

List-Decoding Reed-Solomon Codes in the Lee, Euclidean, and Other Metrics

ACCESS

Alexandra Veliche Hostetler

University of South Florida

based on joint work with Chris Peikert

Generalized Reed-Solomon Codes

GRS Code: n blocklength, $\mathbb{F}_q$ finite field of size $q \geq n$, k dimension,

$\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n) \in \mathbb{F}_q^n$ evaluation points, $\boldsymbol{t} = (t_1, \dots, t_n) \in \mathbb{F}_q^n$ non-zero twist factors

$$GRS_{q,k}(\boldsymbol{\alpha}, \boldsymbol{t}) := \{(t_1 \cdot f(\alpha_1), \dots, t_n \cdot f(\alpha_n)) : f \in \mathbb{F}_q[x], \deg(f) < k\} \subseteq \mathbb{F}_q^n.$$

Generalized Reed-Solomon Codes

GRS Code: n blocklength, $\mathbb{F}_q$ finite field of size $q \geq n$, k dimension,

$\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{F}_q^n$ evaluation points, $\mathbf{t} = (t_1, \dots, t_n) \in \mathbb{F}_q^n$ non-zero twist factors

$$GRS_{q,k}(\alpha, \mathbf{t}) := \{(t_1 \cdot f(\alpha_1), \dots, t_n \cdot f(\alpha_n)) : f \in \mathbb{F}_q[x], \deg(f) < k\} \subseteq \mathbb{F}_q^n.$$

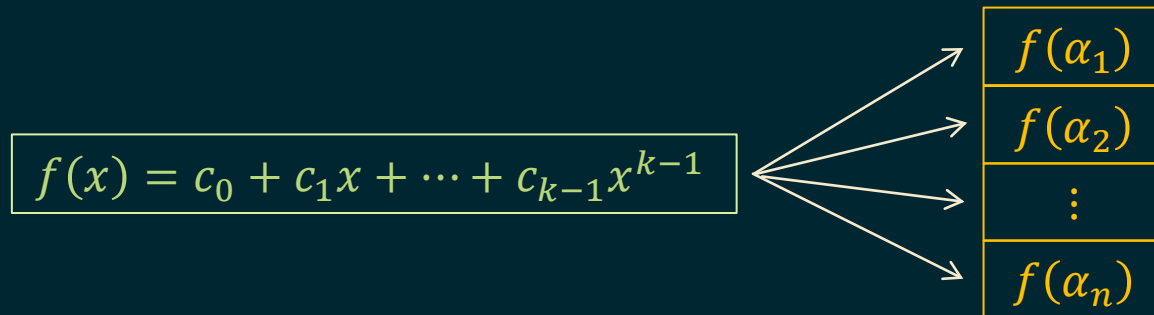
$$f(x) = c_0 + c_1x + \dots + c_{k-1}x^{k-1}$$

Generalized Reed-Solomon Codes

GRS Code: n blocklength, $\mathbb{F}_q$ finite field of size $q \geq n$, k dimension,

$\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n) \in \mathbb{F}_q^n$ evaluation points, $\boldsymbol{t} = (t_1, \dots, t_n) \in \mathbb{F}_q^n$ non-zero twist factors

$$GRS_{q,k}(\boldsymbol{\alpha}, \boldsymbol{t}) := \{(t_1 \cdot f(\alpha_1), \dots, t_n \cdot f(\alpha_n)) : f \in \mathbb{F}_q[x], \deg(f) < k\} \subseteq \mathbb{F}_q^n.$$

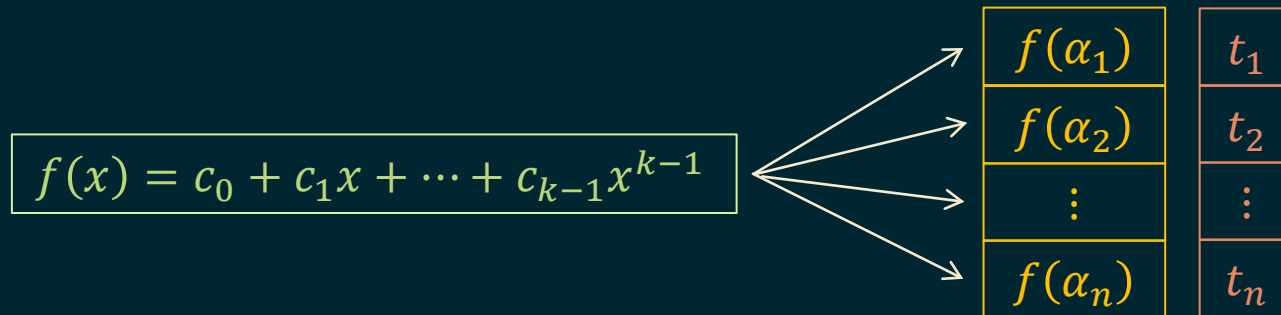


Generalized Reed-Solomon Codes

GRS Code: n blocklength, $\mathbb{F}_q$ finite field of size $q \geq n$, k dimension,

$\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{F}_q^n$ evaluation points, $\mathbf{t} = (t_1, \dots, t_n) \in \mathbb{F}_q^n$ non-zero twist factors

$$GRS_{q,k}(\alpha, \mathbf{t}) := \{(t_1 \cdot f(\alpha_1), \dots, t_n \cdot f(\alpha_n)) : f \in \mathbb{F}_q[x], \deg(f) < k\} \subseteq \mathbb{F}_q^n.$$

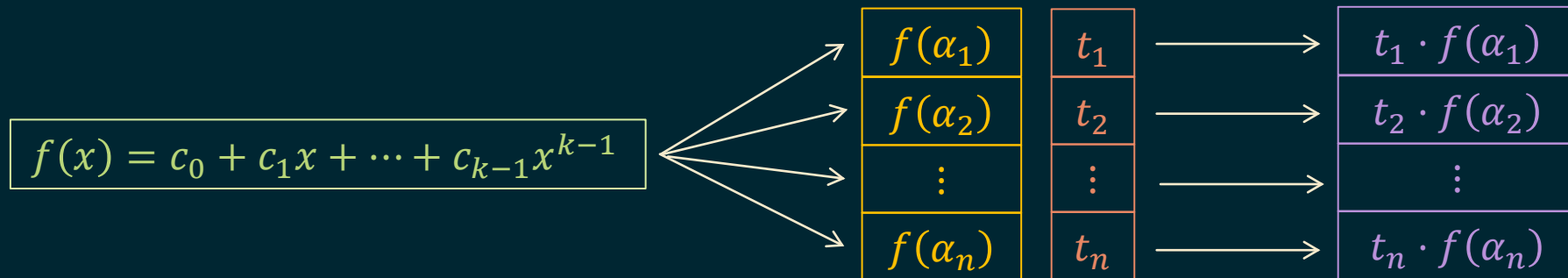


Generalized Reed-Solomon Codes

GRS Code: n blocklength, $\mathbb{F}_q$ finite field of size $q \geq n$, k dimension,

$\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{F}_q^n$ evaluation points, $\mathbf{t} = (t_1, \dots, t_n) \in \mathbb{F}_q^n$ non-zero twist factors

$$GRS_{q,k}(\alpha, \mathbf{t}) := \{(t_1 \cdot f(\alpha_1), \dots, t_n \cdot f(\alpha_n)) : f \in \mathbb{F}_q[x], \deg(f) < k\} \subseteq \mathbb{F}_q^n.$$

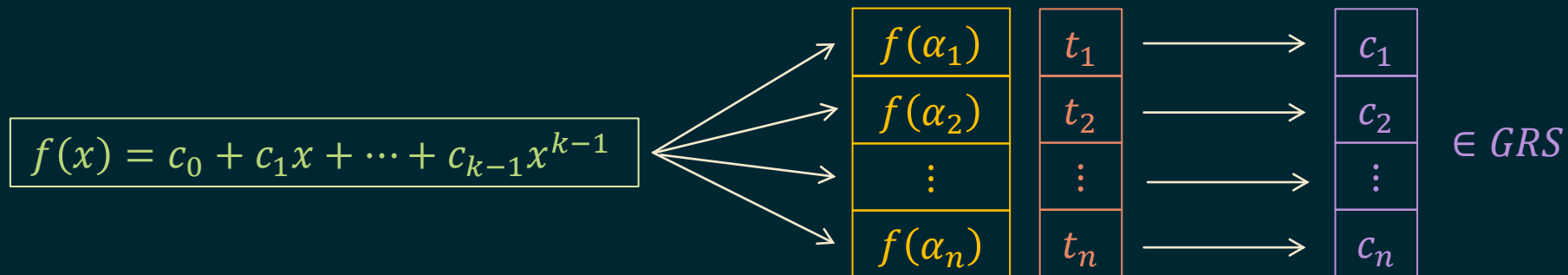


Generalized Reed-Solomon Codes

GRS Code: n blocklength, $\mathbb{F}_q$ finite field of size $q \geq n$, k dimension,

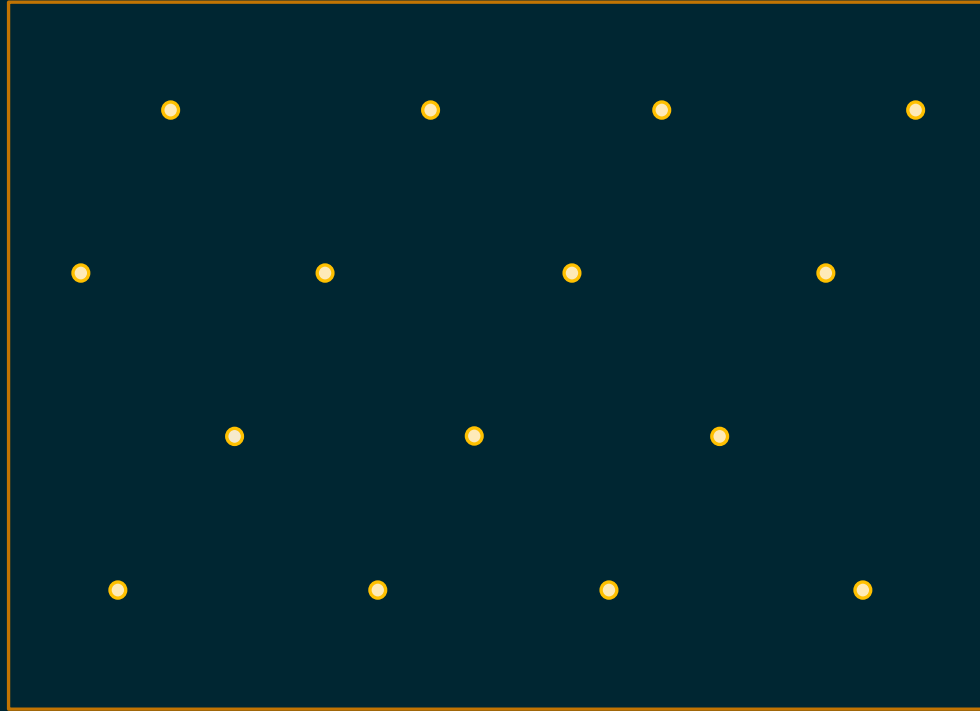
$\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{F}_q^n$ evaluation points, $\mathbf{t} = (t_1, \dots, t_n) \in \mathbb{F}_q^n$ non-zero twist factors

$$GRS_{q,k}(\alpha, \mathbf{t}) := \{(t_1 \cdot f(\alpha_1), \dots, t_n \cdot f(\alpha_n)) : f \in \mathbb{F}_q[x], \deg(f) < k\} \subseteq \mathbb{F}_q^n.$$



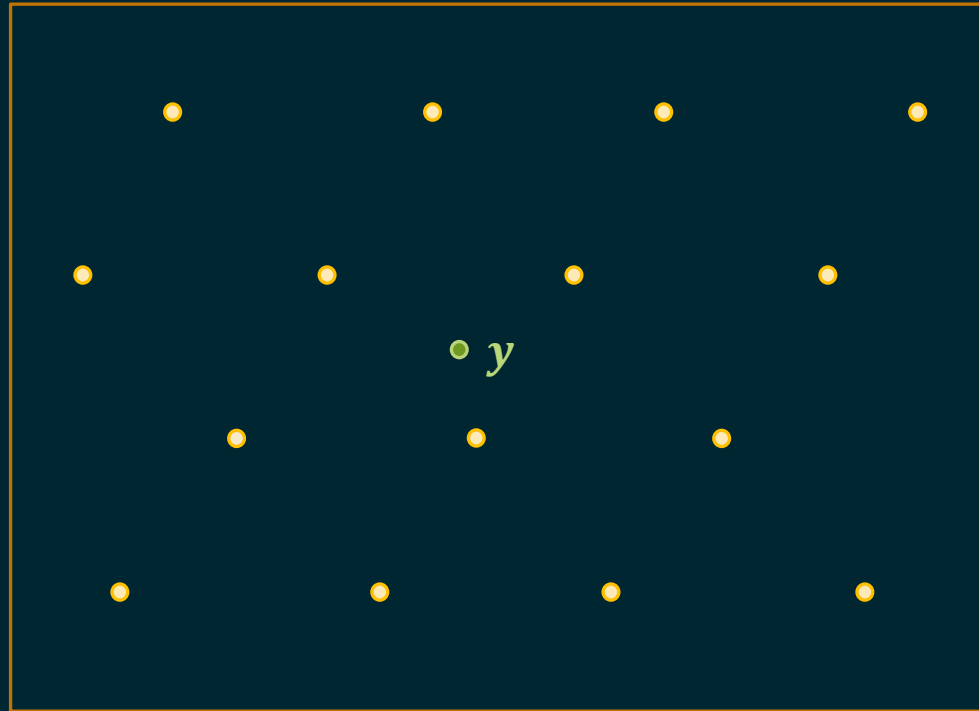
List-Decoding Problem

$\mathcal{C}$ code



List-Decoding Problem

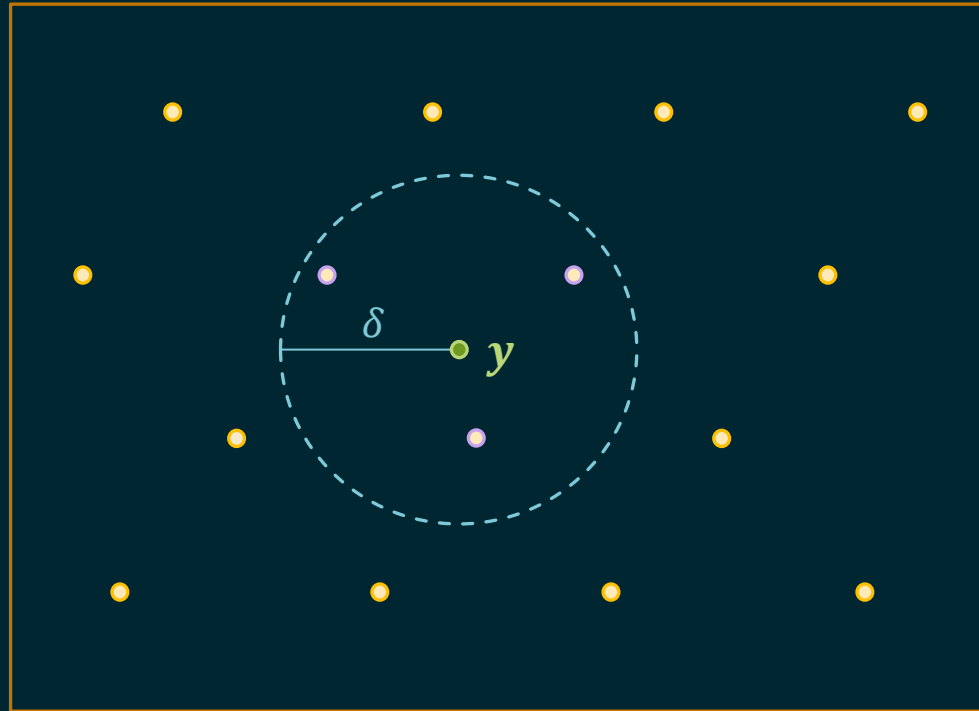
$\mathcal{C}$ code



Given a received word y

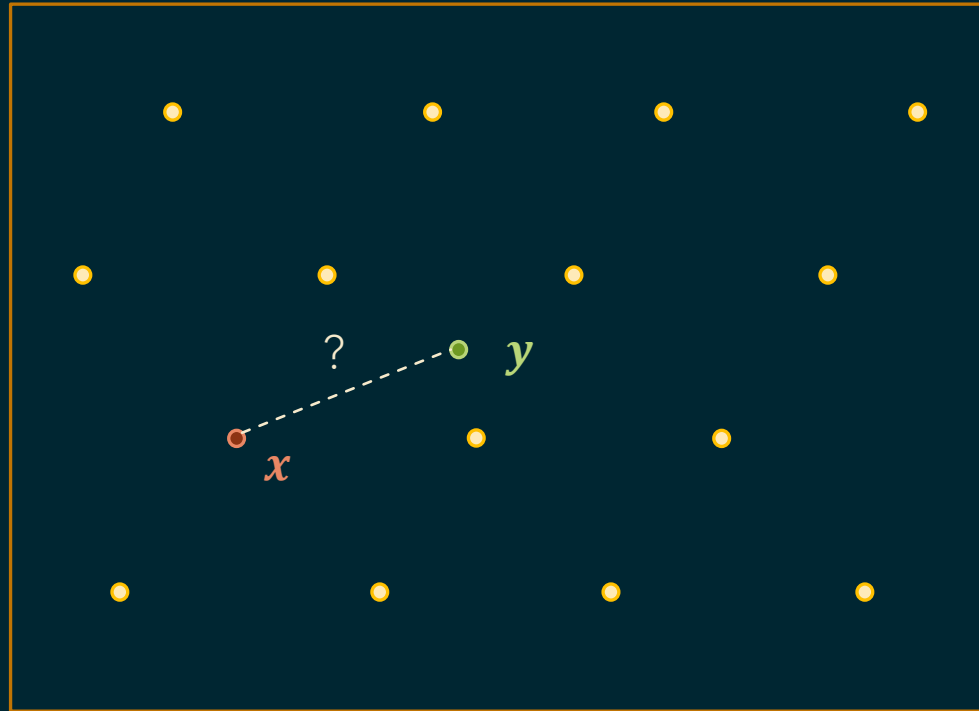
List-Decoding Problem

$\mathcal{C}$ code



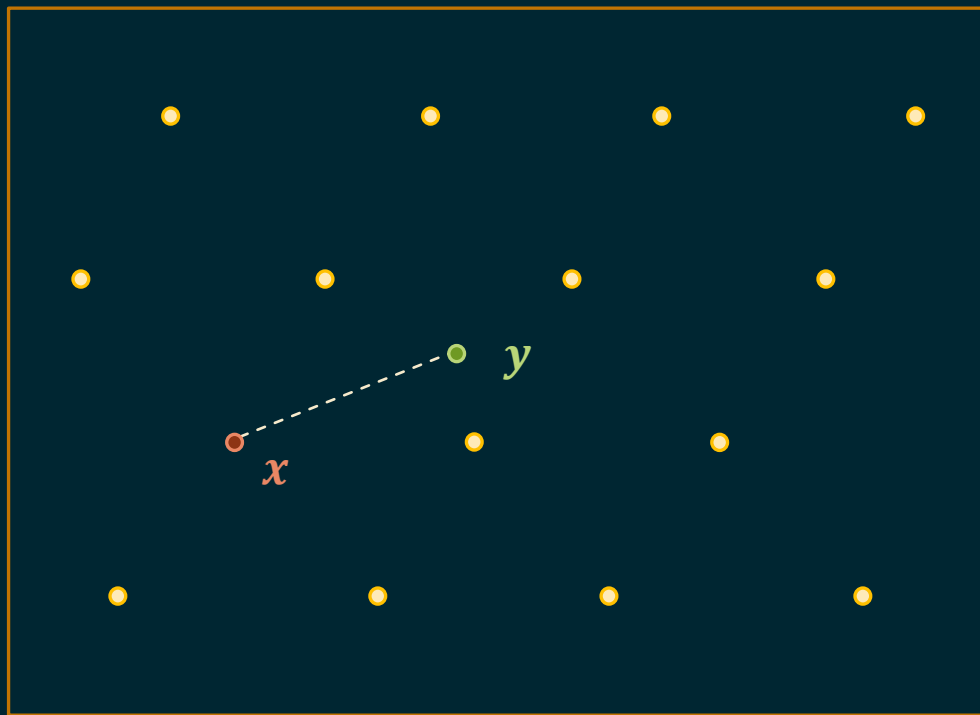
find all codewords within distance δ of y .

Measuring Distance



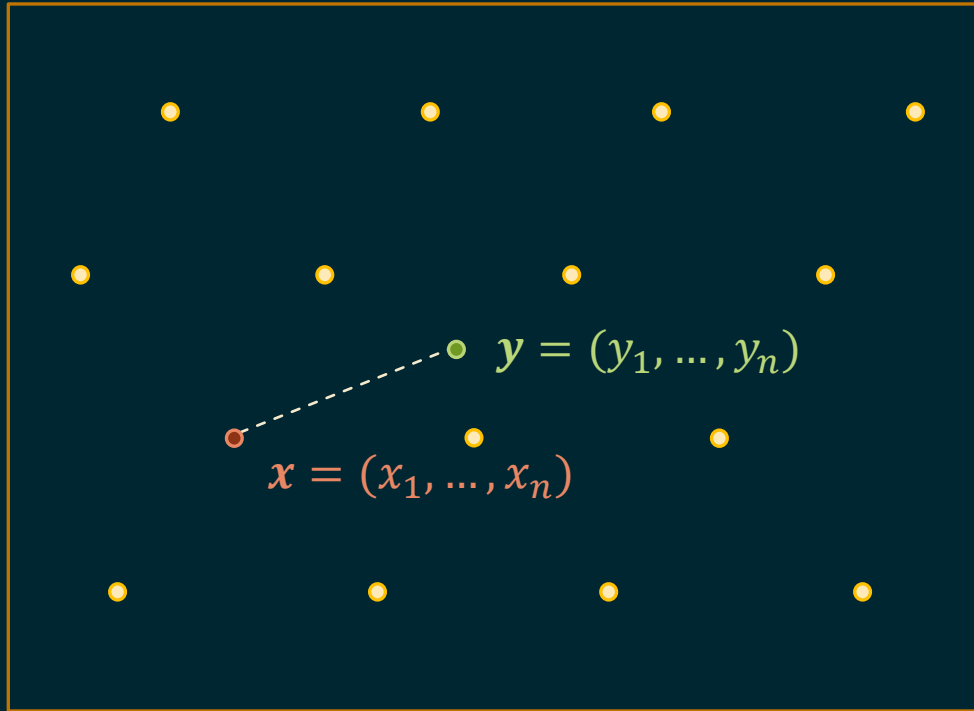
How is distance measured?

Measuring Distance

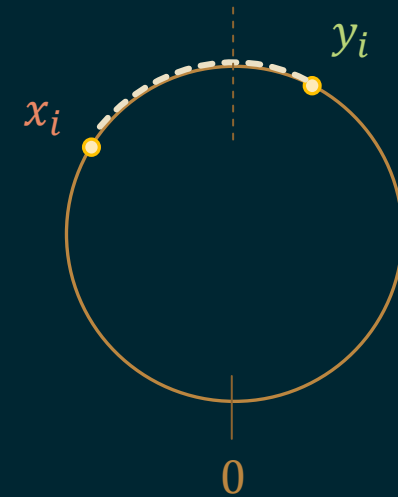


Often in Hamming metric,
but we consider Lee (ℓ_1), Euclidean (ℓ_2), and other ℓ_p metrics.

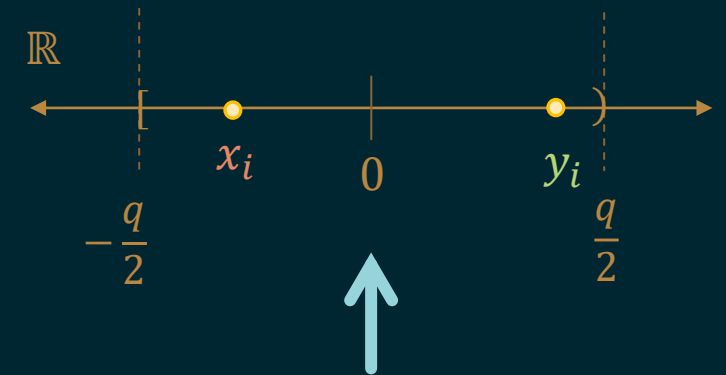
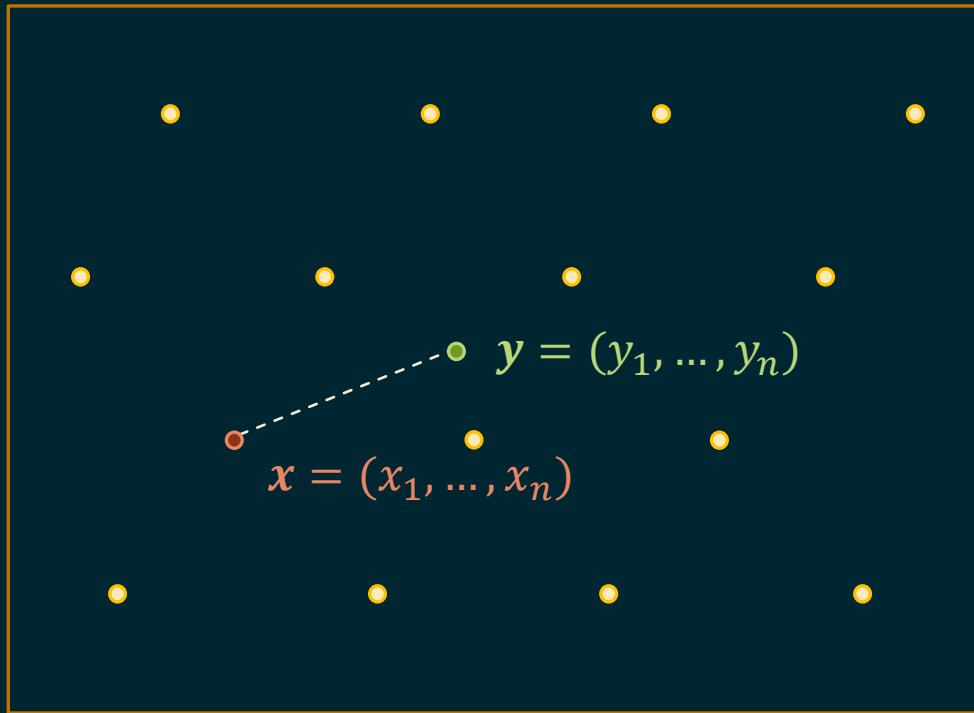
ℓ_p (Semi)Metric



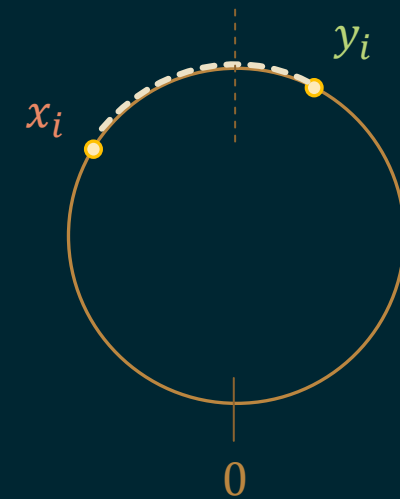
$\mathbb{R}_q = \mathbb{R}/q\mathbb{Z}$ for q prime



ℓ_p (Semi)Metric



$\mathbb{R}_q = \mathbb{R}/q\mathbb{Z}$ for q prime



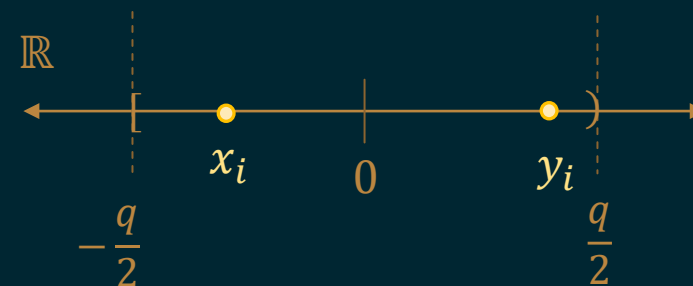
ℓ_p (Semi)Metric

ℓ_p (semi)metric: (on $\mathbb{R}_q^n$) For any $p > 0$ and $\mathbf{x}, \mathbf{y} \in \mathbb{R}_q^n$,

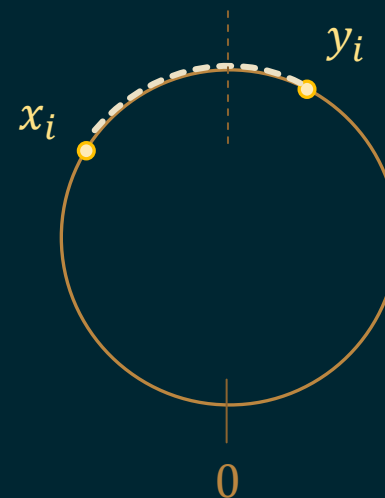
$$d(\mathbf{x}, \mathbf{y}) := \underbrace{\|\mathbf{x} - \mathbf{y}\|_p}_{\text{p-norm distance}}.$$

ℓ_p (quasi)norm on $\mathbb{R}^n$ given by

$$\|\mathbf{z}\|_p := (z_1^p + \cdots + z_n^p)^{1/p}$$



$\mathbb{R}_q = \mathbb{R}/q\mathbb{Z}$ for q prime



ℓ_p (Semi)Metric

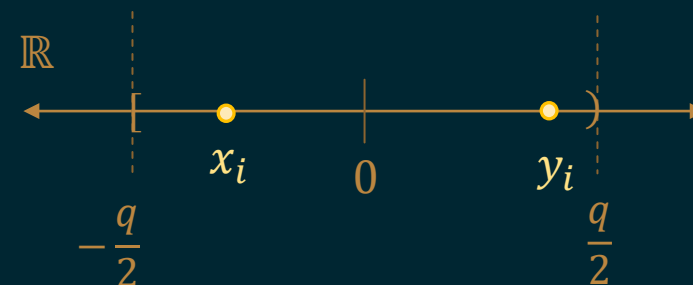
ℓ_p (semi)metric: (on $\mathbb{R}_q^n$) For any $p > 0$ and $\mathbf{x}, \mathbf{y} \in \mathbb{R}_q^n$,

$$d(\mathbf{x}, \mathbf{y}) := \underbrace{\|\mathbf{x} - \mathbf{y}\|_p}_{\text{L}_p \text{ distance}}$$

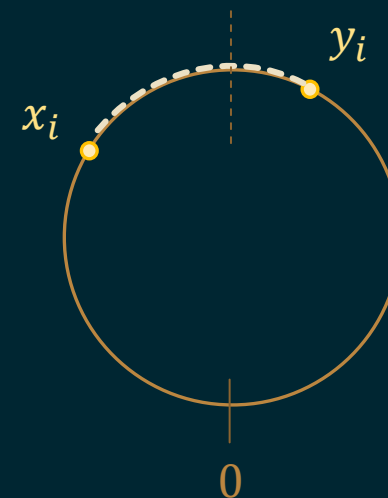
ℓ_p (quasi)norm on $\mathbb{R}^n$ given by

$$\|\mathbf{z}\|_p := (z_1^p + \cdots + z_n^p)^{1/p}$$

Relative decoding distance: $\delta = d/n^{1/p}$.



$\mathbb{R}_q = \mathbb{R}/q\mathbb{Z}$ for q prime



Our (Informal) Results

Theorem: (*worst-case*) There is an efficient algorithm that list-decodes any prime-field GRS code from *continuous error* in the Lee, Euclidean, or other ℓ_p (semi)metric for $0 < p \leq 2$, up to *arbitrarily large* (relative) distance $\delta > 0$ for corresponding small enough rate R .

Our (Informal) Results

Theorem: (*worst-case*) There is an efficient algorithm that list-decodes any prime-field GRS code from *continuous error* in the Lee, Euclidean, or other ℓ_p (semi)metric for $0 < p \leq 2$, up to *arbitrarily large* (relative) distance $\delta > 0$ for corresponding small enough rate R .

Theorem: (*average-case*) ...and similarly for Laplacian / Gaussian channels, with better rate-distance trade-off than for the Lee / Euclidean metrics (respectively).

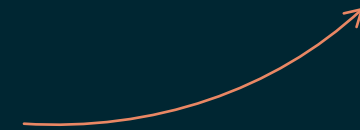
Prior Algorithms

Work	Metric	Codes	Decoder Type	Error Type	Rel. Decoding Distance (δ)
[Guruswami-Sudan, 1999]	Hamming	GRS	list	discrete	$\leq 1 - \sqrt{R}$
[Mook-Peikert, 2022]	Euclidean (ℓ_2)	prime-field GRS	list	continuous	$\leq \sqrt{(1 - R)/2}$
[Roth-Siegel, 1994]	Lee (ℓ_1)	subclass of GRS, BCH	unique	discrete	$\leq 1 - R$
[Wu-Kuijper-Udaya, 2003]	Lee (ℓ_1)	prime-field GRS	list	discrete	$\leq g(R)$ piecewise
[Peikert-V. Hostetler, 2025]	any ℓ_p , $0 < p \leq 2$	prime-field GRS	list	continuous	$\leq 1/(R \cdot c_p(e p)^{1/p})$

Prior Algorithms

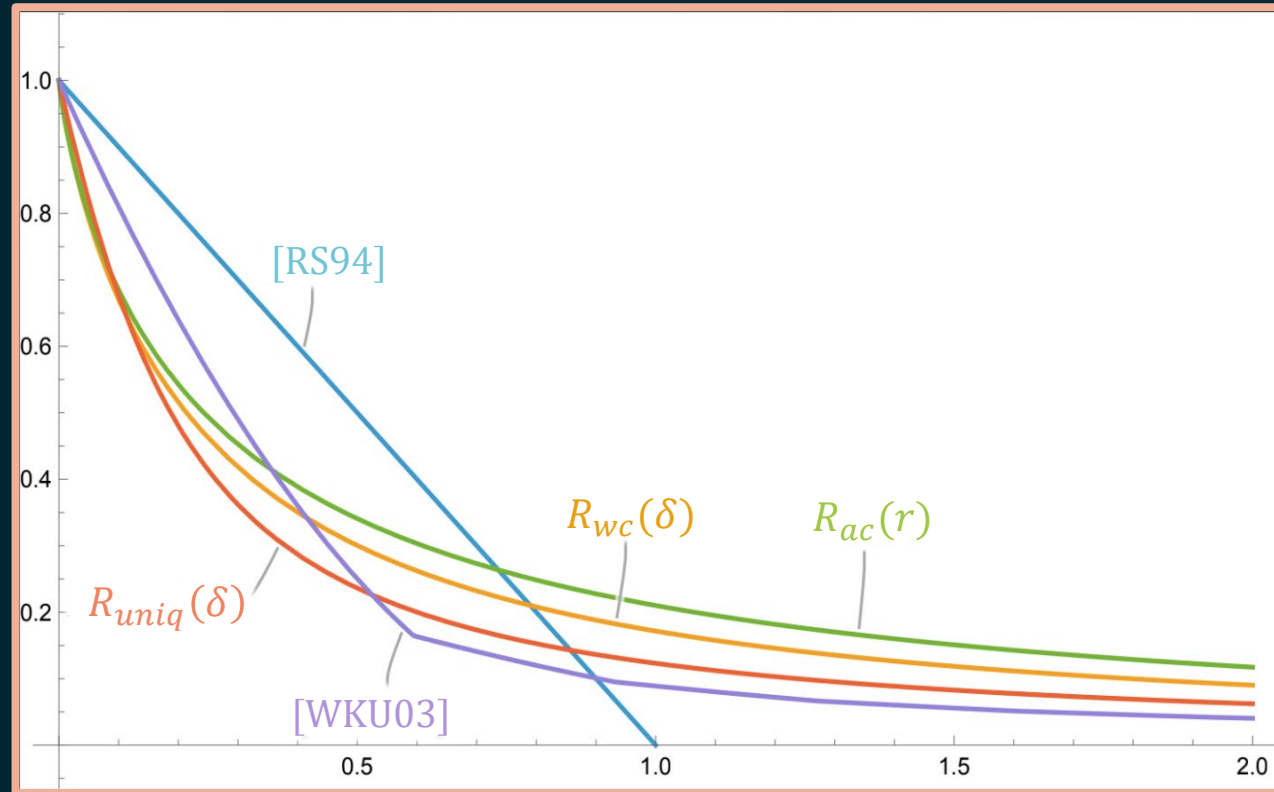
Work	Metric	Codes	Decoder Type	Error Type	Rel. Decoding Distance (δ)
[Guruswami-Sudan, 1999]	Hamming	GRS	list	discrete	$\leq 1 - \sqrt{R}$
[Mook-Peikert, 2022]	Euclidean (ℓ_2)	prime-field GRS	list	continuous	$\leq \sqrt{(1 - R)/2}$
[Roth-Siegel, 1994]	Lee (ℓ_1)	subclass of GRS, BCH	unique	discrete	$\leq 1 - R$
[Wu-Kuijper-Udaya, 2003]	Lee (ℓ_1)	prime-field GRS	list	discrete	$\leq g(R)$ piecewise
[Peikert-V. Hostetler, 2025]	any ℓ_p , $0 < p \leq 2$	prime-field GRS	list	continuous	$\leq 1/(R \cdot c_p(e p)^{1/p})$

(dimension-normalized) volume of n -dim. ℓ_p ball of radius $n^{1/p}$



Comparison to Prior Algorithms

rate R

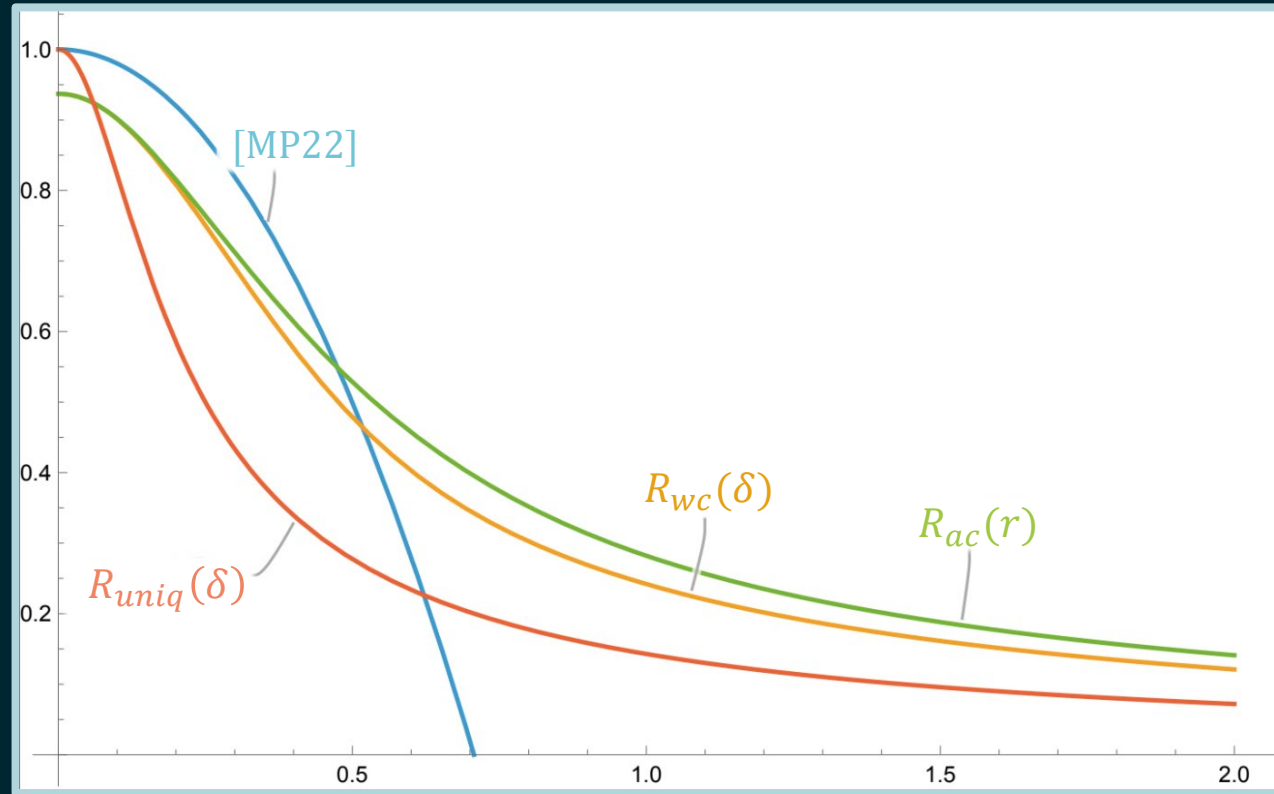


distance $\delta = \frac{r}{2}$

Rate-distance trade-off for Lee (ℓ_1) metric

Comparison to Prior Algorithms

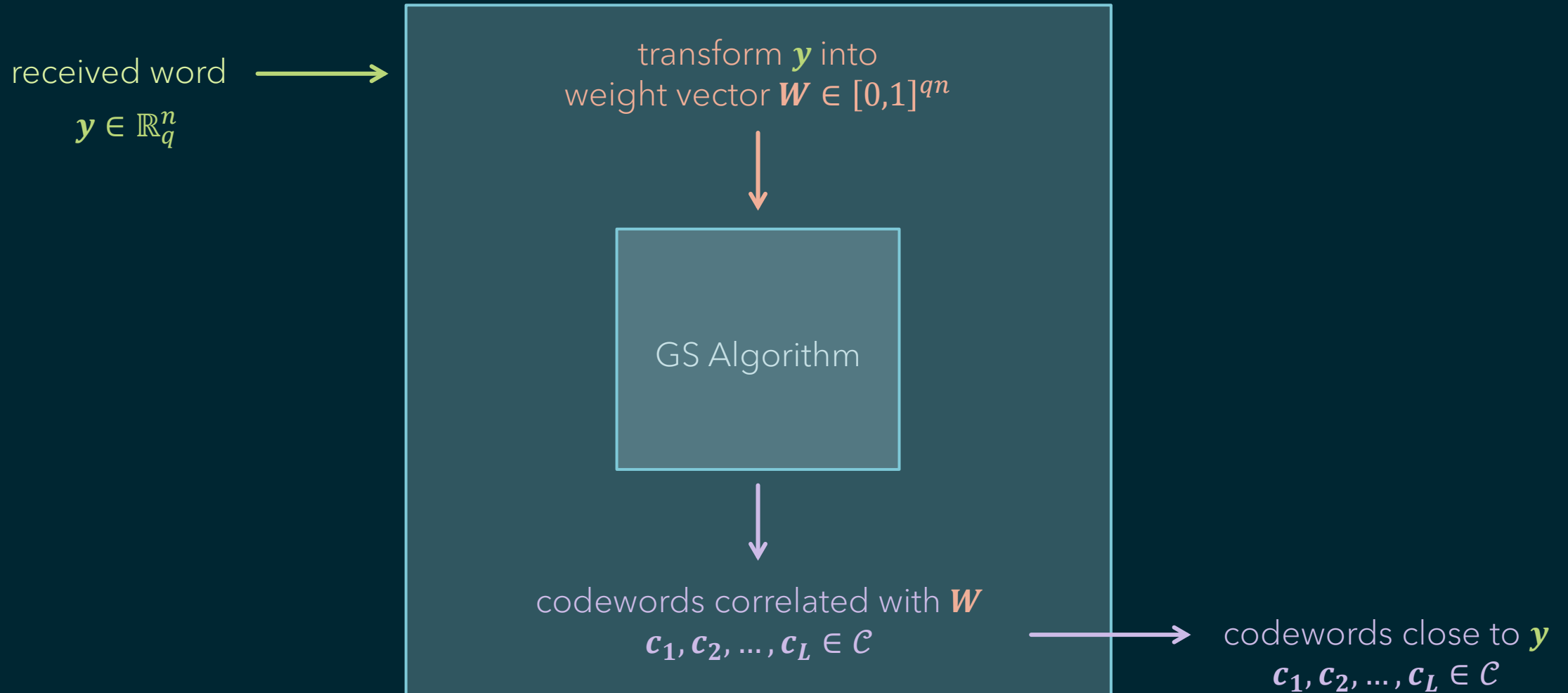
rate R



distance $\delta = \frac{r}{\sqrt{2\pi}}$

Rate-distance trade-off for Euclidean (ℓ_2) metric

Our List-decoding Algorithm



Guruswami-Sudan Algorithm

[Guruswami-Sudan, 1998], [Koetter-Vardy, 2003], [Guruswami, 2001]

There is a deterministic *soft-decoding* algorithm for (Generalized) Reed-Solomon codes $\mathcal{C} \subseteq \mathbb{F}_q^n$, dimension k , adjusted rate $R^* = \frac{k-1}{n}$, with

Input: weight vector $\mathbf{W} = (\overrightarrow{w_1}, \dots, \overrightarrow{w_n}) \in [0,1]^{qn}$,

Output: list of all codewords $\mathbf{c} \in \mathcal{C}$ that are “closely correlated” with $\mathbf{W}$

$$\text{corr}(\mathbf{W}, \mathbf{c}) := \frac{\langle \mathbf{W}, [\mathbf{c}] \rangle}{\|\mathbf{W}\| \cdot \sqrt{n}} \gtrsim \sqrt{R^*}.$$

Guruswami-Sudan Algorithm

[Guruswami-Sudan, 1998], [Koetter-Vardy, 2003], [Guruswami, 2001]

There is a deterministic *soft-decoding* algorithm for (Generalized) Reed-Solomon codes $\mathcal{C} \subseteq \mathbb{F}_q^n$, dimension k , adjusted rate $R^* = \frac{k-1}{n}$, with

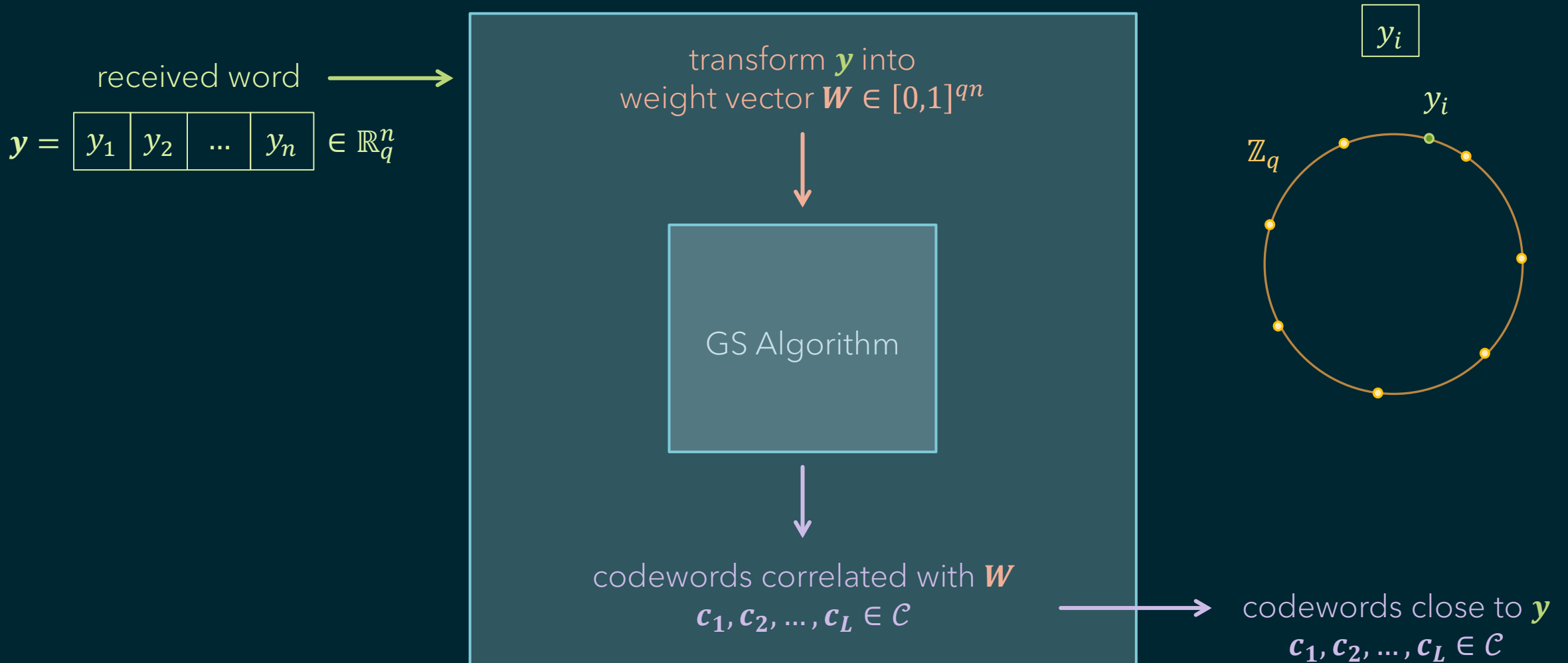
Input: weight vector $\mathbf{W} = (\overrightarrow{w_1}, \dots, \overrightarrow{w_n}) \in [0,1]^{qn}$,
tolerance parameter $\tau > 0$

Output: list of all codewords $\mathbf{c} \in \mathcal{C}$ that are “closely correlated” with $\mathbf{W}$

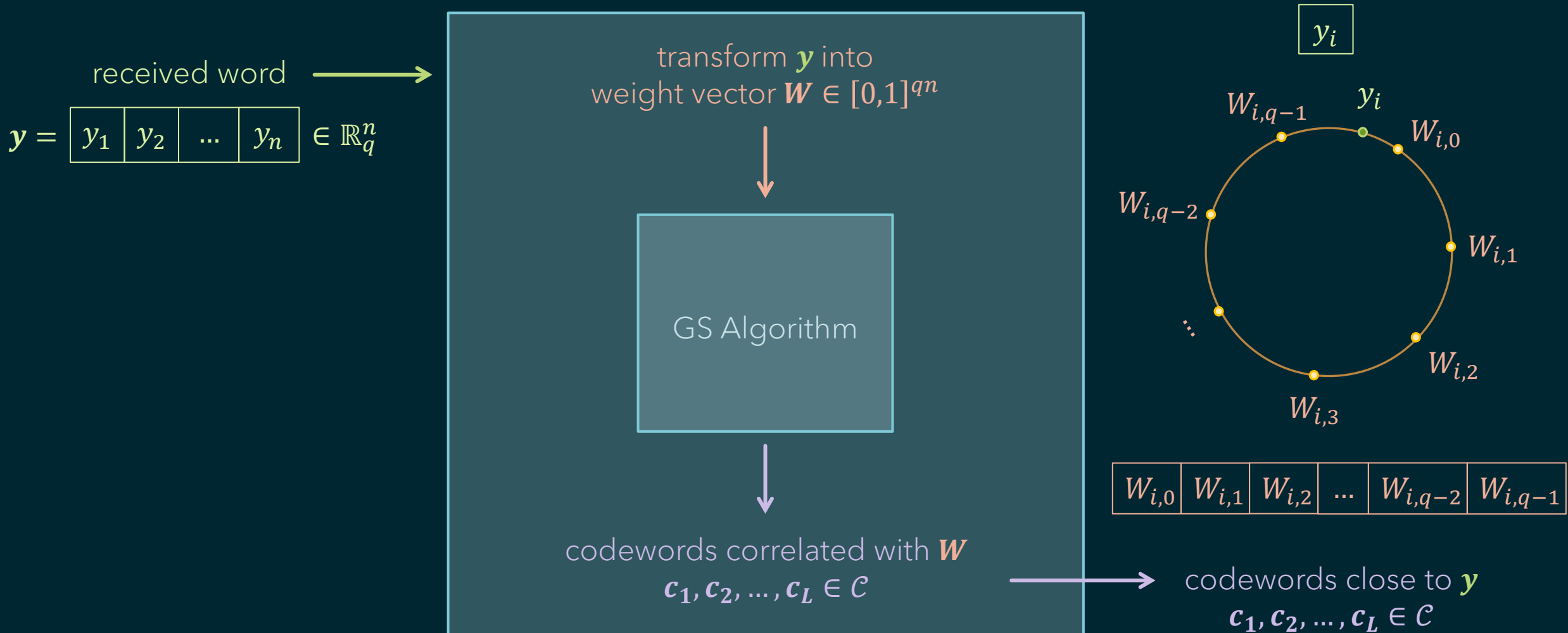
$$\text{corr}(\mathbf{W}, \mathbf{c}) := \frac{\langle \mathbf{W}, [\mathbf{c}] \rangle}{\|\mathbf{W}\| \cdot \sqrt{n}} \geq \sqrt{R^*} + \tau.$$

running in $\text{poly}\left(n, q, \frac{1}{\tau \|\mathbf{W}\|}\right)$ time.

Transforming into Weights

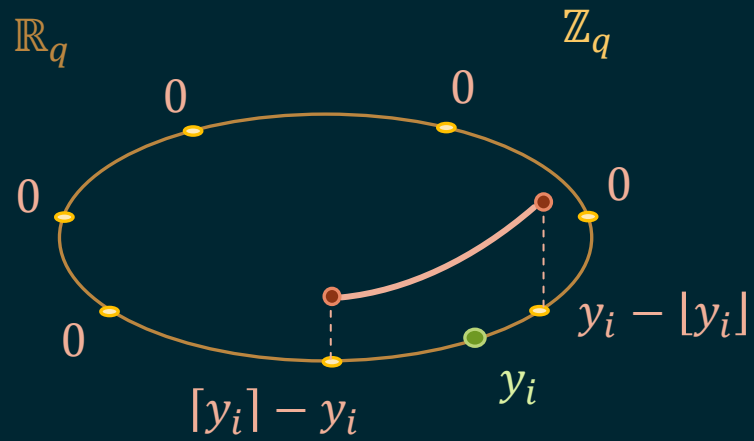


Transforming into Weights



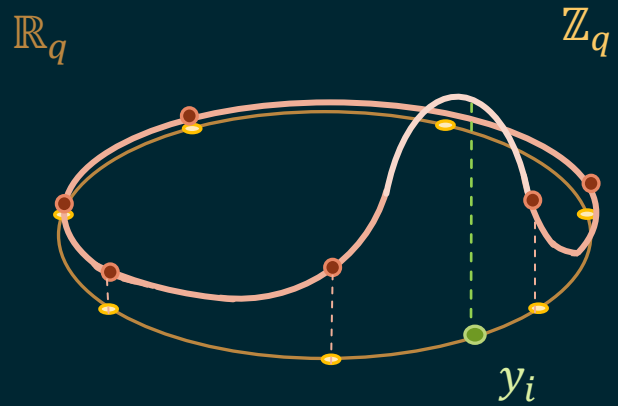
Transforming into Weights

[Mook-Peikert, 2022] :



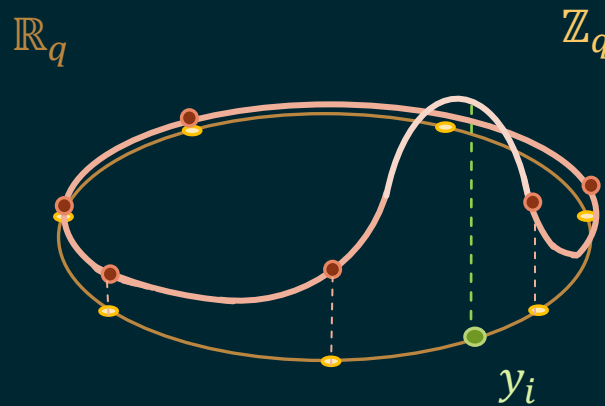
Transforming into Weights

Our weight function :



Transforming into Weights

Our weight function :

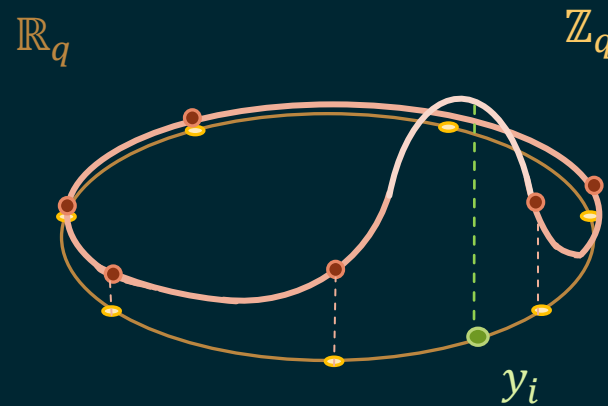


weights given by a
function f_s of width $s > 0$

$$f_s(x) := \exp(-(c_p |x/s|)^p)$$

Transforming into Weights

Our weight function :



weights given by a
function f_s of width $s > 0$

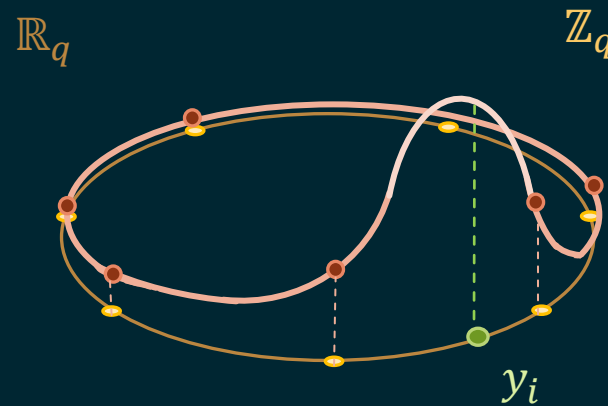
$$f_s(x) := \exp(-(c_p |x/s|)^p)$$

$$\underbrace{\quad}_{2 \cdot \Gamma\left(1 + \frac{1}{p}\right)}$$

makes $\widehat{f_s(0)} := 1$

Transforming into Weights

Our weight function :



weights given by a
function f_s of width $s > 0$

$$f_s(x) := \exp(-(c_p |x/s|)^p)$$

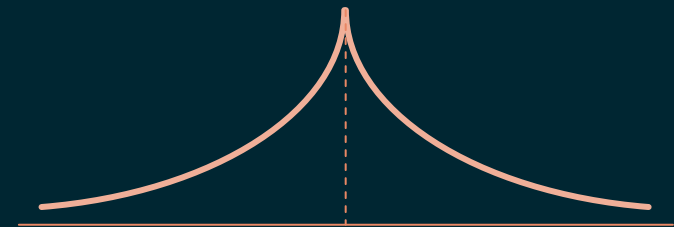
We cannot handle $p > 2$ because $\widehat{f_s(x)}$ can be negative.

Our Weight Function

For distances measured in the Lee (ℓ_1) metric:

$$f_s(x) := \exp(-2 |x/s|^1)$$

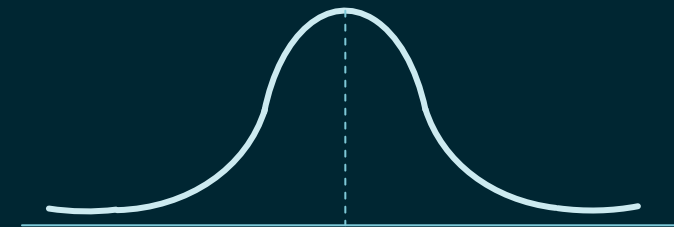
Laplacian function



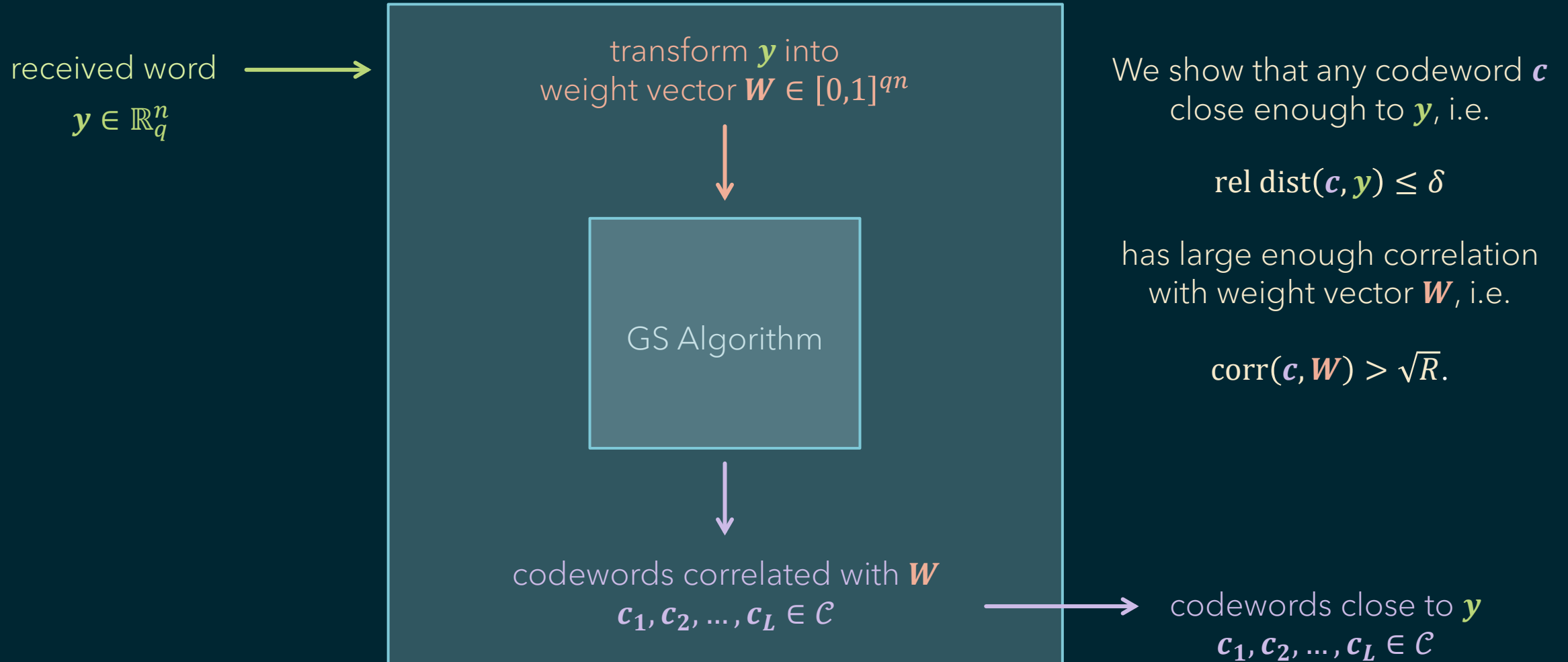
For distances measured in the Euclidean (ℓ_2) metric:

$$f_s(x) := \exp(-\pi |x/s|^2)$$

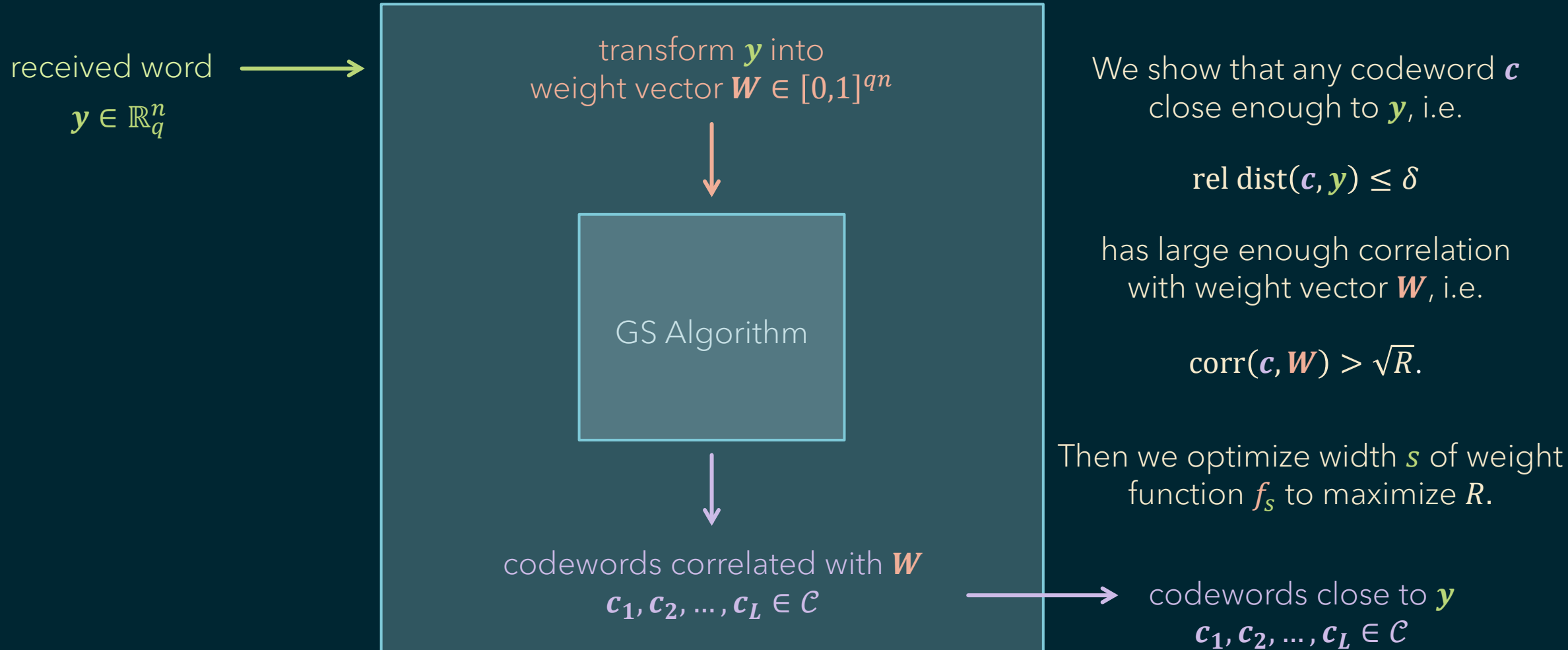
Gaussian function



Our Analysis



Our Analysis



Our Results

Theorem: (*worst-case*) For any metric parameter $0 < p \leq 2$, prime field size q , and distance $\delta > 0$, the GS soft-decision algorithm using weight vectors defined by $f_s^{(p)}$ for any $s > 0$, list-decodes up to ℓ_p distance $d = \delta \cdot n^{1/p}$ any GRS code $\mathcal{C} \subseteq \mathbb{F}_q^n$ with adjusted rate

$$R^* < \underbrace{\frac{f_s(\delta)^2}{f_s(\mathcal{L}_q)}}_{\tau}$$

$\tau :=$ gap between rate and upper bound

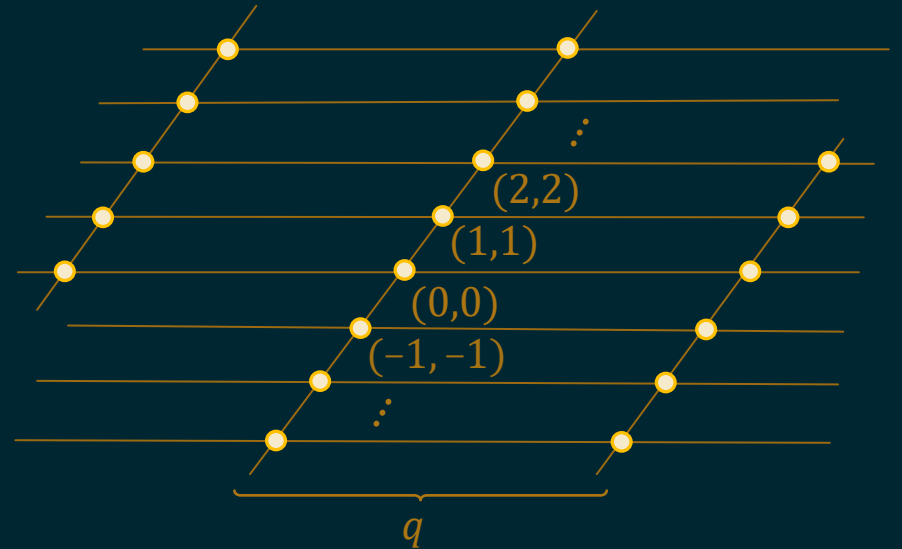
in $\text{poly}(n, q, \exp(1/s^p)/\tau)$ time.

Our Results

Theorem: (*worst-case*) For any metric parameter $0 < p \leq 2$, prime field size q , and distance $\delta > 0$, the GS soft-decision algorithm using weight vectors defined by $f_s^{(p)}$ for any $s > 0$, list-decodes up to ℓ_p distance $d = \delta \cdot n^{1/p}$ any GRS code $\mathcal{C} \subseteq \mathbb{F}_q^n$ with adjusted rate

$$R^* < \underbrace{\frac{f_s(\delta)^2}{f_s(\mathcal{L}_q)}}_{\parallel} \sum_{x \in \mathcal{L}_q} f_s(x)$$

in $\text{poly}(n, q, \exp(1/s^p)/\tau)$ time.



Our Results

Theorem: (*worst-case*) For any metric parameter $0 < p \leq 2$, prime field size q , and distance $\delta > 0$, the GS soft-decision algorithm using weight vectors defined by $f_s^{(p)}$ for any $s > 0$, list-decodes up to ℓ_p distance $d = \delta \cdot n^{1/p}$ any GRS code $\mathcal{C} \subseteq \mathbb{F}_q^n$ with adjusted rate

$$R^* < \frac{f_s(\delta)^2}{f_s(\mathcal{L}_q)} =: W_{q,\delta}^{(p)}(s)$$

in $\text{poly}(n, q, \exp(1/s^p)/\tau)$ time.

Our Results

Theorem: (*worst-case*) For any metric parameter $0 < p \leq 2$, prime field size q , and distance $\delta > 0$, the GS soft-decision algorithm using weight vectors defined by $f_s^{(p)}$ for any $s > 0$, list-decodes up to ℓ_p distance $d = \delta \cdot n^{1/p}$ any GRS code $\mathcal{C} \subseteq \mathbb{F}_q^n$ with adjusted rate

$$R^* < \frac{f_s(\delta)^2}{f_s(\mathcal{L}_q)} =: W_{q,\delta}^{(p)}(s) \xrightarrow{s, q/s \rightarrow \infty} \frac{1}{\delta \cdot c_p \cdot (ep)^{1/p}}$$

in $\text{poly}(n, q, \exp(1/s^p)/\tau)$ time.

Our Results

Theorem: (*worst-case*) For any metric parameter $0 < p \leq 2$, prime field size q , and distance $\delta > 0$, the GS soft-decision algorithm using weight vectors defined by $f_s^{(p)}$ for any $s > 0$, list-decodes up to ℓ_p distance $d = \delta \cdot n^{1/p}$ any GRS code $\mathcal{C} \subseteq \mathbb{F}_q^n$ with adjusted rate

$$R^* < \frac{f_s(\delta)^2}{f_s(\mathcal{L}_q)} =: W_{q,\delta}^{(p)}(s) \xrightarrow{s, q/s \rightarrow \infty} \frac{1}{\delta \cdot \underbrace{c_p \cdot (ep)^{1/p}}_{\parallel}}$$

in $\text{poly}(n, q, \exp(1/s^p)/\tau)$ time.

$\parallel$
volume of the n -dim. ℓ_p ball of radius $n^{1/p}$
(dimension-normalized)

Our Results

Theorem: (*average-case*) For any metric $0 < p \leq 2$, $\alpha \in (0,1)$, prime q , channel parameter $r > 0$, under a memoryless, additive (continuous or discrete) channel whose distribution is D_r , the GS soft-decision algorithm using weight vectors defined by $f_s^{(p)}$ for any $s > 0$, list-decodes any GRS code $\mathcal{C} \subseteq \mathbb{F}_q^n$ with adjusted rate

$$\begin{aligned} pdf: D_r(x) &= f_r(x)/r \\ pmf: D_r(x) &= f_r(x)/f_r(\mathbb{Z}) \end{aligned}$$

$$R^* < \frac{s^2 / \|(r, s)\|_p^2}{f_s(\mathcal{L}_q)} =: A_{q,r}^{(p)}(s)$$

in $\text{poly}(n, q, \exp(1/s^p)/\tau)$ time, except with probability $< \exp(-2n \cdot f_s(\mathcal{L}_q) \cdot \alpha^2 \cdot \tau^2)$.

Open Directions

- The product of the rate R and distance δ for which our algorithm works approaches

$$R \cdot \delta \rightarrow \text{relative radius of a unit-volume } n\text{-dim. } \ell_p \text{ ball.}$$

Why should this be the case?

- What is the list-decoding capacity for decoding over general ℓ_p norms?

How do our algorithmic bounds compare?

- Prove a better lower bound on the minimum distance for *all* GRS codes, not just a natural subclass.
- Extend our results to folded Reed-Solomon (FRS) codes.

Can we achieve a better rate-distance trade-off?

Open Directions

- The product of the rate R and distance δ for which our algorithm works approaches

$$R \cdot \delta \rightarrow \text{relative radius of a unit-volume } n\text{-dim. } \ell_p \text{ ball.}$$

Why should this be the case?

- What is the list-decoding capacity for decoding over general ℓ_p norms?

How do our algorithmic bounds compare?

- Prove a better lower bound on the minimum distance for *all* GRS codes, not just a natural subclass.
- Extend our results to folded Reed-Solomon (FRS) codes.

Can we achieve a better rate-distance trade-off?

Open Directions

- The product of the rate R and distance δ for which our algorithm works approaches

$$R \cdot \delta \rightarrow \text{relative radius of a unit-volume } n\text{-dim. } \ell_p \text{ ball.}$$

Why should this be the case?

- What is the list-decoding capacity for decoding over general ℓ_p norms?

How do our algorithmic bounds compare?

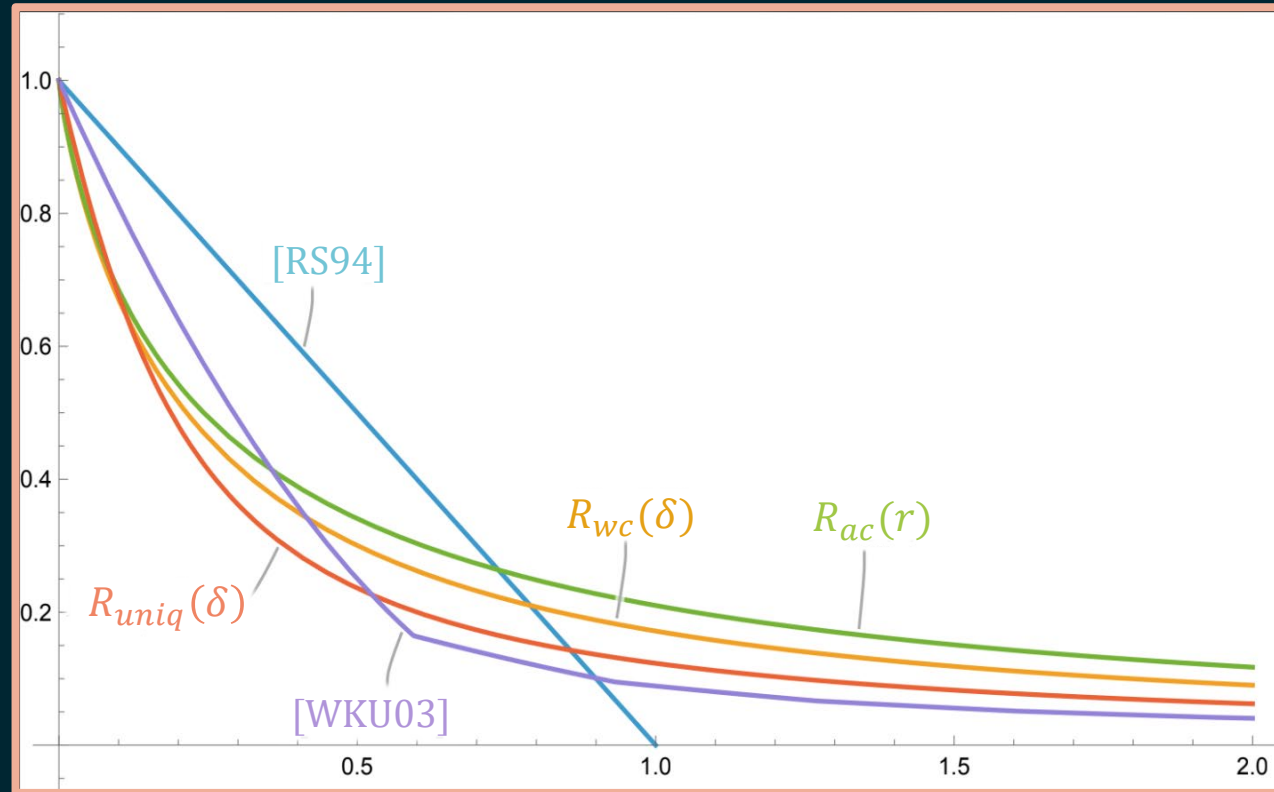
- Prove a better lower bound on the minimum distance for *all* GRS codes, not just a natural subclass.

- Extend our results to folded Reed-Solomon (FRS) codes.

Can we achieve a better rate-distance trade-off?

Comparison to Prior Algorithms

rate R



distance $\delta = \frac{r}{2}$

Rate-distance trade-off for Lee (ℓ_1) metric

Open Directions

- The product of the rate R and distance δ for which our algorithm works approaches

$$R \cdot \delta \rightarrow \text{relative radius of a unit-volume } n\text{-dim. } \ell_p \text{ ball.}$$

Why should this be the case?

- What is the list-decoding capacity for decoding over general ℓ_p norms?

How do our algorithmic bounds compare?

- Prove a better lower bound on the minimum distance for *all* GRS codes, not just a natural subclass.
- Extend our results to folded Reed-Solomon (FRS) codes.

Can we achieve a better rate-distance trade-off?

Questions?