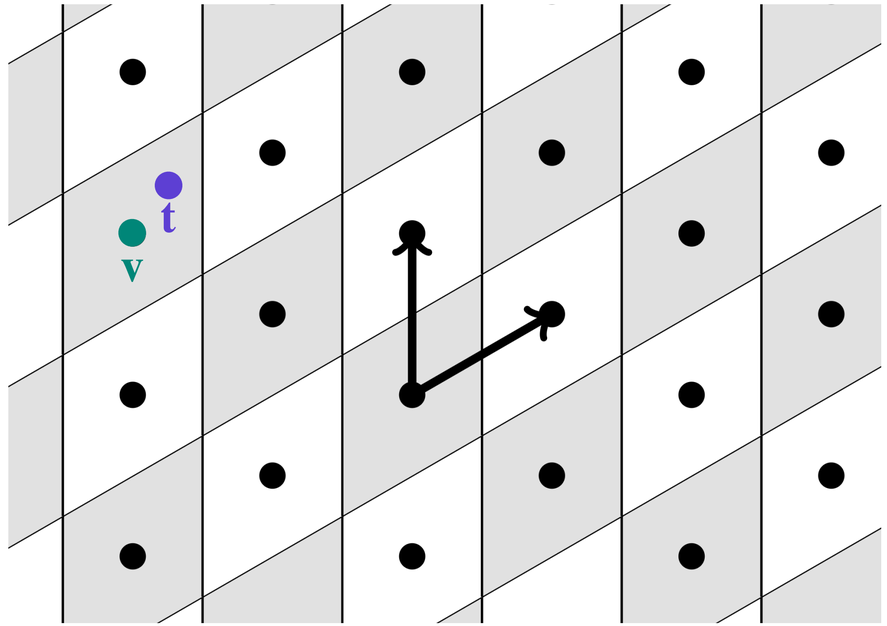


Lattices and Error Correction

A **lattice** is a discrete subgroup $\mathscr{L}$ of $(\mathbb{R}^n, +)$.

Every lattice is of the form $\mathscr{L} = \mathbf{B} \cdot \mathbb{Z}^d$, for some **basis** $\mathbf{B} \in \mathbb{R}^{n \times d}$ and **dimension** d.

- Alice wants to send a message to Bob.
- Alice encodes her message as $\mathbf{v} \in \mathscr{L}$.
- Bob receives noisy $\mathbf{t} \approx \mathbf{v}$.

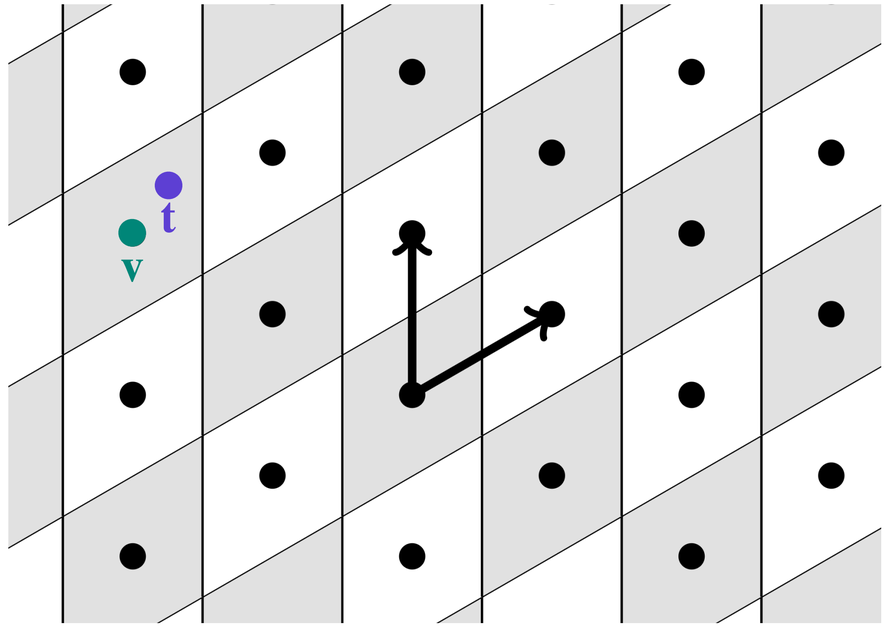


Lattices and Error Correction

A **lattice** is a discrete subgroup $\mathscr{L}$ of $(\mathbb{R}^n, +)$.

Every lattice is of the form $\mathscr{L} = \mathbf{B} \cdot \mathbb{Z}^d$, for some **basis** $\mathbf{B} \in \mathbb{R}^{n \times d}$ and **dimension** d.

- Alice wants to send a message to Bob.
- Alice encodes her message as $\mathbf{v} \in \mathscr{L}$.
- Bob receives noisy $\mathbf{t} \approx \mathbf{v}$.
- Bob tries to recover $\mathbf{v}$ by computing a closest lattice vector to $\mathbf{t}$.

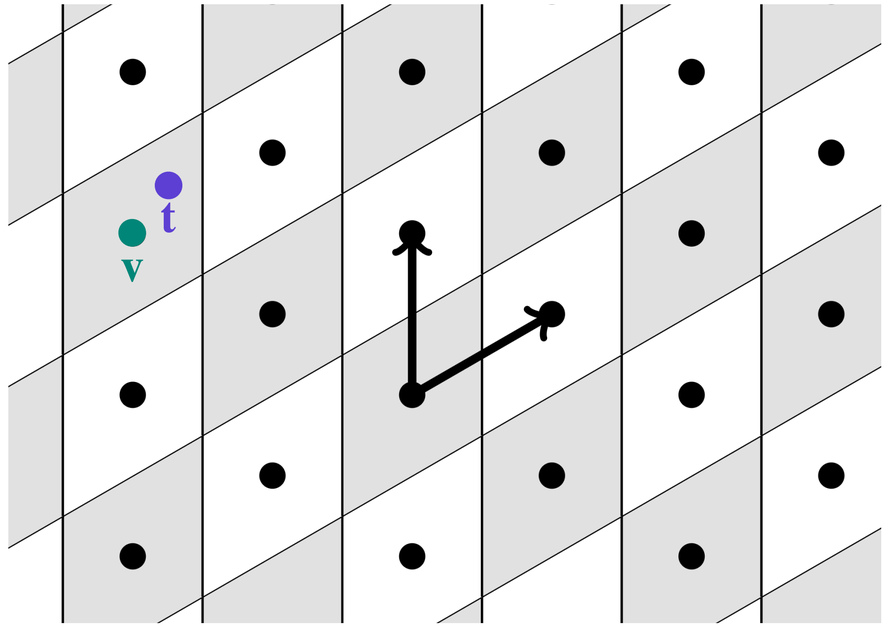


Lattices and Error Correction

A **lattice** is a discrete subgroup $\mathscr{L}$ of $(\mathbb{R}^n, +)$.

Every lattice is of the form $\mathscr{L} = \mathbf{B} \cdot \mathbb{Z}^d$, for some **basis** $\mathbf{B} \in \mathbb{R}^{n \times d}$ and **dimension** d.

- Alice wants to send a message to Bob.
- Alice encodes her message as $\mathbf{v} \in \mathscr{L}$.
- Bob receives noisy $\mathbf{t} \approx \mathbf{v}$.
- Bob tries to recover $\mathbf{v}$ by computing a closest lattice vector to $\mathbf{t}$.



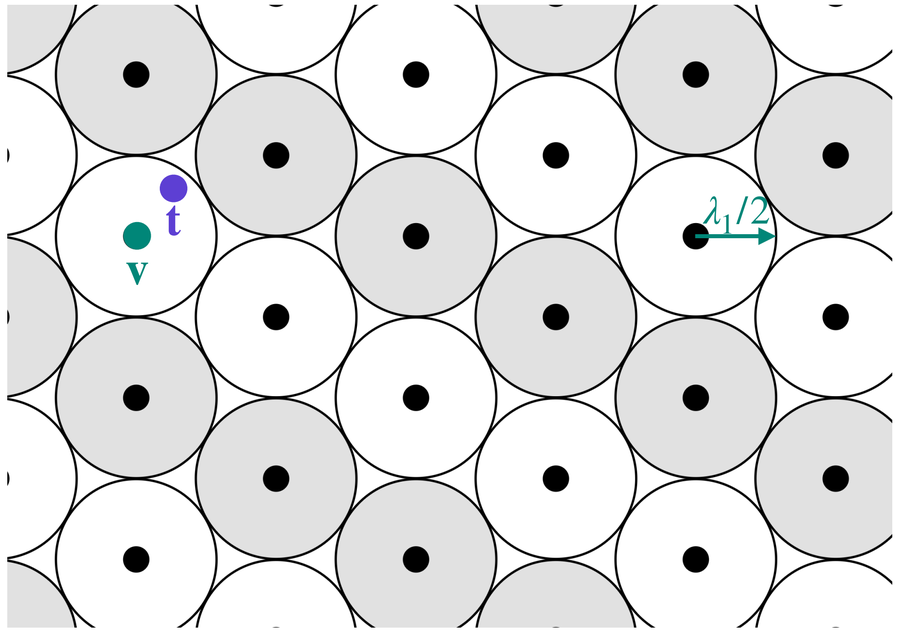
$$\lambda_1(\mathscr{L}) := \min_{\mathbf{v},\mathbf{w} \in \mathscr{L},\ \mathbf{v} \neq \mathbf{w}} \|\mathbf{v} - \mathbf{w}\|$$

Lattices and Error Correction

A **lattice** is a discrete subgroup $\mathscr{L}$ of $(\mathbb{R}^n, +)$.

Every lattice is of the form $\mathscr{L} = \mathbf{B} \cdot \mathbb{Z}^d$, for some **basis** $\mathbf{B} \in \mathbb{R}^{n \times d}$ and **dimension** d.

- Alice wants to send a message to Bob.
- Alice encodes her message as $\mathbf{v} \in \mathscr{L}$.
- Bob receives noisy $\mathbf{t} \approx \mathbf{v}$.
- Bob tries to recover $\mathbf{v}$ by computing a closest lattice vector to $\mathbf{t}$.



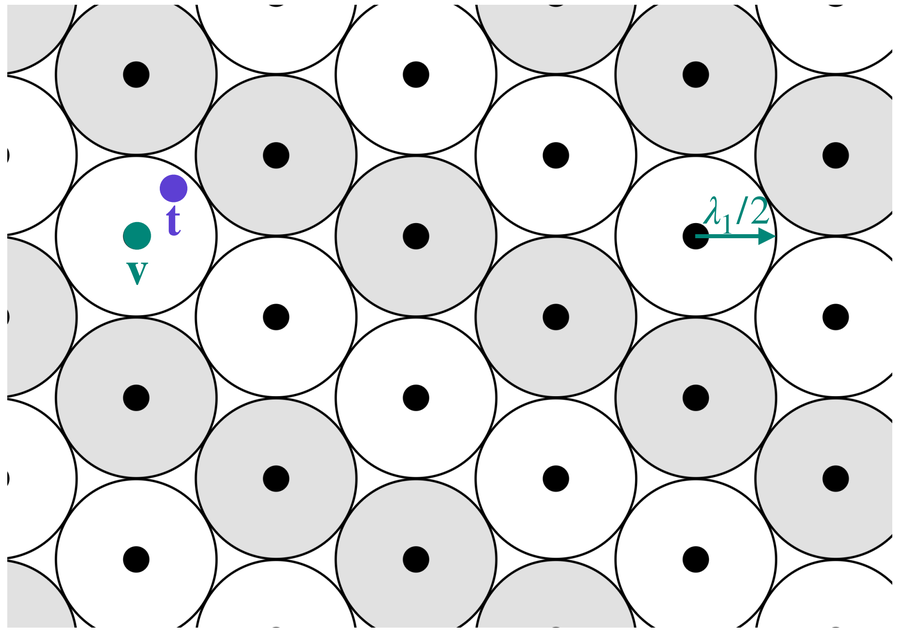
$$\lambda_1(\mathscr{L}) := \min_{\mathbf{v},\mathbf{w} \in \mathscr{L},\ \mathbf{v} \neq \mathbf{w}} \|\mathbf{v} - \mathbf{w}\|$$

Lattices and Error Correction

A **lattice** is a discrete subgroup $\mathscr{L}$ of $(\mathbb{R}^n, +)$.

Every lattice is of the form $\mathscr{L} = \mathbf{B} \cdot \mathbb{Z}^d$, for some **basis** $\mathbf{B} \in \mathbb{R}^{n \times d}$ and **dimension** d.

- Alice wants to send a message to Bob.
- Alice encodes her message as $\mathbf{v} \in \mathscr{L}$.
- Bob receives noisy $\mathbf{t} \approx \mathbf{v}$.
- Bob tries to recover $\mathbf{v}$ by computing a closest lattice vector to $\mathbf{t}$.
- Succeeds if $\|\mathbf{t} - \mathbf{v}\| < \lambda_1/2$.



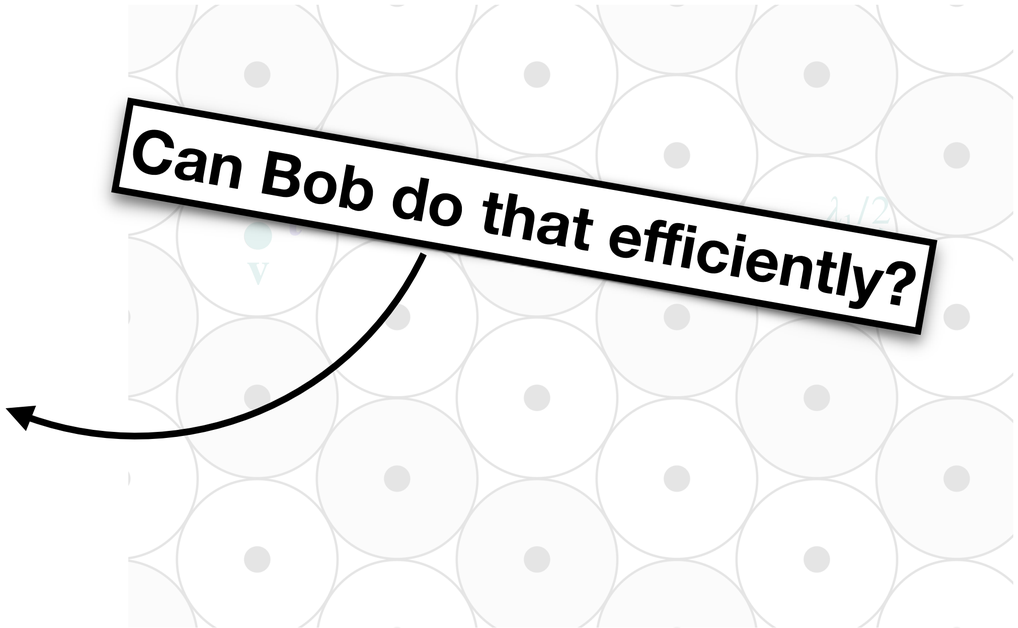
$$\lambda_1(\mathscr{L}) := \min_{\mathbf{v},\mathbf{w} \in \mathscr{L},\ \mathbf{v} \neq \mathbf{w}} \|\mathbf{v} - \mathbf{w}\|$$

Lattices and Error Correction

A **lattice** is a discrete subgroup $\mathscr{L}$ of $(\mathbb{R}^n, +)$.

Every lattice is of the form $\mathscr{L} = \mathbf{B} \cdot \mathbb{Z}^d$, for some **basis** $\mathbf{B} \in \mathbb{R}^{n \times d}$ and **dimension** d.

- Alice wants to send a message to Bob.
- Alice encodes her message as $\mathbf{v} \in \mathscr{L}$.
- Bob receives noisy $\mathbf{t} \approx \mathbf{v}$.
- Bob tries to recover $\mathbf{v}$ by computing a closest lattice vector to $\mathbf{t}$.
- Succeeds if $\|\mathbf{t} - \mathbf{v}\| < \lambda_1/2$.



$$\lambda_1(\mathscr{L}) := \min_{\mathbf{v},\mathbf{w} \in \mathscr{L},\, \mathbf{v} \neq \mathbf{w}} \|\mathbf{v} - \mathbf{w}\|$$

Efficiently Decodable Lattices

We need lattices for which the following problem can be solved efficiently.

Lattice List Decoding

Given:

- basis $\mathbf{B} \in \mathbb{R}^{n \times d}$ of lattice $\mathscr{L}$, $\mathbf{t} \in \mathbf{B} \cdot \mathbb{R}^d$, $\alpha \geq 0$

Find:

- all $\mathbf{v} \in \mathscr{L}$ with $\|\mathbf{t} - \mathbf{v}\| < \alpha \cdot \lambda_1(\mathscr{L})$

Efficiently Decodable Lattices

We need lattices for which the following problem can be solved efficiently.

Lattice List Decoding

Given:

- basis $\mathbf{B} \in \mathbb{R}^{n \times d}$ of lattice $\mathscr{L}$, $\mathbf{t} \in \mathbf{B} \cdot \mathbb{R}^d$, $\alpha \geq 0$

Find:

- all $\mathbf{v} \in \mathscr{L}$ with $\|\mathbf{t} - \mathbf{v}\| < \alpha \cdot \lambda_1(\mathscr{L})$

- At most one solution, if $\alpha \leq 1/2$.

Efficiently Decodable Lattices

We need lattices for which the following problem can be solved efficiently.

Lattice List Decoding

Given:

- basis $\mathbf{B} \in \mathbb{R}^{n \times d}$ of lattice $\mathscr{L}$, $\mathbf{t} \in \mathbf{B} \cdot \mathbb{R}^d$, $\alpha \geq 0$

Find:

- all $\mathbf{v} \in \mathscr{L}$ with $\|\mathbf{t} - \mathbf{v}\| < \alpha \cdot \lambda_1(\mathscr{L})$

- At most one solution, if $\alpha \leq 1/2$.
- At most $2d$ solutions, if $\alpha \leq 1/\sqrt{2}$.

☞ Rankin 1955

Efficiently Decodable Lattices

We need lattices for which the following problem can be solved efficiently.

Lattice List Decoding

Given:

- basis $\mathbf{B} \in \mathbb{R}^{n \times d}$ of lattice $\mathscr{L}$, $\mathbf{t} \in \mathbf{B} \cdot \mathbb{R}^d$, $\alpha \geq 0$

Find:

- all $\mathbf{v} \in \mathscr{L}$ with $\|\mathbf{t} - \mathbf{v}\| < \alpha \cdot \lambda_1(\mathscr{L})$

- At most one solution, if $\alpha \leq 1/2$.
- At most $2d$ solutions, if $\alpha \leq 1/\sqrt{2}$.

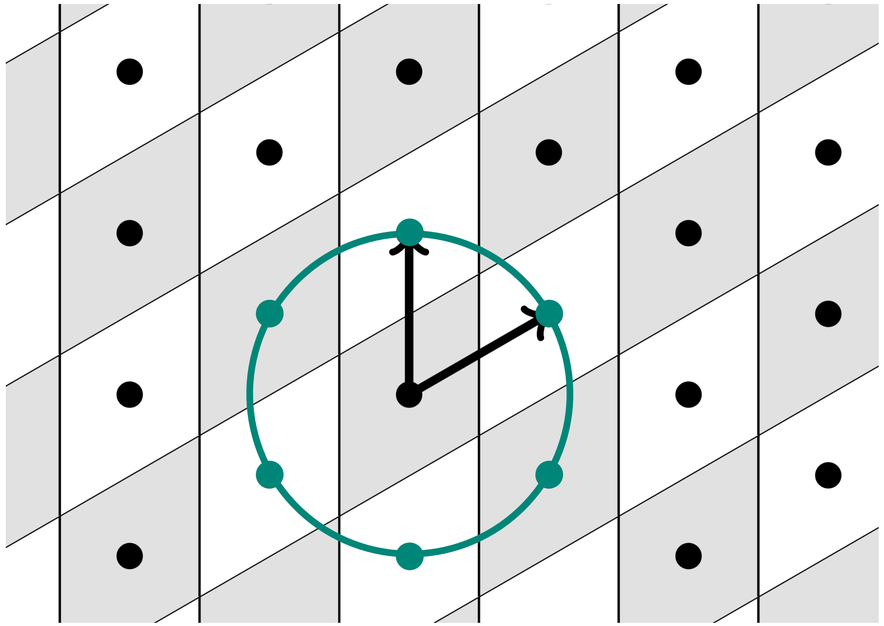
☞ Rankin 1955

- For $\alpha > 1/\sqrt{2}$, there are instances with $2^{\Omega(d)}$ solutions.

☞ cf. literature on **locally dense lattices,** e.g., Micciancio 1998

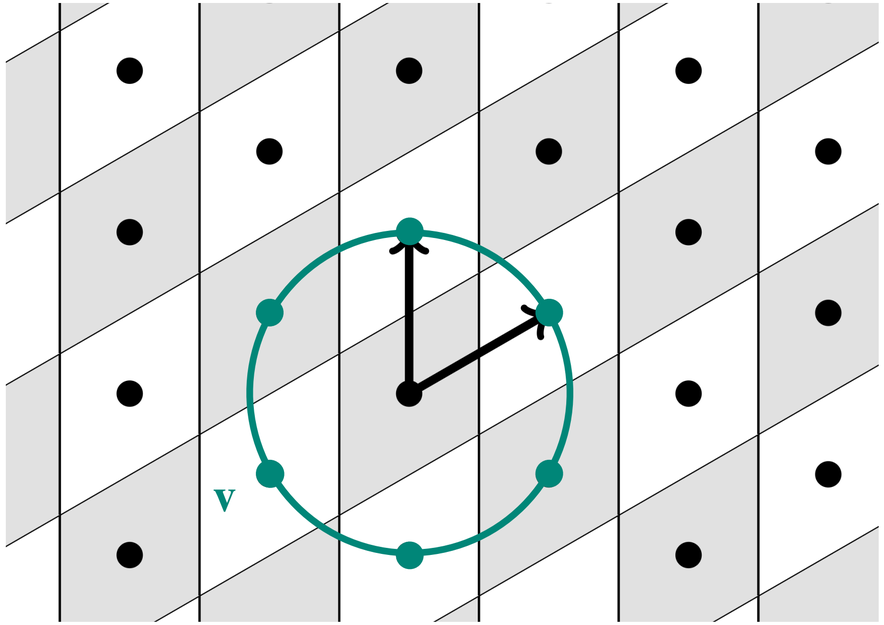
Spherical Codes from Lattices

The **minimal shell** of $\mathscr{L}$ is $S(\mathscr{L}) := \left\{\mathbf{v} \in \mathscr{L} \mid \|\mathbf{v}\| = \lambda_1(\mathscr{L})\right\}$



Spherical Codes from Lattices

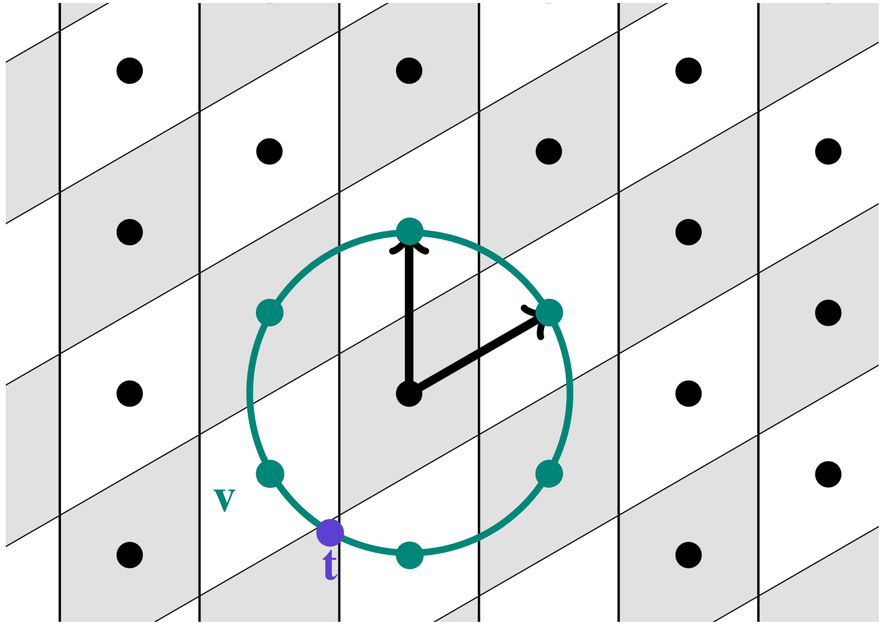
The **minimal shell** of $\mathscr{L}$ is $S(\mathscr{L}) := \left\{\mathbf{v} \in \mathscr{L} \mid \|\mathbf{v}\| = \lambda_1(\mathscr{L})\right\}$



- Alice encodes her message as $\mathbf{v} \in S(\mathscr{L})$.

Spherical Codes from Lattices

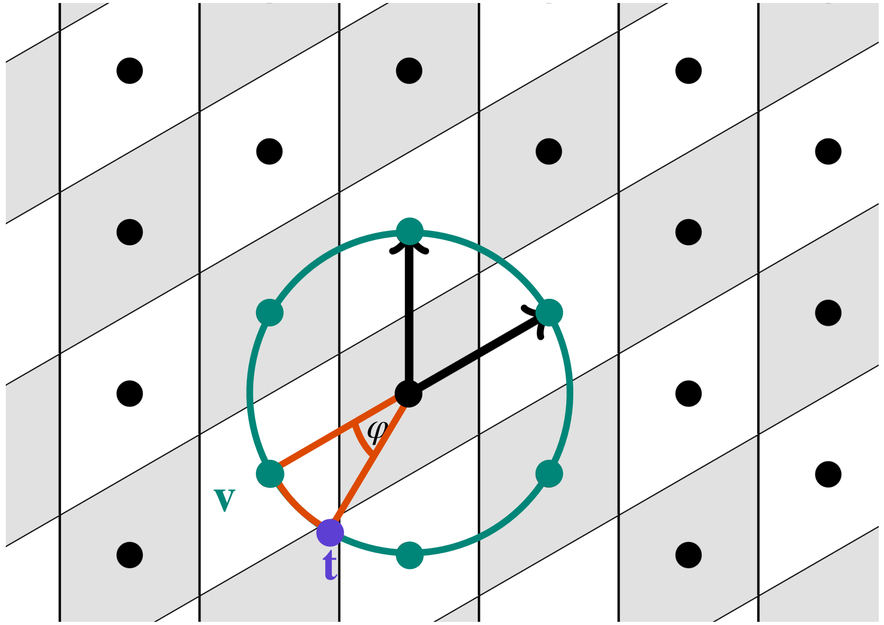
The **minimal shell** of $\mathscr{L}$ is $S(\mathscr{L}) := \left\{\mathbf{v} \in \mathscr{L} \mid \|\mathbf{v}\| = \lambda_1(\mathscr{L})\right\}$



- Alice encodes her message as $\mathbf{v} \in S(\mathscr{L})$.
- Bob receives noisy $\mathbf{t} \approx \mathbf{v}$, $\|\mathbf{t}\| = \lambda_1(\mathscr{L})$.

Spherical Codes from Lattices

The **minimal shell** of $\mathscr{L}$ is $S(\mathscr{L}) := \left\{\mathbf{v} \in \mathscr{L} \mid \|\mathbf{v}\| = \lambda_1(\mathscr{L})\right\}$



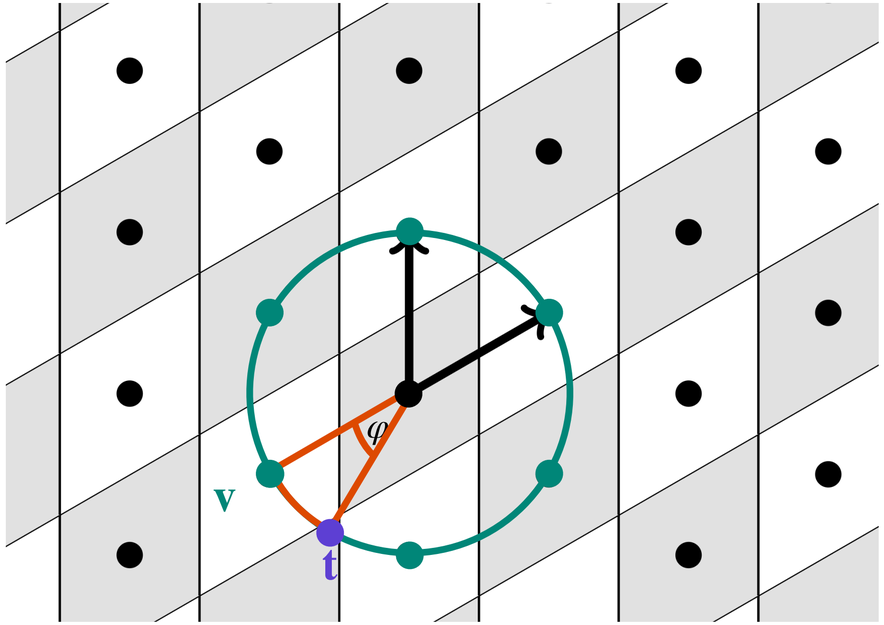
- Alice encodes her message as $\mathbf{v} \in S(\mathscr{L})$.
- Bob receives noisy $\mathbf{t} \approx \mathbf{v}$, $\|\mathbf{t}\| = \lambda_1(\mathscr{L})$.

- Distance depends only on the angle

$$\varphi := \arccos\left(\frac{\langle \mathbf{v}, \mathbf{t}\rangle}{\|\mathbf{v}\|\|\mathbf{t}\|}\right) = \arccos\left(\frac{\langle \mathbf{v}, \mathbf{t}\rangle}{\lambda_1^2}\right)$$

Spherical Codes from Lattices

The **minimal shell** of $\mathscr{L}$ is $S(\mathscr{L}) := \{\mathbf{v} \in \mathscr{L} \mid \|\mathbf{v}\| = \lambda_1(\mathscr{L})\}$



- Alice encodes her message as $\mathbf{v} \in S(\mathscr{L})$.
- Bob receives noisy $\mathbf{t} \approx \mathbf{v}$, $\|\mathbf{t}\| = \lambda_1(\mathscr{L})$.

- Distance depends only on the angle

$$\varphi := \arccos\left(\frac{\langle \mathbf{v}, \mathbf{t}\rangle}{\|\mathbf{v}\|\|\mathbf{t}\|}\right) = \arccos\left(\frac{\langle \mathbf{v}, \mathbf{t}\rangle}{\lambda_1^2}\right)$$

$\mathbf{v}, \mathbf{t}$ are close $\iff$ φ is small $\iff$ $\langle \mathbf{v}, \mathbf{t}\rangle$ is large

Spherical Codes from Lattices

The **minimal shell** of $\mathscr{L}$



e as $\mathbf{v} \in S(\mathscr{L})$.

$\|\mathbf{t}\| = \lambda_1(\mathscr{L})$.

the angle

$= \arccos\left(\frac{\langle \mathbf{v}, \mathbf{t} \rangle}{\lambda_1^2}\right)$

Spherical List Decoding

Given:

- basis $\mathbf{B} \in \mathbb{R}^{n \times d}$ of lattice $\mathscr{L}$,
- $\mathbf{t} \in \mathbf{B} \cdot \mathbb{R}^d$, $\|\mathbf{t}\| = \lambda_1(\mathscr{L})$,
- $\rho \in [-1, 1]$

Find:

- all $\mathbf{v} \in S(\mathscr{L})$ with $\langle \mathbf{v}, \mathbf{t} \rangle > \rho \cdot \lambda_1(\mathscr{L})^2$

$\mathbf{v}, \mathbf{t}$ are close $\iff$ φ is small $\iff$ $\langle \mathbf{v}, \mathbf{t} \rangle$ is large

Spherical Codes from Lattices

The **minimal shell** of $\mathscr{L}$



e as $\mathbf{v} \in S(\mathscr{L})$.

$\|\mathbf{t}\| = \lambda_1(\mathscr{L})$.

the angle

$$= \arccos\left(\frac{\langle \mathbf{v}, \mathbf{t} \rangle}{\lambda_1^2}\right)$$

Spherical List Decoding

Given:

- basis $\mathbf{B} \in \mathbb{R}^{n \times d}$ of lattice $\mathscr{L}$,
- $\mathbf{t} \in \mathbf{B} \cdot \mathbb{R}^d$, $\|\mathbf{t}\| = \lambda_1(\mathscr{L})$,
- $\rho \in [-1, 1]$

Find:

- all $\mathbf{v} \in S(\mathscr{L})$ with $\langle \mathbf{v}, \mathbf{t} \rangle > \rho \cdot \lambda_1(\mathscr{L})^2$

- At most one solution, if $\rho \geq \cos(30°)$.
- At most $2d$ solutions, if $\rho \geq \cos(45°)$.

$\mathbf{v}, \mathbf{t}$ rge

Large Efficiently Decodable Codes

We need lattices $\mathscr{L}$ with the following properties:

- efficient list decoding of $S(\mathscr{L})$
- $|S(\mathscr{L})|$ as large as possible

Large Efficiently Decodable Codes

We need lattices $\mathscr{L}$ with the following properties:

- efficient list decoding of $S(\mathscr{L})$
- $|S(\mathscr{L})|$ as large as possible



Large Efficiently Decodable Codes

We need lattices $\mathscr{L}$ with the following properties:

- efficient list decoding of $S(\mathscr{L})$
- $|S(\mathscr{L})|$ as large as possible

kissing number $\kappa(\mathscr{L})$

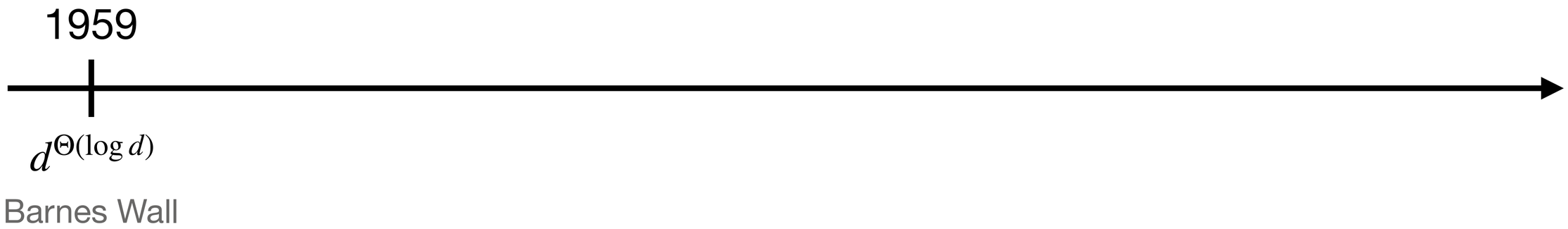
Table I.2(b) Highest kissing numbers τ presently known for packings in dimensions $n \leq 128$.

n	τ (lattice)	Lattice
23	93150	Λ_{23}
24	196560	Λ_{24}
25	196656	Λ_{25}
26	196848	Λ_{26}
27	197142	Λ_{27}
28	197736	Λ_{28}
29	198506	Λ_{29}
30	200046	Λ_{30}
31	202692	Λ_{31}
32	261120	Q_{32} and others
33	262272	Q_{33} (
34	264576	Q_{34} (
35	268032	Q_{35} (
36	274944	Q_{36}
37	284160	Q_{37}
38	302592	Q_{38}
39	333696	Q_{39}
40	399360	Q_{40}
44	2708112	MW_{44}
48	52416000	P_{48n}, P_{48p}, P_{48q}
64	138458880	Ne_{64} [Nebe98b]
80	1250172000	L_{80} [BacoN98] (
128	218044170240	MW_{128} [Elki]

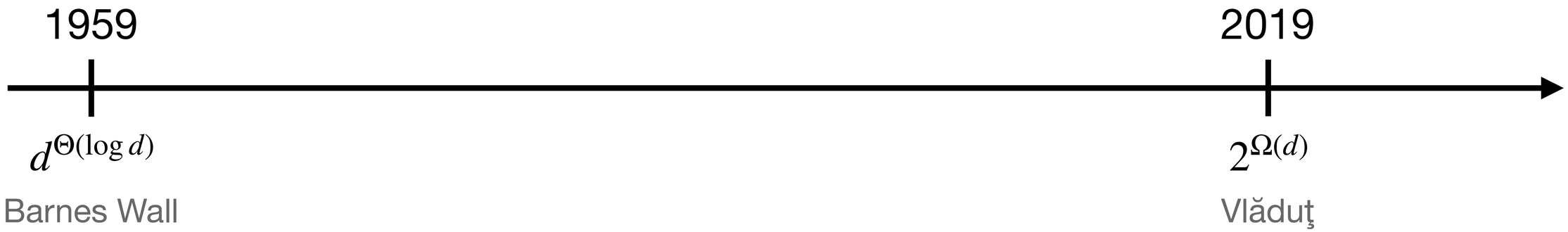
$> 2^{37}$

taken from Conway, Sloane 1999

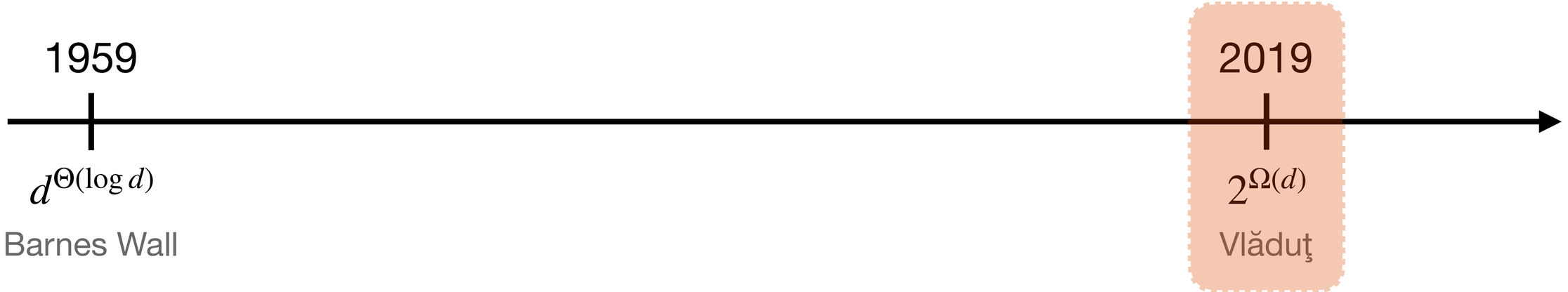
Asymptotically Large Kissing Numbers



Asymptotically Large Kissing Numbers

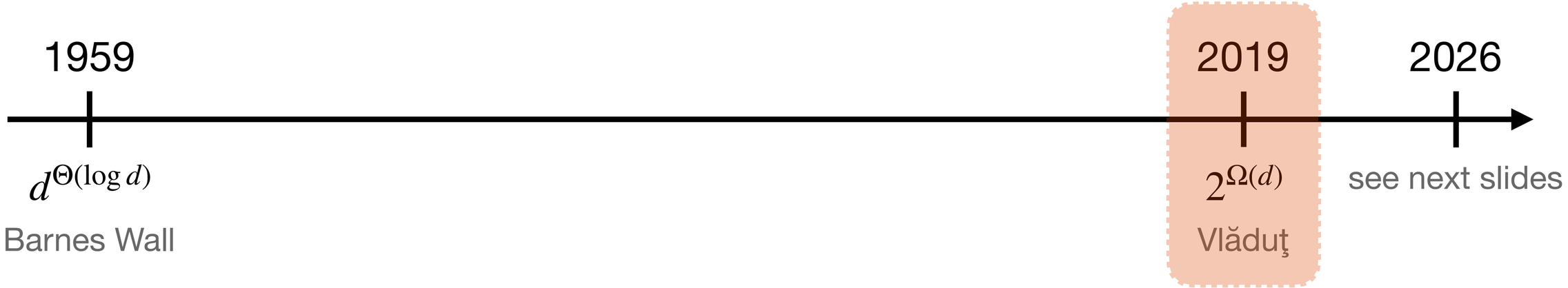


Asymptotically Large Kissing Numbers



⚠ **Bennett, Golovnev, Stephens-Davidowitz (2025):**
Vlăduţ's proof is incorrect

Asymptotically Large Kissing Numbers



⚠ **Bennett, Golovnev, Stephens-Davidowitz (2025):**
Vlăduţ's proof is incorrect

Craig’s Lattice

Craig's Lattice (Craig 1984)

Let p be prime, and $k < p$.

Craig's Lattice A^k_{p-1} is the ideal $(1-X)^k$ in $\mathbb{Z}[X]/(X^p-1)$.

Craig's Lattice (Craig 1984)

Let p be prime, and $k < p$.

Craig's Lattice A_{p-1}^{k} is the ideal $(1-X)^k$ in $\mathbb{Z}[X]/(X^p-1)$.

☞ $f_0 + f_1 X + \ldots + f_{p-1} X^{p-1} \in \mathbb{Z}[X]/(X^p-1) \simeq (f_0, f_1, \ldots, f_{p-1})^T \in \mathbb{Z}^p$

Craig's Lattice (Craig 1984)

Let p be prime, and $k < p$.

Craig's Lattice A_{p-1}^{k} is the ideal $(1-X)^k$ in $\mathbb{Z}[X]/(X^p-1)$.

$\dim(A_{p-1}^{k}) = p-1$

☞ $f_0 + f_1 X + \ldots + f_{p-1}X^{p-1} \in \mathbb{Z}[X]/(X^p-1) \simeq (f_0, f_1, \ldots, f_{p-1})^T \in \mathbb{Z}^p$

Craig's Lattice (Craig 1984)

Let p be prime, and $k < p$.

Craig's Lattice A_{p-1}^k is the ideal $(1-X)^k$ in $\mathbb{Z}[X]/(X^p-1)$.

$\dim(A_{p-1}^k) = p-1$

☞ $f_0 + f_1 X + \ldots + f_{p-1}X^{p-1} \in \mathbb{Z}[X]/(X^p-1) \simeq (f_0, f_1, \ldots, f_{p-1})^T \in \mathbb{Z}^p$

Bacher (2015):

If $k = o(\log p / \log\log p)$, then $\kappa(A_{p-1}^k) = \omega(p^k)$.

Craig's Lattice (Craig 1984)

Let p be prime, and $k < p$.

Craig's Lattice A_{p-1}^k is the ideal $(1-X)^k$ in $\mathbb{Z}[X]/(X^p-1)$.

$\dim(A_{p-1}^k) = p-1$

☞ $f_0 + f_1 X + \ldots + f_{p-1}X^{p-1} \in \mathbb{Z}[X]/(X^p-1) \simeq (f_0, f_1, \ldots, f_{p-1})^T \in \mathbb{Z}^p$

Bacher (2015):

If $k = o(\log p / \log\log p)$, then $\kappa(A_{p-1}^k) = \omega(p^k)$.

☞ Bacher's lower bound comes close to $d^{\Theta(\log d)}$ of Barnes-Wall.

The Minimal Shell of Craig's Lattice

$$\mathbf{H} := \begin{bmatrix} 0^0 & 1^0 & 2^0 & \cdots & (p-1)^0 \\ 0^1 & 1^1 & 2^1 & \cdots & (p-1)^1 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0^{k-1} & 1^{k-1} & 2^{k-1} & \cdots & (p-1)^{k-1} \end{bmatrix}$$

$$C := \left\{ \mathbf{v}_1 - \mathbf{v}_2 \in \mathbb{Z}^p \setminus \{\mathbf{0}\} \;\middle|\; \begin{array}{c} \mathbf{v}_1, \mathbf{v}_2 \in \{0,1\}^p, \\ \|\mathbf{v}_1\|_1 = \|\mathbf{v}_2\|_1 = k, \\ \mathbf{H}\mathbf{v}_1 \equiv \mathbf{H}\mathbf{v}_2 \mod p \end{array} \right\}$$

The Minimal Shell of Craig's Lattice

$$\mathbf{H} := \begin{bmatrix} 0^0 & 1^0 & 2^0 & \cdots & (p-1)^0 \\ 0^1 & 1^1 & 2^1 & \cdots & (p-1)^1 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0^{k-1} & 1^{k-1} & 2^{k-1} & \cdots & (p-1)^{k-1} \end{bmatrix}$$

$$C := \left\{ \mathbf{v}_1 - \mathbf{v}_2 \in \mathbb{Z}^p \setminus \{\mathbf{0}\} \;\middle|\; \begin{array}{c} \mathbf{v}_1, \mathbf{v}_2 \in \{0,1\}^p, \\ \|\mathbf{v}_1\|_1 = \|\mathbf{v}_2\|_1 = k, \\ \mathbf{H}\mathbf{v}_1 \equiv \mathbf{H}\mathbf{v}_2 \mod p \end{array} \right\}$$

Lemma:

If $C \neq \emptyset$, then $C = S(A_{p-1}^k)$.

The Minimal Shell of Craig's Lattice

$$\mathbf{H} := \begin{bmatrix} 0^0 & 1^0 & 2^0 & \cdots & (p-1)^0 \\ 0^1 & 1^1 & 2^1 & \cdots & (p-1)^1 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0^{k-1} & 1^{k-1} & 2^{k-1} & \cdots & (p-1)^{k-1} \end{bmatrix}$$

$$C := \left\{ \mathbf{v}_1 - \mathbf{v}_2 \in \mathbb{Z}^p \setminus \{\mathbf{0}\} \;\middle|\; \begin{array}{c} \mathbf{v}_1, \mathbf{v}_2 \in \{0,1\}^p, \\ \|\mathbf{v}_1\|_1 = \|\mathbf{v}_2\|_1 = k, \\ \mathbf{H}\mathbf{v}_1 \equiv \mathbf{H}\mathbf{v}_2 \mod p \end{array} \right\}$$

Lemma:

If $C \neq \emptyset$, then $C = S(A_{p-1}^k)$.

- $B := \left\{ \mathbf{v} \in \{0,1\}^p \mid \|\mathbf{v}\|_1 = k \right\}$
- $\varphi : B \to \mathbb{F}_p^{k-1}, \mathbf{v} \mapsto \mathbf{H}\mathbf{v}$

The Minimal Shell of Craig's Lattice

$$\mathbf{H} := \begin{bmatrix} 0^0 & 1^0 & 2^0 & \cdots & (p-1)^0 \\ 0^1 & 1^1 & 2^1 & \cdots & (p-1)^1 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0^{k-1} & 1^{k-1} & 2^{k-1} & \cdots & (p-1)^{k-1} \end{bmatrix}$$

$$C := \left\{ \mathbf{v}_1 - \mathbf{v}_2 \in \mathbb{Z}^p \setminus \{\mathbf{0}\} \;\middle|\; \begin{array}{c} \mathbf{v}_1, \mathbf{v}_2 \in \{0,1\}^p, \\ \|\mathbf{v}_1\|_1 = \|\mathbf{v}_2\|_1 = k, \\ \mathbf{H}\mathbf{v}_1 \equiv \mathbf{H}\mathbf{v}_2 \mod p \end{array} \right\}$$

Lemma:
If $C \neq \emptyset$, then $C = S(A_{p-1}^k)$.

- $|C| = \sum_{\mathbf{s} \in \mathbb{F}_p^{k-1}} |\varphi^{-1}(\mathbf{s})| \left(|\varphi^{-1}(\mathbf{s})| - 1 \right)$

- $B := \left\{ \mathbf{v} \in \{0,1\}^p \mid \|\mathbf{v}\|_1 = k \right\}$
- $\varphi : B \to \mathbb{F}_p^{k-1}, \mathbf{v} \mapsto \mathbf{H}\mathbf{v}$

The Minimal Shell of Craig's Lattice

$$\mathbf{H} := \begin{bmatrix} 0^0 & 1^0 & 2^0 & \cdots & (p-1)^0 \\ 0^1 & 1^1 & 2^1 & \cdots & (p-1)^1 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0^{k-1} & 1^{k-1} & 2^{k-1} & \cdots & (p-1)^{k-1} \end{bmatrix}$$

$$C := \left\{ \mathbf{v}_1 - \mathbf{v}_2 \in \mathbb{Z}^p \setminus \{\mathbf{0}\} \;\middle|\; \begin{array}{c} \mathbf{v}_1, \mathbf{v}_2 \in \{0,1\}^p, \\ \|\mathbf{v}_1\|_1 = \|\mathbf{v}_2\|_1 = k, \\ \mathbf{H}\mathbf{v}_1 \equiv \mathbf{H}\mathbf{v}_2 \mod p \end{array} \right\}$$

Lemma:
If $C \neq \emptyset$, then $C = S(A_{p-1}^k)$.

- $B := \left\{ \mathbf{v} \in \{0,1\}^p \mid \|\mathbf{v}\|_1 = k \right\}$
- $\varphi : B \to \mathbb{F}_p^{k-1}, \mathbf{v} \mapsto \mathbf{H}\mathbf{v}$

- $$|C| = \sum_{\mathbf{s} \in \mathbb{F}_p^{k-1}} |\varphi^{-1}(\mathbf{s})| \left(|\varphi^{-1}(\mathbf{s})| - 1 \right)$$
$$= \sum_{\mathbf{s} \in \mathbb{F}_p^{k-1}} \left(|\varphi^{-1}(\mathbf{s})|^2 - |\varphi^{-1}(\mathbf{s})| \right)$$

The Minimal Shell of Craig's Lattice

Lemma:
If $C \neq \emptyset$, then $C = S(A^k_{p-1})$.

- $B := \left\{ \mathbf{v} \in \{0,1\}^p \mid \|\mathbf{v}\|_1 = k \right\}$
- $\varphi : B \to \mathbb{F}_p^{k-1}, \mathbf{v} \mapsto \mathbf{H}\mathbf{v}$

- $$|C| = \sum_{\mathbf{s} \in \mathbb{F}_p^{k-1}} |\varphi^{-1}(\mathbf{s})| \left(|\varphi^{-1}(\mathbf{s})| - 1 \right)$$
$$= \sum_{\mathbf{s} \in \mathbb{F}_p^{k-1}} \left(|\varphi^{-1}(\mathbf{s})|^2 - |\varphi^{-1}(\mathbf{s})| \right)$$

The Minimal Shell of Craig's Lattice

Lemma:
If $C \neq \emptyset$, then $C = S(A^k_{p-1})$.

- $B := \left\{ \mathbf{v} \in \{0,1\}^p \mid \|\mathbf{v}\|_1 = k \right\}$
- $\varphi : B \to \mathbb{F}_p^{k-1}, \mathbf{v} \mapsto \mathbf{H}\mathbf{v}$

- $$|C| = \sum_{\mathbf{s} \in \mathbb{F}_p^{k-1}} |\varphi^{-1}(\mathbf{s})| \left(|\varphi^{-1}(\mathbf{s})| - 1 \right)$$
$$= \sum_{\mathbf{s} \in \mathbb{F}_p^{k-1}} \left(|\varphi^{-1}(\mathbf{s})|^2 - |\varphi^{-1}(\mathbf{s})| \right)$$

$$\sum_{\mathbf{s} \in \mathbb{F}_p^{k-1}} |\varphi^{-1}(\mathbf{s})| = |B| = \binom{p}{k}$$

The Minimal Shell of Craig's Lattice

Lemma:
If $C \neq \emptyset$, then $C = S(A^k_{p-1})$.

- $B := \left\{ \mathbf{v} \in \{0,1\}^p \mid \|\mathbf{v}\|_1 = k \right\}$
- $\varphi : B \to \mathbb{F}_p^{k-1}, \mathbf{v} \mapsto \mathbf{H}\mathbf{v}$

- $$|C| = \sum_{\mathbf{s} \in \mathbb{F}_p^{k-1}} |\varphi^{-1}(\mathbf{s})| \left(|\varphi^{-1}(\mathbf{s})| - 1 \right)$$
$$= \sum_{\mathbf{s} \in \mathbb{F}_p^{k-1}} \left(|\varphi^{-1}(\mathbf{s})|^2 - |\varphi^{-1}(\mathbf{s})| \right)$$

$$\sum_{\mathbf{s} \in \mathbb{F}_p^{k-1}} |\varphi^{-1}(\mathbf{s})| = |B| = \binom{p}{k}$$

$$\sum_{\mathbf{s} \in \mathbb{F}_p^{k-1}} |\varphi^{-1}(\mathbf{s})|^2 \geq \left(\sum_{\mathbf{s} \in \mathbb{F}_p^{k-1}} |\varphi^{-1}(\mathbf{s})| \right)^2 \cdot |\mathbb{F}_p^{k-1}|^{-1} = \binom{p}{k}^2 p^{1-k}$$

Bounding $\kappa(A_{p-1}^{k})$

Bacher (2015):

- $\kappa(A_{p-1}^{k}) \geq \binom{p}{k}^{2} p^{1-k} - \binom{p}{k}$

Bounding $\kappa(A_{p-1}^k)$

Bacher (2015):

- $\kappa(A_{p-1}^k) \geq \binom{p}{k}^2 p^{1-k} - \binom{p}{k} = \binom{p}{k}^2 p^{1-k}\left(1 - o(1)\right) \sim \frac{p^{k+1}}{(k!)^2} = \omega(p^k)$

$k = o(\log p / \log\log p)$

Bounding $\kappa(A_{p-1}^k)$

Bacher (2015):

- $\kappa(A_{p-1}^k) \geq \binom{p}{k}^2 p^{1-k} - \binom{p}{k} = \binom{p}{k}^2 p^{1-k}\left(1 - o(1)\right) \sim \frac{p^{k+1}}{(k!)^2} = \omega(p^k)$

  $k = o(\log p / \log\log p)$

Our result:

- $\kappa(A_{p-1}^k) = \binom{p}{k}^2 p^{1-k} - \binom{p}{k} + O\left(\frac{\left(k(\sqrt{p}+1)\right)^{2k}}{(k!)^2}\right)$

Bounding $\kappa(A_{p-1}^k)$

Bacher (2015):

- $\kappa(A_{p-1}^k) \geq \binom{p}{k}^2 p^{1-k} - \binom{p}{k} = \binom{p}{k}^2 p^{1-k}\left(1 - o(1)\right) \sim \frac{p^{k+1}}{(k!)^2} = \omega(p^k)$

  $k = o(\log p / \log\log p)$

Our result:

- $\kappa(A_{p-1}^k) = \binom{p}{k}^2 p^{1-k} - \binom{p}{k} + O\left(\frac{\left(k(\sqrt{p}+1)\right)^{2k}}{(k!)^2}\right) = \binom{p}{k}^2 p^{1-k}\left(1 \pm o(1)\right)$

  $k = o(\log p / \log\log p)$

Extrapolating $\kappa(A_{p-1}^k)$

Barnes (1957), Bacher (2015):

If $k \leq 4$, then

$$\kappa(A_{p-1}^k) = \frac{p - 2k^2 + 3k - 2}{(k!)^2} p^k + o\left(p^k\right).$$

Extrapolating $\kappa(A_{p-1}^k)$

Barnes (1957), Bacher (2015):

If $k \leq 4$, then

$$\kappa(A_{p-1}^k) = \frac{p - 2k^2 + 3k - 2}{(k!)^2} p^k + o\left(p^k\right).$$

Numerical data:

We computed $\kappa(A_{p-1}^k)$ for $k \leq 9, p \leq 521$.

We consistently have

$$\kappa(A_{p-1}^k) \geq \frac{p - 2k^2 + 3k - 2}{(k!)^2} p^k.$$

Extrapolating $\kappa(A_{p-1}^k)$

Barnes (1957), Bacher (2015):

If $k \leq 4$, then

$$\kappa(A_{p-1}^k) = \frac{p - 2k^2 + 3k - 2}{(k!)^2} p^k + o\left(p^k\right).$$

Numerical data:

We computed $\kappa(A_{p-1}^k)$ for $k \leq 9, p \leq 521$.

We consistently have

$$\kappa(A_{p-1}^k) \geq \frac{p - 2k^2 + 3k - 2}{(k!)^2} p^k.$$

☞ Using symmetries of $(X-1)^k \subset \mathbb{Z}[X]/(X^p - 1)$,

we managed to compute $\kappa(A_{p-1}^k)$ in time $\widetilde{\Theta}(p^{k-2})$.

Extrapolating $\kappa(A_{p-1}^k)$

Barnes (1957), Bacher (2015):

If $k \leq 4$, then

$$\kappa(A_{p-1}^k) = \frac{p - 2k^2 + 3k - 2}{(k!)^2} p^k + o\left(p^k\right).$$

Numerical data:

We computed $\kappa(A_{p-1}^k)$ for $k \leq 9, p \leq 521$.

We consistently have

$$\kappa(A_{p-1}^k) \geq \frac{p - 2k^2 + 3k - 2}{(k!)^2} p^k.$$

☞ Using symmetries of $(X-1)^k \subset \mathbb{Z}[X]/(X^p - 1)$,
we managed to compute $\kappa(A_{p-1}^k)$ in time $\widetilde{\Theta}(p^{k-2})$.

If $k \leq \sqrt{p/2}$, then

$$\frac{p - 2k^2 + 3k - 2}{(k!)^2} p^k \geq \frac{3k-2}{(k!)^2} p^k$$

Extrapolating $\kappa(A_{p-1}^k)$

Barnes (1957), Bacher (2015):

If $k \leq 4$, then

$$\kappa(A_{p-1}^k) = \frac{p - 2k^2 + 3k - 2}{(k!)^2} p^k + o\left(p^k\right).$$

Numerical data:

We computed $\kappa(A_{p-1}^k)$ for $k \leq 9, p \leq 521$.

We consistently have

$$\kappa(A_{p-1}^k) \geq \frac{p - 2k^2 + 3k - 2}{(k!)^2} p^k.$$

☞ Using symmetries of $(X-1)^k \subset \mathbb{Z}[X]/(X^p - 1)$,
we managed to compute $\kappa(A_{p-1}^k)$ in time $\widetilde{\Theta}(p^{k-2})$.

If $k \leq \sqrt{p/2}$, then

$$\frac{p - 2k^2 + 3k - 2}{(k!)^2} p^k \geq \frac{3k-2}{(k!)^2} p^k$$

$$\sim \frac{3}{2\pi} \left(\frac{e^2}{k^2}\right)^k p^k$$

Extrapolating $\kappa(A_{p-1}^k)$

Barnes (1957), Bacher (2015):

If $k \leq 4$, then

$$\kappa(A_{p-1}^k) = \frac{p - 2k^2 + 3k - 2}{(k!)^2} p^k + o\left(p^k\right).$$

Numerical data:

We computed $\kappa(A_{p-1}^k)$ for $k \leq 9, p \leq 521$.

We consistently have

$$\kappa(A_{p-1}^k) \geq \frac{p - 2k^2 + 3k - 2}{(k!)^2} p^k.$$

☞ Using symmetries of $(X-1)^k \subset \mathbb{Z}[X]/(X^p - 1)$,
we managed to compute $\kappa(A_{p-1}^k)$ in time $\widetilde{\Theta}(p^{k-2})$.

If $k \leq \sqrt{p/2}$, then

$$\begin{aligned}
\frac{p - 2k^2 + 3k - 2}{(k!)^2} p^k &\geq \frac{3k-2}{(k!)^2} p^k \\
&\sim \frac{3}{2\pi} \left(\frac{e^2}{k^2}\right)^k p^k \\
&\geq \frac{3}{2\pi} (2e^2)^k.
\end{aligned}$$

Extrapolating $\kappa(A_{p-1}^k)$

Barnes (1957), Bacher (2015):

If $k \le 4$, then

$$\kappa(A_{p-1}^k) = \frac{p - 2k^2 + 3k - 2}{(k!)^2} p^k + o\left(p^k\right).$$

Numerical data:

We computed $\kappa(A_{p-1}^k)$ for $k \le 9, p \le 521$.

We consistently have

$$\kappa(A_{p-1}^k) \ge \frac{p - 2k^2 + 3k - 2}{(k!)^2} p^k.$$

☞ Using symmetries of $(X-1)^k \subset \mathbb{Z}[X]/(X^p - 1)$, we managed to compute $\kappa(A_{p-1}^k)$ in time $\widetilde{\Theta}(p^{k-2})$.

If $k \le \sqrt{p/2}$, then

$$\frac{p - 2k^2 + 3k - 2}{(k!)^2} p^k \ge \frac{3k-2}{(k!)^2} p^k$$

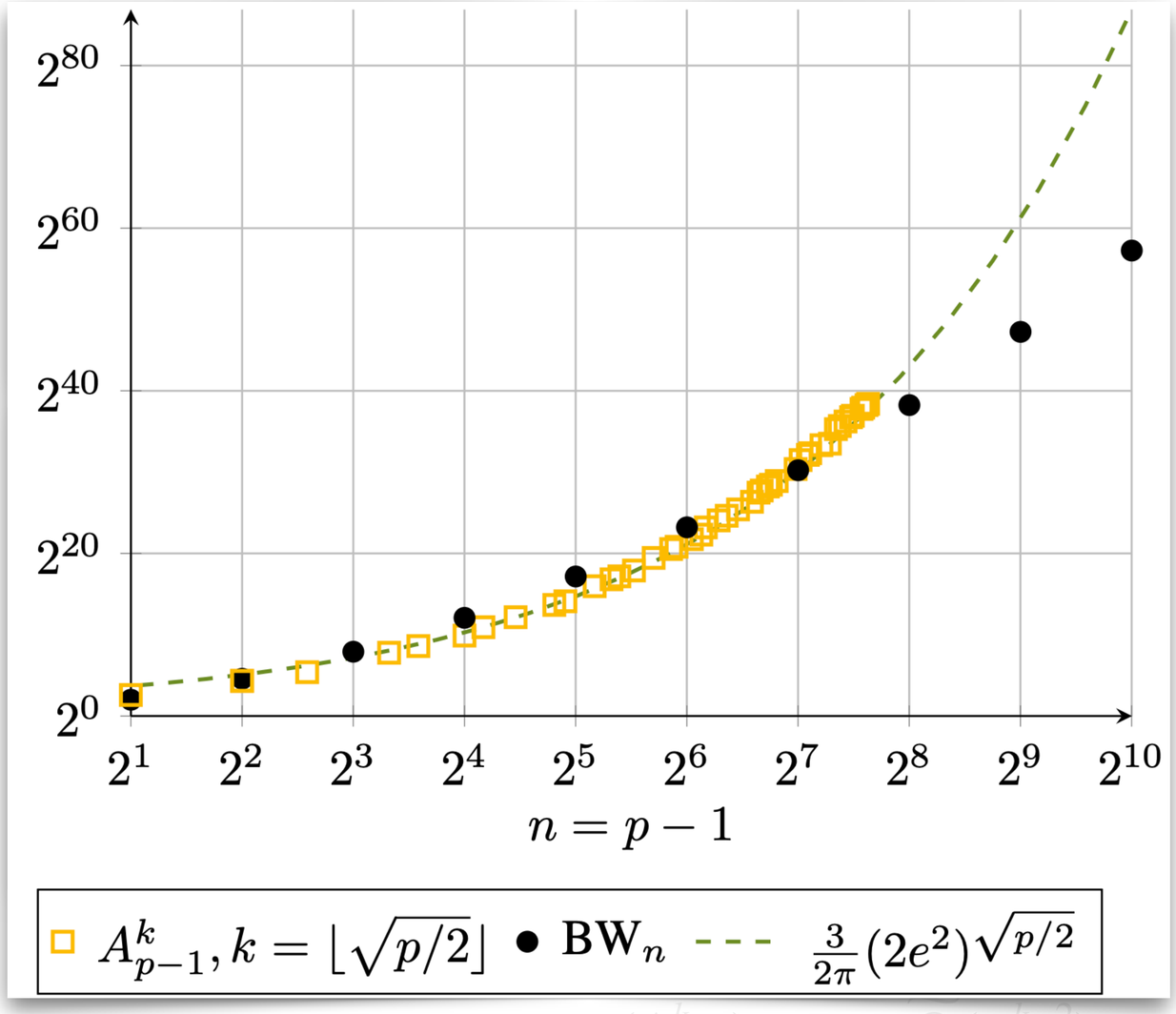
$$\sim \frac{3}{2\pi} \left(\frac{e^2}{k^2}\right)^k p^k$$

$$\ge \frac{3}{2\pi} (2e^2)^k.$$

Open Question:

$$\kappa\left(A_{p-1}^{\lfloor\sqrt{p/2}\rfloor}\right) \stackrel{?}{=} e^{\Omega(\sqrt{p})}$$

Extrapolating $\kappa(A_{p-1}^k)$



If $k \le \sqrt{p/2}$, then

$$\frac{p - 2k^2 + 3k - 2}{(k!)^2} p^k \ge \frac{3k-2}{(k!)^2} p^k$$

$$\sim \frac{3}{2\pi}\left(\frac{e^2}{k^2}\right)^k p^k$$

$$\ge \frac{3}{2\pi}(2e^2)^k.$$

Open Question:

$$\kappa\left(A_{p-1}^{\lfloor\sqrt{p/2}\rfloor}\right) \stackrel{?}{=} e^{\Omega(\sqrt{p})}$$

we managed to compute $\kappa(A_{p-1}^k)$ in time $\Theta(p^{k-2})$.

Concurrent Work: Laarhoven, Kominers (2026)

- $k := \lfloor \sqrt{p}/2 \rfloor$
- Pick $\mathbf{v} \in \{0,1\}^p$ with $\|\mathbf{v}\|_1 = 2k$ uniformly at random.
- $\mathscr{L} := A_{p-1}^k + \mathbb{Z} \cdot \mathbf{v}$.

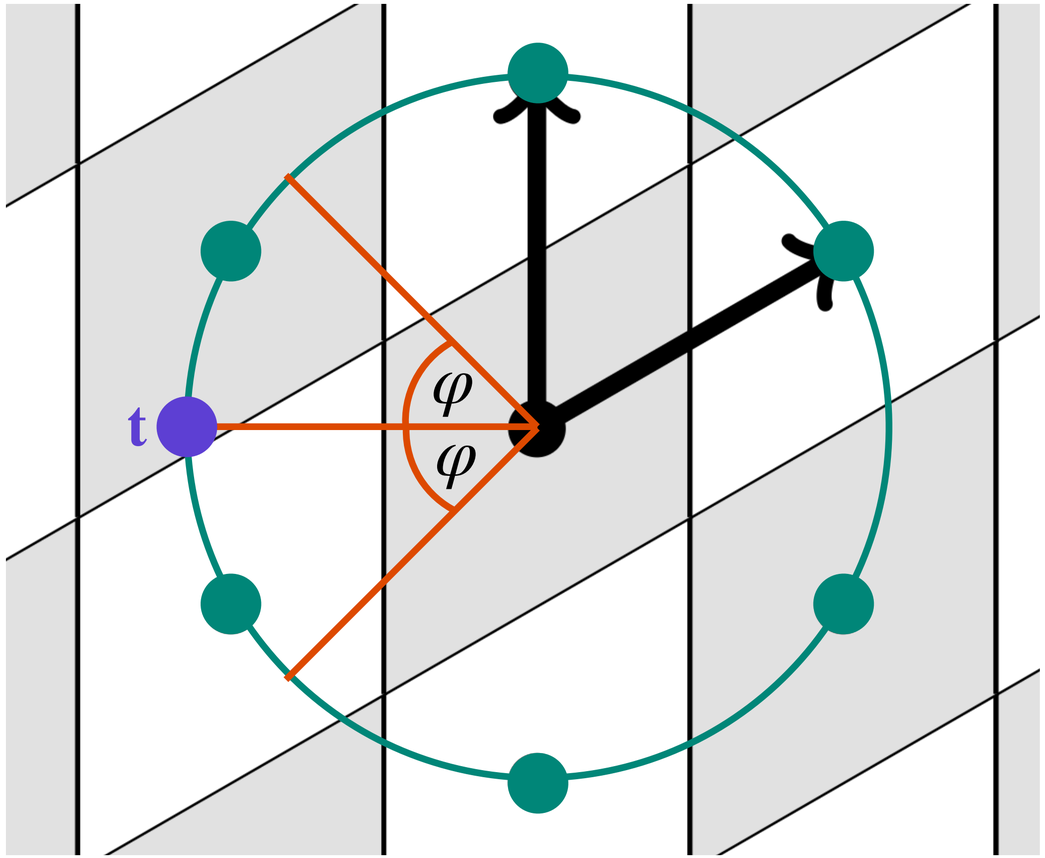
Concurrent Work: Laarhoven, Kominers (2026)

- $k := \lfloor \sqrt{p}/2 \rfloor$
- Pick $\mathbf{v} \in \{0,1\}^p$ with $\|\mathbf{v}\|_1 = 2k$ uniformly at random.
- $\mathscr{L} := A_{p-1}^k + \mathbb{Z} \cdot \mathbf{v}$.

- $\kappa(\mathscr{L}) = e^{\Omega(\sqrt{p})}$ with constant probability.

Decoding $S(A_{p-1}^{k})$ efficiently

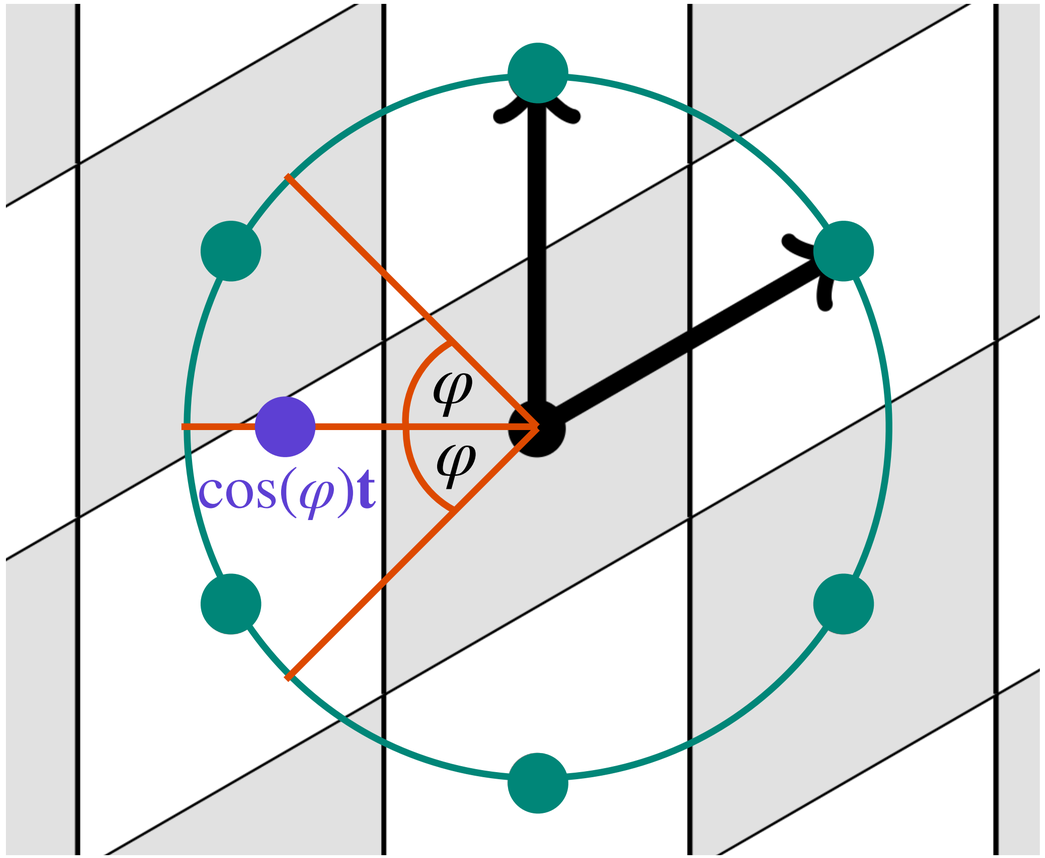
Lattice Decoding $\Longrightarrow$ Spherical Decoding



Problem:

Find all $\mathbf{v} \in S(\mathscr{L})$ with $\langle \mathbf{v}, \mathbf{t} \rangle > \cos(\varphi)\lambda_1^2$

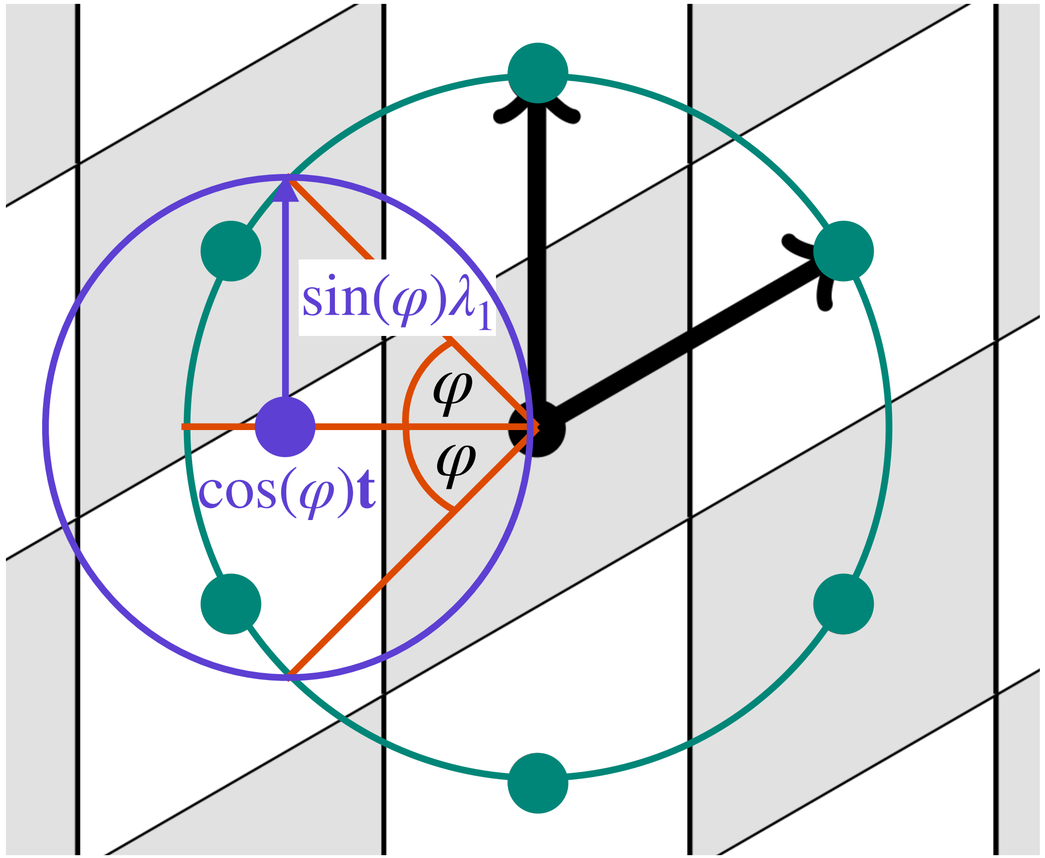
Lattice Decoding $\Longrightarrow$ Spherical Decoding



Problem:

Find all $\mathbf{v} \in S(\mathscr{L})$ with $\langle \mathbf{v}, \mathbf{t} \rangle > \cos(\varphi)\lambda_1^2$

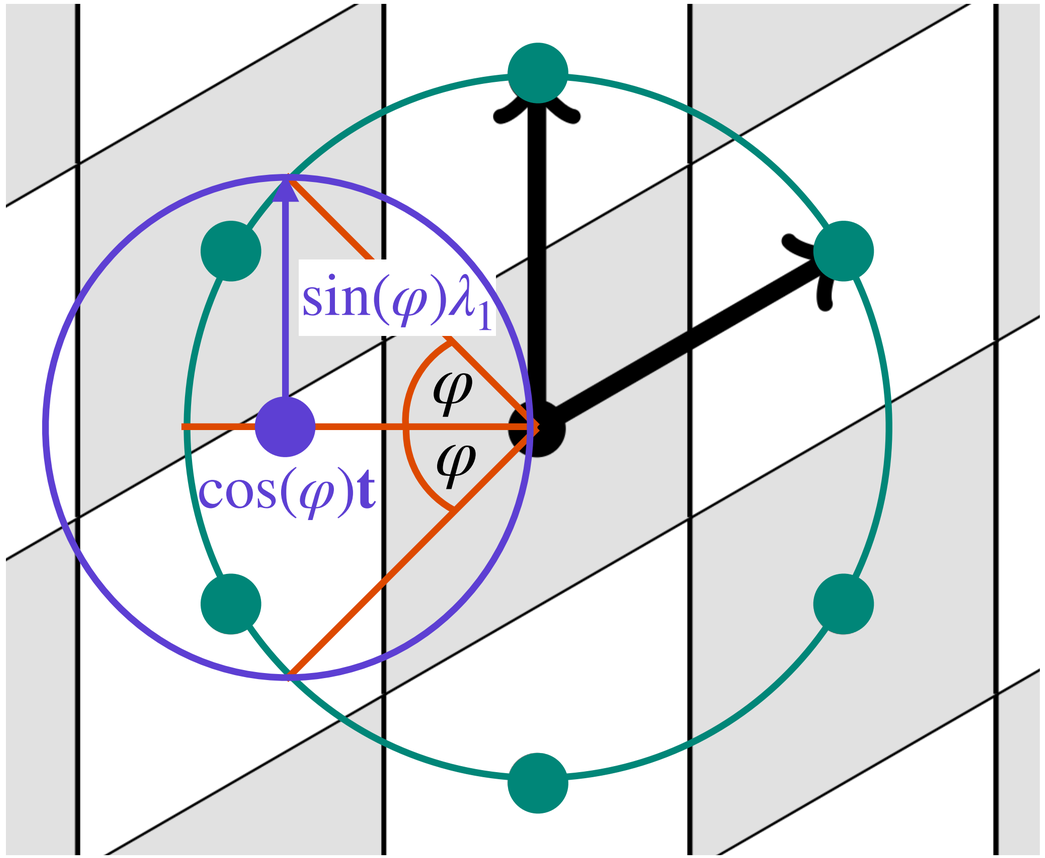
Lattice Decoding $\Longrightarrow$ Spherical Decoding



Problem:

Find all $\mathbf{v} \in S(\mathscr{L})$ with $\langle \mathbf{v}, \mathbf{t} \rangle > \cos(\varphi)\lambda_1^2$

Lattice Decoding $\Longrightarrow$ Spherical Decoding

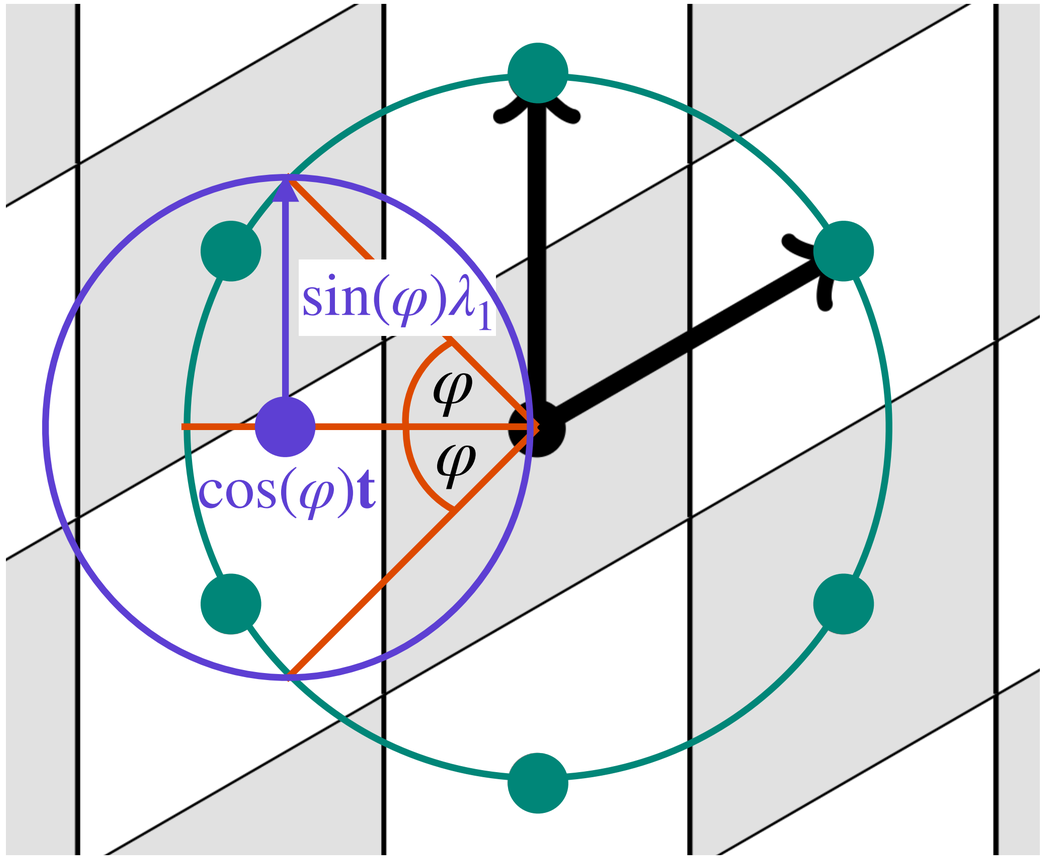


Problem:

Find all $\mathbf{v} \in S(\mathscr{L})$ with $\langle \mathbf{v}, \mathbf{t} \rangle > \cos(\varphi)\lambda_1^2$

$$\|\mathbf{v} - \cos(\varphi)\mathbf{t}\|^2 = \|\mathbf{v}\|^2 + \cos(\varphi)^2 \|\mathbf{t}\|^2 - 2\cos(\varphi) \langle \mathbf{v}, \mathbf{t} \rangle$$

Lattice Decoding $\Longrightarrow$ Spherical Decoding

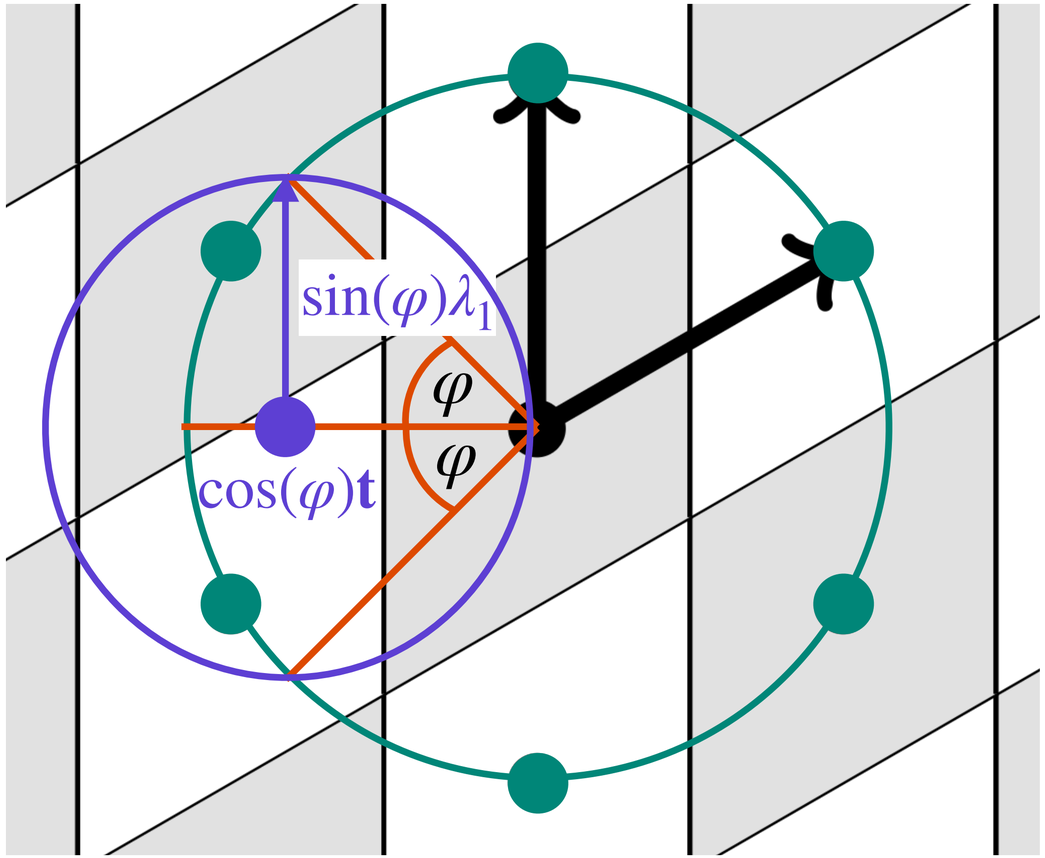


Problem:

Find all $\mathbf{v} \in S(\mathscr{L})$ with $\langle \mathbf{v}, \mathbf{t} \rangle > \cos(\varphi)\lambda_1^2$

$$\|\mathbf{v} - \cos(\varphi)\mathbf{t}\|^2 = \underbrace{\|\mathbf{v}\|^2}_{=\lambda_1^2} + \cos(\varphi)^2 \underbrace{\|\mathbf{t}\|^2}_{=\lambda_1^2} - 2\cos(\varphi) \underbrace{\langle \mathbf{v}, \mathbf{t} \rangle}_{>\cos(\varphi)\lambda_1^2}$$

Lattice Decoding $\Longrightarrow$ Spherical Decoding

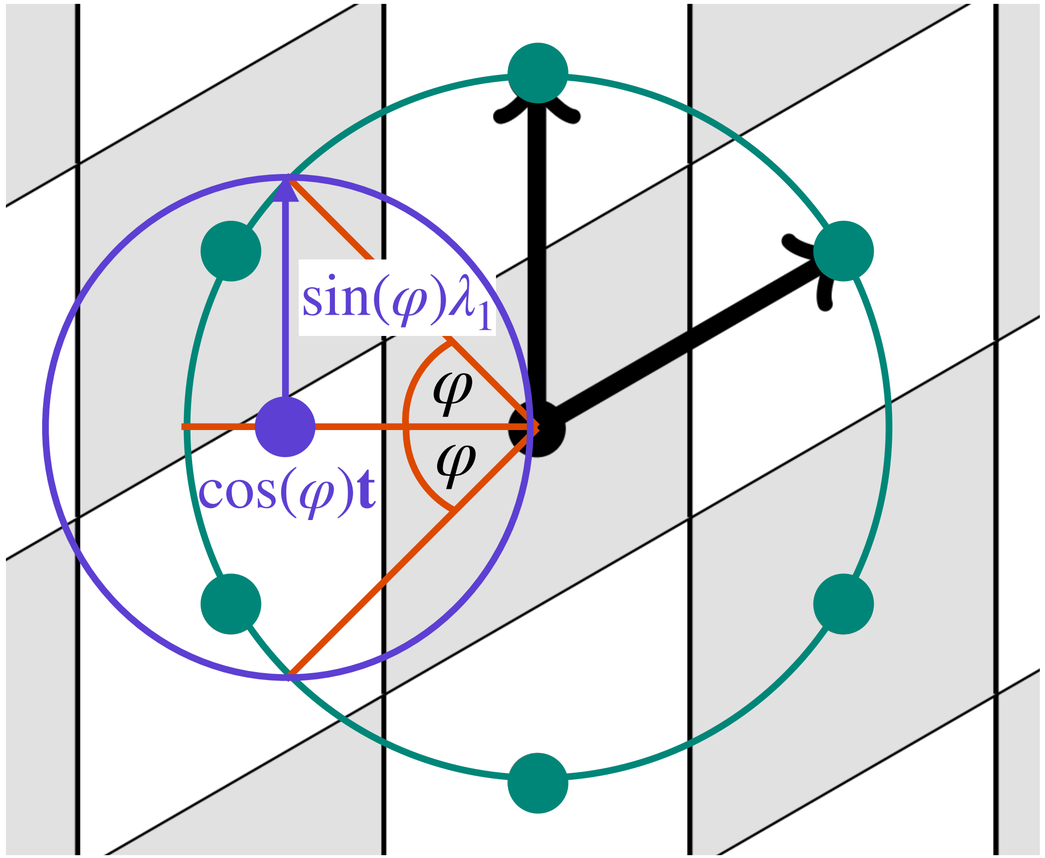


Problem:

Find all $\mathbf{v} \in S(\mathscr{L})$ with $\langle \mathbf{v}, \mathbf{t} \rangle > \cos(\varphi)\lambda_1^2$

$$\|\mathbf{v} - \cos(\varphi)\mathbf{t}\|^2 = \underbrace{\|\mathbf{v}\|^2}_{=\lambda_1^2} + \cos(\varphi)^2 \underbrace{\|\mathbf{t}\|^2}_{=\lambda_1^2} - 2\cos(\varphi) \underbrace{\langle \mathbf{v}, \mathbf{t} \rangle}_{>\cos(\varphi)\lambda_1^2} < (1 - \cos(\varphi)^2)\lambda_1^2 = \sin(\varphi)^2\lambda_1^2$$

Lattice Decoding $\Longrightarrow$ Spherical Decoding



Problem:

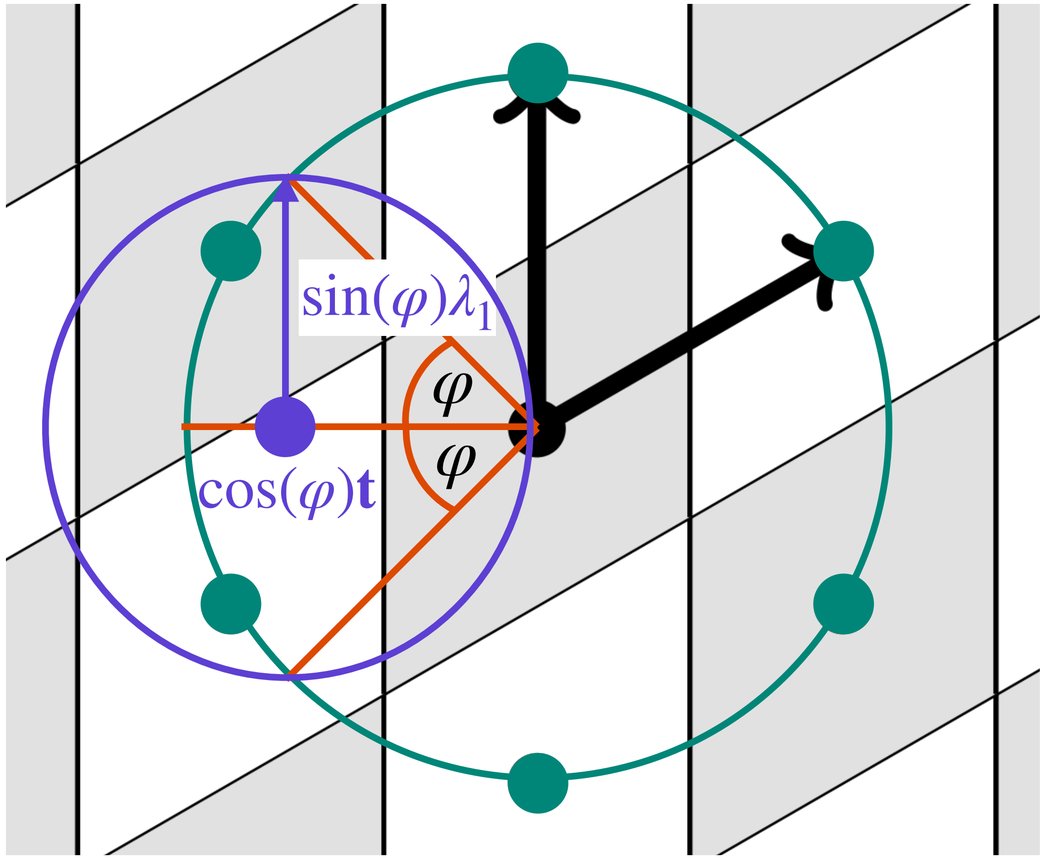
Find all $\mathbf{v} \in S(\mathscr{L})$ with $\langle \mathbf{v}, \mathbf{t} \rangle > \cos(\varphi)\lambda_1^2$

Solution:

Find all $\mathbf{v} \in \mathscr{L}$ with $\|\mathbf{v} - \cos(\varphi)\mathbf{t}\| < \sin(\varphi)\lambda_1$

$$\|\mathbf{v} - \cos(\varphi)\mathbf{t}\|^2 = \underbrace{\|\mathbf{v}\|^2}_{=\lambda_1^2} + \cos(\varphi)^2 \underbrace{\|\mathbf{t}\|^2}_{=\lambda_1^2} - 2\cos(\varphi) \underbrace{\langle \mathbf{v}, \mathbf{t} \rangle}_{>\cos(\varphi)\lambda_1^2} < (1 - \cos(\varphi)^2)\lambda_1^2 = \sin(\varphi)^2\lambda_1^2$$

Lattice Decoding $\Longrightarrow$ Spherical Decoding



Problem:

Find all $\mathbf{v} \in S(\mathscr{L})$ with $\langle \mathbf{v}, \mathbf{t} \rangle > \cos(\varphi)\lambda_1^2$

Solution:

Find all $\mathbf{v} \in \mathscr{L}$ with $\|\mathbf{v} - \cos(\varphi)\mathbf{t}\| < \sin(\varphi)\lambda_1$

Interesting cases:

- $\varphi \leq 30° \implies \sin(\varphi) \leq 1/2$
- $\varphi \leq 45° \implies \sin(\varphi) \leq 1/\sqrt{2}$

$$\|\mathbf{v} - \cos(\varphi)\mathbf{t}\|^2 = \underbrace{\|\mathbf{v}\|^2}_{=\lambda_1^2} + \cos(\varphi)^2 \underbrace{\|\mathbf{t}\|^2}_{=\lambda_1^2} - 2\cos(\varphi) \underbrace{\langle \mathbf{v}, \mathbf{t} \rangle}_{>\cos(\varphi)\lambda_1^2} < (1 - \cos(\varphi)^2)\lambda_1^2 = \sin(\varphi)^2\lambda_1^2$$

Decoding Craig's Lattice

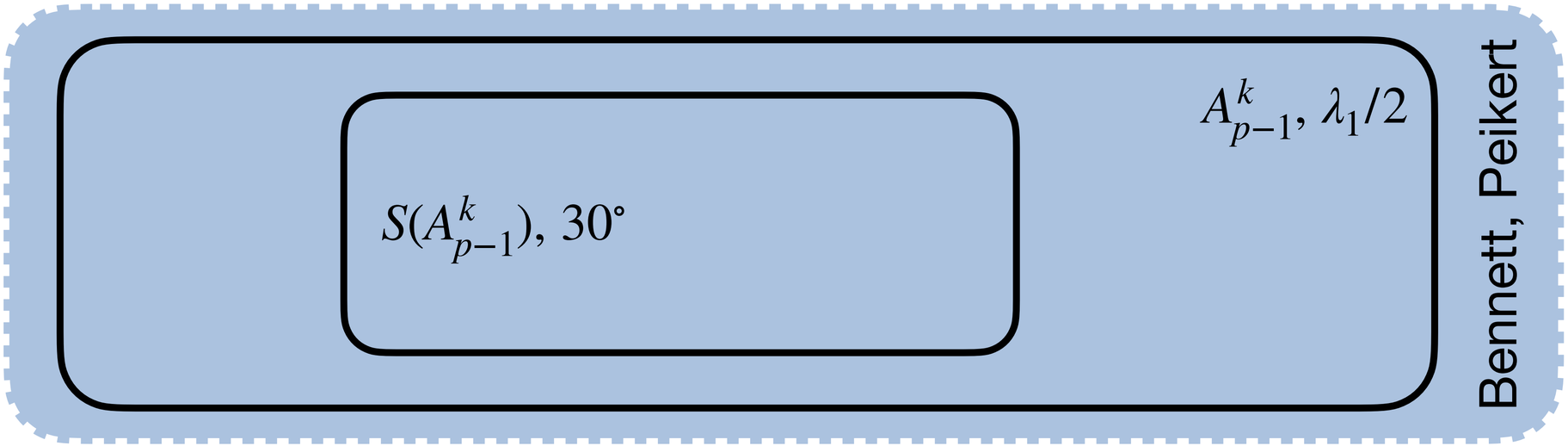
Bennett, Peikert (2023):
Polynomial time lattice list decoder for $\|\mathbf{v} - \mathbf{t}\| < \alpha\lambda_1(A_{p-1}^k)$ with α slightly above $1/2$.

☞ $\alpha \leq \frac{1}{2}\sqrt{(1-\varepsilon)(1+1/k)}$, $\varepsilon > 1/\mathrm{poly}(p)$

Decoding Craig's Lattice

Bennett, Peikert (2023):
Polynomial time lattice list decoder for $\|\mathbf{v} - \mathbf{t}\| < \alpha\lambda_1(A_{p-1}^k)$ with α slightly above $1/2$.

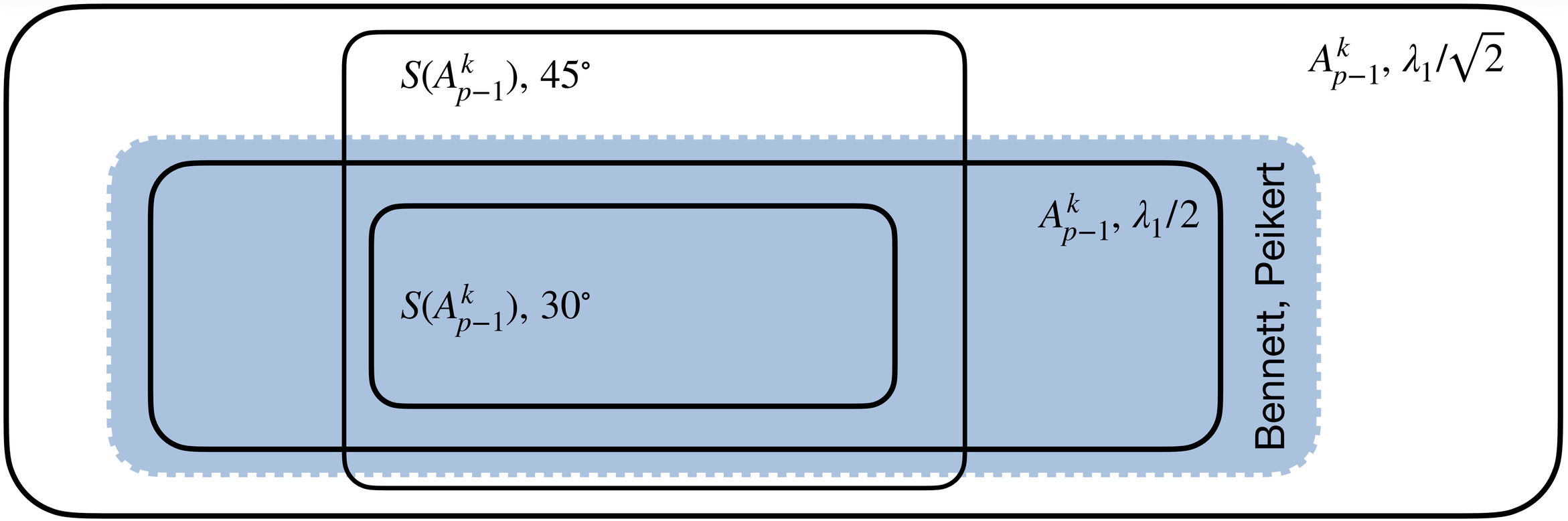
☞ $\alpha \leq \frac{1}{2}\sqrt{(1-\varepsilon)(1+1/k)}$, $\varepsilon > 1/\mathrm{poly}(p)$



Decoding Craig's Lattice

Bennett, Peikert (2023):
Polynomial time lattice list decoder for $\|\mathbf{v} - \mathbf{t}\| < \alpha\lambda_1(A^k_{p-1})$ with α slightly above $1/2$.

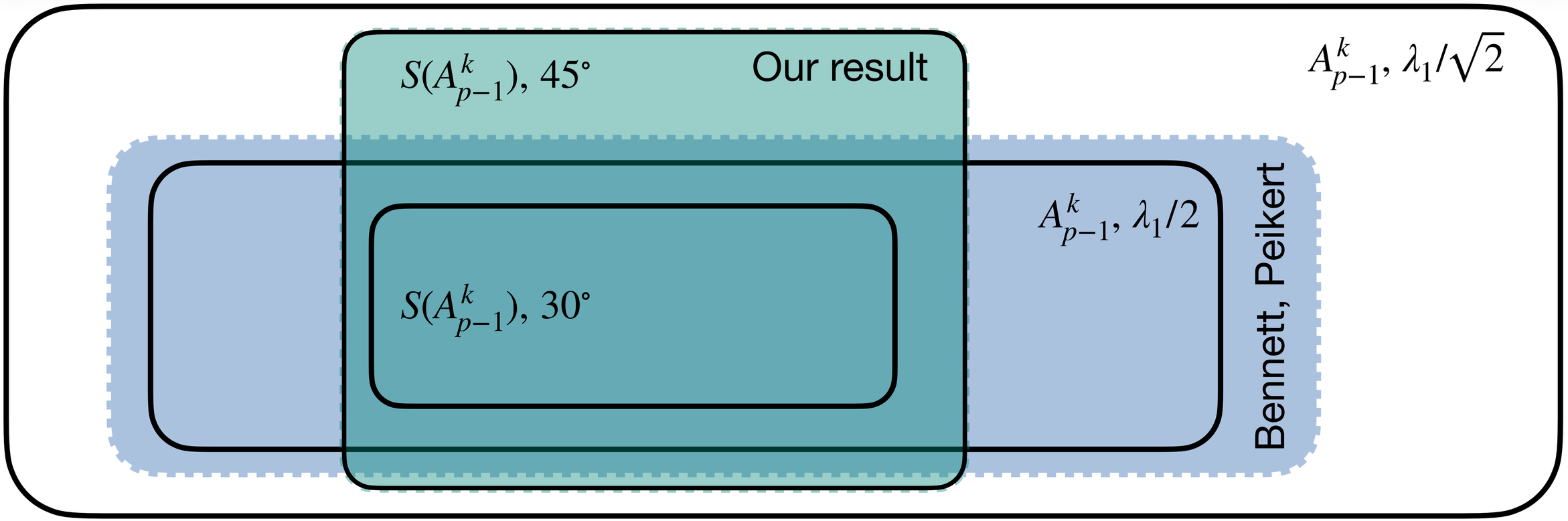
☞ $\alpha \le \frac{1}{2}\sqrt{(1-\varepsilon)(1+1/k)}$, $\varepsilon > 1/\mathrm{poly}(p)$



Decoding Craig's Lattice

Bennett, Peikert (2023):
Polynomial time lattice list decoder for $\|\mathbf{v} - \mathbf{t}\| < \alpha\lambda_1(A^k_{p-1})$ with α slightly above $1/2$.

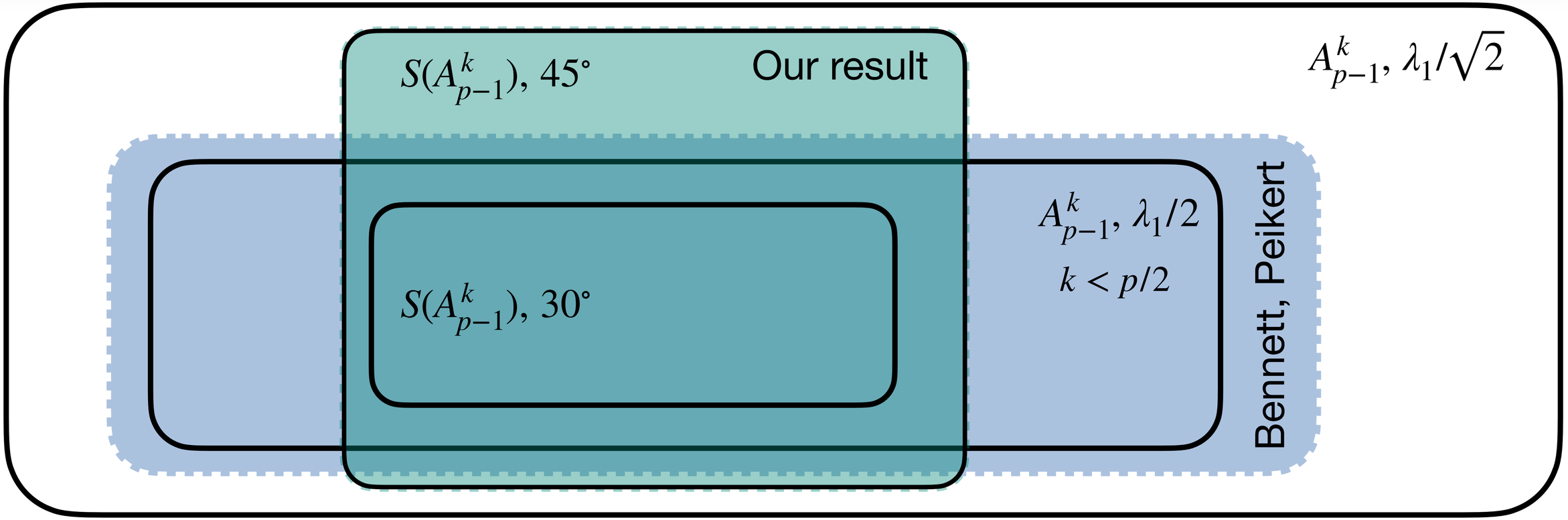
☞ $\alpha \le \frac{1}{2}\sqrt{(1-\varepsilon)(1+1/k)}$, $\varepsilon > 1/\mathrm{poly}(p)$



Decoding Craig's Lattice

Bennett, Peikert (2023):
Polynomial time lattice list decoder for $\|\mathbf{v} - \mathbf{t}\| < \alpha\lambda_1(A^k_{p-1})$ with α slightly above $1/2$.

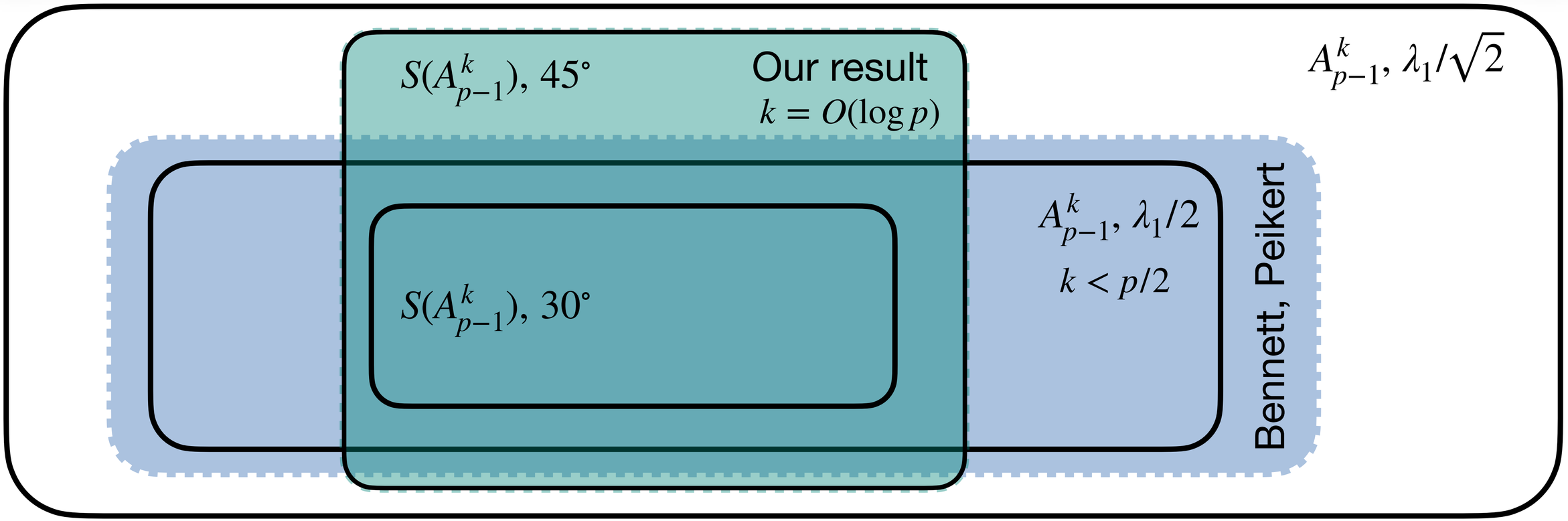
☞ $\alpha \le \frac{1}{2}\sqrt{(1-\varepsilon)(1+1/k)}$, $\varepsilon > 1/\mathrm{poly}(p)$



Decoding Craig's Lattice

Bennett, Peikert (2023):
Polynomial time lattice list decoder for $\|\mathbf{v} - \mathbf{t}\| < \alpha\lambda_1(A^k_{p-1})$ with α slightly above $1/2$.

☞ $\alpha \le \frac{1}{2}\sqrt{(1-\varepsilon)(1+1/k)}$, $\varepsilon > 1/\mathrm{poly}(p)$



Decoding via Discrete ℓ_1-Approximation

$\mathbf{t} \in \mathbb{R}^p$

$$\{\mathbf{v} \in S(A^k_{p-1}) \mid \langle \mathbf{v}, \mathbf{t} \rangle \geq \rho \lambda_1(A^k_{p-1})^2\}$$

$\mathbf{v}_1$
$\mathbf{v}_2$
$\vdots$
$\mathbf{v}_M$

Decoding via Discrete ℓ_1-Approximation

$L \subseteq \{0, \pm 1\}^p, |L| = e^{O(k)}$

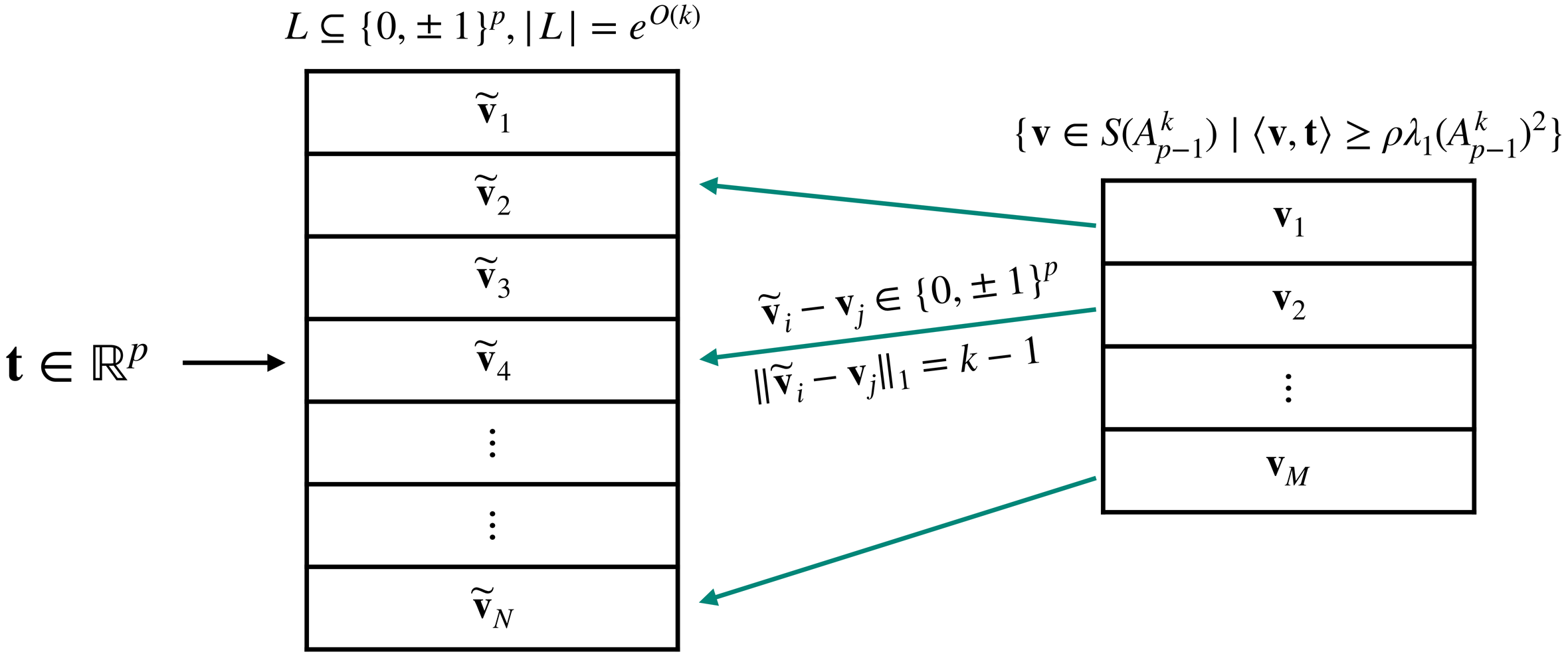
$\mathbf{t} \in \mathbb{R}^p$ ⟶

$\widetilde{\mathbf{v}}_1$
$\widetilde{\mathbf{v}}_2$
$\widetilde{\mathbf{v}}_3$
$\widetilde{\mathbf{v}}_4$
⋮
⋮
$\widetilde{\mathbf{v}}_N$

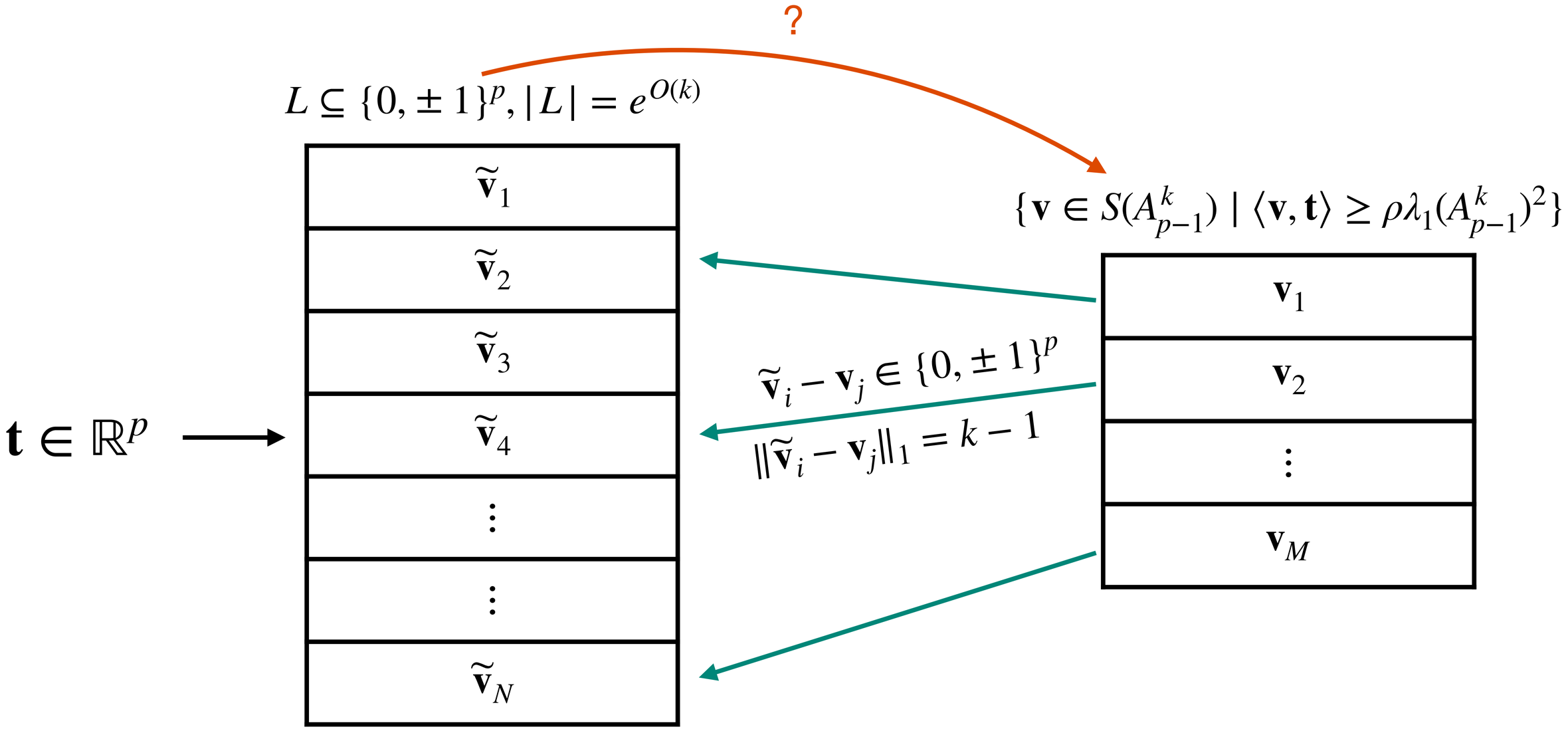
$\{\mathbf{v} \in S(A_{p-1}^k) \mid \langle \mathbf{v}, \mathbf{t} \rangle \geq \rho \lambda_1(A_{p-1}^k)^2\}$

$\mathbf{v}_1$
$\mathbf{v}_2$
⋮
$\mathbf{v}_M$

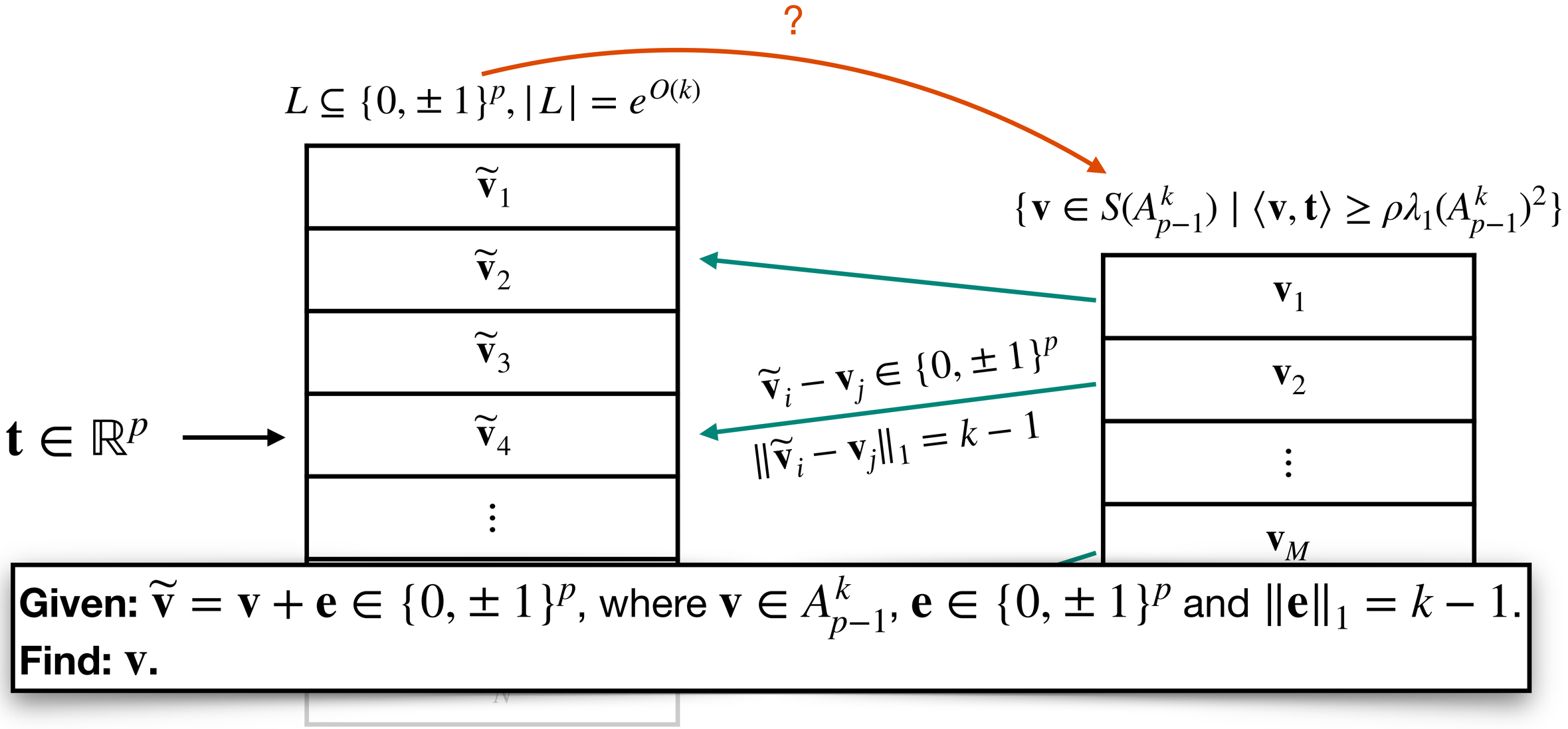
Decoding via Discrete ℓ_1-Approximation



Decoding via Discrete ℓ_1-Approximation



Decoding via Discrete ℓ_1-Approximation



Given: $\widetilde{\mathbf{v}} = \mathbf{v} + \mathbf{e} \in \{0, \pm 1\}^p$, where $\mathbf{v} \in A^k_{p-1}$, $\mathbf{e} \in \{0, \pm 1\}^p$ and $\|\mathbf{e}\|_1 = k - 1$.

Find: $\mathbf{v}$.

Decoding via Discrete ℓ_1-Approximation

Given: $\widetilde{\mathbf{v}} = \mathbf{v} + \mathbf{e} \in \{0, \pm 1\}^p$, where $\mathbf{v} \in A_{p-1}^k$, $\mathbf{e} \in \{0, \pm 1\}^p$ and $\|\mathbf{e}\|_1 = k - 1$.

Find: $\mathbf{v}$.

Decoding via Discrete ℓ_1-Approximation

Given: $\widetilde{\mathbf{v}} = \mathbf{v} + \mathbf{e} \in \{0, \pm 1\}^p$, where $\mathbf{v} \in A_{p-1}^k$, $\mathbf{e} \in \{0, \pm 1\}^p$ and $\|\mathbf{e}\|_1 = k - 1$.
Find: $\mathbf{v}$.

$$\mathbf{H} := \begin{bmatrix} 0^0 & 1^0 & 2^0 & \cdots & (p-1)^0 \\ 0^1 & 1^1 & 2^1 & \cdots & (p-1)^1 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0^{k-1} & 1^{k-1} & 2^{k-1} & \cdots & (p-1)^{k-1} \end{bmatrix}$$

Lemma (Conway, Sloane):
If $\mathbf{v} \in A_{p-1}^k$, then $\mathbf{Hv} \equiv \mathbf{0} \mod p$.

$$\Longrightarrow \mathbf{H}\widetilde{\mathbf{v}} \equiv \mathbf{He} \mod p$$

Decoding via Discrete ℓ_1-Approximation

Given: $\widetilde{\mathbf{v}} = \mathbf{v} + \mathbf{e} \in \{0, \pm 1\}^p$, where $\mathbf{v} \in A_{p-1}^k$, $\mathbf{e} \in \{0, \pm 1\}^p$ and $\|\mathbf{e}\|_1 = k - 1$.
Find: $\mathbf{v}$.

$$\mathbf{H} := \begin{bmatrix} 0^0 & 1^0 & 2^0 & \cdots & (p-1)^0 \\ 0^1 & 1^1 & 2^1 & \cdots & (p-1)^1 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0^{k-1} & 1^{k-1} & 2^{k-1} & \cdots & (p-1)^{k-1} \end{bmatrix}$$

Lemma (Conway, Sloane):
If $\mathbf{v} \in A_{p-1}^k$, then $\mathbf{Hv} \equiv \mathbf{0} \mod p$.

$$\implies \mathbf{H}\widetilde{\mathbf{v}} \equiv \mathbf{He} \mod p$$

Computing $\mathbf{e} \in \{0, \pm 1\}^p$ as a solution to

$$\mathbf{H}\widetilde{\mathbf{v}} \equiv \mathbf{He} \mod p$$

is a **syndrome decoding problem** over $\mathbb{F}_p$ for a **GRS code** in the **Lee metric**.

Decoding via Discrete ℓ_1-Approximation

Given: $\widetilde{\mathbf{v}} = \mathbf{v} + \mathbf{e} \in \{0, \pm 1\}^p$, where $\mathbf{v} \in A_{p-1}^k$, $\mathbf{e} \in \{0, \pm 1\}^p$ and $\|\mathbf{e}\|_1 = k - 1$.
Find: $\mathbf{v}$.

$$\mathbf{H} := \begin{bmatrix} 0^0 & 1^0 & 2^0 & \cdots & (p-1)^0 \\ 0^1 & 1^1 & 2^1 & \cdots & (p-1)^1 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0^{k-1} & 1^{k-1} & 2^{k-1} & \cdots & (p-1)^{k-1} \end{bmatrix}$$

Computing $\mathbf{e} \in \{0, \pm 1\}^p$ as a solution to

$$\mathbf{H}\widetilde{\mathbf{v}} \equiv \mathbf{He} \mod p$$

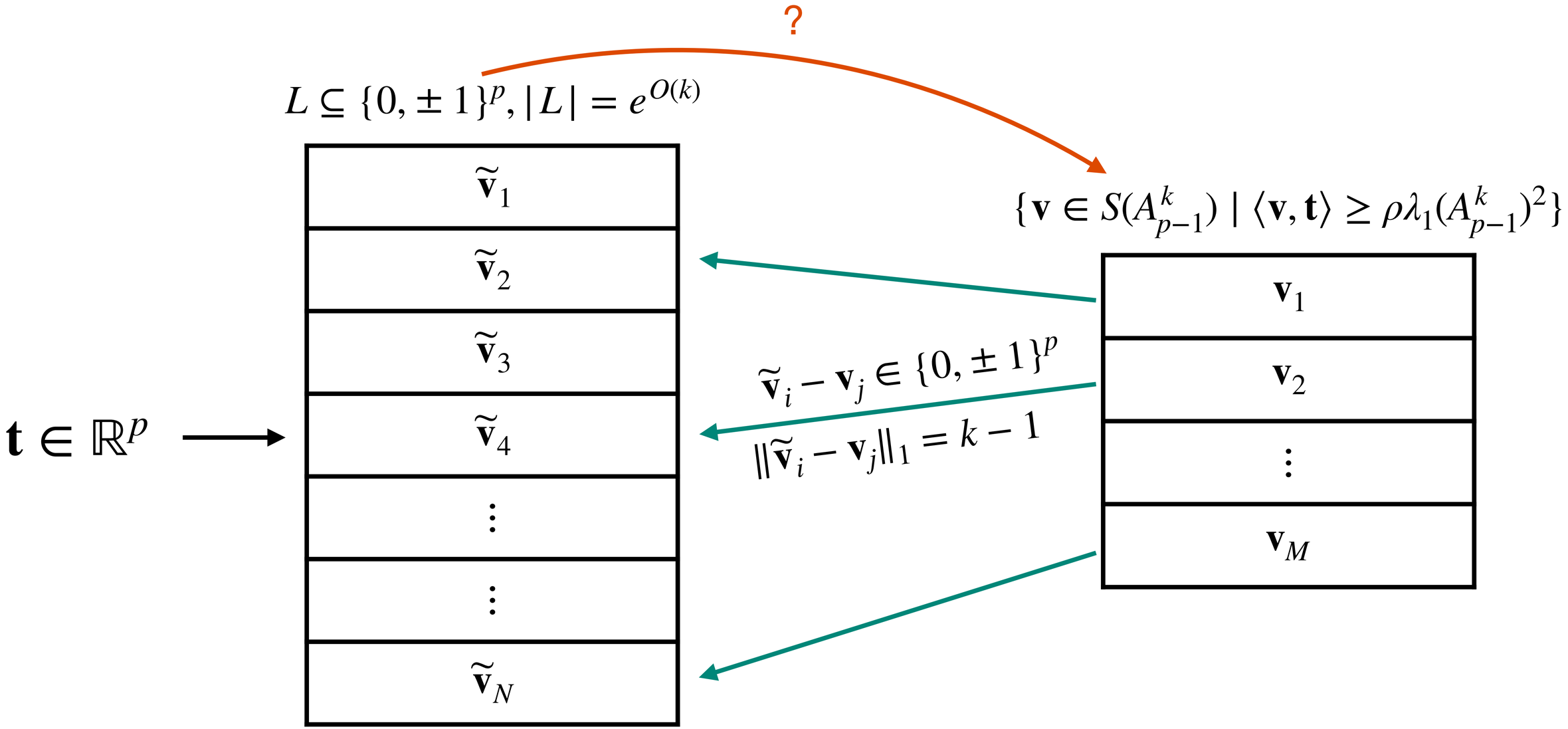
is a **syndrome decoding problem** over $\mathbb{F}_p$ for a **GRS code** in the **Lee metric**.

Lemma (Conway, Sloane):
If $\mathbf{v} \in A_{p-1}^k$, then $\mathbf{Hv} \equiv \mathbf{0} \mod p$.

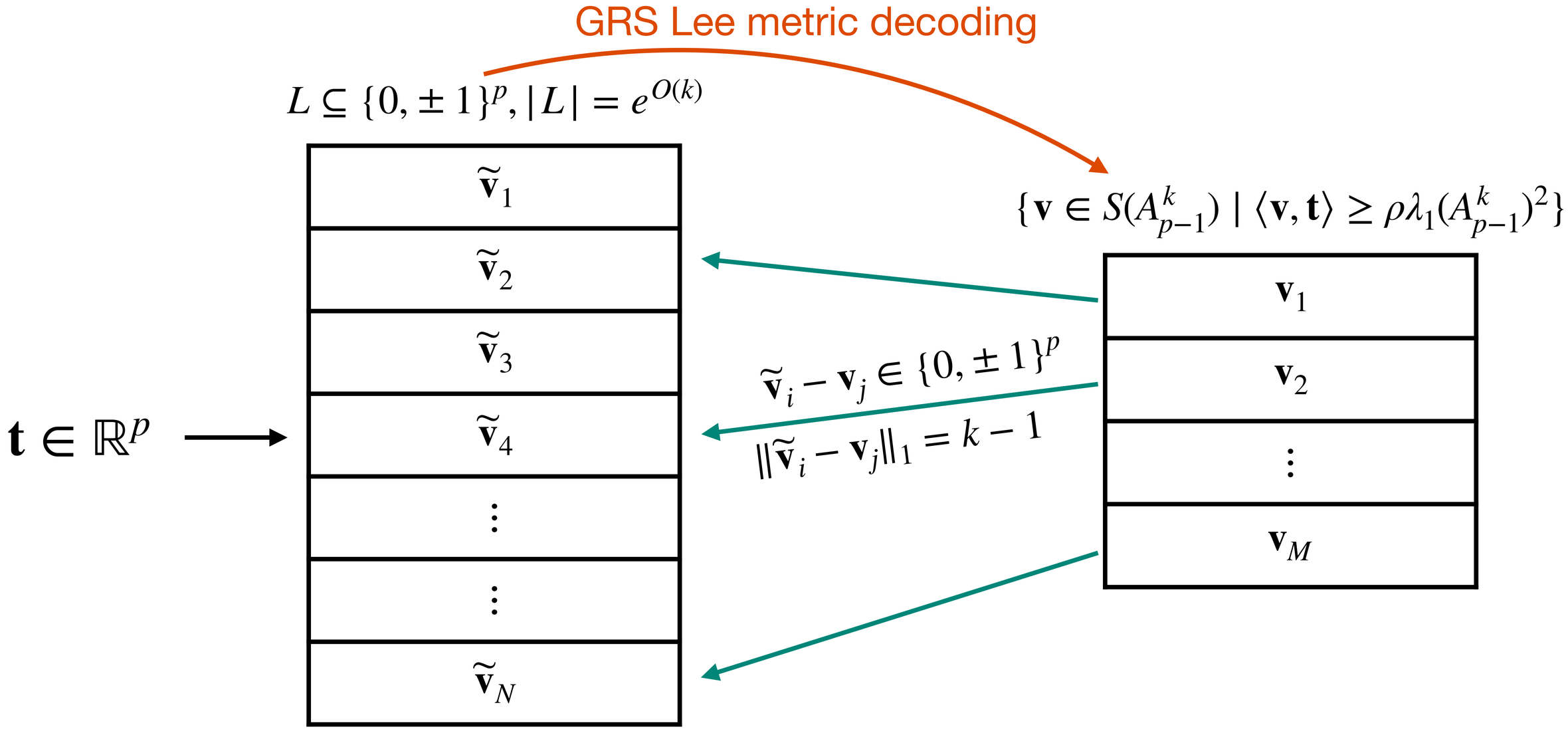
$$\implies \mathbf{H}\widetilde{\mathbf{v}} \equiv \mathbf{He} \mod p$$

Lemma (Roth, Siegel):
If $\|\mathbf{e}\|_1 < k$, we can recover $\mathbf{e}$ in poly. time.

Decoding via Discrete ℓ_1-Approximation



Decoding via Discrete ℓ_1-Approximation



Computing the Discrete ℓ_1-Approximation

Lemma:
If $\mathbf{v} \in S(A_{p-1}^k)$, then $\mathbf{v} \in \{0, \pm 1\}^p$ and $\|\mathbf{v}\|_1 = 2k$.

provided p is sufficiently large.

Computing the Discrete ℓ_1-Approximation

Lemma:
If $\mathbf{v} \in S(A_{p-1}^k)$, then $\mathbf{v} \in \{0, \pm 1\}^p$ and $\|\mathbf{v}\|_1 = 2k$.

provided p is sufficiently large.

Idea for decoding $\mathbf{t}$:

- Write $\mathbf{t} = (t_1, \ldots, t_p)$.
- Pick a threshold $\tau > 0$.
- Define $\mathbf{w} := (w_1, \ldots, w_p)$ with

$$w_i = \begin{cases} 1, & \text{if } t_i \geq \tau, \\ -1, & \text{if } t_i \leq -\tau, \\ 0, & \text{else.} \end{cases}$$

Computing the Discrete ℓ_1-Approximation

Lemma:
If $\mathbf{v} \in S(A_{p-1}^k)$, then $\mathbf{v} \in \{0, \pm 1\}^p$ and $\|\mathbf{v}\|_1 = 2k$.

provided p is sufficiently large.

Idea for decoding $\mathbf{t}$:

- Write $\mathbf{t} = (t_1, \ldots, t_p)$.
- Pick a threshold $\tau > 0$.
- Define $\mathbf{w} := (w_1, \ldots, w_p)$ with

$$w_i = \begin{cases} 1, & \text{if } t_i \geq \tau, \\ -1, & \text{if } t_i \leq -\tau, \\ 0, & \text{else.} \end{cases}$$

Intuition:

- $\mathbf{w} \approx \mathbf{v}$, for every $\mathbf{v}$ with $\langle \mathbf{v}, \mathbf{t} \rangle \geq \rho \lambda_1(A_{p-1}^k)^2$.

Computing the Discrete ℓ_1-Approximation

Lemma:
If $\mathbf{v} \in S(A_{p-1}^k)$, then $\mathbf{v} \in \{0, \pm 1\}^p$ and $\|\mathbf{v}\|_1 = 2k$.

provided p is sufficiently large.

Idea for decoding $\mathbf{t}$:

- Write $\mathbf{t} = (t_1, \ldots, t_p)$.
- Pick a threshold $\tau > 0$.
- Define $\mathbf{w} := (w_1, \ldots, w_p)$ with

$$w_i = \begin{cases} 1, & \text{if } t_i \geq \tau, \\ -1, & \text{if } t_i \leq -\tau, \\ 0, & \text{else.} \end{cases}$$

Intuition:

- $\mathbf{w} \approx \mathbf{v}$, for every $\mathbf{v}$ with $\langle \mathbf{v}, \mathbf{t} \rangle \geq \rho \lambda_1(A_{p-1}^k)^2$.

Intuition made provable:

- If $\tau = 2(\rho - 1/\sqrt{2})$, then $\mathbf{w}$ coincides with every $\mathbf{v}$ in at least $k+1$ nonzero coordinates.

Computing the Discrete ℓ_1-Approximation

Lemma:
If $\mathbf{v} \in S(A_{p-1}^k)$, then $\mathbf{v} \in \{0, \pm 1\}^p$ and $\|\mathbf{v}\|_1 = 2k$.

provided p is sufficiently large.

Idea for decoding $\mathbf{t}$:

- Write $\mathbf{t} = (t_1, \ldots, t_p)$.
- Pick a threshold $\tau > 0$.
- Define $\mathbf{w} := (w_1, \ldots, w_p)$ with

$$w_i = \begin{cases} 1, & \text{if } t_i \geq \tau, \\ -1, & \text{if } t_i \leq -\tau, \\ 0, & \text{else.} \end{cases}$$

Intuition:

- $\mathbf{w} \approx \mathbf{v}$, for every $\mathbf{v}$ with $\langle \mathbf{v}, \mathbf{t} \rangle \geq \rho \lambda_1(A_{p-1}^k)^2$.

Intuition made provable:

- If $\tau = 2(\rho - 1/\sqrt{2})$, then $\mathbf{w}$ coincides with every $\mathbf{v}$ in at least $k+1$ nonzero coordinates.

☞ $\tau > 0 \iff \rho > 1/\sqrt{2} = \cos(45°)$

Computing the Discrete ℓ_1-Approximation

Lemma:
If $\mathbf{v} \in S(A_{p-1}^k)$, then $\mathbf{v} \in \{0, \pm 1\}^p$ and $\|\mathbf{v}\|_1 = 2k$.

provided p is sufficiently large.

Idea for decoding $\mathbf{t}$:

- Write $\mathbf{t} = (t_1, \ldots, t_p)$.
- Pick a threshold $\tau > 0$.
- Define $\mathbf{w} := (w_1, \ldots, w_p)$ with

$$w_i = \begin{cases} 1, & \text{if } t_i \geq \tau, \\ -1, & \text{if } t_i \leq -\tau, \\ 0, & \text{else.} \end{cases}$$

Intuition:

- $\mathbf{w} \approx \mathbf{v}$, for every $\mathbf{v}$ with $\langle \mathbf{v}, \mathbf{t} \rangle \geq \rho \lambda_1(A_{p-1}^k)^2$.

Intuition made provable:

- If $\tau = 2(\rho - 1/\sqrt{2})$, then $\mathbf{w}$ coincides with every $\mathbf{v}$ in at least $k+1$ nonzero coordinates.

☞ $\tau > 0 \iff \rho > 1/\sqrt{2} = \cos(45°)$

- $\|\mathbf{w}\|_1 \leq 2k\tau^{-2}$

Computing the Discrete ℓ_1-Approximation

$\mathbf{t}$ | | | | | | | | | | | | $\in \mathbb{R}^p$

$\mathbf{v}$ | 0 | 1 | 0 | -1 | 0 | 0 | -1 | 0 | 1 | 0 | 0 | 0 | $\in A_{p-1}^k$

Computing the Discrete ℓ_1-Approximation

$\mathbf{t}$

$\leq -\tau$			$\leq -\tau$		$\geq \tau$	$\leq -\tau$		$\geq \tau$			$\leq -\tau$

$\in \mathbb{R}^p$

$\mathbf{v}$

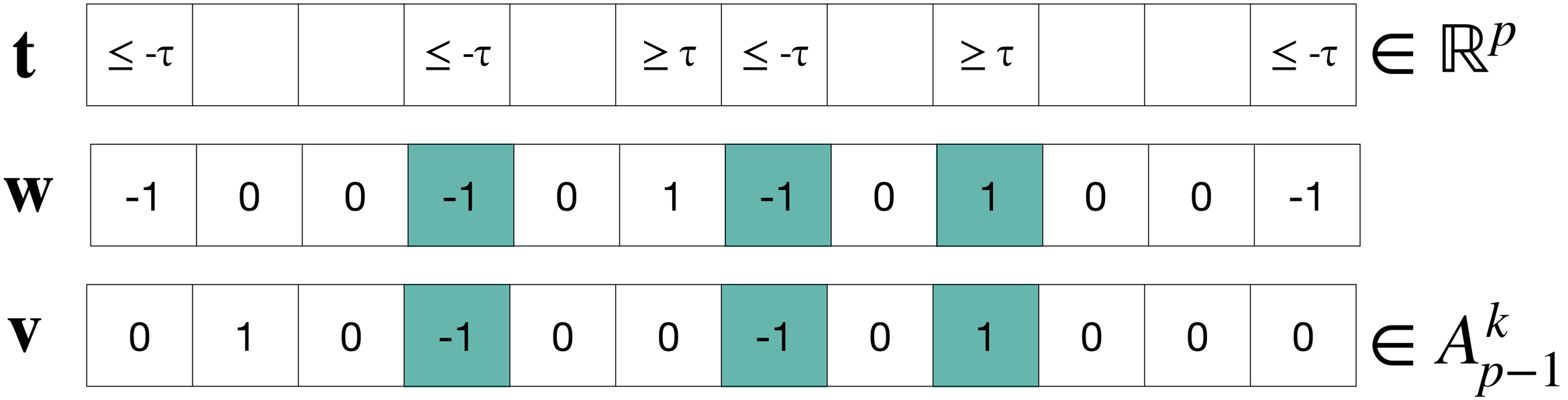
0	1	0	-1	0	0	-1	0	1	0	0	0

$\in A_{p-1}^k$

Computing the Discrete ℓ_1-Approximation

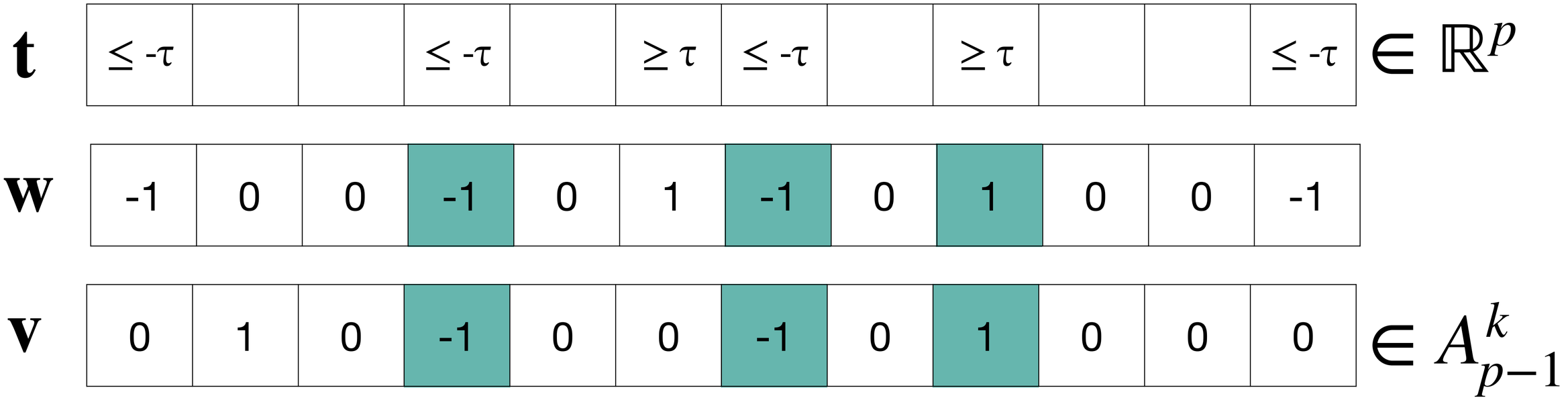
$\mathbf{t}$	$\leq -\tau$			$\leq -\tau$		$\geq \tau$	$\leq -\tau$		$\geq \tau$			$\leq -\tau$	$\in \mathbb{R}^p$
$\mathbf{w}$	-1	0	0	-1	0	1	-1	0	1	0	0	-1	
$\mathbf{v}$	0	1	0	-1	0	0	-1	0	1	0	0	0	$\in A_{p-1}^k$

Computing the Discrete ℓ_1-Approximation



$k+1$ of the $2k$ nonzero coordinates of $\mathbf{v}$ **coincide** with $\mathbf{w}$

Computing the Discrete ℓ_1-Approximation



$k+1$ of the $2k$ nonzero coordinates of $\mathbf{v}$ **coincide** with $\mathbf{w}$

At most $2k\tau^{-2}$ nonzero coordinates in $\mathbf{w}$.

Computing the Discrete ℓ_1-Approximation

$\mathbf{t}$	$\leq -\tau$			$\leq -\tau$		$\geq \tau$	$\leq -\tau$		$\geq \tau$			$\leq -\tau$
$\mathbf{w}$	-1	0	0	-1	0	1	-1	0	1	0	0	-1
$\mathbf{v}$	0	1	0	-1	0	0	-1	0	1	0	0	0

$\in \mathbb{R}^p$

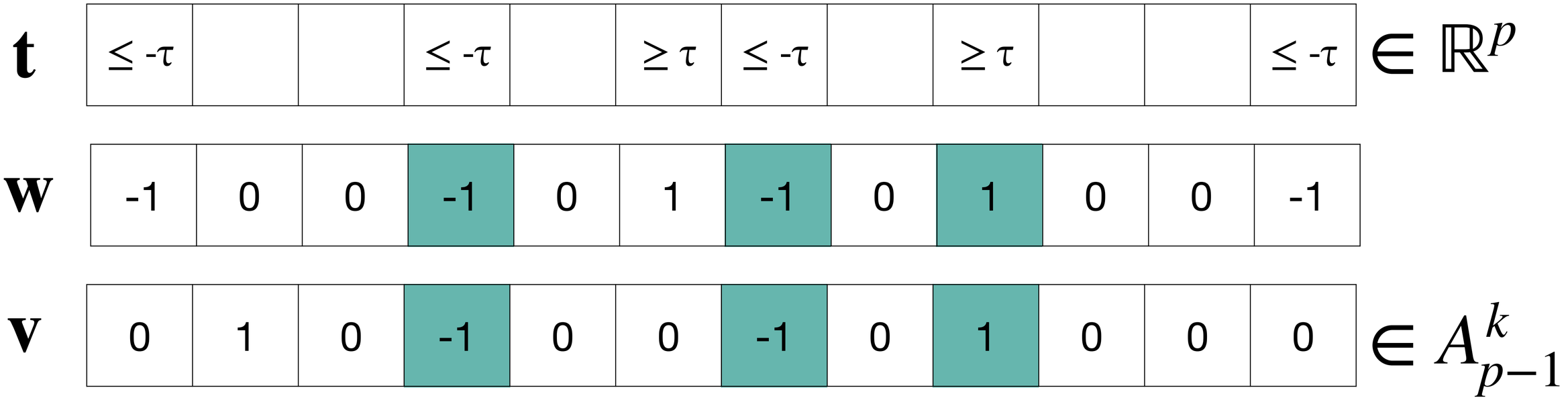
$\in A^k_{p-1}$

$k+1$ of the $2k$ nonzero coordinates of $\mathbf{v}$ **coincide** with $\mathbf{w}$

At most $2k\tau^{-2}$ nonzero coordinates in $\mathbf{w}$.

Goal: Identify the coinciding coordinates.

Computing the Discrete ℓ_1-Approximation



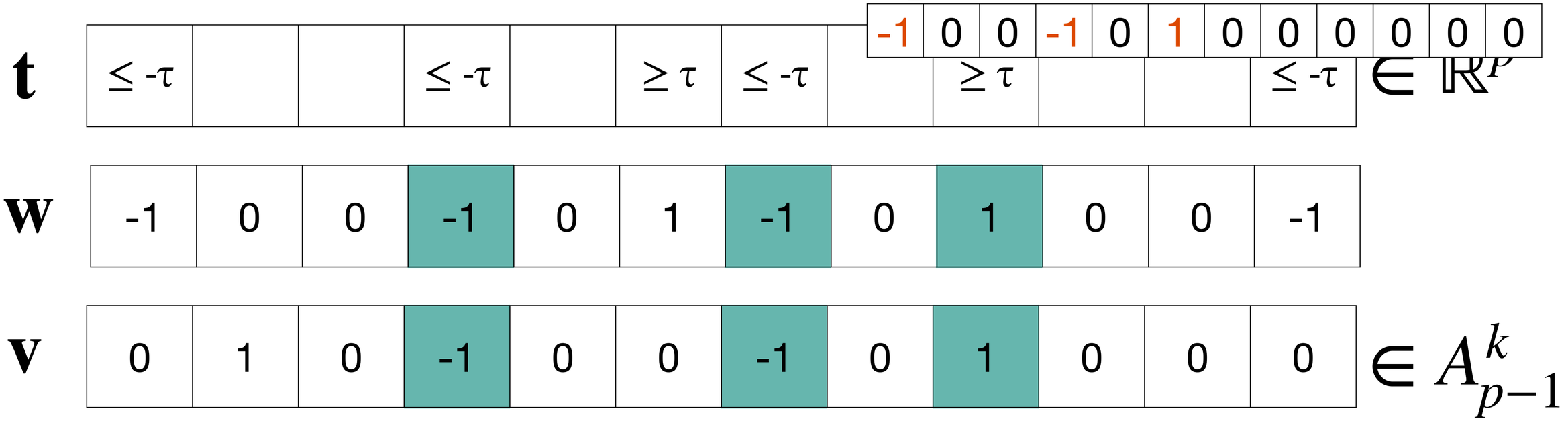
$k+1$ of the $2k$ nonzero coordinates of $\mathbf{v}$ **coincide** with $\mathbf{w}$

At most $2k\tau^{-2}$ nonzero coordinates in $\mathbf{w}$.

Goal: Identify the coinciding coordinates.

Strategy: Enumerate all candidates.

Computing the Discrete ℓ_1-Approximation



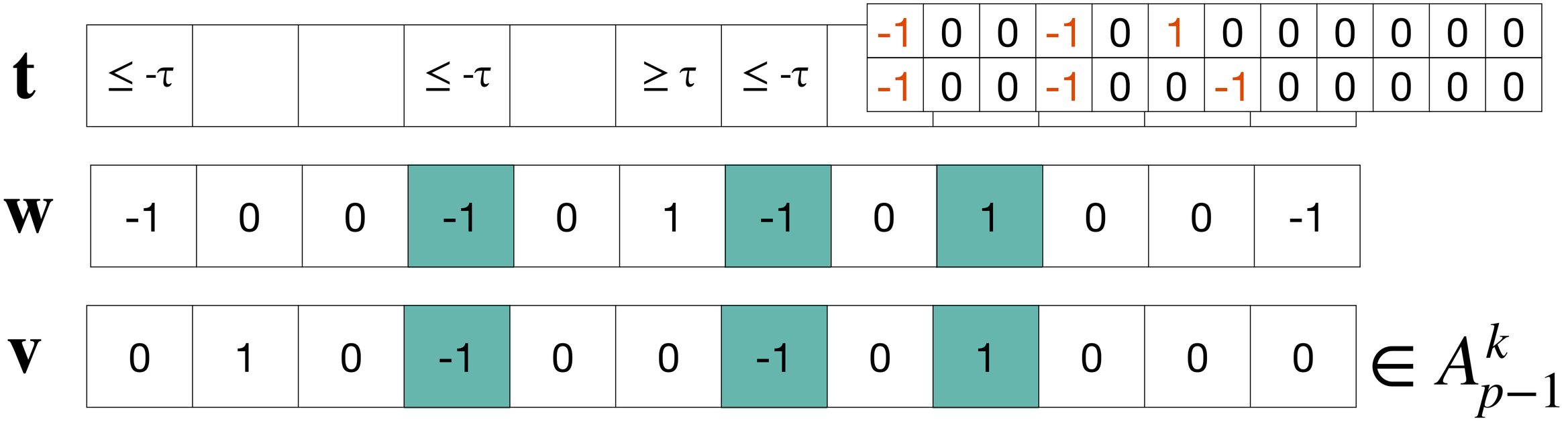
$k+1$ of the $2k$ nonzero coordinates of $\mathbf{v}$ **coincide** with $\mathbf{w}$

At most $2k\tau^{-2}$ nonzero coordinates in $\mathbf{w}$.

Goal: Identify the coinciding coordinates.

Strategy: Enumerate all candidates.

Computing the Discrete ℓ_1-Approximation



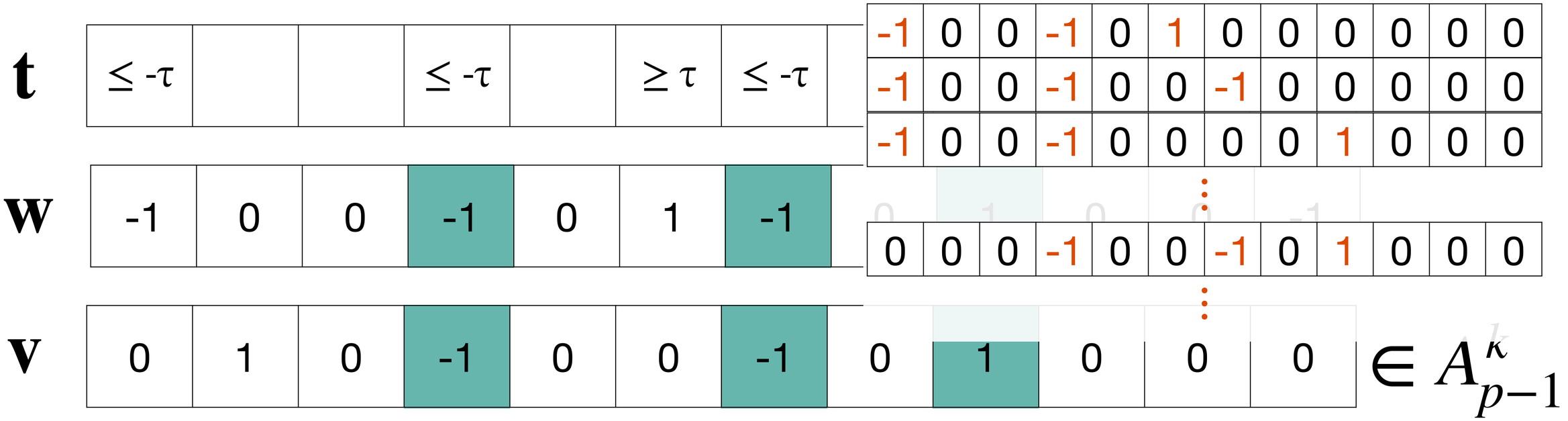
$k+1$ of the $2k$ nonzero coordinates of $\mathbf{v}$ **coincide** with $\mathbf{w}$

At most $2k\tau^{-2}$ nonzero coordinates in $\mathbf{w}$.

Goal: Identify the coinciding coordinates.

Strategy: Enumerate all candidates.

Computing the Discrete ℓ_1-Approximation



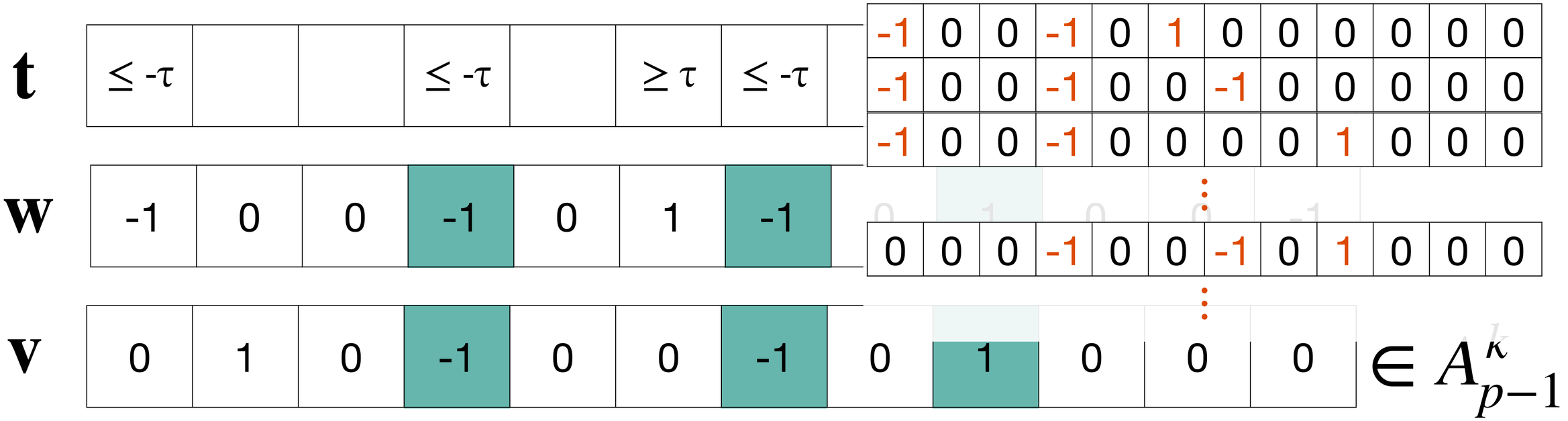
$k+1$ of the $2k$ nonzero coordinates of $\mathbf{v}$ **coincide** with $\mathbf{w}$

At most $2k\tau^{-2}$ nonzero coordinates in $\mathbf{w}$.

Goal: Identify the coinciding coordinates.

Strategy: Enumerate all candidates.

Computing the Discrete ℓ_1-Approximation



$k+1$ of the $2k$ nonzero coordinates of $\mathbf{v}$ **coincide** with $\mathbf{w}$

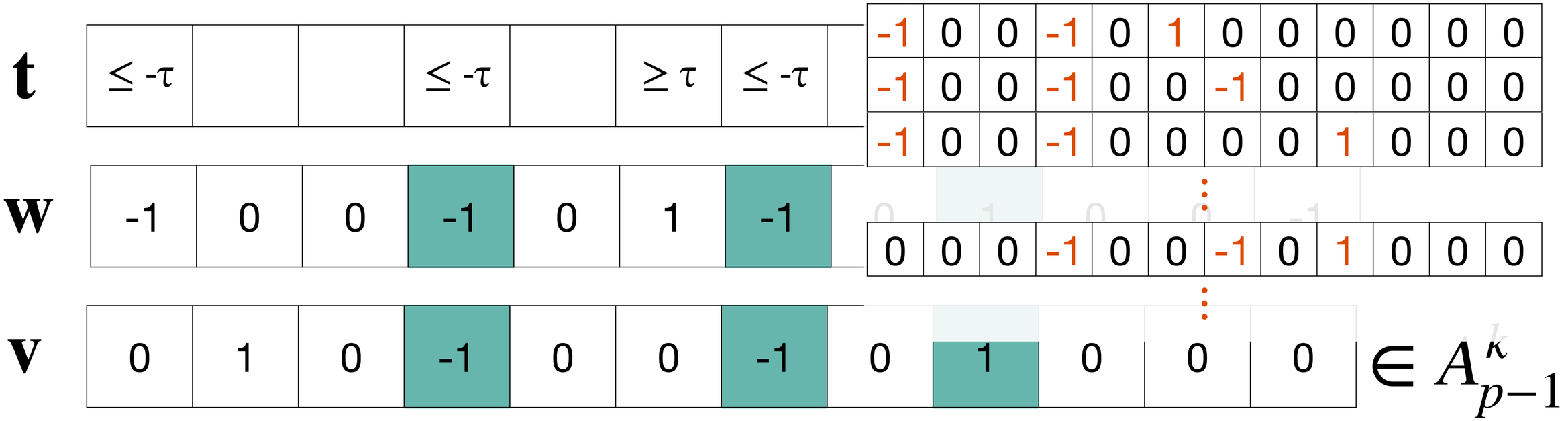
At most $2k\tau^{-2}$ nonzero coordinates in $\mathbf{w}$.

Goal: Identify the coinciding coordinates.

Strategy: Enumerate all candidates.

☞ at most $\binom{\lceil 2k\tau^{-2} \rceil}{k+1} \leq e^{O(k \log(1/\tau))}$ candidates

Computing the Discrete ℓ_1-Approximation



$k+1$ of the $2k$ nonzero coordinates of $\mathbf{v}$ **coincide** with $\mathbf{w}$

At most $2k\tau^{-2}$ nonzero coordinates in $\mathbf{w}$.

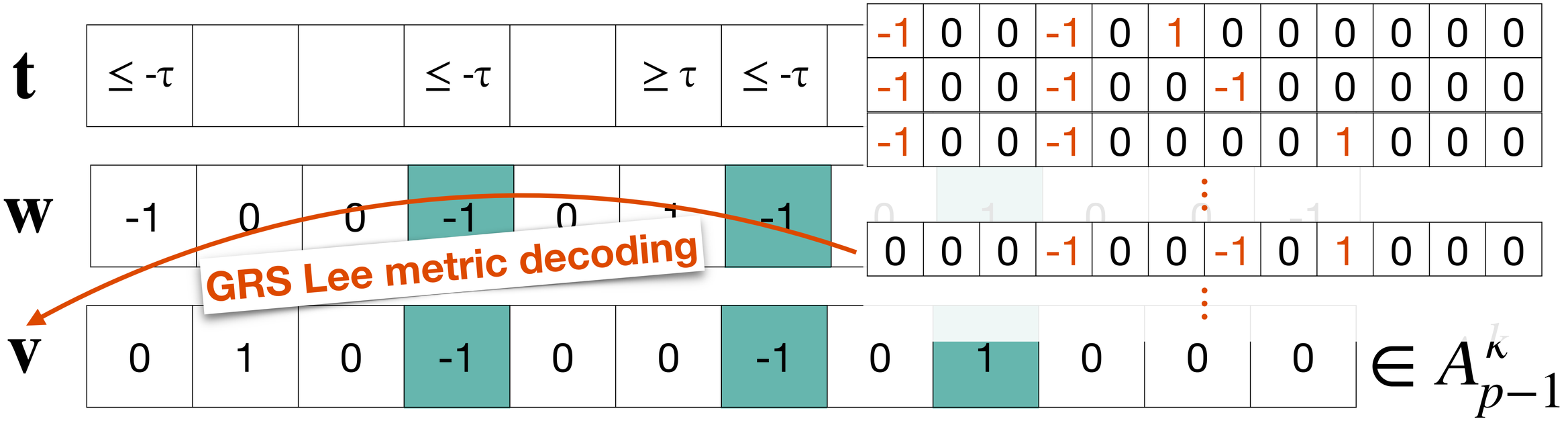
Goal: Identify the coinciding coordinates.

Strategy: Enumerate all candidates.

☞ at most $\binom{\lceil 2k\tau^{-2} \rceil}{k+1} \leq e^{O(k \log(1/\tau))}$ candidates

The correct candidate approximates $\mathbf{v}$ in the ℓ_1-norm up to a $k-1$ error.

Computing the Discrete ℓ_1-Approximation



$k+1$ of the $2k$ nonzero coordinates of $\mathbf{v}$ **coincide** with $\mathbf{w}$

At most $2k\tau^{-2}$ nonzero coordinates in $\mathbf{w}$.

Goal: Identify the coinciding coordinates.

Strategy: Enumerate all candidates.

☞ at most $\binom{\lceil 2k\tau^{-2} \rceil}{k+1} \leq e^{O(k \log(1/\tau))}$ candidates

The correct candidate approximates $\mathbf{v}$ in the ℓ_1-norm up to a $k-1$ error.

Summary

- $\kappa(A_{p-1}^k) = \binom{p}{k}^2 p^{1-k} - \binom{p}{k} + O\left(\frac{\left(k(\sqrt{p}+1)\right)^{2k}}{(k!)^2}\right)$
- $\kappa(A_{p-1}^k) \stackrel{?}{=} e^{\Omega(k)}$ for $k \leq \sqrt{p/2}$
- Efficient decoding of $S(A_{p-1}^k)$ up to $45°$.

Appendix

The Minimal Shell of Craig's Lattice

- Let $f = f_0 + f_1 X + \ldots + f_{p-1} X^{p-1} \in \mathbb{Z}[X]/(X^p - 1)$.

The Minimal Shell of Craig's Lattice

- Let $f = f_0 + f_1 X + \ldots + f_{p-1} X^{p-1} \in \mathbb{Z}[X]/(X^p - 1)$.
- $f \in (X-1)^k \iff \begin{cases} \sum_{i=0}^{p-1} f_i = 0, \\ \sum_{i=0}^{p-1} i^j \cdot f_i \equiv 0 \mod p, j = 0,1\ldots, k-1. \end{cases}$

The Minimal Shell of Craig's Lattice

- Let $f = f_0 + f_1 X + \ldots + f_{p-1} X^{p-1} \in \mathbb{Z}[X]/(X^p - 1)$.
- $f \in (X-1)^k \iff \begin{cases} \sum_{i=0}^{p-1} f_i = 0, \\ \sum_{i=0}^{p-1} i^j \cdot f_i \equiv 0 \mod p, j = 0,1\ldots, k-1. \end{cases}$



$X = 1$ is a root of f in $\mathbb{F}_p[X]$ of multiplicity $\geq k$.

The Minimal Shell of Craig's Lattice

- Let $f = f_0 + f_1 X + \ldots + f_{p-1} X^{p-1} \in \mathbb{Z}[X]/(X^p - 1)$.
- $f \in (X-1)^k \iff \begin{cases} \sum_{i=0}^{p-1} f_i = 0, \\ \sum_{i=0}^{p-1} i^j \cdot f_i \equiv 0 \mod p, j = 0,1\ldots, k-1. \end{cases}$

$\Updownarrow$

$X = 1$ is a root of f in $\mathbb{F}_p[X]$ of multiplicity $\geq k$.

$\Updownarrow$

$f = (X-1)^k \cdot q(X) + p \cdot r(X)$ (over $\mathbb{Z}[X]$)

The Minimal Shell of Craig's Lattice

- Let $f = f_0 + f_1 X + \ldots + f_{p-1} X^{p-1} \in \mathbb{Z}[X]/(X^p - 1)$.
- $f \in (X-1)^k \iff \begin{cases} \sum_{i=0}^{p-1} f_i = 0, \\ \sum_{i=0}^{p-1} i^j \cdot f_i \equiv 0 \mod p, j = 0,1\ldots, k-1. \end{cases}$

$\Updownarrow$

$X = 1$ is a root of f in $\mathbb{F}_p[X]$ of multiplicity $\geq k$.

$\Updownarrow$

$$f = (X-1)^k \cdot q(X) + p \cdot r(X) \quad \text{(over } \mathbb{Z}[X]\text{)}$$

$$= (X-1)^k \cdot q(X) + p \cdot (X-1) \cdot \underbrace{\frac{r(X)}{X-1}}_{\in \mathbb{Z}[X]}$$

The Minimal Shell of Craig's Lattice

- Let $f = f_0 + f_1 X + \ldots + f_{p-1} X^{p-1} \in \mathbb{Z}[X]/(X^p - 1)$.
- $f \in (X-1)^k \iff \begin{cases} \sum_{i=0}^{p-1} f_i = 0, \iff f(1) = 0 \\ \sum_{i=0}^{p-1} i^j \cdot f_i \equiv 0 \mod p, j = 0,1\ldots, k-1. \end{cases}$

$\Updownarrow$

$X = 1$ is a root of f in $\mathbb{F}_p[X]$ of multiplicity $\geq k$.

$\Updownarrow$

$$f = (X-1)^k \cdot q(X) + p \cdot r(X) \quad \text{(over } \mathbb{Z}[X]\text{)}$$

$$= (X-1)^k \cdot q(X) + p \cdot (X-1) \cdot \underbrace{\frac{r(X)}{X-1}}_{\in \mathbb{Z}[X]}$$

The Minimal Shell of Cyclotomic Polynomials

$(p \cdot (X-1)) = (X-1)^p$ as ideals of $\mathbb{Z}[X]/(X^p-1)$

- Let $f = f_0 + f_1 X + \ldots + f_{p-1} X^{p-1} \in \mathbb{Z}[X]/(X^p - 1)$.
- $f \in (X-1)^k \iff$ $\begin{cases} \sum_{i=0}^{p-1} f_i = 0, \iff f(1) = 0 \\ \sum_{i=0}^{p-1} i^j \cdot f_i \equiv 0 \mod p, j = 0,1\ldots, k-1. \end{cases}$

$\Updownarrow$

$X = 1$ is a root of f in $\mathbb{F}_p[X]$ of multiplicity $\geq k$.

$\Updownarrow$

$$f = (X-1)^k \cdot q(X) + p \cdot r(X) \quad \text{(over } \mathbb{Z}[X]\text{)}$$

$$= (X-1)^k \cdot q(X) + p \cdot (X-1) \cdot \underbrace{\frac{r(X)}{X-1}}_{\in \mathbb{Z}[X]}$$

The Minimal Shell of Cyclotomic Ideals

$(p \cdot (X-1)) = (X-1)^p$ as ideals of $\mathbb{Z}[X]/(X^p-1)$

- Let $f = f_0 + f_1 X + \ldots + f_{p-1} X^{p-1} \in \mathbb{Z}[X]/(X^p - 1)$.
- $f \in (X-1)^k \iff \begin{cases} \sum_{i=0}^{p-1} f_i = 0, \iff f(1) = 0 \\ \sum_{i=0}^{p-1} i^j \cdot f_i \equiv 0 \mod p, j = 0,1\ldots, k-1. \end{cases}$

$\Updownarrow$

$X = 1$ is a root of f in $\mathbb{F}_p[X]$ of multiplicity $\geq k$.

$\Updownarrow$

$$f = (X-1)^k \cdot q(X) + p \cdot r(X) \quad \text{(over } \mathbb{Z}[X]\text{)}$$

$$= (X-1)^k \cdot q(X) + p \cdot (X-1) \cdot \underbrace{\frac{r(X)}{X-1}}_{\in \mathbb{Z}[X]} \in (X-1)^k + (X-1)^p = (X-1)^k$$

$k < p$

The Minimal Shell of Craig's Lattice

- Let $f = f_0 + f_1 X + \ldots + f_{p-1} X^{p-1} \in \mathbb{Z}[X]/(X^p - 1)$.
- $f \in (X-1)^k \iff \begin{cases} \sum_{i=0}^{p-1} f_i = 0, \\ \sum_{i=0}^{p-1} i^j \cdot f_i \equiv 0 \mod p, j = 0,1\ldots, k-1. \end{cases}$
- Let $\mathbf{v} \in \mathbb{Z}^p$.
- $\mathbf{v} \in A_{p-1}^k \iff \begin{cases} \langle \mathbf{v}, \mathbf{1}^p \rangle = 0, \\ \mathbf{H}\mathbf{v} \equiv \mathbf{0} \mod p, \end{cases} \quad \mathbf{H} := \begin{bmatrix} 0^j & 1^j & \cdots & (p-1)^j \end{bmatrix}_{j=0,\ldots,k-1} \in \mathbb{Z}^{k \times p}$

The Minimal Shell of Craig's Lattice

- $\mathbf{v} \in A_{p-1}^{k} \iff \begin{cases} \langle \mathbf{v}, \mathbf{1}^p \rangle = 0, \\ \mathbf{H}\mathbf{v} \equiv \mathbf{0} \mod p, \end{cases} \quad \mathbf{H} := \begin{bmatrix} 0^j & 1^j & \cdots & (p-1)^j \end{bmatrix}_{j=0,\ldots,k-1} \in \mathbb{Z}^{k \times p}$

The Minimal Shell of Craig's Lattice

- $\mathbf{v} \in A_{p-1}^{k} \iff \begin{cases} \langle \mathbf{v}, \mathbf{1}^p \rangle = 0, \\ \mathbf{H}\mathbf{v} \equiv \mathbf{0} \mod p, \end{cases} \quad \mathbf{H} := \left[0^j \quad 1^j \quad \cdots \quad (p-1)^j \right]_{j=0,\ldots,k-1} \in \mathbb{Z}^{k \times p}$

- $C := \left\{ \mathbf{v}_1 - \mathbf{v}_2 \in \mathbb{Z}^p \;\middle|\; \begin{array}{c} \mathbf{v}_1, \mathbf{v}_2 \in \{0,1\}^p, \\ \|\mathbf{v}_1\|_1 = \|\mathbf{v}_2\|_1 = k, \\ \mathbf{H}\mathbf{v}_1 \equiv \mathbf{H}\mathbf{v}_2 \mod p \end{array} \right\} \subset A_{p-1}^{k}$

The Minimal Shell of Craig's Lattice

- $\mathbf{v} \in A_{p-1}^{k} \iff \begin{cases} \langle \mathbf{v}, \mathbf{1}^p \rangle = 0, \\ \mathbf{H}\mathbf{v} \equiv \mathbf{0} \mod p, \end{cases} \quad \mathbf{H} := \left[0^j \quad 1^j \quad \cdots \quad (p-1)^j \right]_{j=0,\ldots,k-1} \in \mathbb{Z}^{k \times p}$

- $C := \left\{ \mathbf{v}_1 - \mathbf{v}_2 \in \mathbb{Z}^p \;\middle|\; \begin{array}{c} \mathbf{v}_1, \mathbf{v}_2 \in \{0,1\}^p, \\ \|\mathbf{v}_1\|_1 = \|\mathbf{v}_2\|_1 = k, \\ \mathbf{H}\mathbf{v}_1 \equiv \mathbf{H}\mathbf{v}_2 \mod p \end{array} \right\} \subset A_{p-1}^{k}$

Lemma:

If $C \neq \emptyset$, then $C = S(A_{p-1}^{k})$.

The Minimal Shell of Craig's Lattice

- $\mathbf{v} \in A_{p-1}^k \iff \begin{cases} \langle \mathbf{v}, \mathbf{1}^p \rangle = 0, \\ \mathbf{H}\mathbf{v} \equiv \mathbf{0} \mod p, \end{cases} \quad \mathbf{H} := \begin{bmatrix} 0^j & 1^j & \cdots & (p-1)^j \end{bmatrix}_{j=0,\ldots,k-1} \in \mathbb{Z}^{k \times p}$

- $C := \left\{ \mathbf{v}_1 - \mathbf{v}_2 \in \mathbb{Z}^p \;\middle|\; \begin{array}{c} \mathbf{v}_1, \mathbf{v}_2 \in \{0,1\}^p, \\ \|\mathbf{v}_1\|_1 = \|\mathbf{v}_2\|_1 = k, \\ \mathbf{H}\mathbf{v}_1 \equiv \mathbf{H}\mathbf{v}_2 \mod p \end{array} \right\} \subset A_{p-1}^k$

Lemma:
If $C \neq \emptyset$, then $C = S(A_{p-1}^k)$.

Proof idea:

- Let $\mathbf{v} \in A_{p-1}^k \backslash \{\mathbf{0}\}$. Write $\mathbf{v} = \mathbf{v}_1 - \mathbf{v}_2$ with $\mathbf{v}_i \in \mathbb{Z}_{\geq 0}$.

The Minimal Shell of Craig's Lattice

- $\mathbf{v} \in A_{p-1}^k \iff \begin{cases} \langle \mathbf{v}, \mathbf{1}^p \rangle = 0, \\ \mathbf{H}\mathbf{v} \equiv \mathbf{0} \mod p, \end{cases} \quad \mathbf{H} := \begin{bmatrix} 0^j & 1^j & \cdots & (p-1)^j \end{bmatrix}_{j=0,\ldots,k-1} \in \mathbb{Z}^{k \times p}$

- $C := \left\{ \mathbf{v}_1 - \mathbf{v}_2 \in \mathbb{Z}^p \;\middle|\; \begin{array}{c} \mathbf{v}_1, \mathbf{v}_2 \in \{0,1\}^p, \\ \|\mathbf{v}_1\|_1 = \|\mathbf{v}_2\|_1 = k, \\ \mathbf{H}\mathbf{v}_1 \equiv \mathbf{H}\mathbf{v}_2 \mod p \end{array} \right\} \subset A_{p-1}^k$

Lemma:
If $C \neq \emptyset$, then $C = S(A_{p-1}^k)$.

Proof idea:

- Let $\mathbf{v} \in A_{p-1}^k \setminus \{\mathbf{0}\}$. Write $\mathbf{v} = \mathbf{v}_1 - \mathbf{v}_2$ with $\mathbf{v}_i \in \mathbb{Z}_{\geq 0}$.
- $\langle \mathbf{v}_1, \mathbf{1}^p \rangle = \langle \mathbf{v}_2, \mathbf{1}^p \rangle$ and $\mathbf{H}\mathbf{v}_1 \equiv \mathbf{H}\mathbf{v}_2 \mod p$.

The Minimal Shell of Craig's Lattice

- $\mathbf{v} \in A_{p-1}^k \iff \begin{cases} \langle \mathbf{v}, \mathbf{1}^p \rangle = 0, \\ \mathbf{H}\mathbf{v} \equiv \mathbf{0} \mod p, \end{cases} \quad \mathbf{H} := \begin{bmatrix} 0^j & 1^j & \cdots & (p-1)^j \end{bmatrix}_{j=0,\ldots,k-1} \in \mathbb{Z}^{k \times p}$

- $C := \left\{ \mathbf{v}_1 - \mathbf{v}_2 \in \mathbb{Z}^p \;\middle|\; \begin{array}{c} \mathbf{v}_1, \mathbf{v}_2 \in \{0,1\}^p, \\ \|\mathbf{v}_1\|_1 = \|\mathbf{v}_2\|_1 = k, \\ \mathbf{H}\mathbf{v}_1 \equiv \mathbf{H}\mathbf{v}_2 \mod p \end{array} \right\} \subset A_{p-1}^k$

Lemma:
If $C \neq \emptyset$, then $C = S(A_{p-1}^k)$.

Proof idea:

- Let $\mathbf{v} \in A_{p-1}^k \setminus \{\mathbf{0}\}$. Write $\mathbf{v} = \mathbf{v}_1 - \mathbf{v}_2$ with $\mathbf{v}_i \in \mathbb{Z}_{\geq 0}$.
- $\langle \mathbf{v}_1, \mathbf{1}^p \rangle = \langle \mathbf{v}_2, \mathbf{1}^p \rangle$ and $\mathbf{H}\mathbf{v}_1 \equiv \mathbf{H}\mathbf{v}_2 \mod p$.
- $\implies \|\mathbf{v}_1\|_1 = \|\mathbf{v}_2\|_1 \geq k$.

The Minimal Shell of Craig's Lattice

- $\mathbf{v} \in A_{p-1}^k \iff \begin{cases} \langle \mathbf{v}, \mathbf{1}^p \rangle = 0, \\ \mathbf{H}\mathbf{v} \equiv \mathbf{0} \mod p, \end{cases} \quad \mathbf{H} := \begin{bmatrix} 0^j & 1^j & \cdots & (p-1)^j \end{bmatrix}_{j=0,\ldots,k-1} \in \mathbb{Z}^{k \times p}$

- $C := \left\{ \mathbf{v}_1 - \mathbf{v}_2 \in \mathbb{Z}^p \;\middle|\; \begin{array}{c} \mathbf{v}_1, \mathbf{v}_2 \in \{0,1\}^p, \\ \|\mathbf{v}_1\|_1 = \|\mathbf{v}_2\|_1 = k, \\ \mathbf{H}\mathbf{v}_1 \equiv \mathbf{H}\mathbf{v}_2 \mod p \end{array} \right\} \subset A_{p-1}^k$

Lemma:
If $C \neq \emptyset$, then $C = S(A_{p-1}^k)$.

Proof idea:

- Let $\mathbf{v} \in A_{p-1}^k \setminus \{\mathbf{0}\}$. Write $\mathbf{v} = \mathbf{v}_1 - \mathbf{v}_2$ with $\mathbf{v}_i \in \mathbb{Z}_{\geq 0}$.
- $\langle \mathbf{v}_1, \mathbf{1}^p \rangle = \langle \mathbf{v}_2, \mathbf{1}^p \rangle$ and $\mathbf{H}\mathbf{v}_1 \equiv \mathbf{H}\mathbf{v}_2 \mod p$.
- $\implies \|\mathbf{v}_1\|_1 = \|\mathbf{v}_2\|_1 \geq k$.
- $\|\mathbf{v}\|^2 \geq \|\mathbf{v}\|_1 = \|\mathbf{v}_1\|_1 + \|\mathbf{v}_2\|_1 \geq 2k$.

The Minimal Shell of Craig's Lattice

- $\mathbf{v} \in A_{p-1}^k \iff \begin{cases} \langle \mathbf{v}, \mathbf{1}^p \rangle = 0, \\ \mathbf{H}\mathbf{v} \equiv \mathbf{0} \mod p, \end{cases} \quad \mathbf{H} := \left[0^j \quad 1^j \quad \cdots \quad (p-1)^j \right]_{j=0,\ldots,k-1} \in \mathbb{Z}^{k \times p}$

- $C := \left\{ \mathbf{v}_1 - \mathbf{v}_2 \in \mathbb{Z}^p \;\middle|\; \begin{array}{c} \mathbf{v}_1, \mathbf{v}_2 \in \{0,1\}^p, \\ \|\mathbf{v}_1\|_1 = \|\mathbf{v}_2\|_1 = k, \\ \mathbf{H}\mathbf{v}_1 \equiv \mathbf{H}\mathbf{v}_2 \mod p \end{array} \right\} \subset A_{p-1}^k$

Lemma:
If $C \neq \emptyset$, then $C = S(A_{p-1}^k)$.

"$\geq$" becomes "$=$" iff $\mathbf{v} \in C$

Proof idea:

- Let $\mathbf{v} \in A_{p-1}^k \setminus \{\mathbf{0}\}$. Write $\mathbf{v} = \mathbf{v}_1 - \mathbf{v}_2$ with $\mathbf{v}_i \in \mathbb{Z}_{\geq 0}$.
- $\langle \mathbf{v}_1, \mathbf{1}^p \rangle = \langle \mathbf{v}_2, \mathbf{1}^p \rangle$ and $\mathbf{H}\mathbf{v}_1 \equiv \mathbf{H}\mathbf{v}_2 \mod p$.
- $\implies \|\mathbf{v}_1\|_1 = \|\mathbf{v}_2\|_1 \geq k$.
- $\|\mathbf{v}\|^2 \geq \|\mathbf{v}\|_1 = \|\mathbf{v}_1\|_1 + \|\mathbf{v}_2\|_1 \geq 2k$.