All Polynomial Generators Preserve Distance with Mutual Correlated Agreement

Sarah Bordage, Alessandro Chiesa, **IM**, Ziyi Guan

Why Do We Care?

Why Do We Care?

PCP/IOP soundness

Why Do We Care?

Low-degree testing → PCP/IOP soundness

Why Do We Care?

Proximity Gaps → Low-degree testing → PCP/IOP soundness

Why Do We Care?

Proximity Gaps → Low-degree testing → PCP/IOP soundness

(δ, ϵ)-proximity gaps for $\mathsf{C} \subset 2^{\Sigma^n}$, $\mathsf{P} \subset \Sigma^n$ under distance Δ:
$\forall E \in \mathsf{C}$ either

1. $\Pr_{s \in E}[\Delta(s, \mathsf{P}) \leq \delta] = 1$

2. $\Pr_{s \in E}[\Delta(s, \mathsf{P}) \leq \delta] \leq \epsilon$

Why Do We Care?

Proximity Gaps $\rightarrow$ Low-degree testing $\rightarrow$ PCP/IOP soundness

(δ, ϵ)-proximity gaps for $\mathsf{C} \subset 2^{\Sigma^n}$, $\mathsf{P} \subset \Sigma^n$ under distance Δ:
$\forall E \in \mathsf{C}$ either

1. $\Pr_{s \in E}[\Delta(s, \mathsf{P}) \leq \delta] = 1$
2. $\Pr_{s \in E}[\Delta(s, \mathsf{P}) \leq \delta] \leq \epsilon$

In this work: consider spans of polynomial proximity generators, $\mathsf{P} = \mathscr{C}$ linear code, under the Hamming distance.

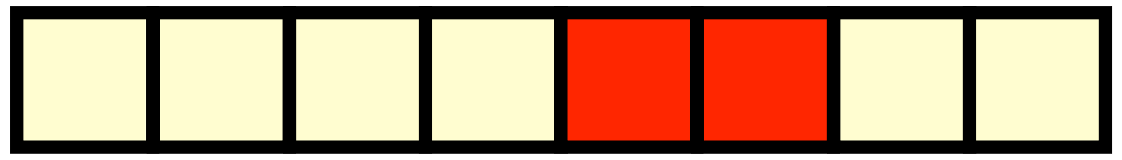
Distance Preservation

Distance Preservation

Let $\mathscr{C} \subseteq \mathbb{F}^n$ be a linear code

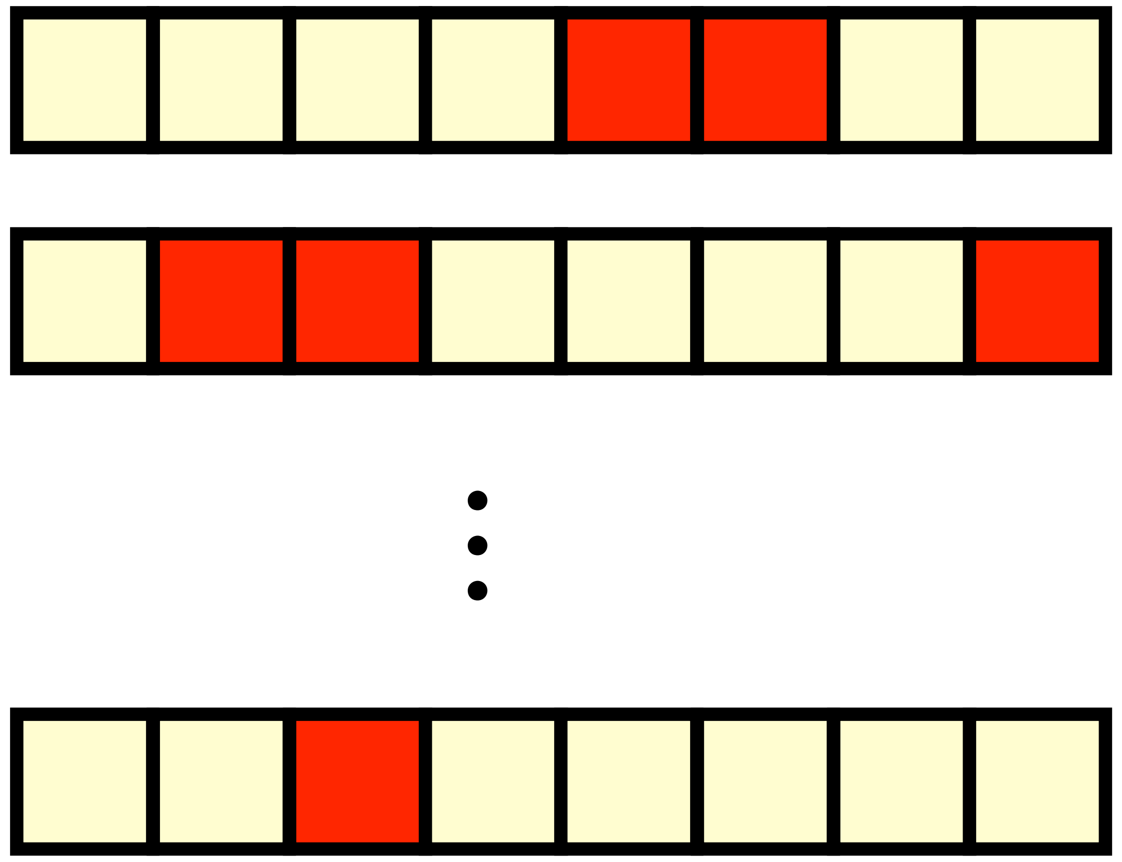
Distance Preservation

Let $\mathscr{C} \subseteq \mathbb{F}^n$ be a linear code

$\mathbf{u}_1$  $\delta_1 := \Delta(u_1, \mathscr{C})$

Distance Preservation

Let $\mathscr{C} \subseteq \mathbb{F}^n$ be a linear code



$\mathbf{u}_1$ $\delta_1 := \Delta(u_1, \mathscr{C})$

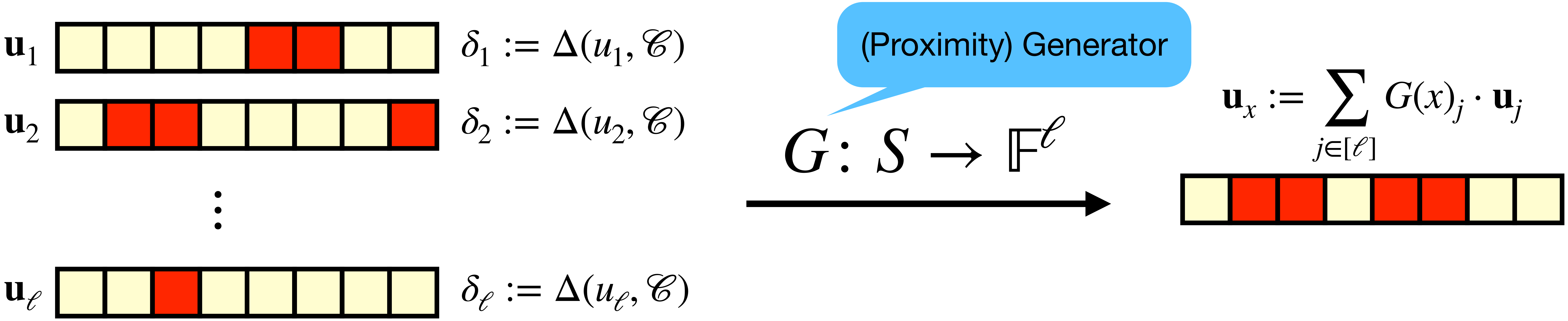
$\mathbf{u}_2$ $\delta_2 := \Delta(u_2, \mathscr{C})$

$\vdots$

$\mathbf{u}_\ell$ $\delta_\ell := \Delta(u_\ell, \mathscr{C})$

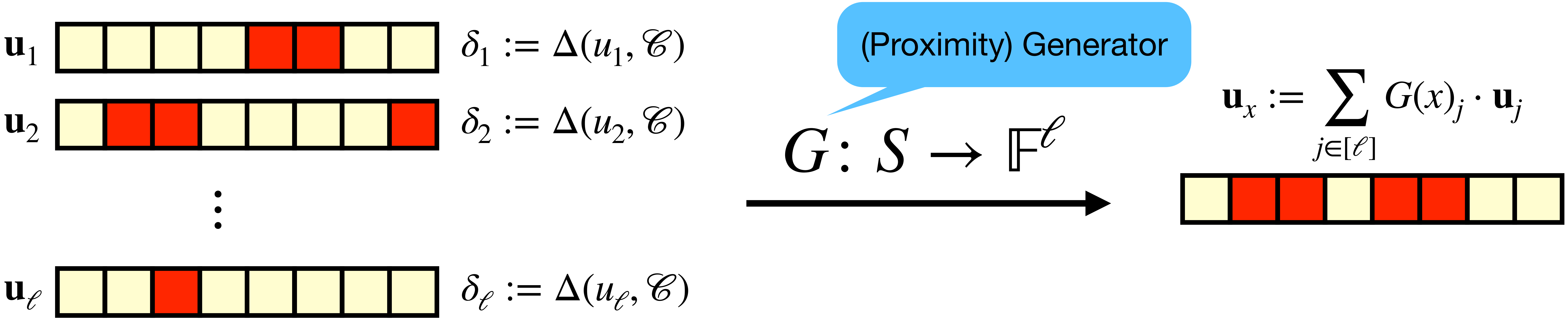
Distance Preservation

Let $\mathscr{C} \subseteq \mathbb{F}^n$ be a linear code



Distance Preservation

Let $\mathscr{C} \subseteq \mathbb{F}^n$ be a linear code



We want $\Pr_{x \in S}\left[\Delta(\mathbf{u}_x, \mathscr{C}) < \max_j \delta_j\right]$ to be small

Preserving Max Distance is not Enough

Preserving Max Distance is not Enough

[RVW13]

When $G(x_1, \ldots, x_\ell) = (x_1, \ldots, x_\ell)$,

$$\Pr_{\vec{x} \in \mathbb{F}^\ell}\left[\Delta(\mathbf{u}_{\vec{x}}, \mathscr{C}) < \max_j \frac{\delta_j}{2}\right] \leq \frac{1}{|\mathbb{F}|}$$

Preserving Max Distance is not Enough

[RVW13]

When $G(x_1, \ldots, x_\ell) = (x_1, \ldots, x_\ell)$,

$$\Pr_{\vec{x} \in \mathbb{F}^\ell}\left[\Delta(\mathbf{u}_{\vec{x}}, \mathscr{C}) < \max_j \frac{\delta_j}{2}\right] \leq \frac{1}{|\mathbb{F}|}$$

Not enough for some applications!
(e.g. batch proximity testing)

- Distance drop
- Only one generator
- No control over the agreement set

Preserving Max Distance is not Enough

[RVW13]

When $G(x_1, \ldots, x_\ell) = (x_1, \ldots, x_\ell)$,

$$\Pr_{\vec{x} \in \mathbb{F}^\ell}\left[\Delta(\mathbf{u}_{\vec{x}}, \mathscr{C}) < \max_j \frac{\delta_j}{2}\right] \leq \frac{1}{|\mathbb{F}|}$$

[AHIV17],[BKS18],[BGKS20]

Not enough for some applications!
(e.g. batch proximity testing)

- Distance drop
- Only one generator
- No control over the agreement set

Preserving Max Distance is not Enough

[RVW13]

When $G(x_1, \ldots, x_\ell) = (x_1, \ldots, x_\ell)$,

$$\Pr_{\vec{x} \in \mathbb{F}^\ell}\left[\Delta(\mathbf{u}_{\vec{x}}, \mathscr{C}) < \max_j \frac{\delta_j}{2}\right] \leq \frac{1}{|\mathbb{F}|}$$

[AHIV17],[BKS18],[BGKS20]

[BCIKS20],[BCL22],[BCGL22],[DP24],[MZ25],[BMMS25],…

Not enough for some applications!
(e.g. batch proximity testing)

- Distance drop
- Only one generator
- No control over the agreement set

Preserving Max Distance is not Enough

[RVW13]

When $G(x_1, \ldots, x_\ell) = (x_1, \ldots, x_\ell)$,

$$\Pr_{\vec{x} \in \mathbb{F}^\ell}\left[\Delta(\mathbf{u}_{\vec{x}}, \mathscr{C}) < \max_j \frac{\delta_j}{2}\right] \leq \frac{1}{|\mathbb{F}|}$$

[AHIV17],[BKS18],[BGKS20]

[BCIKS20],[BCL22],[BCGL22],[DP24],[MZ25],[BMMS25],…

[BCIKS20],*[ACFY24]*

Not enough for some applications!
(e.g. batch proximity testing)

- Distance drop
- Only one generator
- No control over the agreement set

Mutual Correlated Agreement (MCA)

Mutual Correlated Agreement (MCA)

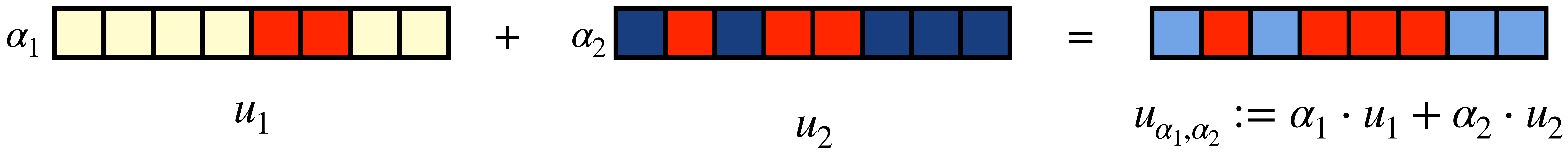
Fix $G(\alpha_1, \alpha_2) = (\alpha_1, \alpha_2)$ for simplicity.

Goal: except for a small error over (α_1, α_2), this happens:

Mutual Correlated Agreement (MCA)

Fix $G(\alpha_1, \alpha_2) = (\alpha_1, \alpha_2)$ for simplicity.

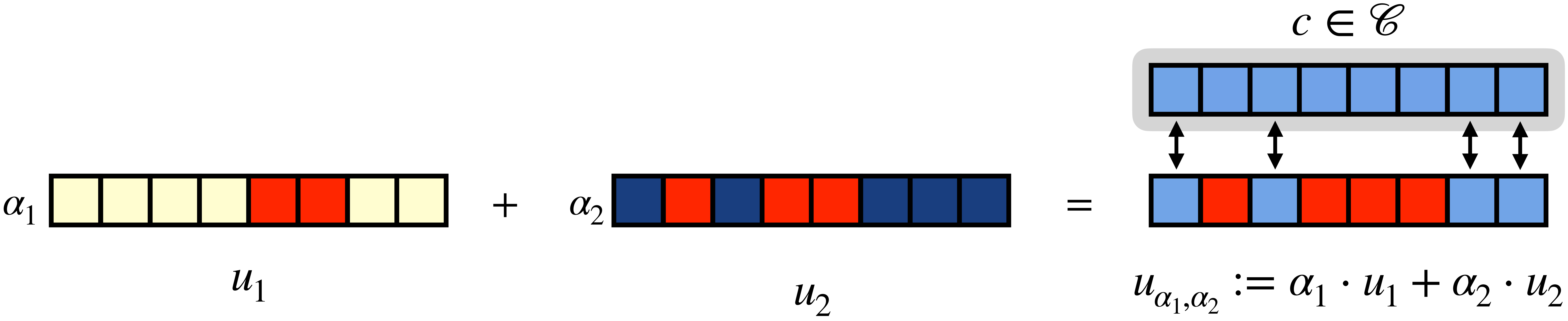
Goal: except for a small error over (α_1, α_2), this happens:



Mutual Correlated Agreement (MCA)

Fix $G(\alpha_1, \alpha_2) = (\alpha_1, \alpha_2)$ for simplicity.

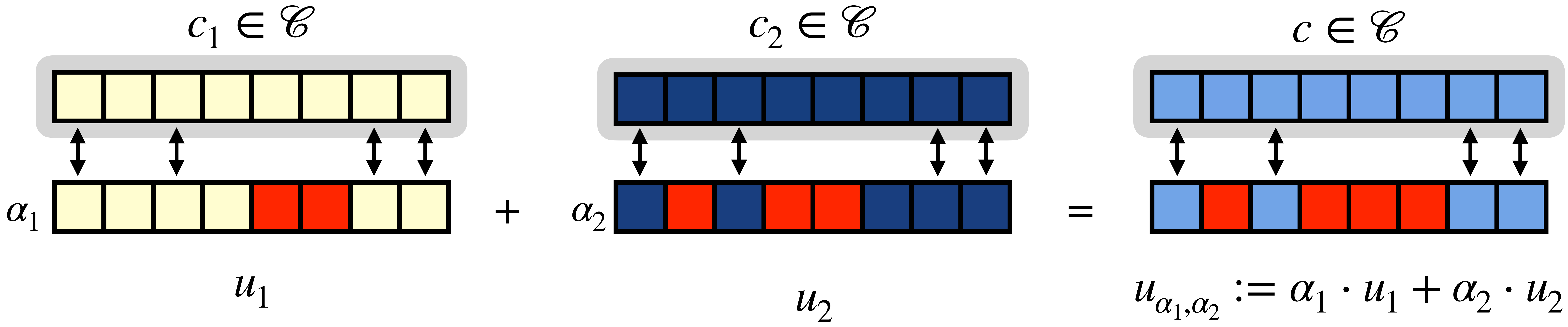
Goal: except for a small error over (α_1, α_2), this happens:



Mutual Correlated Agreement (MCA)

Fix $G(\alpha_1, \alpha_2) = (\alpha_1, \alpha_2)$ for simplicity.

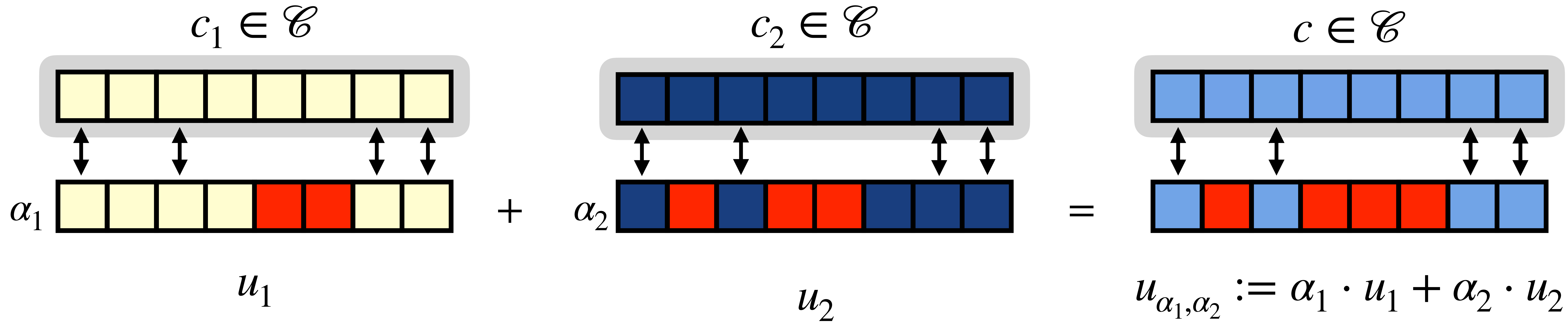
Goal: except for a small error over (α_1, α_2), this happens:



Mutual Correlated Agreement (MCA)

Fix $G(\alpha_1, \alpha_2) = (\alpha_1, \alpha_2)$ for simplicity.

Goal: except for a small error over (α_1, α_2), this happens:



$T := \{1,3,7,8\}$ - the common agreement set

MCA, formally

MCA, formally

Definition:

$G\colon S \to \mathbb{F}^\ell$ has **MCA error** $\epsilon_{\mathsf{MCA}} : [0,1] \to [0,1]$ for $\mathscr{C} \subseteq \mathbb{F}^n$ if

$$\forall \mathbf{U} = \begin{pmatrix} \mathbf{u}_1 \\ \vdots \\ \mathbf{u}_\ell \end{pmatrix} \in \mathbb{F}^{\ell \times n} \quad \forall \gamma \in [0,1] \quad \Pr_{x \in S}\left[\begin{array}{l} \exists T \subseteq [n] : \\ \quad |T| \geq n \cdot (1-\gamma) \\ \quad (G(x) \cdot \mathbf{U})|_T \in \mathscr{C}|_T \\ \quad \bigvee_{j \in [\ell]} \mathbf{u}_j|_T \notin \mathscr{C}|_T \end{array}\right] \leq \epsilon_{\mathsf{MCA}}(\gamma)$$

MCA, formally

Definition:

$G \colon S \to \mathbb{F}^\ell$ has **MCA error** $\epsilon_{\mathsf{MCA}} : [0,1] \to [0,1]$ for $\mathscr{C} \subseteq \mathbb{F}^n$ if

$$\forall \mathbf{U} = \begin{pmatrix} \mathbf{u}_1 \\ \vdots \\ \mathbf{u}_\ell \end{pmatrix} \in \mathbb{F}^{\ell \times n} \quad \forall \gamma \in [0,1] \quad \Pr_{x \in S}\begin{bmatrix} \exists T \subseteq [n] : \\ |T| \geq n \cdot (1-\gamma) \\ (G(x) \cdot \mathbf{U})|_T \in \mathscr{C}|_T \\ \vee_{j \in [\ell]} \mathbf{u}_j|_T \notin \mathscr{C}|_T \end{bmatrix} \leq \epsilon_{\mathsf{MCA}}(\gamma)$$

Distance param

MCA, formally

Definition:

$G\colon S \to \mathbb{F}^{\ell}$ has **MCA error** $\epsilon_{\mathsf{MCA}} : [0,1] \to [0,1]$ for $\mathscr{C} \subseteq \mathbb{F}^n$ if

$$\forall \mathbf{U} = \begin{pmatrix} \mathbf{u}_1 \\ \vdots \\ \mathbf{u}_\ell \end{pmatrix} \in \mathbb{F}^{\ell \times n} \quad \forall \gamma \in [0,1] \quad \Pr_{x \in S}\left[\begin{array}{c} \exists T \subseteq [n] : \\ |T| \geq n \cdot (1-\gamma) \\ (G(x) \cdot \mathbf{U})|_T \in \mathscr{C}|_T \\ \vee_{j \in [\ell]} \mathbf{u}_j|_T \notin \mathscr{C}|_T \end{array}\right] \leq \epsilon_{\mathsf{MCA}}(\gamma)$$

Large agreement

Distance param

MCA, formally

Definition:

$G\colon S \to \mathbb{F}^{\ell}$ has **MCA error** $\epsilon_{\mathsf{MCA}} : [0,1] \to [0,1]$ for $\mathscr{C} \subseteq \mathbb{F}^n$ if

$$\forall \mathbf{U} = \begin{pmatrix} \mathbf{u}_1 \\ \vdots \\ \mathbf{u}_\ell \end{pmatrix} \in \mathbb{F}^{\ell \times n} \quad \forall \gamma \in [0,1] \quad \Pr_{x \in S}\left[\begin{array}{c} \exists T \subseteq [n] : \\ |T| \geq n \cdot (1-\gamma) \\ (G(x) \cdot \mathbf{U})|_T \in \mathscr{C}|_T \\ \bigvee_{j \in [\ell]} \mathbf{u}_j|_T \notin \mathscr{C}|_T \end{array}\right] \leq \epsilon_{\mathsf{MCA}}(\gamma)$$

Large agreement

Distance param

Combination agrees

MCA, formally

Definition:

$G\colon S \to \mathbb{F}^{\ell}$ has **MCA error** $\epsilon_{\text{MCA}} : [0,1] \to [0,1]$ for $\mathscr{C} \subseteq \mathbb{F}^n$ if

$$\forall \mathbf{U} = \begin{pmatrix} \mathbf{u}_1 \\ \vdots \\ \mathbf{u}_\ell \end{pmatrix} \in \mathbb{F}^{\ell \times n} \quad \forall \gamma \in [0,1] \quad \Pr_{x \in S}\left[\begin{array}{c} \exists T \subseteq [n] : \\ |T| \geq n \cdot (1-\gamma) \\ (G(x) \cdot \mathbf{U})|_T \in \mathscr{C}|_T \\ \vee_{j \in [\ell]} \mathbf{u}_j|_T \notin \mathscr{C}|_T \end{array}\right] \leq \epsilon_{\text{MCA}}(\gamma)$$

Large agreement

Distance param

Combination agrees

Some word doesn't

MCA, formally

Definition:

$G : S \to \mathbb{F}^\ell$ has **MCA error** $\epsilon_{\mathsf{MCA}} : [0,1] \to [0,1]$ for $\mathscr{C} \subseteq \mathbb{F}^n$ if

Large agreement

$$\forall \mathbf{U} = \begin{pmatrix} \mathbf{u}_1 \\ \vdots \\ \mathbf{u}_\ell \end{pmatrix} \in \mathbb{F}^{\ell \times n} \quad \forall \gamma \in [0,1] \quad \Pr_{x \in S}\left[\begin{array}{l} \exists T \subseteq [n] : \\ \quad |T| \geq n \cdot (1-\gamma) \\ \quad (G(x) \cdot \mathbf{U})|_T \in \mathscr{C}|_T \\ \quad \vee_{j \in [\ell]} \mathbf{u}_j|_T \notin \mathscr{C}|_T \end{array}\right] \leq \epsilon_{\mathsf{MCA}}(\gamma)$$

Distance param

Combination agrees

Some word doesn't

E.g., for $\gamma = 0$:

$$\forall \mathbf{U} = \begin{pmatrix} \mathbf{u}_1 \\ \vdots \\ \mathbf{u}_\ell \end{pmatrix} \in \mathbb{F}^{\ell \times n}, \quad \Pr_{x \in S}\left[\begin{array}{l} (G(x) \cdot \mathbf{U}) \in \mathscr{C} \\ \vee_{j \in [\ell]} \mathbf{u}_j \notin \mathscr{C} \end{array}\right] \leq \epsilon_{\mathsf{MCA}}(0)$$

MCA, formally

Definition:

$G\colon S \to \mathbb{F}^{\ell}$ has **MCA error** $\epsilon_{\text{MCA}} : [0,1] \to [0,1]$ for $\mathscr{C} \subseteq \mathbb{F}^n$ if

$$\forall \mathbf{U} = \begin{pmatrix} \mathbf{u}_1 \\ \vdots \\ \mathbf{u}_\ell \end{pmatrix} \in \mathbb{F}^{\ell \times n} \quad \forall \gamma \in [0,1] \quad \Pr_{x \in S}\left[\begin{array}{l} \exists T \subseteq [n] : \\ \quad |T| \geq n \cdot (1-\gamma) \\ \quad (G(x) \cdot \mathbf{U})|_T \in \mathscr{C}|_T \\ \quad \bigvee_{j \in [\ell]} \mathbf{u}_j|_T \notin \mathscr{C}|_T \end{array}\right] \leq \epsilon_{\text{MCA}}(\gamma)$$

Large agreement

Distance param

Combination agrees

Some word doesn't

E.g., for $\gamma = 0$:

$$\forall \mathbf{U} = \begin{pmatrix} \mathbf{u}_1 \\ \vdots \\ \mathbf{u}_\ell \end{pmatrix} \in \mathbb{F}^{\ell \times n}, \quad \Pr_{x \in S}\left[\begin{array}{l} (G(x) \cdot \mathbf{U}) \in \mathscr{C} \\ \bigvee_{j \in [\ell]} \mathbf{u}_j \notin \mathscr{C} \end{array}\right] \leq \epsilon_{\text{MCA}}(0)$$

Testing membership to the code!

MCA Makes Things Nice

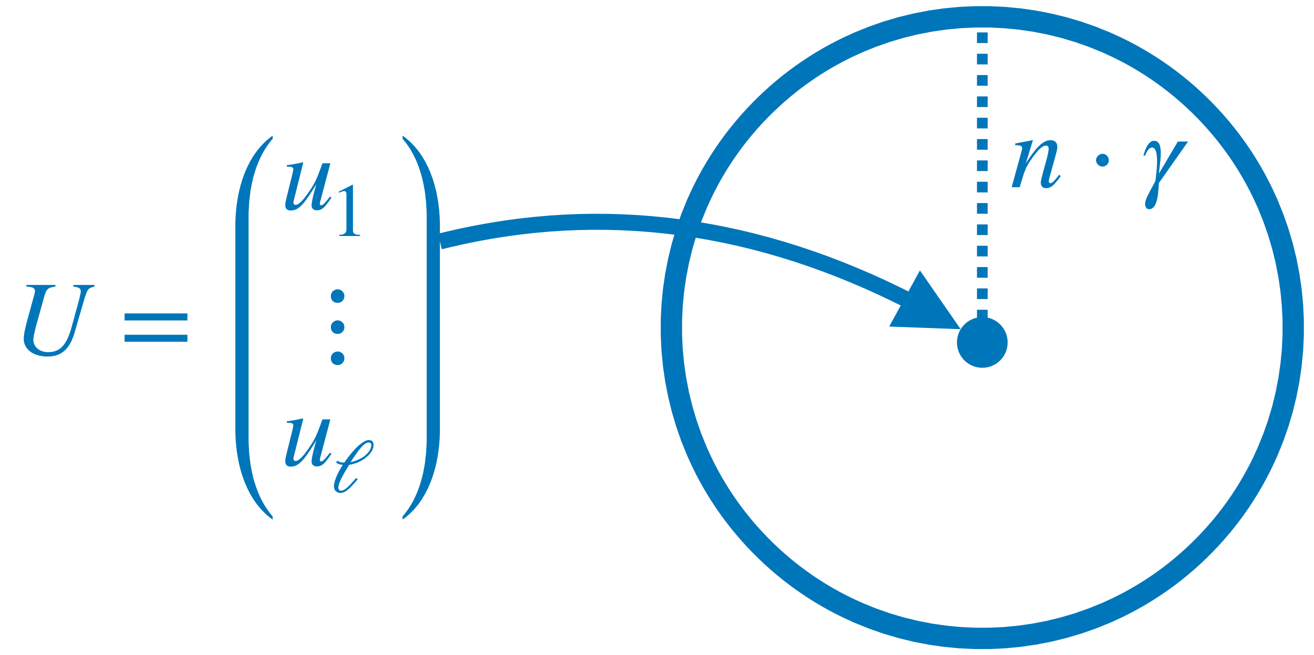
MCA Makes Things Nice

List decoding Key step in security reduction of IOPs

MCA Makes Things Nice

List decoding

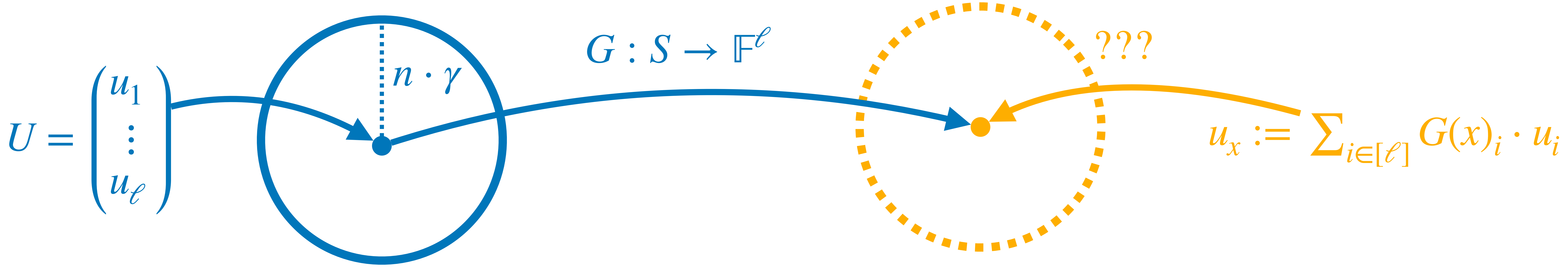
Key step in security reduction of IOPs



MCA Makes Things Nice

List decoding

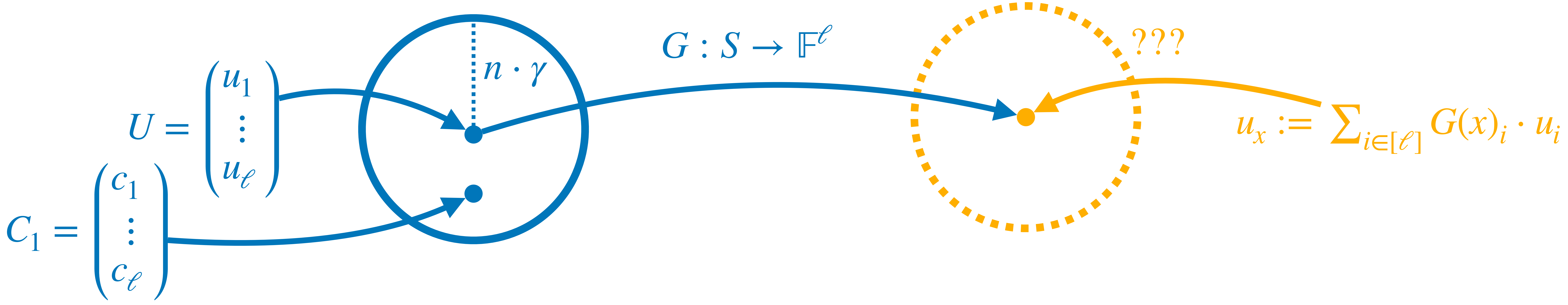
Key step in security reduction of IOPs



MCA Makes Things Nice

List decoding

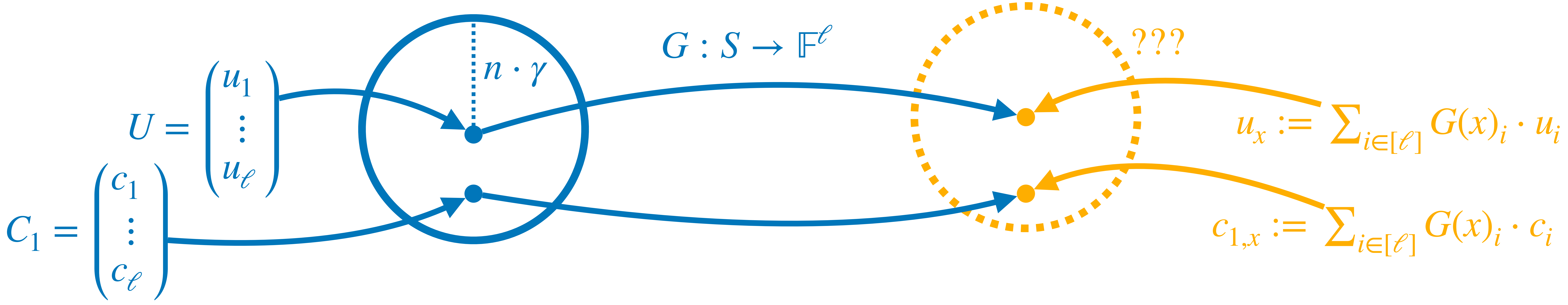
Key step in security reduction of IOPs



MCA Makes Things Nice

List decoding

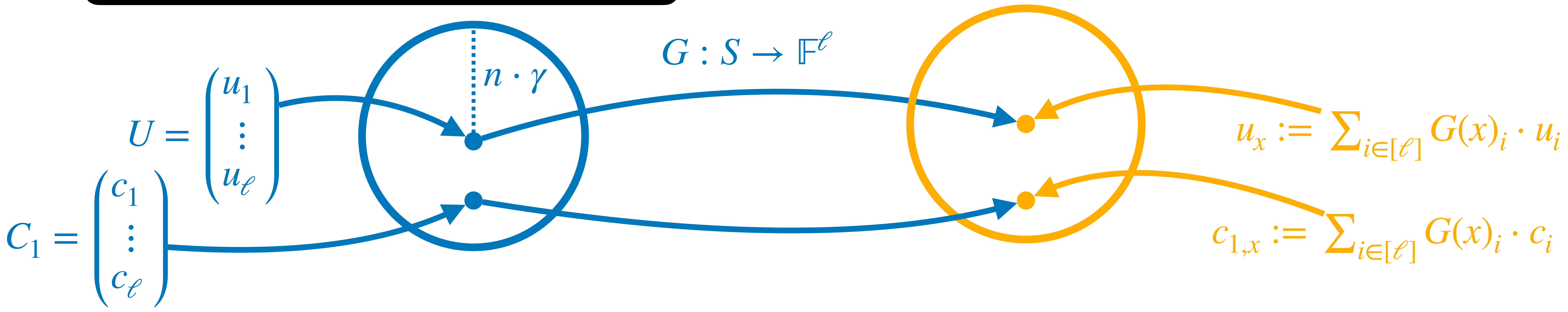
Key step in security reduction of IOPs



MCA Makes Things Nice

List decoding

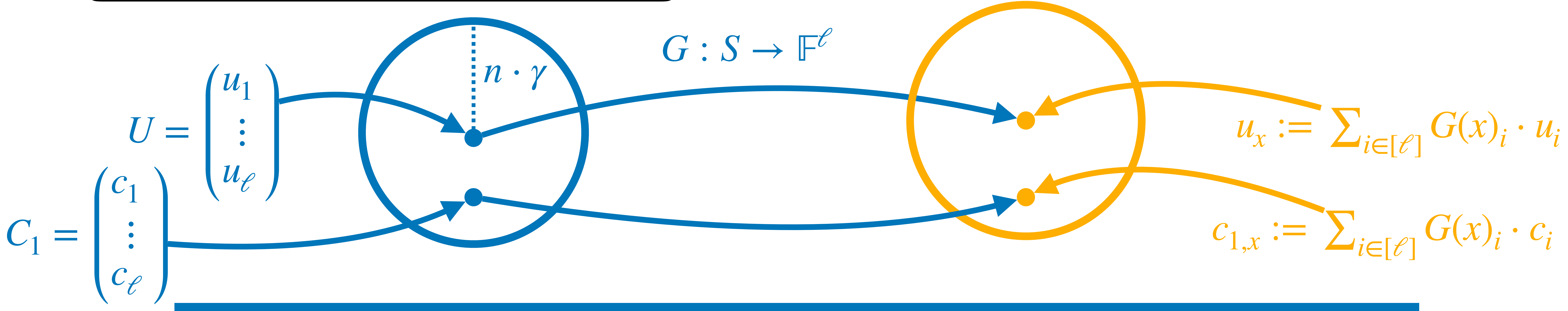
Key step in security reduction of IOPs



MCA Makes Things Nice

List decoding

Key step in security reduction of IOPs

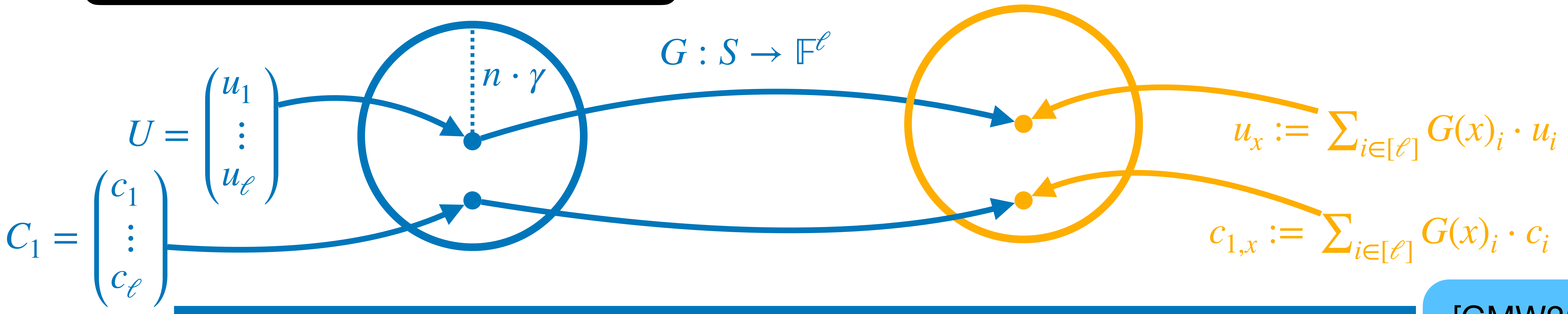


"List-decode and combine" ⇔ "Combine and list-decode"

MCA Makes Things Nice

List decoding

Key step in security reduction of IOPs



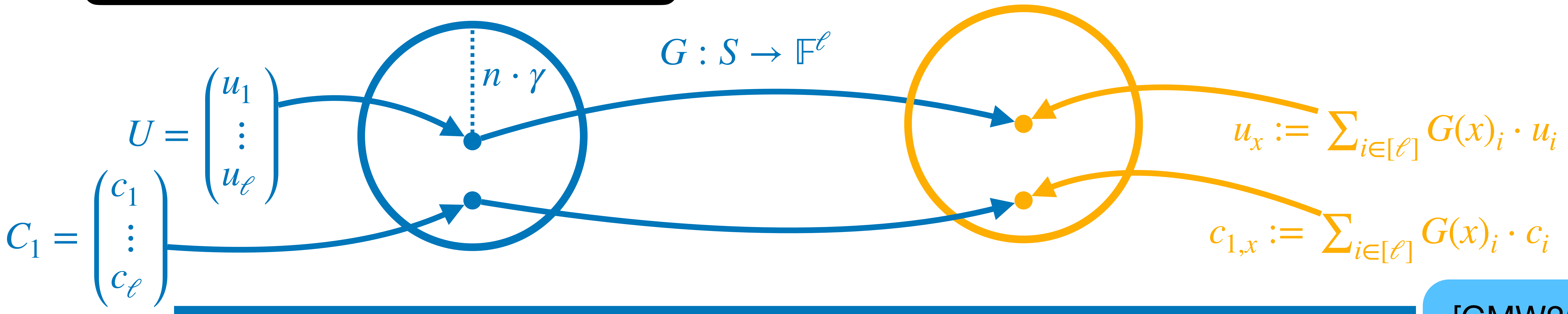
"List-decode and combine" ⇔ "Combine and list-decode"

[GMW25]

MCA Makes Things Nice

List decoding

Key step in security reduction of IOPs



"List-decode and combine" ⇔ "Combine and list-decode"

[GMW25]

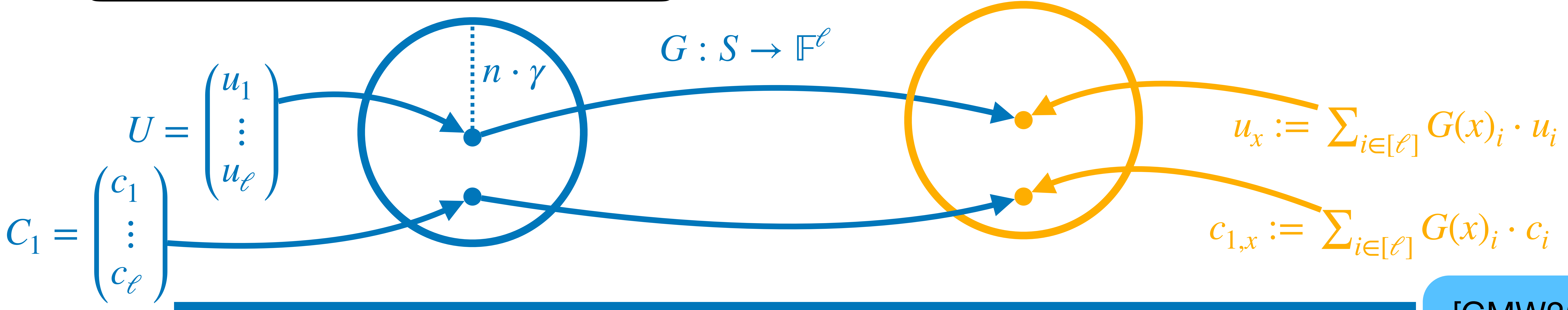
Straightline Extraction

Easier analyses, better parameters

MCA Makes Things Nice

List decoding

Key step in security reduction of IOPs



"List-decode and combine" ⇔ "Combine and list-decode"

[GMW25]

Straightline Extraction

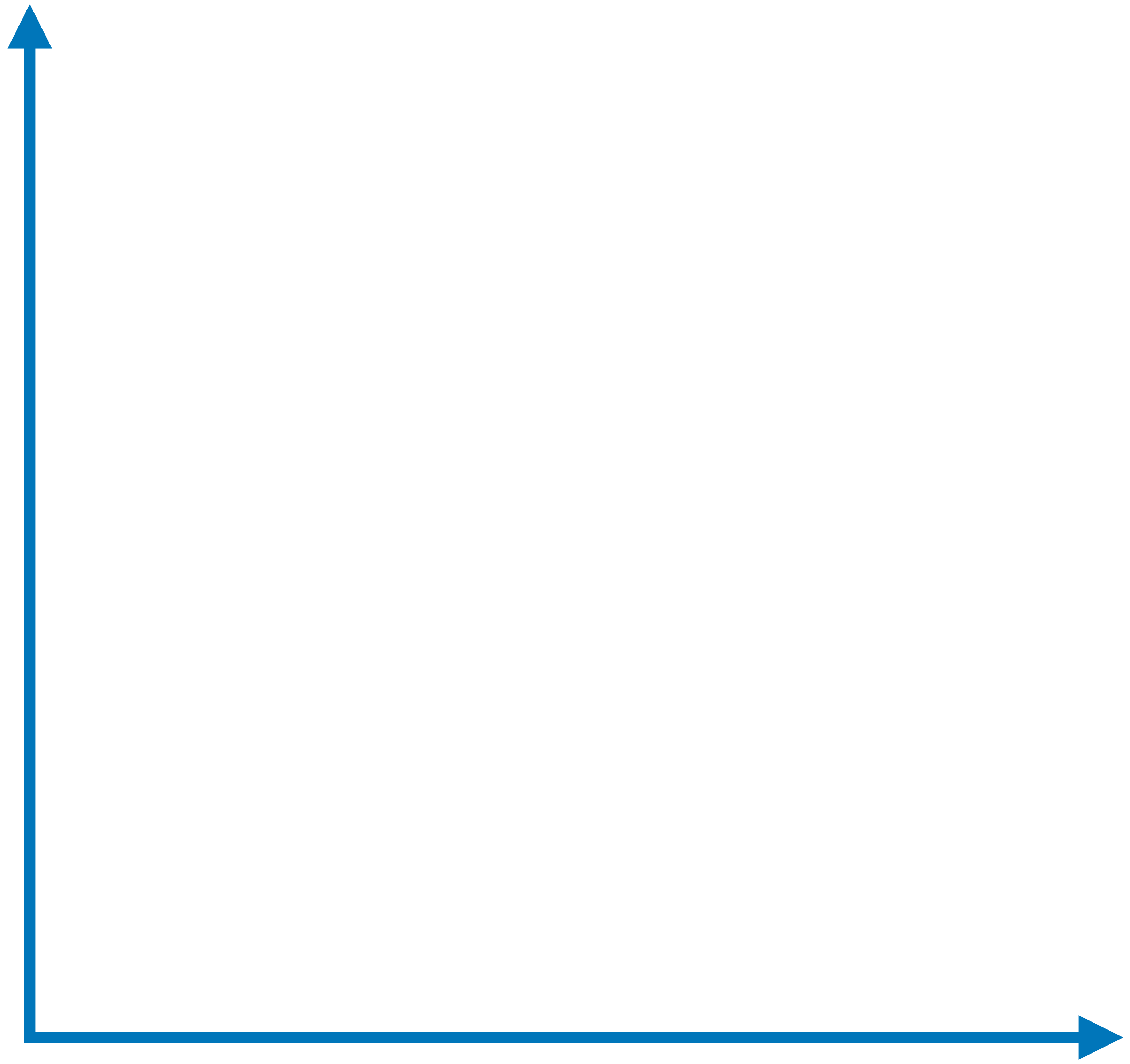
Easier analyses, better parameters

RBR Security

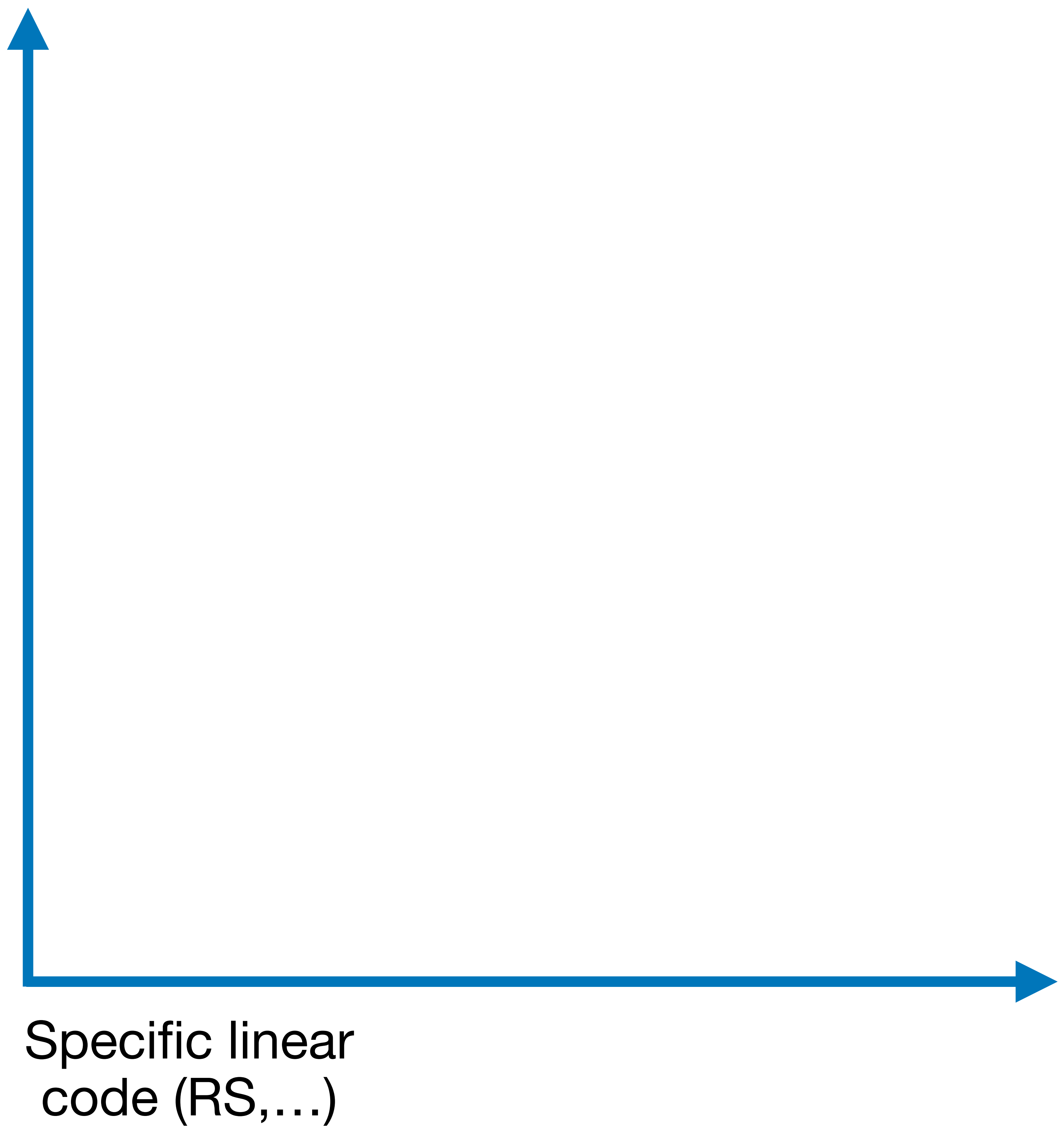
Essential for Fiat—Shamir

The Old MCA Landscape

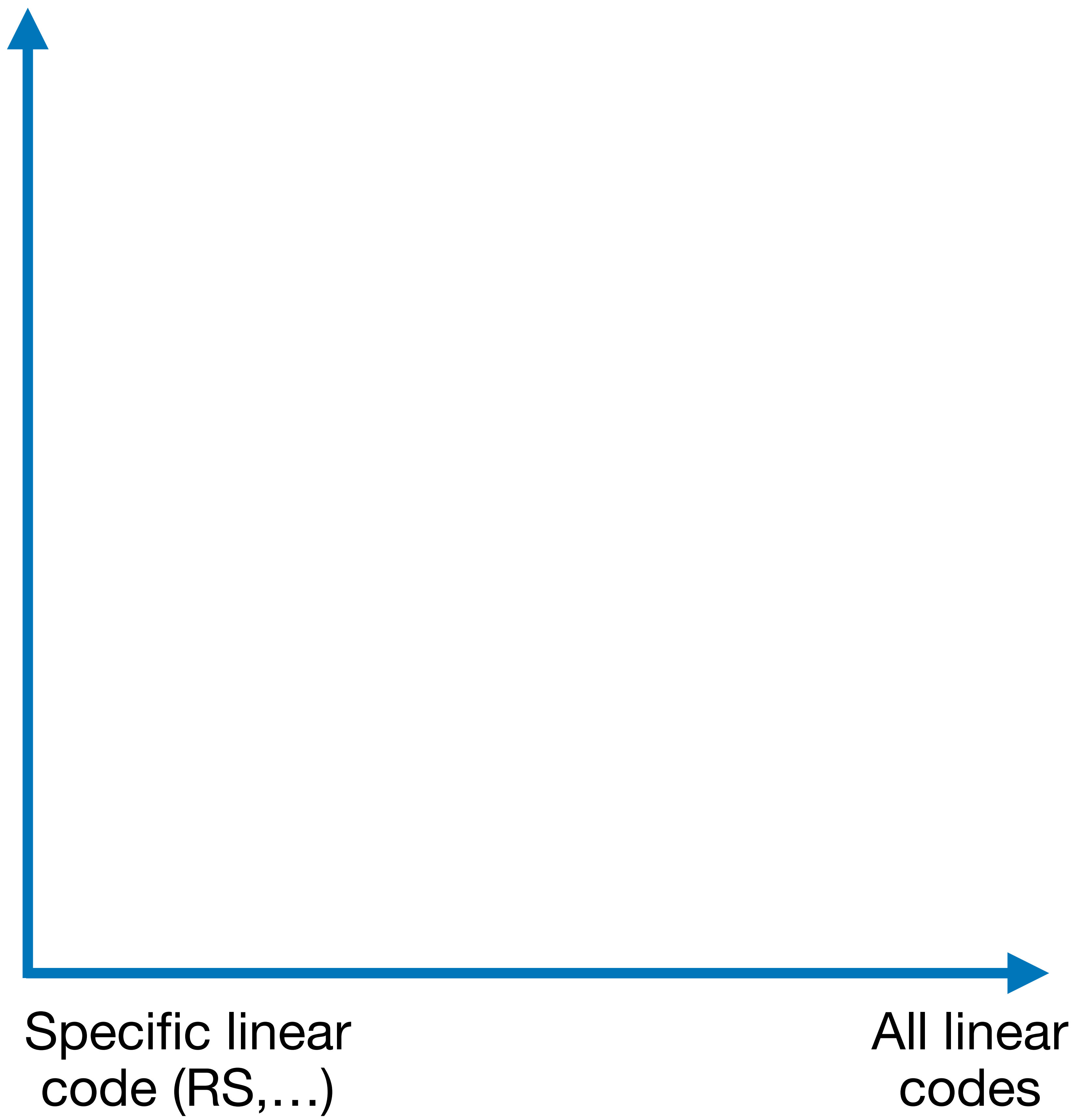
The Old MCA Landscape



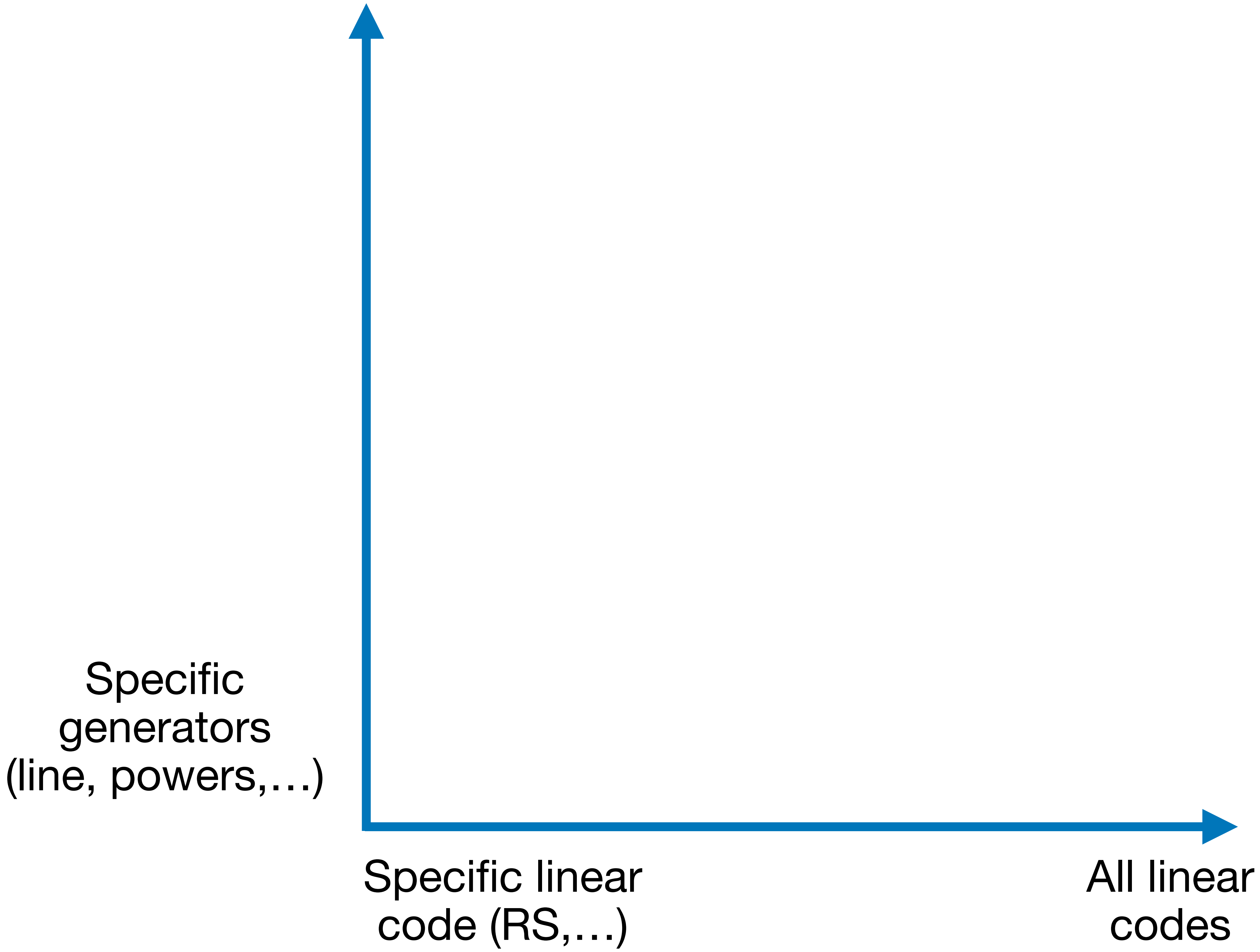
The Old MCA Landscape



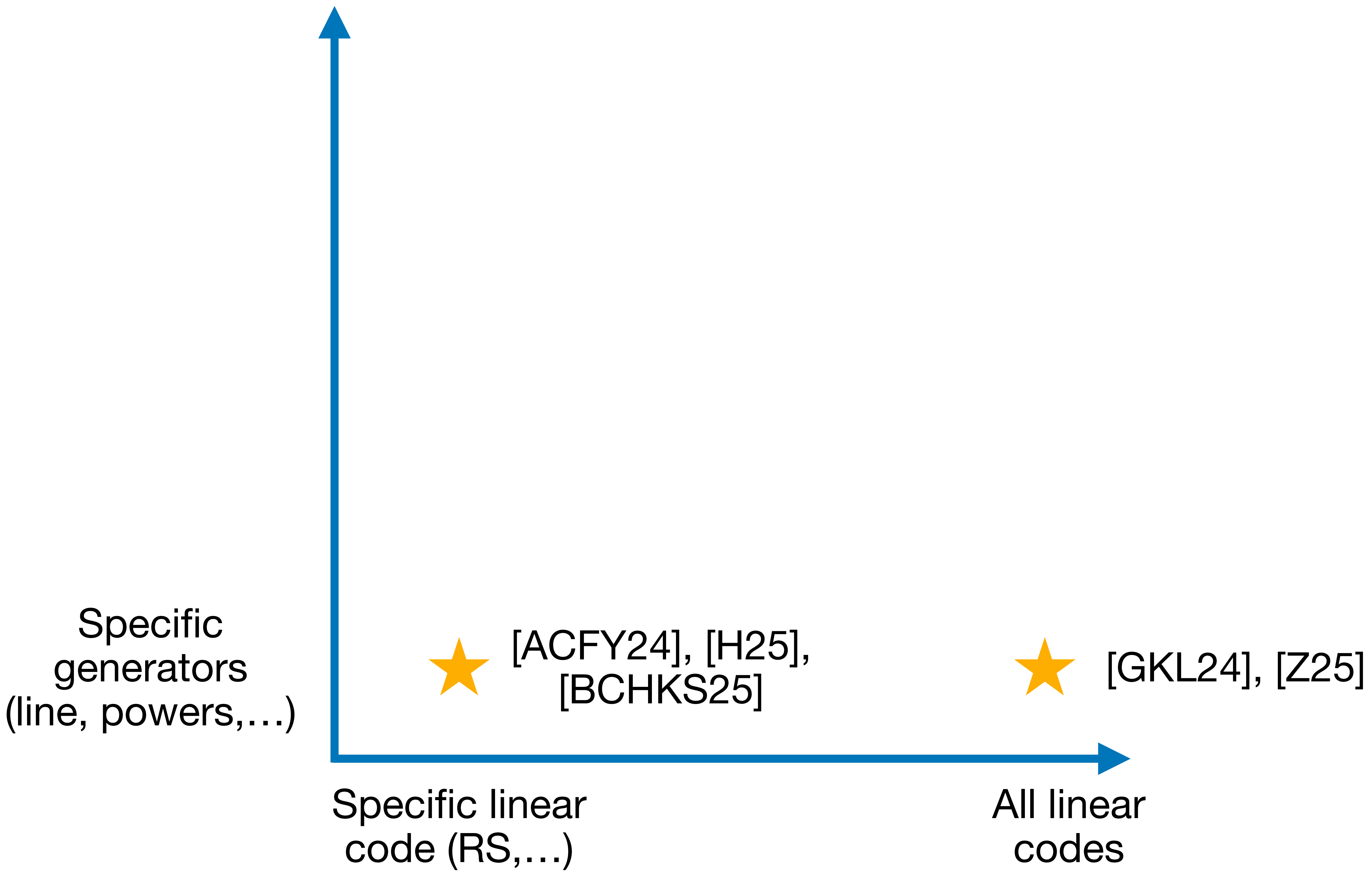
The Old MCA Landscape



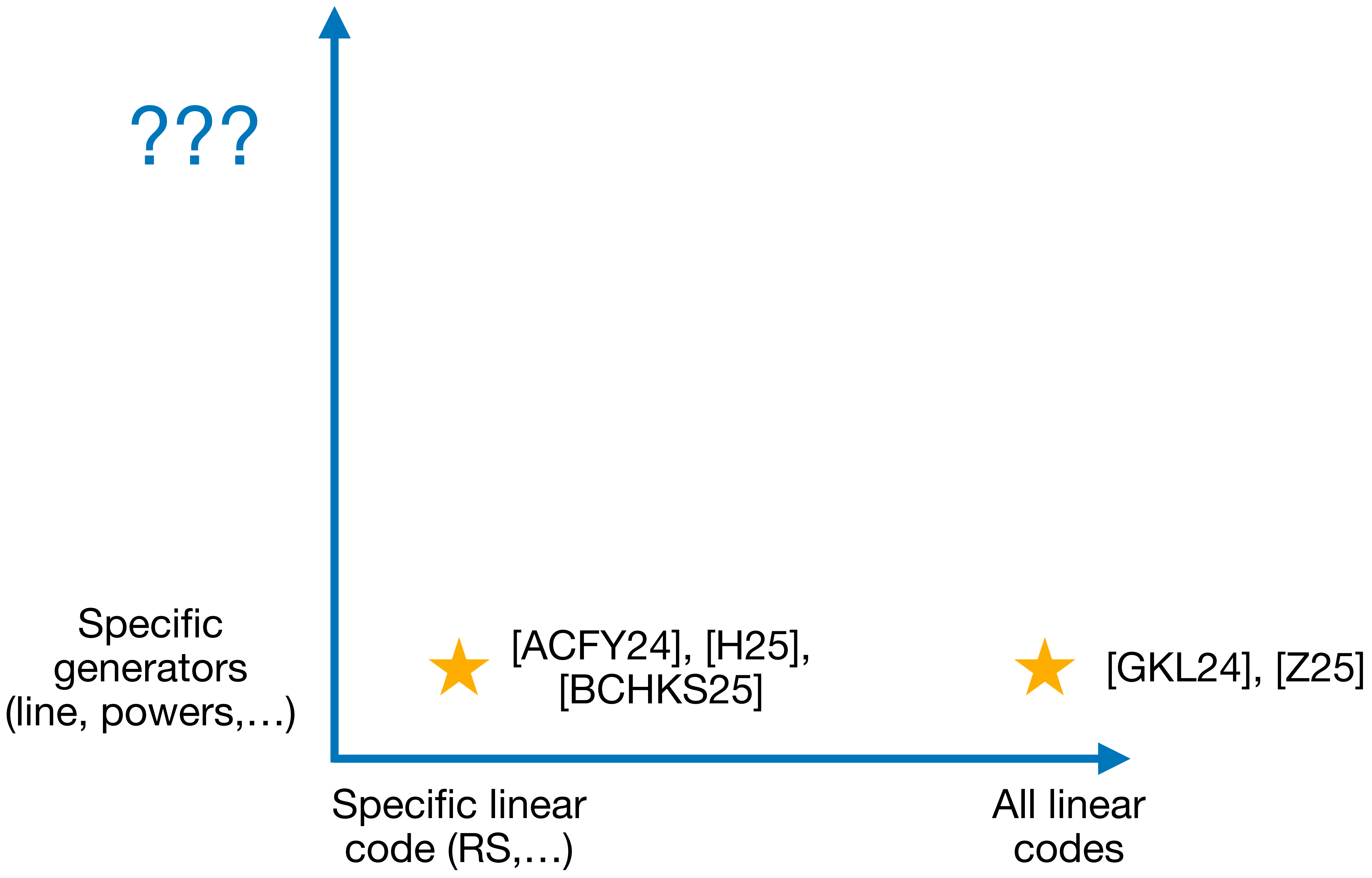
The Old MCA Landscape



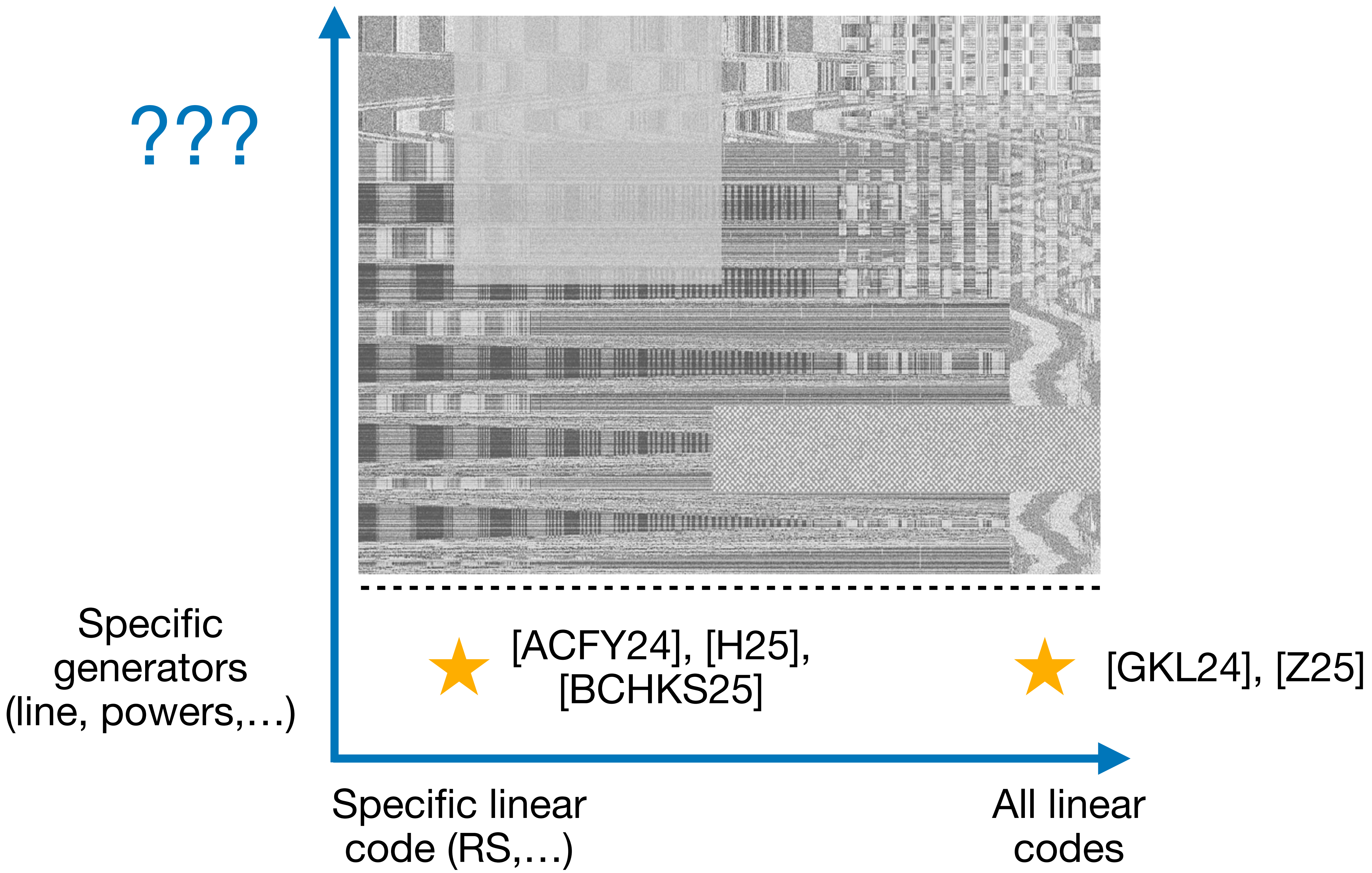
The Old MCA Landscape



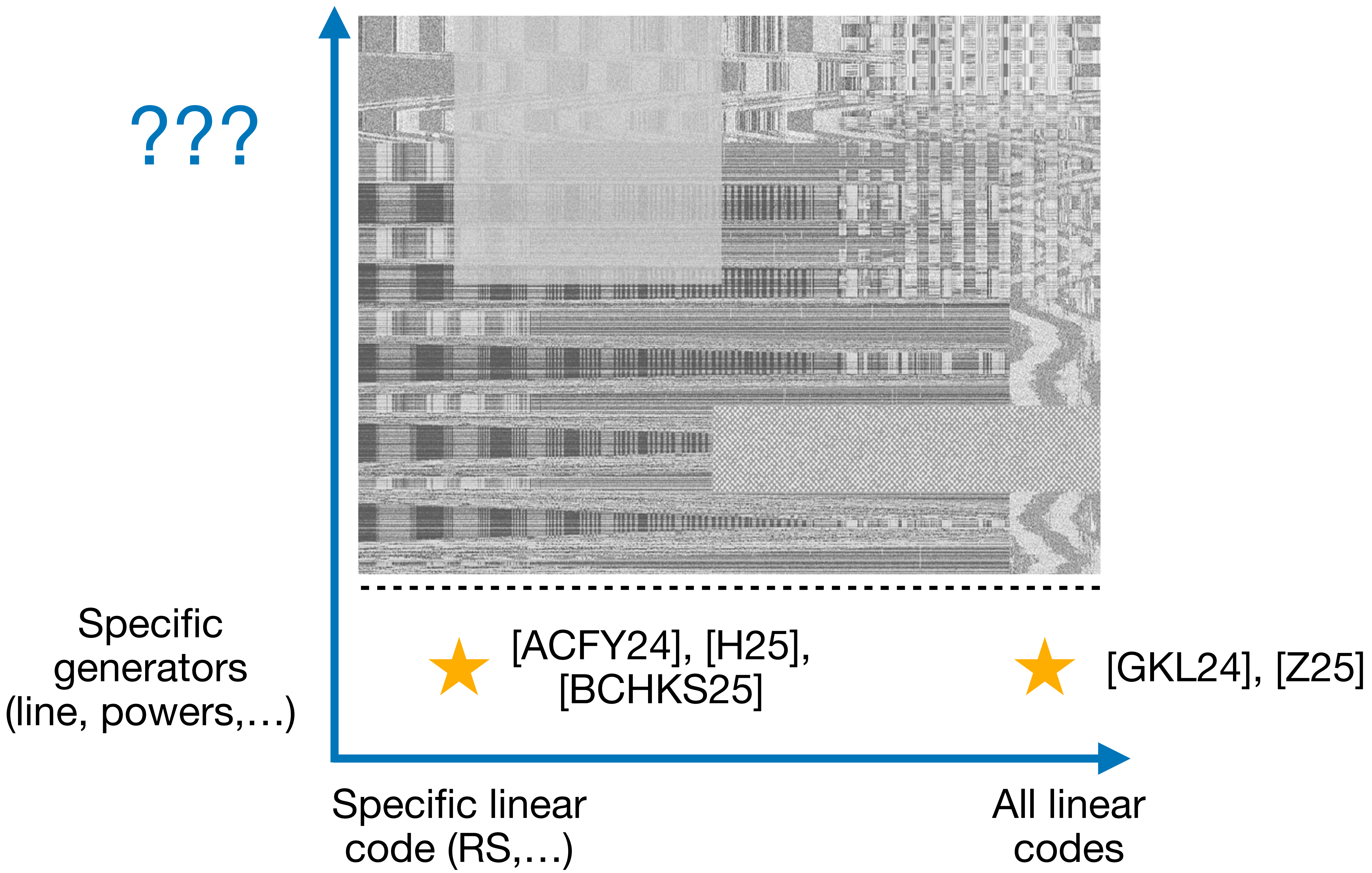
The Old MCA Landscape



The Old MCA Landscape



The Old MCA Landscape



Which generators have MCA?

Our Results

Our Results

1. Every MCA generator is ***zero-evading***

Our Results

A necessary condition

1. Every MCA generator is ***zero-evading***

Our Results

A necessary condition

1. Every MCA generator is ***zero-evading***

2. Every ***polynomial*** generator has ***MCA***

Our Results

A necessary condition

1. Every MCA generator is ***zero-evading***
2. Every ***polynomial*** generator has ***MCA***

A sufficient condition

Our Results

A necessary condition

1. Every MCA generator is ***zero-evading***

2. Every ***polynomial*** generator has ***MCA***

A sufficient condition

- ***Our MCA error is tight:*** in unique decoding, the error scales linearly with distance

Our Results

A necessary condition

1. Every MCA generator is ***zero-evading***

2. Every ***polynomial*** generator has ***MCA***

A sufficient condition

- ***Our MCA error is tight:*** in unique decoding, the error scales linearly with distance

- ∃ generators ***with very high degree*** with ***good MCA error***

Our Results

A necessary condition

1. Every MCA generator is ***zero-evading***

A sufficient condition

2. Every ***polynomial*** generator has ***MCA***

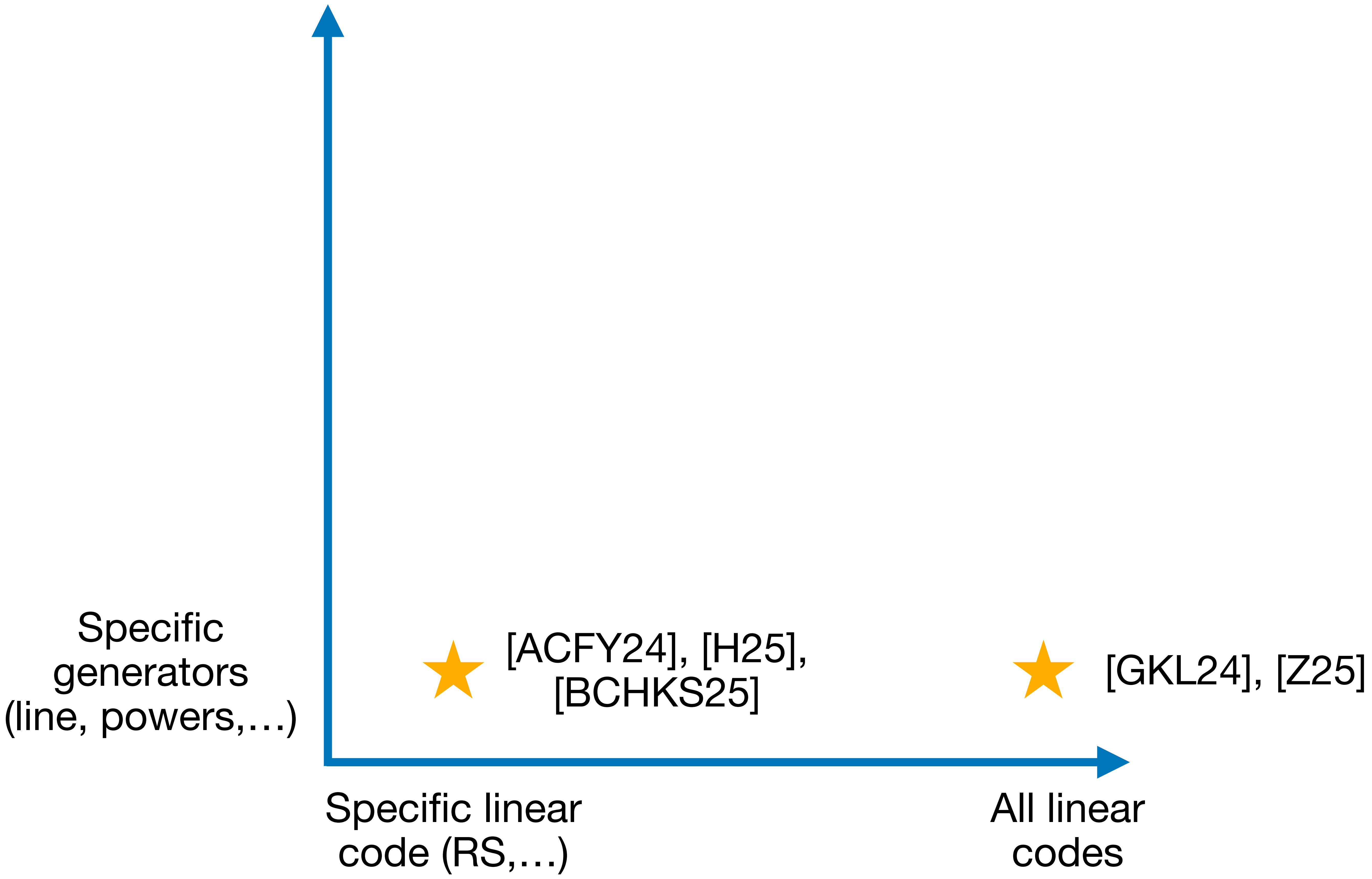
    - ***Our MCA error is tight:*** in unique decoding, the error scales linearly with distance

    - $\exists$ generators ***with very high degree*** with ***good MCA error***

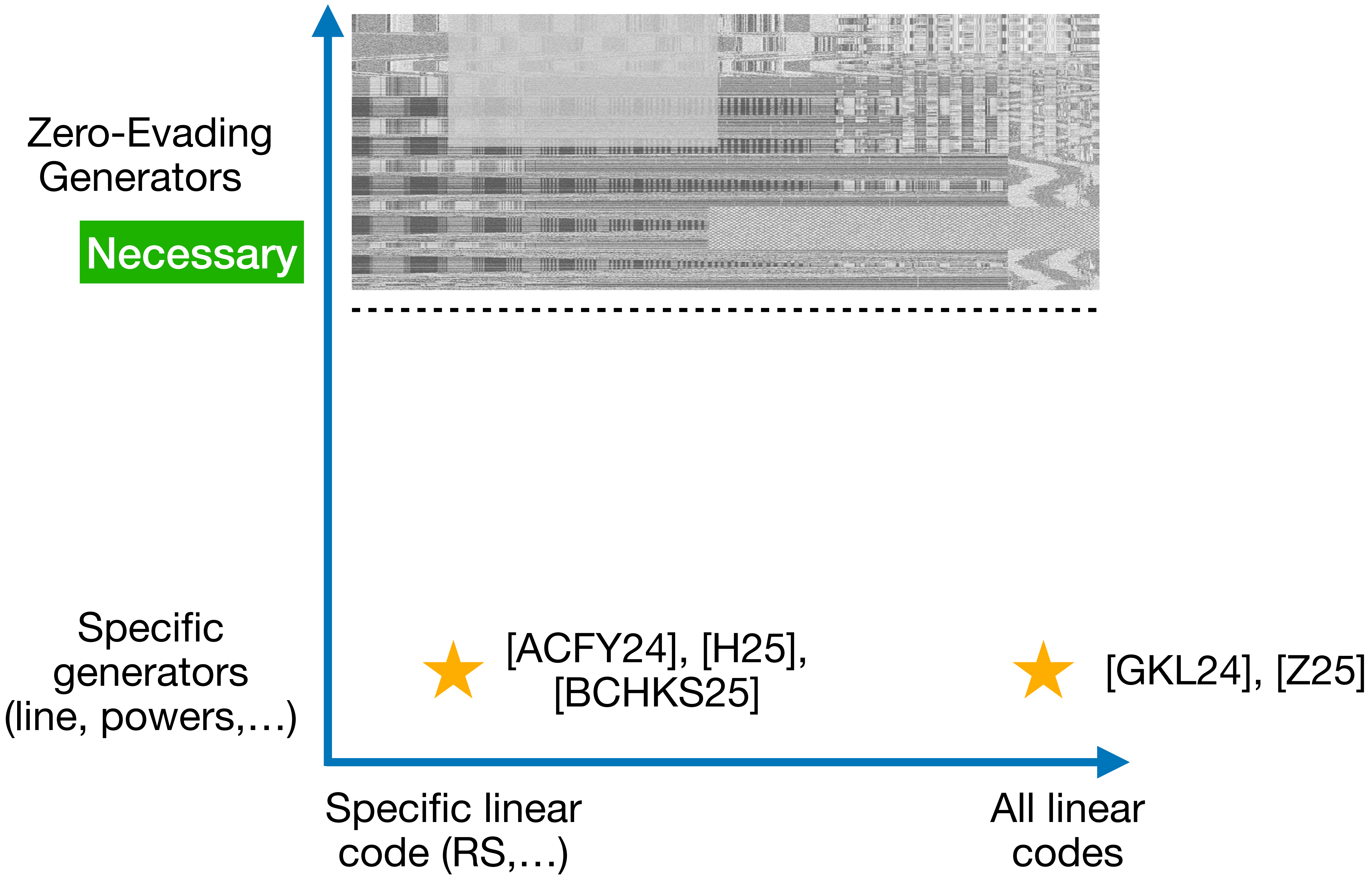
3. ***MCA Toolbox***

The new MCA landscape

The new MCA landscape



The new MCA landscape



The new MCA landscape

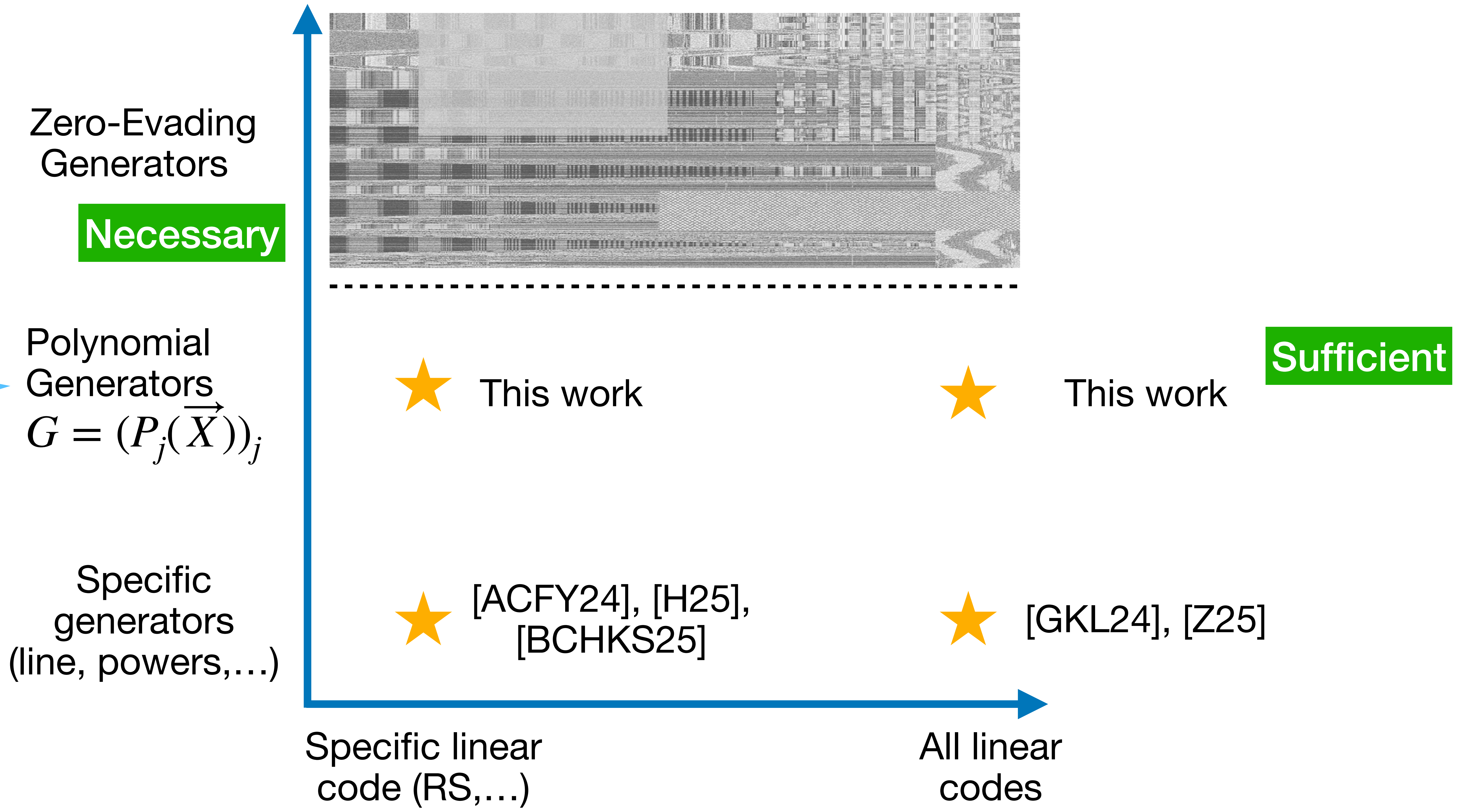
$\overrightarrow{X} \mapsto (\overrightarrow{X}^{\mathbf{v}})_{v \in \{0,1\}^s}$

$(X_1, \ldots, X_s) \mapsto (X_1, \ldots, X_s)$

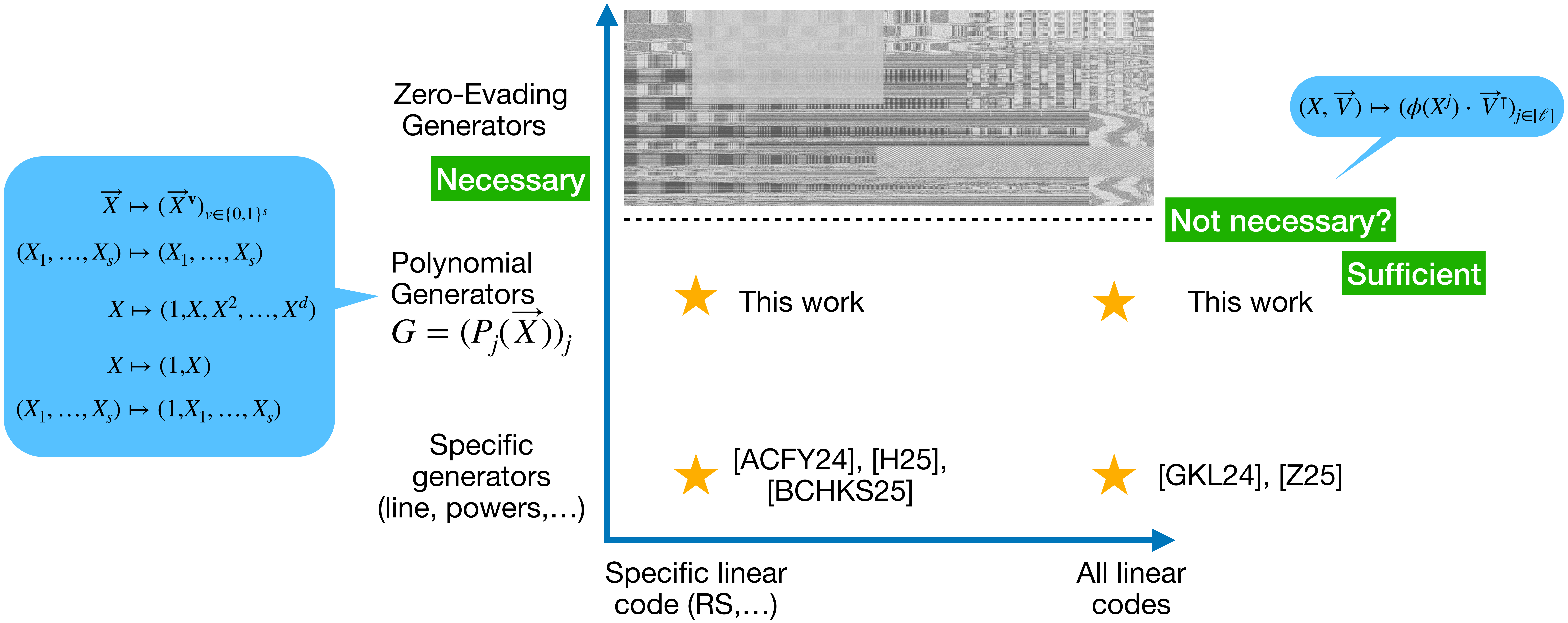
$X \mapsto (1, X, X^2, \ldots, X^d)$

$X \mapsto (1, X)$

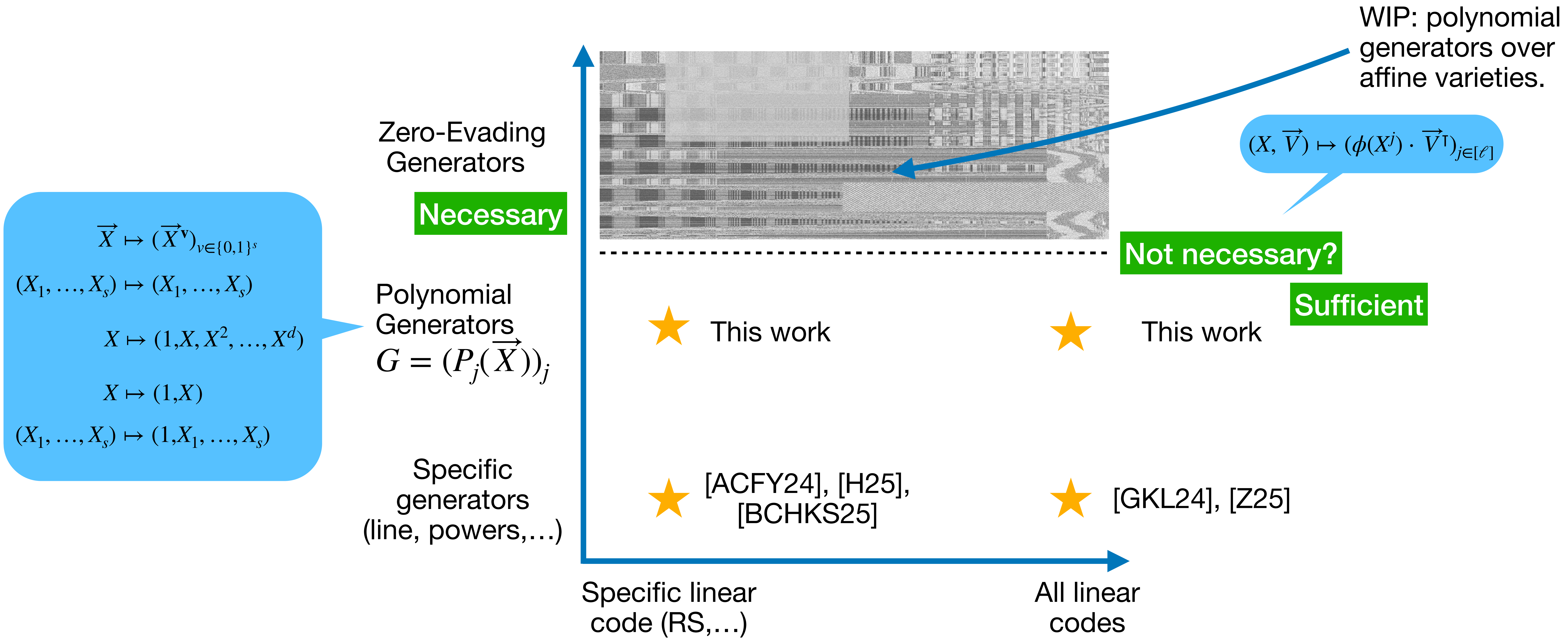
$(X_1, \ldots, X_s) \mapsto (1, X_1, \ldots, X_s)$



The new MCA landscape

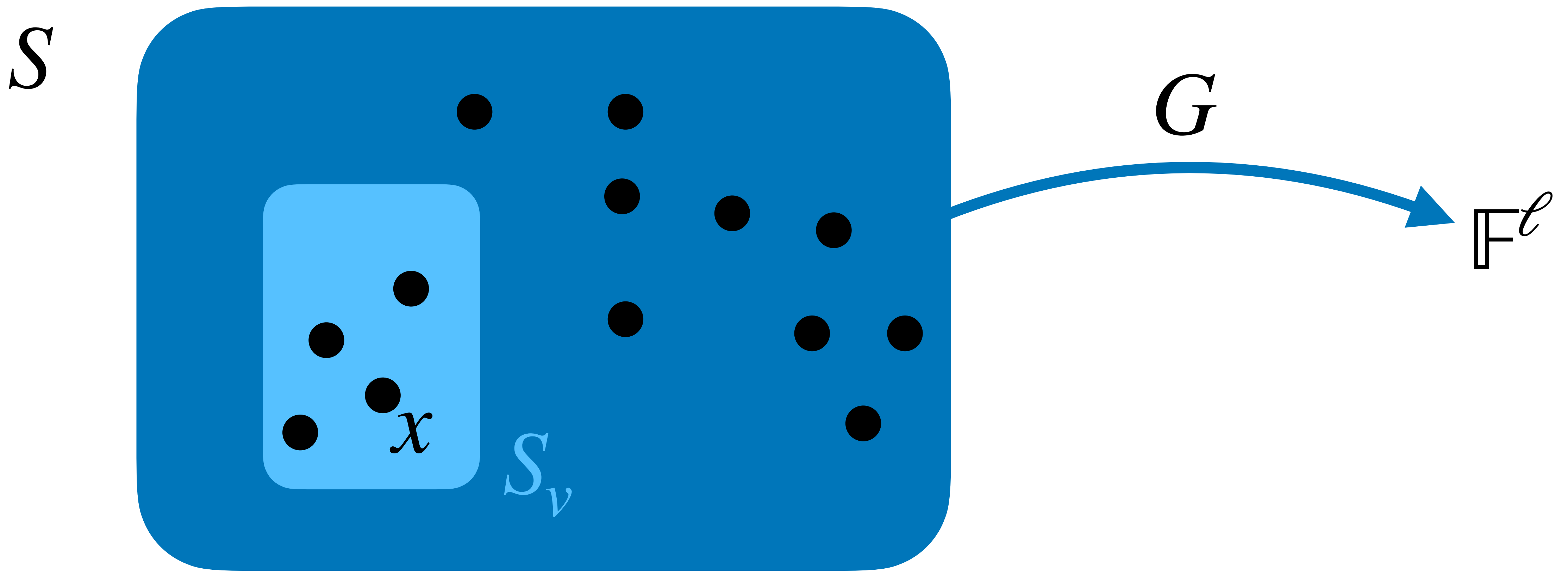


The new MCA landscape



ZE is Necessary

Zero-evading is necessary for MCA: $\epsilon_{ZE} \leq \epsilon_{MCA}$



$$S_v := \{x \mid G(x) \cdot v^\top = 0\} \quad (v \neq 0)$$

$$\max_{v \neq 0} |S_v| / |S| \leq \epsilon_{ZE}$$

ZE is Necessary

Zero-evading is necessary for MCA: $\epsilon_{ZE} \leq \epsilon_{MCA}$

$$\epsilon_{MCA}(0) = \Pr_{x \in S}\begin{bmatrix} G(x) \cdot \mathbf{U} \in \mathscr{C} \\ \vee_{j \in [\ell]} \mathbf{u}_j \notin \mathscr{C} \end{bmatrix}$$

ZE is Necessary

Zero-evading is necessary for MCA: $\epsilon_{ZE} \leq \epsilon_{MCA}$

proof: $\mathscr{C} \subseteq \mathbb{F}^n$ of codimension r, $M \in \mathbb{F}^{r \times n}$ parity check matrix.

$$\epsilon_{MCA}(0) = \Pr_{x \in S}\begin{bmatrix} G(x) \cdot \mathbf{U} \in \mathscr{C} \\ \vee_{j \in [\ell]} \mathbf{u}_j \notin \mathscr{C} \end{bmatrix}$$

ZE is Necessary

Zero-evading is necessary for MCA: $\epsilon_{ZE} \leq \epsilon_{MCA}$

proof: $\mathscr{C} \subseteq \mathbb{F}^n$ of codimension r, $M \in \mathbb{F}^{r \times n}$ parity check matrix.

$$\epsilon_{MCA}(0) = \Pr_{x \in S}\begin{bmatrix} G(x) \cdot \mathbf{U} \in \mathscr{C} \\ \vee_{j \in [\ell]} \mathbf{u}_j \notin \mathscr{C} \end{bmatrix}$$

Let $\mathbf{u}_1, \ldots, \mathbf{u}_\ell \in \mathbb{F}^n$ with some $\mathbf{u}_j \notin \mathscr{C}$, then $\mathbf{w}_j := M \cdot \mathbf{u}_j^\intercal \neq \vec{0}$.

ZE is Necessary

Zero-evading is necessary for MCA: $\epsilon_{ZE} \leq \epsilon_{MCA}$

proof: $\mathscr{C} \subseteq \mathbb{F}^n$ of codimension r, $M \in \mathbb{F}^{r \times n}$ parity check matrix.

$$\epsilon_{MCA}(0) = \Pr_{x \in S}\begin{bmatrix} G(x) \cdot \mathbf{U} \in \mathscr{C} \\ \vee_{j \in [\ell]} \mathbf{u}_j \notin \mathscr{C} \end{bmatrix}$$

Let $\mathbf{u}_1, \ldots, \mathbf{u}_\ell \in \mathbb{F}^n$ with some $\mathbf{u}_j \notin \mathscr{C}$, then $\mathbf{w}_j := M \cdot \mathbf{u}_j^\intercal \neq \vec{0}$.

$$\Pr_{x \in S}\begin{bmatrix} \sum_{j \in [\ell]} G(x)_j \cdot \mathbf{w}_j = \vec{0} \\ \vee_{j \in [\ell]} \mathbf{w}_j \neq \vec{0} \end{bmatrix} \leq \Pr_{x \in S}\left[G(x) \cdot \vec{v}^\intercal = 0\right] \leq \epsilon_{ZE}$$

∎

ZE is Necessary

Zero-evading is necessary for MCA: $\epsilon_{ZE} \leq \epsilon_{MCA}$

proof: $\mathscr{C} \subseteq \mathbb{F}^n$ of codimension r, $M \in \mathbb{F}^{r \times n}$ parity check matrix.

$$\epsilon_{MCA}(0) = \Pr_{x \in S}\begin{bmatrix} G(x) \cdot \mathbf{U} \in \mathscr{C} \\ \vee_{j \in [\ell]} \mathbf{u}_j \notin \mathscr{C} \end{bmatrix}$$

Let $\mathbf{u}_1, \ldots, \mathbf{u}_\ell \in \mathbb{F}^n$ with some $\mathbf{u}_j \notin \mathscr{C}$, then $\mathbf{w}_j := M \cdot \mathbf{u}_j^\intercal \neq \vec{0}$.

$$\Pr_{x \in S}\begin{bmatrix} \sum_{j \in [\ell]} G(x)_j \cdot \mathbf{w}_j = \vec{0} \\ \vee_{j \in [\ell]} \mathbf{w}_j \neq \vec{0} \end{bmatrix} \leq \Pr_{x \in S}\left[G(x) \cdot \vec{v}^\intercal = 0\right] \leq \epsilon_{ZE}$$

$\vec{v} = (\mathbf{w}_1[i], \ldots, \mathbf{w}_\ell[i])$
for $i \in [r]$ s.t. $\mathbf{w}_j[i] \neq 0$

$\blacksquare$

Polynomial is Sufficient

Polynomial is Sufficient

Linearly independent over $\mathbb{F}$

Polynomial generator $G(x_1, \ldots, x_s) = (P_1(x_1, \ldots, x_s), \ldots, P_\ell(x_1, \ldots, x_s))$

All polynomial generators have MCA for every linear code

Polynomial is Sufficient

Linearly independent over $\mathbb{F}$

Polynomial generator $G(x_1, \ldots, x_s) = (P_1(x_1, \ldots, x_s), \ldots, P_\ell(x_1, \ldots, x_s))$

All polynomial generators have MCA for every linear code

Pf sketch:

- Write $P_i(X_1, \ldots, X_s) = \sum_{\alpha_1,\ldots,\alpha_s} c_{\alpha_1,\ldots,\alpha_s} \cdot \prod_i X_i^{\alpha_i}$
- Have $G(X_1, \ldots, X_s) = \mathbf{A} \cdot \bigotimes_i (1, X_i, \ldots, X_i^{d_i})$

Polynomial is Sufficient

Linearly independent over $\mathbb{F}$

Polynomial generator $G(x_1, \ldots, x_s) = (P_1(x_1, \ldots, x_s), \ldots, P_\ell(x_1, \ldots, x_s))$

All polynomial generators have MCA for every linear code

Pf sketch:

- Write $P_i(X_1, \ldots, X_s) = \sum_{\alpha_1, \ldots, \alpha_s} c_{\alpha_1, \ldots, \alpha_s} \cdot \prod_i X_i^{\alpha_i}$
- Have $G(X_1, \ldots, X_s) = \mathbf{A} \cdot \bigotimes_i (1, X_i, \ldots, X_i^{d_i})$

Real primitive

Polynomial is Sufficient

Linearly independent over $\mathbb{F}$

Polynomial generator $G(x_1, \ldots, x_s) = (P_1(x_1, \ldots, x_s), \ldots, P_\ell(x_1, \ldots, x_s))$

All polynomial generators have MCA for every linear code

Pf sketch:

- Write $P_i(X_1, \ldots, X_s) = \sum_{\alpha_1, \ldots, \alpha_s} c_{\alpha_1, \ldots, \alpha_s} \cdot \prod_i X_i^{\alpha_i}$
- Have $G(X_1, \ldots, X_s) = \mathbf{A} \cdot \bigotimes_i (1, X_i, \ldots, X_i^{d_i})$

Prove both transformations interact "nicely" with MCA: toolbox for MCA

Real primitive

■

Polynomial is Sufficient

Linearly independent over $\mathbb{F}$

Polynomial generator $G(x_1, \ldots, x_s) = (P_1(x_1, \ldots, x_s), \ldots, P_\ell(x_1, \ldots, x_s))$

All polynomial generators have MCA for every linear code

Can specialize to RS codes and obtain MCA up to Johnson bound for all polynomial generators

Pf sketch:

- Write $P_i(X_1, \ldots, X_s) = \sum_{\alpha_1,\ldots,\alpha_s} c_{\alpha_1,\ldots,\alpha_s} \cdot \prod_i X_i^{\alpha_i}$
- Have $G(X_1, \ldots, X_s) = \mathbf{A} \cdot \bigotimes_i (1, X_i, \ldots, X_i^{d_i})$

Prove both transformations interact "nicely" with MCA: toolbox for MCA

Real primitive

■

Lower Bounds for MCA

$G(x_1, \ldots, x_s) = (P_1(x_1, \ldots, x_s), \ldots, P_\ell(x_1, \ldots, x_s))$, and $d_i := \max_j \{\deg_{X_i}(P_j)\}$

$$\epsilon_{MCA}(\gamma) = \max\{n \cdot \gamma, 1\} \cdot \sum_i \frac{d_i}{|\mathbb{F}|} \quad \text{if } \gamma < \min_i\{\frac{\delta_{\mathscr{C}}}{d_i + 2}\}$$

Lower Bounds for MCA

$$G(x_1, \ldots, x_s) = (P_1(x_1, \ldots, x_s), \ldots, P_\ell(x_1, \ldots, x_s)),$$ and $$d_i := \max_j \{\deg_{X_i}(P_j)\}$$

$$\epsilon_{MCA}(\gamma) = \max\{n \cdot \gamma, 1\} \cdot \sum_i \frac{d_i}{|\mathbb{F}|}$$ if $$\gamma < \min_i \{\frac{\delta_{\mathscr{C}}}{d_i + 2}\}$$

Minimum distance

Lower Bounds for MCA

$G(x_1, \ldots, x_s) = (P_1(x_1, \ldots, x_s), \ldots, P_\ell(x_1, \ldots, x_s))$, and $d_i := \max_j \{\deg_{X_i}(P_j)\}$

$$\epsilon_{MCA}(\gamma) = \max\{n \cdot \gamma, 1\} \cdot \sum_i \frac{d_i}{|\mathbb{F}|} \quad \text{if } \gamma < \min_i\{\frac{\delta_{\mathscr{C}}}{d_i + 2}\}$$

Minimum distance

$\Rightarrow$ for $\gamma \leq \delta_{\mathscr{C}}/(d+2)$, $G_d(x) = (1, x, \ldots, x^d)$ has MCA error $\leq n \cdot \gamma \cdot d/|\mathbb{F}|$.

Matching lower bound: $\exists$ code s.t. when $\gamma \leq \delta_{\mathscr{C}}/2$, the MCA error of G_d is $\geq n \cdot \gamma \cdot d/|\mathbb{F}|$.

Lower Bounds for MCA

$G(x_1, \ldots, x_s) = (P_1(x_1, \ldots, x_s), \ldots, P_\ell(x_1, \ldots, x_s))$, and $d_i := \max_j \{\deg_{X_i}(P_j)\}$

$$\epsilon_{MCA}(\gamma) = \max\{n \cdot \gamma, 1\} \cdot \sum_i \frac{d_i}{|\mathbb{F}|} \quad \text{if } \gamma < \min_i \{\frac{\delta_{\mathscr{C}}}{d_i + 2}\}$$

Minimum distance

$\Rightarrow$ for $\gamma \leq \delta_{\mathscr{C}}/(d+2)$, $G_d(x) = (1, x, \ldots, x^d)$ has MCA error $\leq n \cdot \gamma \cdot d/|\mathbb{F}|$.

Matching lower bound: $\exists$ code s.t. when $\gamma \leq \delta_{\mathscr{C}}/2$, the MCA error of G_d is $\geq n \cdot \gamma \cdot d/|\mathbb{F}|$.

Can we close the gap?

MCA Toolbox

MCA Toolbox

Linear transformation

$$G : S \to \mathbb{F}^\ell$$

$$G' := \mathbf{A} \cdot G$$

MCA Toolbox

Linear transformation

$$G : S \to \mathbb{F}^{\ell}$$

$$G' := \mathbf{A} \cdot G$$

MCA error is preserved exactly

MCA Toolbox

Linear transformation

$$G \colon S \to \mathbb{F}^{\ell}$$

$$G' := \mathbf{A} \cdot G$$

MCA error is preserved exactly

Tensor products

$$G_1 \colon S_1 \to \mathbb{F}^{\ell},\ G_2 \colon S_2 \to \mathbb{F}^{\ell}$$

$$G' := G_1 \otimes G_2$$

MCA Toolbox

Linear transformation

$$G : S \to \mathbb{F}^\ell$$

$$G' := \mathbf{A} \cdot G$$

MCA error is preserved exactly

Tensor products

$$G_1 : S_1 \to \mathbb{F}^\ell,\ G_2 : S_2 \to \mathbb{F}^\ell$$

$$G' := G_1 \otimes G_2$$

MCA errors sum

MCA Toolbox

Linear transformation

$$G\colon S \to \mathbb{F}^{\ell}$$

$$G' := \mathbf{A} \cdot G$$

MCA error is preserved exactly

Tensor products

$$G_1\colon S_1 \to \mathbb{F}^{\ell},\ G_2\colon S_2 \to \mathbb{F}^{\ell}$$

$$G' := G_1 \otimes G_2$$

MCA errors sum

Affine space

$$(x_1, \ldots, x_s) \mapsto (1, x_1, \ldots, x_s) \approx_{\mathbf{MCA}} x \mapsto (1, x)$$

Independent of s

MCA Toolbox

Linear transformation

$$G : S \to \mathbb{F}^{\ell}$$

$$G' := \mathbf{A} \cdot G$$

MCA error is preserved exactly

Tensor products

$$G_1 : S_1 \to \mathbb{F}^{\ell},\ G_2 : S_2 \to \mathbb{F}^{\ell}$$

$$G' := G_1 \otimes G_2$$

MCA errors sum

Affine space

$$(x_1, \ldots, x_s) \mapsto (1, x_1, \ldots, x_s) \approx_{\mathbf{MCA}} x \mapsto (1, x)$$

Independent of s

Matrix-vector product

Can show the generator from [AGHP92] has good MCA error

AGHP Generator

AGHP Generator

$\mathbb{F}_q \subseteq \mathbb{F}_{q^k}$ with $\phi\colon \mathbb{F}_{q^k} \xrightarrow{\simeq} \mathbb{F}_q^k$, and $G\colon \mathbb{F}_{q^k} \times \mathbb{F}_q^k \to \mathbb{F}_q^\ell$ s.t.

$$G(x, \vec{v}) = ((\phi(x^i)) \cdot \vec{y}^\intercal)_{i \in [\ell]}$$

AGHP Generator

$\mathbb{F}_q \subseteq \mathbb{F}_{q^k}$ with $\phi\colon \mathbb{F}_{q^k} \xrightarrow{\simeq} \mathbb{F}_q^k$, and $G\colon \mathbb{F}_{q^k} \times \mathbb{F}_q^k \to \mathbb{F}_q^\ell$ s.t.

$$G(x, \vec{v}) = ((\phi(x^i)) \cdot \vec{y}^\intercal)_{i\in[\ell]}$$

$$G_\ell(x) = (x, \ldots, x^\ell)$$

AGHP Generator

$\mathbb{F}_q \subseteq \mathbb{F}_{q^k}$ with $\phi \colon \mathbb{F}_{q^k} \xrightarrow{\simeq} \mathbb{F}_q^k$, and $G \colon \mathbb{F}_{q^k} \times \mathbb{F}_q^k \to \mathbb{F}_q^\ell$ s.t.

$$G(x, \vec{v}) = ((\phi(x^i)) \cdot \vec{y}^\intercal)_{i \in [\ell]}$$

$G_\ell(x) = (x, \ldots, x^\ell)$

$G_{\mathsf{aff}}(\vec{y}) = \vec{y}$

AGHP Generator

$\mathbb{F}_q \subseteq \mathbb{F}_{q^k}$ with $\phi \colon \mathbb{F}_{q^k} \xrightarrow{\simeq} \mathbb{F}_q^k$, and $G \colon \mathbb{F}_{q^k} \times \mathbb{F}_q^k \to \mathbb{F}_q^\ell$ s.t.

$$G(x, \vec{v}) = ((\phi(x^i)) \cdot \vec{y}^\intercal)_{i \in [\ell]}$$

$G_\ell(x) = (x, \ldots, x^\ell)$

$G_{\mathsf{aff}}(\vec{y}) = \vec{y}$

MCA error is $\sim \dfrac{1}{q} + \dfrac{\ell}{q^k}$

AGHP Generator

$\mathbb{F}_q \subseteq \mathbb{F}_{q^k}$ with $\phi \colon \mathbb{F}_{q^k} \xrightarrow{\simeq} \mathbb{F}_q^k$, and $G \colon \mathbb{F}_{q^k} \times \mathbb{F}_q^k \to \mathbb{F}_q^\ell$ s.t.

$$G(x, \vec{v}) = ((\phi(x^i)) \cdot \vec{y}^\intercal)_{i \in [\ell]}$$

$G_\ell(x) = (x, \ldots, x^\ell)$

$G_{\mathsf{aff}}(\vec{y}) = \vec{y}$

MCA error is $\sim \dfrac{1}{q} + \dfrac{\ell}{q^k}$

Surprising:

AGHP Generator

$\mathbb{F}_q \subseteq \mathbb{F}_{q^k}$ with $\phi \colon \mathbb{F}_{q^k} \xrightarrow{\simeq} \mathbb{F}_q^k$, and $G \colon \mathbb{F}_{q^k} \times \mathbb{F}_q^k \to \mathbb{F}_q^\ell$ s.t.

$$G(x, \vec{v}) = ((\phi(x^i)) \cdot \vec{y}^\intercal)_{i \in [\ell]}$$

$G_\ell(x) = (x, \ldots, x^\ell)$

$G_{\mathsf{aff}}(\vec{y}) = \vec{y}$

MCA error is $\sim \dfrac{1}{q} + \dfrac{\ell}{q^k}$

Surprising:

1. using polynomial result over $\mathbb{F}_q$, error $\sim \dfrac{k \cdot \min\{q, \ell\}}{q}$

AGHP Generator

$\mathbb{F}_q \subseteq \mathbb{F}_{q^k}$ with $\phi : \mathbb{F}_{q^k} \xrightarrow{\simeq} \mathbb{F}_q^k$, and $G : \mathbb{F}_{q^k} \times \mathbb{F}_q^k \to \mathbb{F}_q^\ell$ s.t.

$$G(x, \vec{v}) = ((\phi(x^i)) \cdot \vec{y}^\intercal)_{i \in [\ell]}$$

$G_\ell(x) = (x, \ldots, x^\ell)$

$G_{\mathsf{aff}}(\vec{y}) = \vec{y}$

MCA error is $\sim \dfrac{1}{q} + \dfrac{\ell}{q^k}$

Surprising:

1. using polynomial result over $\mathbb{F}_q$, error $\sim \dfrac{k \cdot \min\{q, \ell\}}{q}$

2. over $\mathbb{F}_{q^k}$, $\phi(x^i)_j = \mathrm{tr}(\beta_j x^i) = \sum_{m=0}^{k-1} (\beta_j x^i)^{q^m}$, distance $\sim \dfrac{\delta_{\mathscr{C}}}{\ell\, q^{k-1}}$

AGHP Generator

AGHP Generator

$\mathbb{F}_q \subseteq \mathbb{F}_{q^k}$ with $\phi\colon \mathbb{F}_{q^k} \xrightarrow{\simeq} \mathbb{F}_q^k$, and $G\colon \mathbb{F}_{q^k} \times \mathbb{F}_q^k \to \mathbb{F}_q^\ell$ s.t.

$$G(x, \vec{v}) = ((\phi(x^i)) \cdot \vec{y}^\intercal)_{i \in [\ell]}$$

AGHP Generator

$\mathbb{F}_q \subseteq \mathbb{F}_{q^k}$ with $\phi\colon \mathbb{F}_{q^k} \xrightarrow{\simeq} \mathbb{F}_q^k$, and $G\colon \mathbb{F}_{q^k} \times \mathbb{F}_q^k \to \mathbb{F}_q^\ell$ s.t.

$$G(x, \vec{v}) = ((\phi(x^i)) \cdot \vec{y}^\intercal)_{i \in [\ell]}$$

proof:

AGHP Generator

$$\mathbb{F}_q \subseteq \mathbb{F}_{q^k} \text{ with } \phi\colon \mathbb{F}_{q^k} \xrightarrow{\simeq} \mathbb{F}_q^k, \text{ and } G\colon \mathbb{F}_{q^k} \times \mathbb{F}_q^k \to \mathbb{F}_q^\ell \text{ s.t.}$$

$$G(x, \vec{v}) = ((\phi(x^i)) \cdot \vec{y}^\intercal)_{i \in [\ell]}$$

proof: $\forall \mathbf{U} := (\mathbf{u}_1, \ldots, \mathbf{u}_\ell) \in \mathbb{F}^{\ell \times n}$ need to bound probability of

AGHP Generator

$$\mathbb{F}_q \subseteq \mathbb{F}_{q^k} \text{ with } \phi\colon \mathbb{F}_{q^k} \xrightarrow{\simeq} \mathbb{F}_q^k, \text{ and } G\colon \mathbb{F}_{q^k} \times \mathbb{F}_q^k \to \mathbb{F}_q^\ell \text{ s.t.}$$

$$G(x, \vec{v}) = ((\phi(x^i)) \cdot \vec{y}^\intercal)_{i \in [\ell]}$$

proof: $\forall \mathbf{U} := (\mathbf{u}_1, \ldots, \mathbf{u}_\ell) \in \mathbb{F}^{\ell \times n}$ need to bound probability of

$$\left[\begin{array}{l} \exists T \subseteq [n], \quad |T| \geq (1-\gamma) \cdot n \\ \qquad\qquad (\sum_{j \in [k]} y_j \sum_{i \in [\ell]} \phi(x^i)_j \cdot \mathbf{u}_i)|_T \in \mathscr{C}|_T \\ \qquad\qquad \exists i \in [\ell], \mathbf{u}_i|_T \notin \mathscr{C}|_T \end{array}\right]$$

AGHP Generator

$$\mathbb{F}_q \subseteq \mathbb{F}_{q^k} \text{ with } \phi\colon \mathbb{F}_{q^k} \xrightarrow{\simeq} \mathbb{F}_q^k, \text{ and } G\colon \mathbb{F}_{q^k} \times \mathbb{F}_q^k \to \mathbb{F}_q^\ell \text{ s.t.}$$
$$G(x, \vec{v}) = ((\phi(x^i)) \cdot \vec{y}^\intercal)_{i\in[\ell]}$$

proof: $\forall \mathbf{U} := (\mathbf{u}_1, \ldots, \mathbf{u}_\ell) \in \mathbb{F}^{\ell\times n}$ need to bound probability of

$$\left[\begin{array}{l} \exists T \subseteq [n], \quad |T| \geq (1-\gamma)\cdot n \\ \qquad (\sum_{j\in[k]} y_j \sum_{i\in[\ell]} \phi(x^i)_j \cdot \mathbf{u}_i)|_T \in \mathscr{C}|_T \\ \qquad \exists i \in [\ell], \mathbf{u}_i|_T \notin \mathscr{C}|_T \end{array}\right]$$

$$\left[\begin{array}{l} \exists T \subseteq [n], \quad |T| \geq (1-\gamma)\cdot n \\ \qquad (\sum_{j\in[k]} y_j \sum_{i\in[\ell]} \phi(x^i)_j \cdot \mathbf{u}_i)|_T \in \mathscr{C}|_T \\ \qquad \exists j \in [k], (\sum_{i\in[\ell]} \phi(x^i)_j \cdot \mathbf{u}_i)|_T \notin \mathscr{C}|_T \end{array}\right] \vee \left[\begin{array}{l} \exists T \subseteq [n], \quad |T| \geq (1-\gamma)\cdot n \\ \qquad \forall j \in [k], (\sum_{i\in[\ell]} \phi(x^i)_j \cdot \mathbf{u}_i)|_T \in \mathscr{C}|_T \\ \qquad \exists i \in [\ell], \mathbf{u}_i|_T \notin \mathscr{C}|_T \end{array}\right]$$

AGHP Generator

$$\mathbb{F}_q \subseteq \mathbb{F}_{q^k} \text{ with } \phi\colon \mathbb{F}_{q^k} \xrightarrow{\simeq} \mathbb{F}_q^k, \text{ and } G\colon \mathbb{F}_{q^k} \times \mathbb{F}_q^k \to \mathbb{F}_q^\ell \text{ s.t.}$$
$$G(x, \vec{v}) = ((\phi(x^i)) \cdot \vec{y}^\intercal)_{i \in [\ell]}$$

proof: $\forall \mathbf{U} := (\mathbf{u}_1, \ldots, \mathbf{u}_\ell) \in \mathbb{F}^{\ell \times n}$ need to bound probability of

$$\begin{bmatrix} \exists T \subseteq [n], \quad |T| \geq (1-\gamma) \cdot n \\ (\sum_{j\in[k]} y_j \sum_{i\in[\ell]} \phi(x^i)_j \cdot \mathbf{u}_i)|_T \in \mathscr{C}|_T \\ \exists i \in [\ell], \mathbf{u}_i|_T \notin \mathscr{C}|_T \end{bmatrix}$$

$$\begin{bmatrix} \exists T \subseteq [n], \quad |T| \geq (1-\gamma) \cdot n \\ (\sum_{j\in[k]} y_j \sum_{i\in[\ell]} \phi(x^i)_j \cdot \mathbf{u}_i)|_T \in \mathscr{C}|_T \\ \exists j \in [k], (\sum_{i\in[\ell]} \phi(x^i)_j \cdot \mathbf{u}_i)|_T \notin \mathscr{C}|_T \end{bmatrix} \vee \begin{bmatrix} \exists T \subseteq [n], \quad |T| \geq (1-\gamma) \cdot n \\ \forall j \in [k], (\sum_{i\in[\ell]} \phi(x^i)_j \cdot \mathbf{u}_i)|_T \in \mathscr{C}|_T \\ \exists i \in [\ell], \mathbf{u}_i|_T \notin \mathscr{C}|_T \end{bmatrix}$$

MCA of $G_{\mathsf{aff}}(\vec{v}) = \vec{v}$

AGHP Generator

AGHP Generator

$$\begin{bmatrix} \exists T \subseteq [n], \quad |T| \geq (1-\gamma)\cdot n \\ \qquad \forall j \in [k], (\sum_{i\in[\ell]} \phi(x^i)_j \cdot \mathbf{u}_i)|_T \in \mathscr{C}|_T \\ \qquad \exists i \in [\ell], \mathbf{u}_i|_T \notin \mathscr{C}|_T \end{bmatrix}$$

AGHP Generator

$$\left[\begin{array}{l} \exists T \subseteq [n], \quad |T| \geq (1-\gamma)\cdot n \\ \qquad\qquad \forall j \in [k], (\sum_{i\in[\ell]} \phi(x^i)_j \cdot \mathbf{u}_i)|_T \in \mathscr{C}|_T \\ \qquad\qquad \exists i \in [\ell], \mathbf{u}_i|_T \notin \mathscr{C}|_T \end{array}\right]$$

Observation 1: $((x^i)_{i\in[\ell]} \cdot \mathrm{U})|_T = (\sum_j \sum_i \phi(x^i)_j \alpha_j \mathbf{u}_i)|_T \in (\mathscr{C} \otimes \mathbb{F}_{q^k})|_T$

AGHP Generator

$$\left[\begin{array}{l} \exists T \subseteq [n], \quad |T| \geq (1-\gamma)\cdot n \\ \qquad\qquad \forall j \in [k], (\sum_{i\in[\ell]} \phi(x^i)_j \cdot \mathbf{u}_i)|_T \in \mathscr{C}|_T \\ \qquad\qquad \exists i \in [\ell], \mathbf{u}_i|_T \notin \mathscr{C}|_T \end{array}\right]$$

Observation 1: $((x^i)_{i\in[\ell]} \cdot \mathbf{U})|_T = (\sum_j \sum_i \phi(x^i)_j \alpha_j \mathbf{u}_i)|_T \in (\mathscr{C} \otimes \mathbb{F}_{q^k})|_T$

Observation 2: $\mathbf{u}_i \notin \mathscr{C}|_T \implies \mathbf{u}_i \notin (\mathscr{C} \otimes \mathbb{F}_{q^k})|_T$

AGHP Generator

$$\begin{bmatrix} \exists T \subseteq [n], \quad |T| \geq (1-\gamma)\cdot n \\ \forall j \in [k], (\sum_{i\in[\ell]} \phi(x^i)_j \cdot \mathbf{u}_i)|_T \in \mathscr{C}|_T \\ \exists i \in [\ell], \mathbf{u}_i|_T \notin \mathscr{C}|_T \end{bmatrix}$$

Observation 1: $((x^i)_{i\in[\ell]} \cdot \mathrm{U})|_T = (\sum_j \sum_i \phi(x^i)_j \alpha_j \mathbf{u}_i)|_T \in (\mathscr{C} \otimes \mathbb{F}_{q^k})|_T$

Observation 2: $\mathbf{u}_i \notin \mathscr{C}|_T \implies \mathbf{u}_i \notin (\mathscr{C} \otimes \mathbb{F}_{q^k})|_T$

$$\begin{bmatrix} \exists T \subseteq [n], \quad |T| \geq (1-\gamma)\cdot n \\ ((x^i)_{i\in[\ell]} \cdot \mathrm{U})|_T \in (\mathscr{C} \otimes \mathbb{F}_{q^k})|_T \\ \exists i \in [\ell], \mathbf{u}_i|_T \notin (\mathscr{C} \otimes \mathbb{F}_{q^k})|_T \end{bmatrix}$$

AGHP Generator

$$\begin{bmatrix} \exists T \subseteq [n], \quad |T| \geq (1-\gamma)\cdot n \\ \forall j \in [k], (\sum_{i\in[\ell]} \phi(x^i)_j \cdot \mathbf{u}_i)|_T \in \mathscr{C}|_T \\ \exists i \in [\ell], \mathbf{u}_i|_T \notin \mathscr{C}|_T \end{bmatrix}$$

Observation 1: $((x^i)_{i\in[\ell]} \cdot \mathrm{U})|_T = (\sum_j \sum_i \phi(x^i)_j \alpha_j \mathbf{u}_i)|_T \in (\mathscr{C} \otimes \mathbb{F}_{q^k})|_T$

Observation 2: $\mathbf{u}_i \notin \mathscr{C}|_T \implies \mathbf{u}_i \notin (\mathscr{C} \otimes \mathbb{F}_{q^k})|_T$

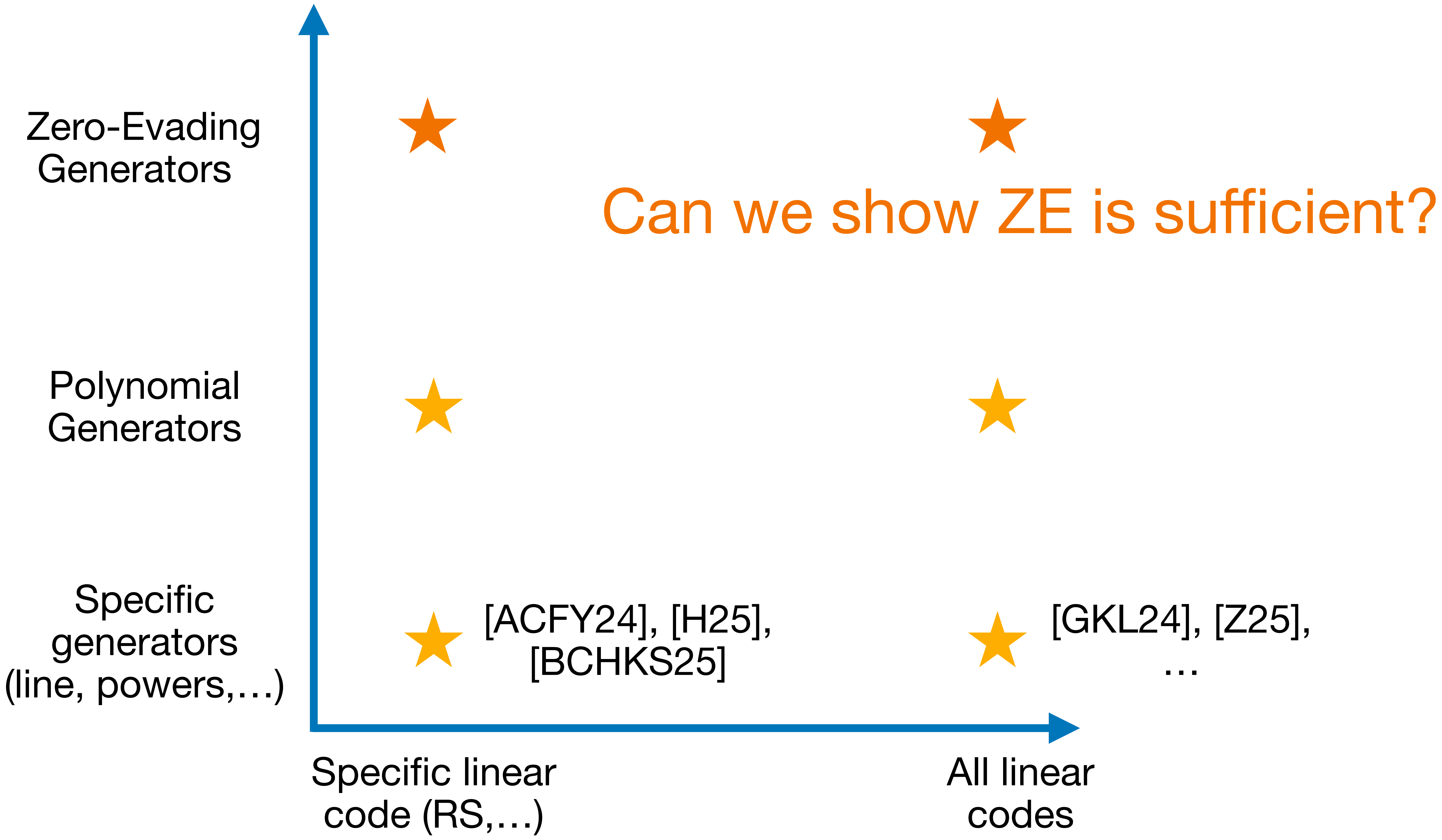
$$\begin{bmatrix} \exists T \subseteq [n], \quad |T| \geq (1-\gamma)\cdot n \\ ((x^i)_{i\in[\ell]} \cdot \mathrm{U})|_T \in (\mathscr{C} \otimes \mathbb{F}_{q^k})|_T \\ \exists i \in [\ell], \mathbf{u}_i|_T \notin (\mathscr{C} \otimes \mathbb{F}_{q^k})|_T \end{bmatrix}$$

Use univariate powers MCA over extended code

$\blacksquare$

Open Problems & Discussion

A Complete Characterization?



Is Structure Necessary?

Random generator: a uniformly random element of the set of functions $S \to \mathbb{F}^\ell$

Can show: w.p. $\geq 1 - \delta$ random generator has $\epsilon_{\mathrm{ZE}} \leq 1/|\mathbb{F}| + \mathrm{err}(\delta, |\mathbb{F}|, |S|)$

Is Structure Necessary?

Random generator: a uniformly random element of the set of functions $S \to \mathbb{F}^{\ell}$

Can show: w.p. $\geq 1 - \delta$ random generator has $\epsilon_{\mathrm{ZE}} \leq 1/|\mathbb{F}| + \mathrm{err}(\delta, |\mathbb{F}|, |S|)$

Does a random generator have MCA with high probability?

Can We Go Beyond Johnson?

$\gamma = 0$ $\gamma = \delta_{\mathscr{C}}$

Can We Go Beyond Johnson?

Multilinear generators
and arbitrary linear codes

$\gamma = 0$

$\gamma = 1 - (1 - \delta_{\mathscr{C}})^{1/3}$

$\gamma = \delta_{\mathscr{C}}$

Can We Go Beyond Johnson?

Multilinear generators
and arbitrary linear codes

Polynomial generators
and RS codes

$\gamma = 0$

$\gamma = 1 - (1 - \delta_{\mathscr{C}})^{1/3}$

$\gamma = 1 - (1 - \delta_{\mathscr{C}})^{1/2}$

$\gamma = \delta_{\mathscr{C}}$

Can We Go Beyond Johnson?

Multilinear generators and arbitrary linear codes

Polynomial generators and RS codes

Can we show something here?

$\gamma = 0$

$\gamma = 1 - (1 - \delta_{\mathscr{C}})^{1/3}$

$\gamma = 1 - (1 - \delta_{\mathscr{C}})^{1/2}$

$\gamma = \delta_{\mathscr{C}}$

Can We Go Beyond Johnson?

The Proximity Prize

initiative by
ethereum foundation

$1,000,000

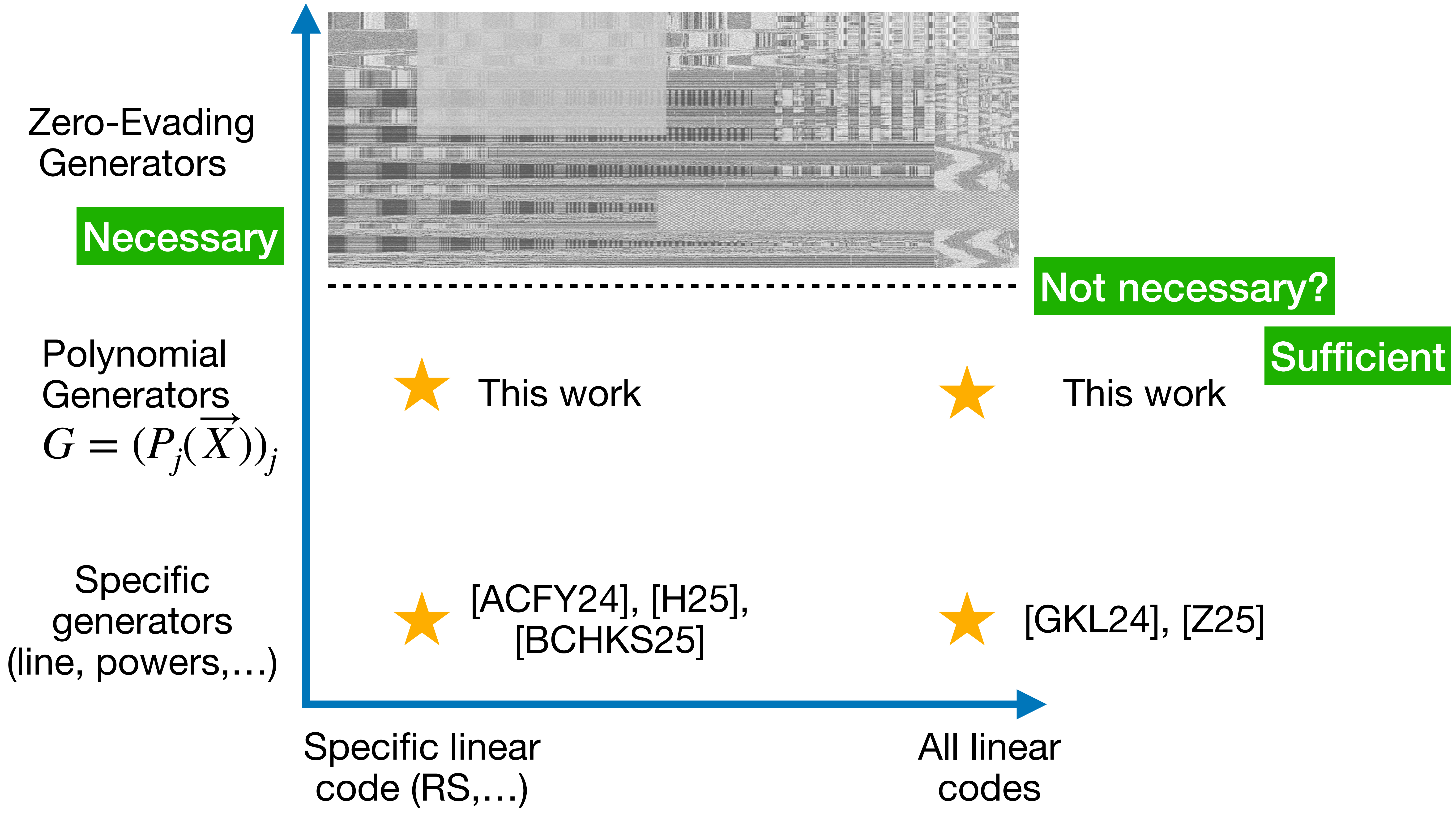
in prizes to prove (or disprove!) Reed-Solomon proximity gaps conjectures—more info soonTM

An initiative by the Ethereum Foundation to advance the foundations of modern zkVMs.

$\gamma = 0$

$\gamma = \delta_{\mathscr{C}}$

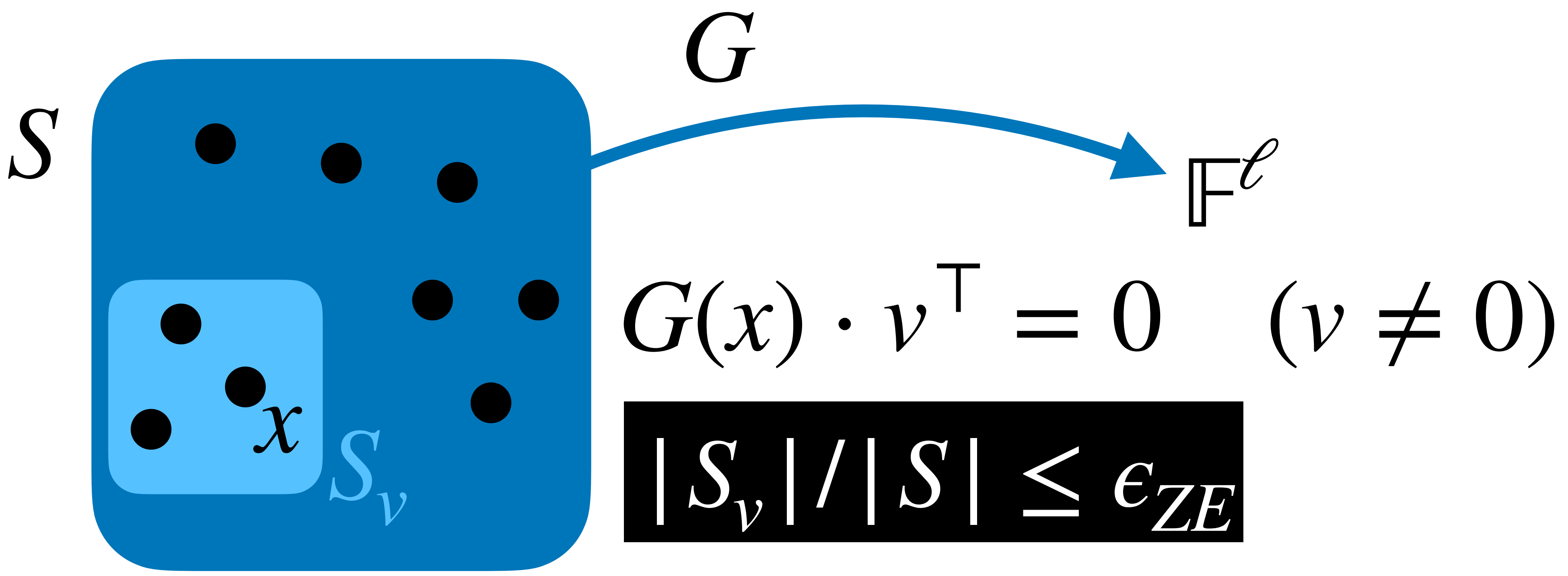
Recap



Thanks!

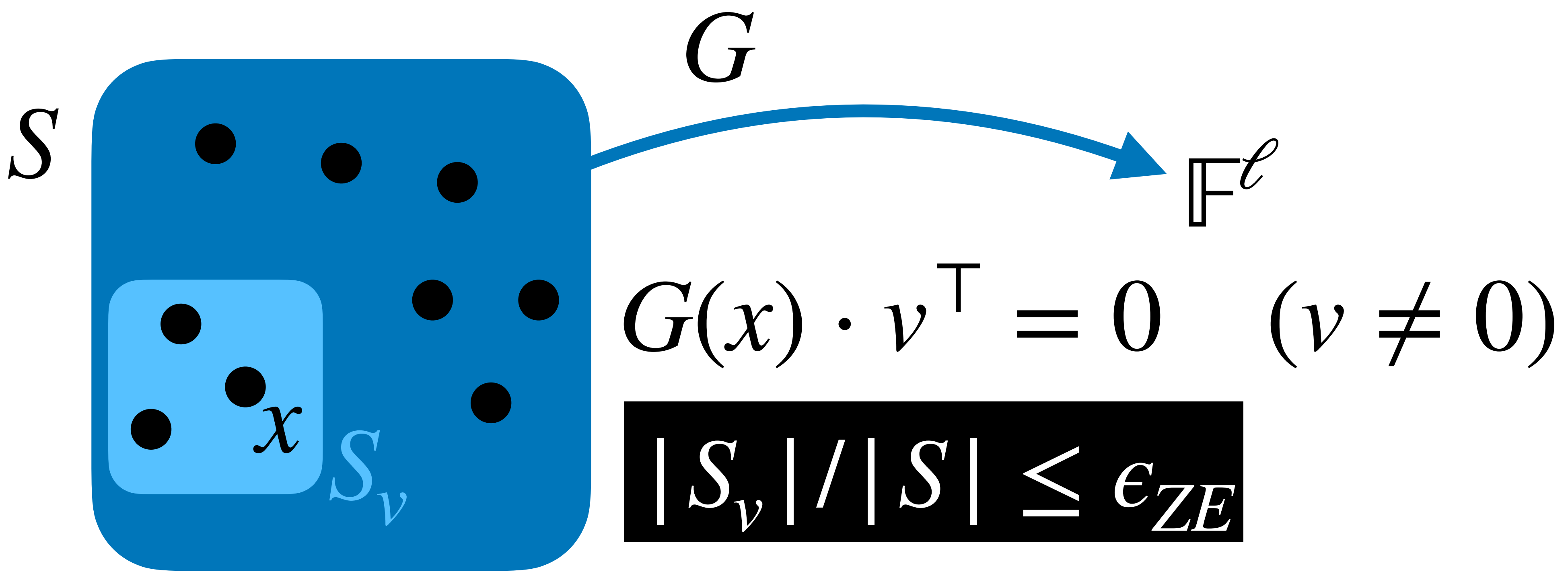
ZE is Necessary

Zero-evading is necessary for MCA: $\epsilon_{ZE} \leq \epsilon_{MCA}$



ZE is Necessary

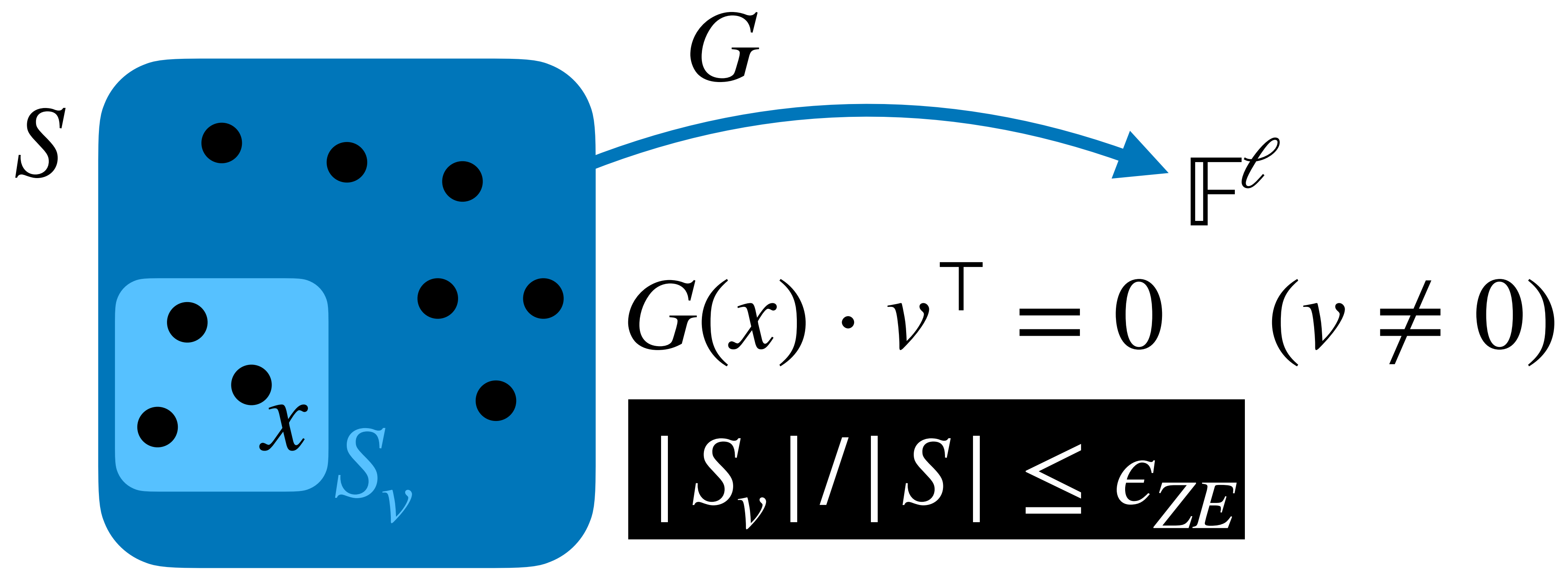
Zero-evading is necessary for MCA: $\epsilon_{ZE} \leq \epsilon_{MCA}$



Pf sketch:

ZE is Necessary

Zero-evading is necessary for MCA: $\epsilon_{ZE} \leq \epsilon_{MCA}$

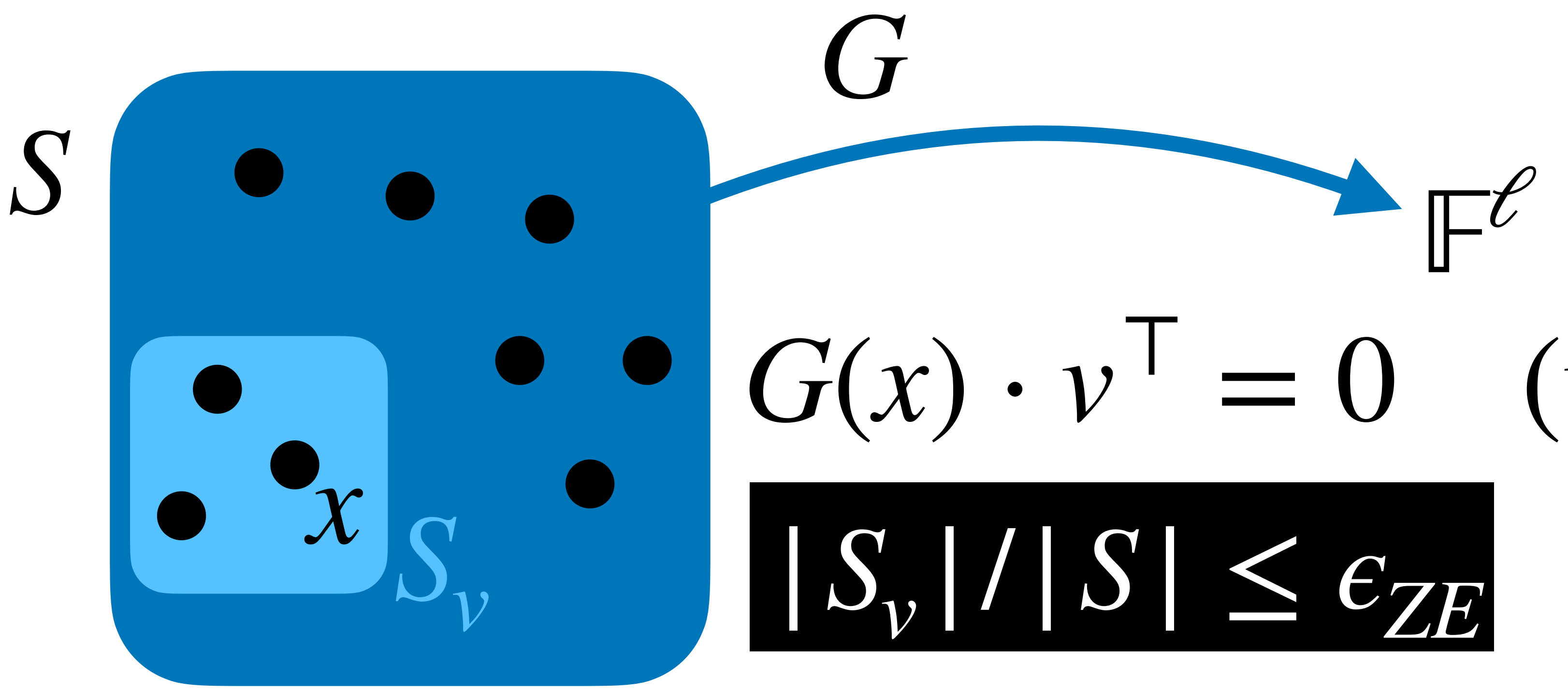


Pf sketch:

- Sufficient to show $\epsilon_{ZE} \leq \epsilon_{MCA}(0)$

ZE is Necessary

Zero-evading is necessary for MCA: $\epsilon_{ZE} \leq \epsilon_{MCA}$



$G(x) \cdot v^\top = 0 \quad (v \neq 0)$

$|S_v|/|S| \leq \epsilon_{ZE}$

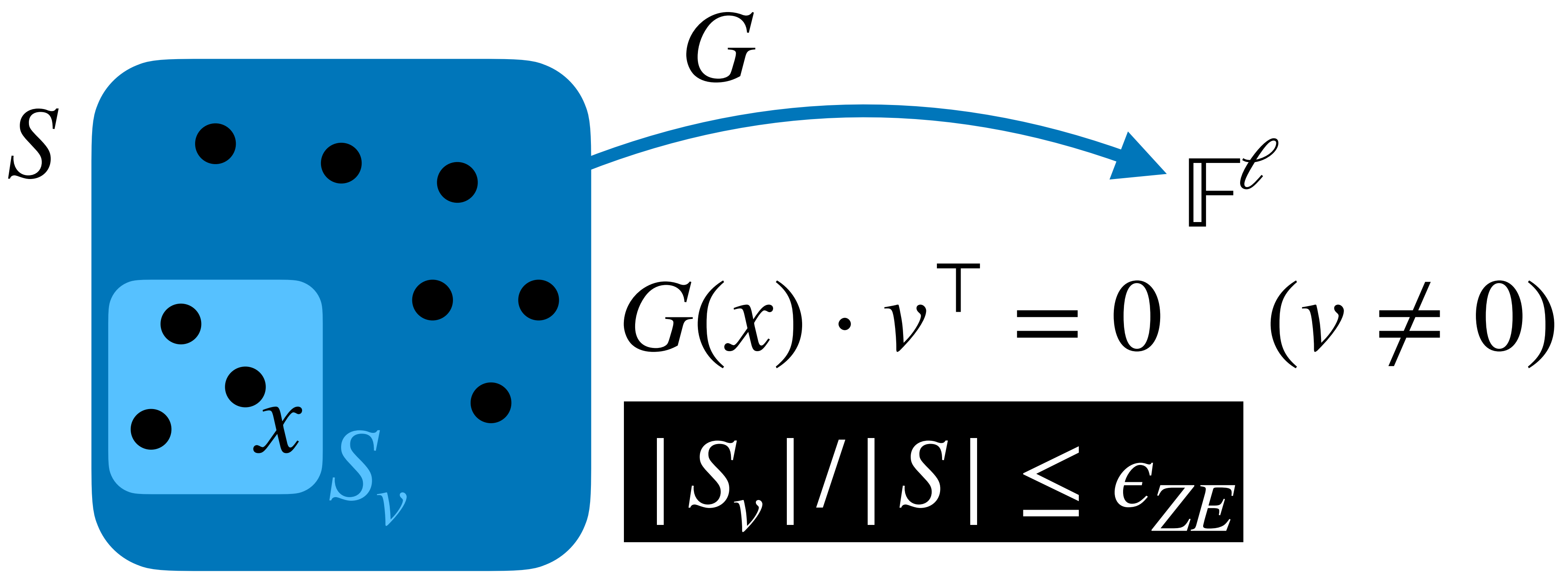
Pf sketch:

Testing membership to the code!

- Sufficient to show $\epsilon_{ZE} \leq \epsilon_{MCA}(0)$

ZE is Necessary

Zero-evading is necessary for MCA: $\epsilon_{ZE} \leq \epsilon_{MCA}$



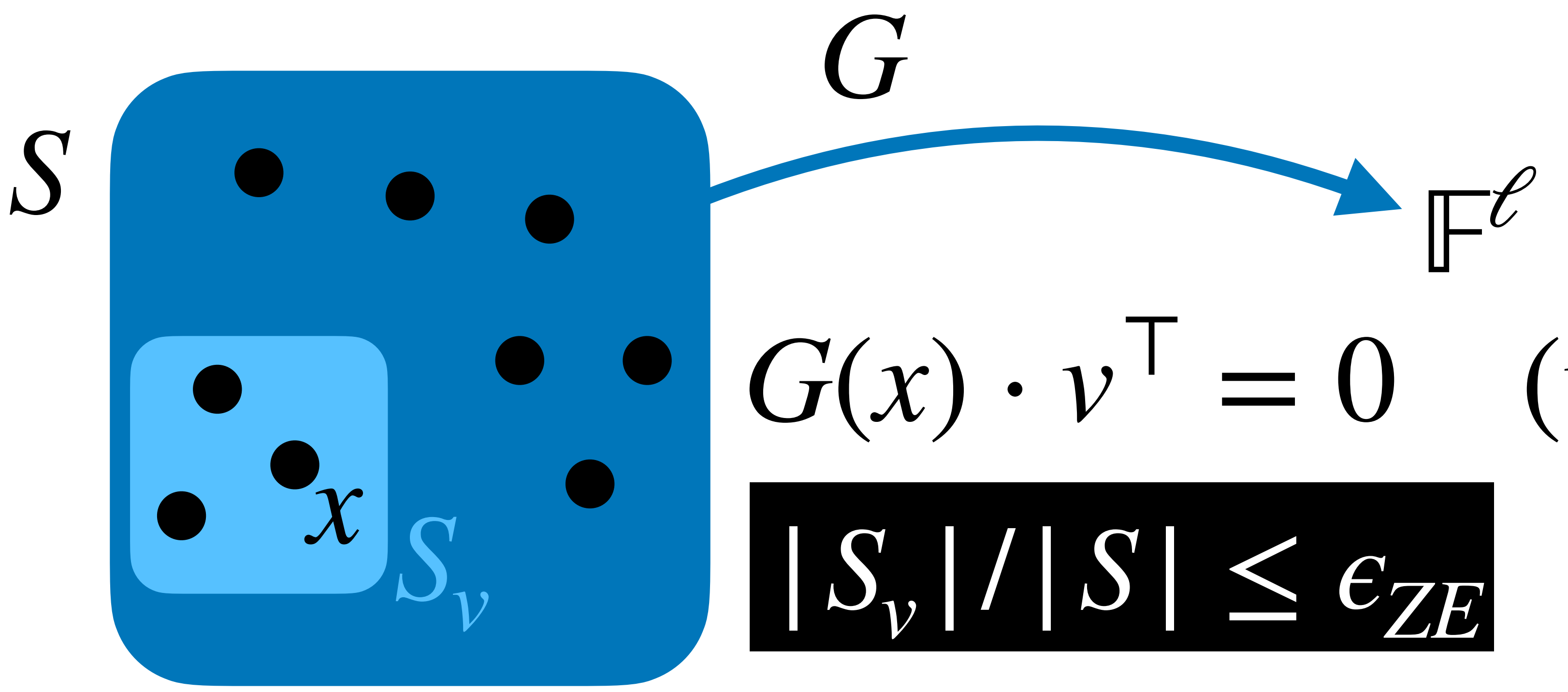
Pf sketch:

Testing membership to the code!

- Sufficient to show $\epsilon_{ZE} \leq \epsilon_{MCA}(0)$
- If $G(x) \cdot (u_1, \ldots, u_\ell)^{\top} \in \mathscr{C} \wedge \exists u_i \notin \mathscr{C}$, find $v \neq \mathbf{0}$ s.t. $G(x) \cdot v^{\top} = 0$

ZE is Necessary

Zero-evading is necessary for MCA: $\epsilon_{ZE} \leq \epsilon_{MCA}$



$G(x) \cdot v^{\top} = 0 \quad (v \neq 0)$

$|S_v|/|S| \leq \epsilon_{ZE}$

Pf sketch:

Testing membership to the code!

- Sufficient to show $\epsilon_{ZE} \leq \epsilon_{MCA}(0)$

Independent of x

- If $G(x) \cdot (u_1, \ldots, u_{\ell})^{\top} \in \mathscr{C} \wedge \exists u_i \notin \mathscr{C}$, find $v \neq \mathbf{0}$ s.t. $G(x) \cdot v^{\top} = 0$ $\blacksquare$

ZE Error Lower Bounds MCA

Lemma: $\epsilon_{ZE} = \epsilon_{MCA}(0) = \min_{\gamma \in [0,1]} \epsilon_{MCA}(\gamma)$

$$\epsilon_{MCA}(0) = \Pr_{x \in S}\begin{bmatrix} G(x) \cdot \mathbf{U} \in \mathscr{C} \\ \vee_{j \in [\ell]} \mathbf{u}_j \notin \mathscr{C} \end{bmatrix}$$

ZE Error Lower Bounds MCA

Lemma: $\epsilon_{ZE} = \epsilon_{MCA}(0) = \min_{\gamma \in [0,1]} \epsilon_{MCA}(\gamma)$

pf (sketch): $\mathscr{C} \subseteq \mathbb{F}^n$ of codimension r, $M \in \mathbb{F}^{r \times n}$ parity check matrix.

$$\epsilon_{MCA}(0) = \Pr_{x \in S} \begin{bmatrix} G(x) \cdot \mathbf{U} \in \mathscr{C} \\ \vee_{j \in [\ell]} \mathbf{u}_j \notin \mathscr{C} \end{bmatrix}$$

ZE Error Lower Bounds MCA

Lemma: $\epsilon_{ZE} = \epsilon_{MCA}(0) = \min_{\gamma \in [0,1]} \epsilon_{MCA}(\gamma)$

pf (sketch): $\mathscr{C} \subseteq \mathbb{F}^n$ of codimension r, $M \in \mathbb{F}^{r \times n}$ parity check matrix.

$$\epsilon_{MCA}(0) = \Pr_{x \in S}\begin{bmatrix} G(x) \cdot \mathbf{U} \in \mathscr{C} \\ \vee_{j \in [\ell]} \mathbf{u}_j \notin \mathscr{C} \end{bmatrix}$$

Let $\mathbf{u}_1, \ldots, \mathbf{u}_\ell \in \mathbb{F}^n$ with some $\mathbf{u}_j \notin \mathscr{C}$, then $\mathbf{w}_j := M \cdot \mathbf{u}_j^\intercal \neq \vec{0}$.

■

ZE Error Lower Bounds MCA

Lemma: $\epsilon_{ZE} = \epsilon_{MCA}(0) = \min_{\gamma \in [0,1]} \epsilon_{MCA}(\gamma)$

pf (sketch): $\mathscr{C} \subseteq \mathbb{F}^n$ of codimension r, $M \in \mathbb{F}^{r \times n}$ parity check matrix.

$$\epsilon_{MCA}(0) = \Pr_{x \in S}\begin{bmatrix} G(x) \cdot \mathbf{U} \in \mathscr{C} \\ \vee_{j \in [\ell]} \mathbf{u}_j \notin \mathscr{C} \end{bmatrix}$$

Let $\mathbf{u}_1, \ldots, \mathbf{u}_\ell \in \mathbb{F}^n$ with some $\mathbf{u}_j \notin \mathscr{C}$, then $\mathbf{w}_j := M \cdot \mathbf{u}_j^\intercal \neq \vec{0}$.

$$\Pr_{x \in S}\begin{bmatrix} \sum_{j \in [\ell]} G(x)_j \cdot \mathbf{w}_j = \vec{0} \\ \vee_{j \in [\ell]} \mathbf{w}_j \neq \vec{0} \end{bmatrix} \leq \Pr_{x \in S}\left[G(x) \cdot \vec{v}^\intercal = 0\right] \leq \epsilon_{ZE}$$

$\blacksquare$

ZE Error Lower Bounds MCA

Lemma: $\epsilon_{ZE} = \epsilon_{MCA}(0) = \min_{\gamma \in [0,1]} \epsilon_{MCA}(\gamma)$

pf (sketch): $\mathscr{C} \subseteq \mathbb{F}^n$ of codimension r, $M \in \mathbb{F}^{r \times n}$ parity check matrix.

$$\epsilon_{MCA}(0) = \Pr_{x \in S}\begin{bmatrix} G(x) \cdot \mathbf{U} \in \mathscr{C} \\ \vee_{j \in [\ell]} \mathbf{u}_j \notin \mathscr{C} \end{bmatrix}$$

Let $\mathbf{u}_1, \ldots, \mathbf{u}_\ell \in \mathbb{F}^n$ with some $\mathbf{u}_j \notin \mathscr{C}$, then $\mathbf{w}_j := M \cdot \mathbf{u}_j^\intercal \neq \vec{0}$.

$$\Pr_{x \in S}\begin{bmatrix} \sum_{j \in [\ell]} G(x)_j \cdot \mathbf{w}_j = \vec{0} \\ \vee_{j \in [\ell]} \mathbf{w}_j \neq \vec{0} \end{bmatrix} \leq \Pr_{x \in S}\left[G(x) \cdot \vec{v}^\intercal = 0\right] \leq \epsilon_{ZE}$$

$\vec{v} = (\mathbf{w}_1[i], \ldots, \mathbf{w}_\ell[i])$
for $i \in [r]$ s.t. $\mathbf{w}_j[i] \neq 0$

■

Zero-evading and MCA

Lemma: $\left|\{x \in S : T \subsetneq T_x\}\right| \leq (n - |T|) \cdot \epsilon_{ZE} \cdot |S|$

$\blacksquare$

Zero-evading and MCA

Lemma: $\left|\{x \in S : T \subsetneq T_x\}\right| \leq (n - |T|) \cdot \epsilon_{ZE} \cdot |S|$

pf: For all $i \in [n]$, define $\vec{v}(i) := (\mathbf{c}_1[i], \ldots, \mathbf{c}_\ell[i]) - (\mathbf{u}_1[i], \ldots, \mathbf{u}_\ell[i])$. Then:

$\blacksquare$

Zero-evading and MCA

Lemma: $\left|\{x \in S : T \subsetneq T_x\}\right| \le (n - |T|) \cdot \epsilon_{ZE} \cdot |S|$

pf: For all $i \in [n]$, define $\vec{v}(i) := (\mathbf{c}_1[i], \ldots, \mathbf{c}_\ell[i]) - (\mathbf{u}_1[i], \ldots, \mathbf{u}_\ell[i])$. Then:

$$\{x \in S : T \subsetneq T_x\} = \{x \in S : \exists i \in [n] \backslash T,\ G(x) \cdot \vec{v}(i)^\intercal = 0\}$$

$\blacksquare$

Zero-evading and MCA

Lemma: $\left|\{x \in S : T \subsetneq T_x\}\right| \leq (n - |T|) \cdot \epsilon_{ZE} \cdot |S|$

pf: For all $i \in [n]$, define $\vec{v}(i) := (\mathbf{c}_1[i], \ldots, \mathbf{c}_\ell[i]) - (\mathbf{u}_1[i], \ldots, \mathbf{u}_\ell[i])$. Then:

$$\{x \in S : T \subsetneq T_x\} = \{x \in S : \exists i \in [n] \backslash T, G(x) \cdot \vec{v}(i)^\intercal = 0\}$$

■

Takeaway: ZE error controls agreement outside of correlated agreement set

MCA for Univariate Powers

Theorem (UDR): $G\colon S \to \mathbb{F}^{d+1}$ defined as $x \mapsto (1, x, \ldots, x^d)$ has MCA for any linear code $\mathscr{C} \subseteq \mathbb{F}^n$, with error

$$\epsilon_{MCA}(\gamma) = n \cdot d / |S| \quad \text{for} \quad 1/n \leq \gamma < \delta_{\mathscr{C}} / (\ell + 1)$$

MCA for Univariate Powers

Theorem (UDR): $G\colon S \to \mathbb{F}^{d+1}$ defined as $x \mapsto (1, x, \ldots, x^d)$ has MCA for any linear code $\mathscr{C} \subseteq \mathbb{F}^n$, with error

$$\epsilon_{MCA}(\gamma) = n \cdot d/|S| \text{ for } 1/n \leq \gamma < \delta_{\mathscr{C}}/(\ell + 1)$$

pf (sketch): Define the set of *bad seeds*:

$$B := \left\{ x \in S : \begin{array}{c} \exists T \subseteq [n] \\ |T| \geq n \cdot (1 - \gamma) \\ (G(x) \cdot \mathbf{U})|_T \in \mathscr{C}|_T \\ \vee_{j \in [\ell]} \mathbf{u}_j|_T \notin \mathscr{C}|_T \end{array} \right\}$$

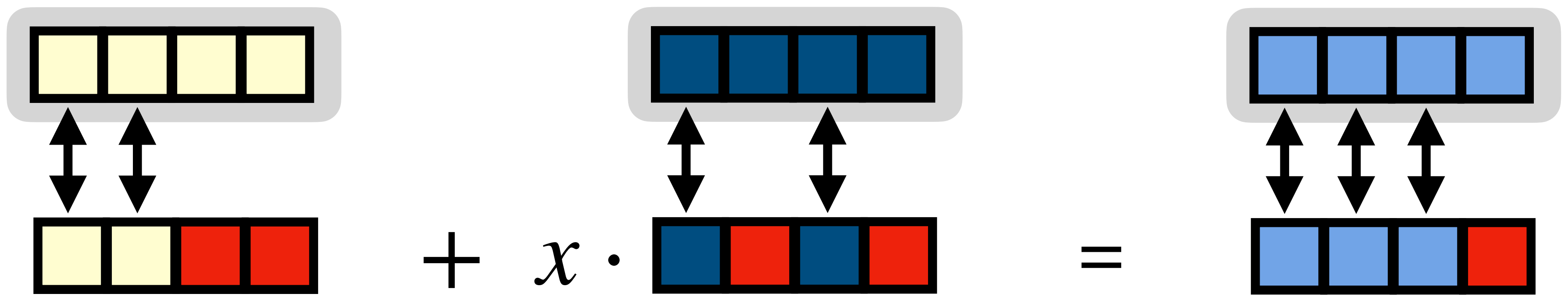
MCA for Univariate Powers

Theorem (UDR): $G\colon S \to \mathbb{F}^{d+1}$ defined as $x \mapsto (1,x,\ldots,x^d)$ has MCA for any linear code $\mathscr{C} \subseteq \mathbb{F}^n$, with error

$$\epsilon_{MCA}(\gamma) = n \cdot d/|S| \quad \text{for} \quad 1/n \leq \gamma < \delta_{\mathscr{C}}/(\ell+1)$$

pf (sketch): Define the set of *bad seeds*:

$$B := \left\{ x \in S : \begin{array}{c} \exists T \subseteq [n] \\ |T| \geq n \cdot (1-\gamma) \\ (G(x) \cdot \mathbf{U})|_T \in \mathscr{C}|_T \\ \vee_{j \in [\ell]} \mathbf{u}_j|_T \notin \mathscr{C}|_T \end{array} \right\}$$



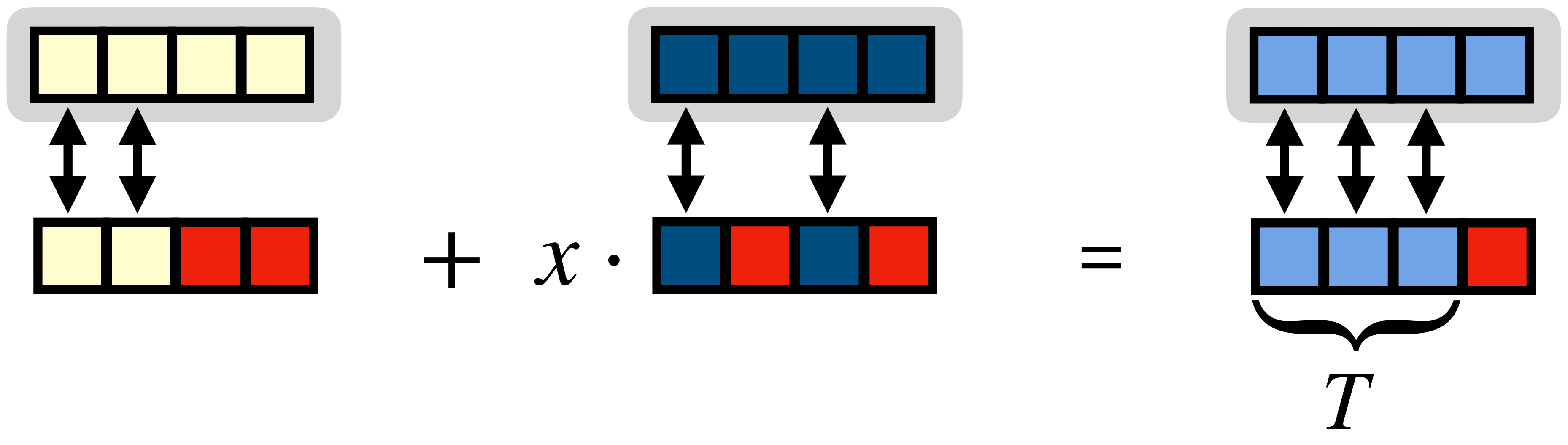
MCA for Univariate Powers

Theorem (UDR): $G\colon S \to \mathbb{F}^{d+1}$ defined as $x \mapsto (1, x, \ldots, x^d)$ has MCA for any linear code $\mathscr{C} \subseteq \mathbb{F}^n$, with error

$$\epsilon_{MCA}(\gamma) = n \cdot d/|S| \ \text{ for } \ 1/n \leq \gamma < \delta_{\mathscr{C}}/(\ell + 1)$$

pf (sketch): Define the set of *bad seeds*:

$$B := \left\{ x \in S : \begin{array}{c} \exists T \subseteq [n] \\ |T| \geq n \cdot (1-\gamma) \\ (G(x) \cdot \mathbf{U})|_T \in \mathscr{C}|_T \\ \vee_{j \in [\ell]} \mathbf{u}_j|_T \notin \mathscr{C}|_T \end{array} \right\}$$



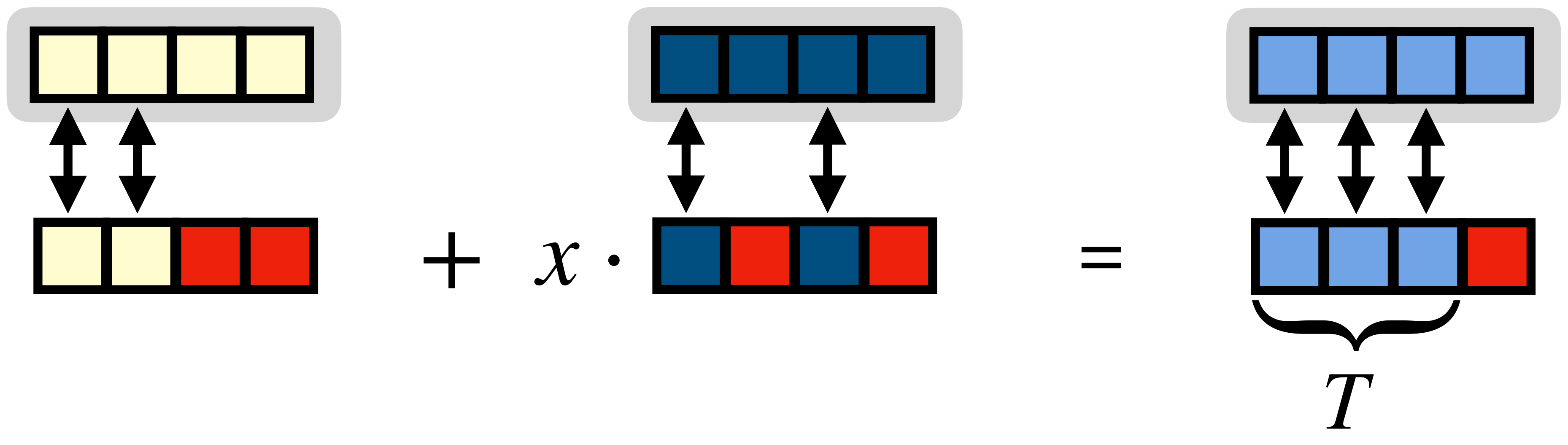
MCA for Univariate Powers

Theorem (UDR): $G: S \to \mathbb{F}^{d+1}$ defined as $x \mapsto (1, x, \ldots, x^d)$ has MCA for any linear code $\mathscr{C} \subseteq \mathbb{F}^n$, with error

$$\epsilon_{MCA}(\gamma) = n \cdot d/|S| \quad \text{for} \quad 1/n \leq \gamma < \delta_{\mathscr{C}}/(\ell + 1)$$

pf (sketch): Define the set of *bad seeds*:

$$B := \left\{ x \in S : \begin{array}{c} \exists T \subseteq [n] \\ |T| \geq n \cdot (1-\gamma) \\ (G(x) \cdot \mathbf{U})|_T \in \mathscr{C}|_T \\ \vee_{j \in [\ell]} \mathbf{u}_j|_T \notin \mathscr{C}|_T \end{array} \right\}$$



Invertibility
+triangle inequality
+UDR

Assume $|B| > n \cdot d$. We find $\mathbf{c}_1^\star, \ldots, \mathbf{c}_\ell^\star \in \mathscr{C}$:

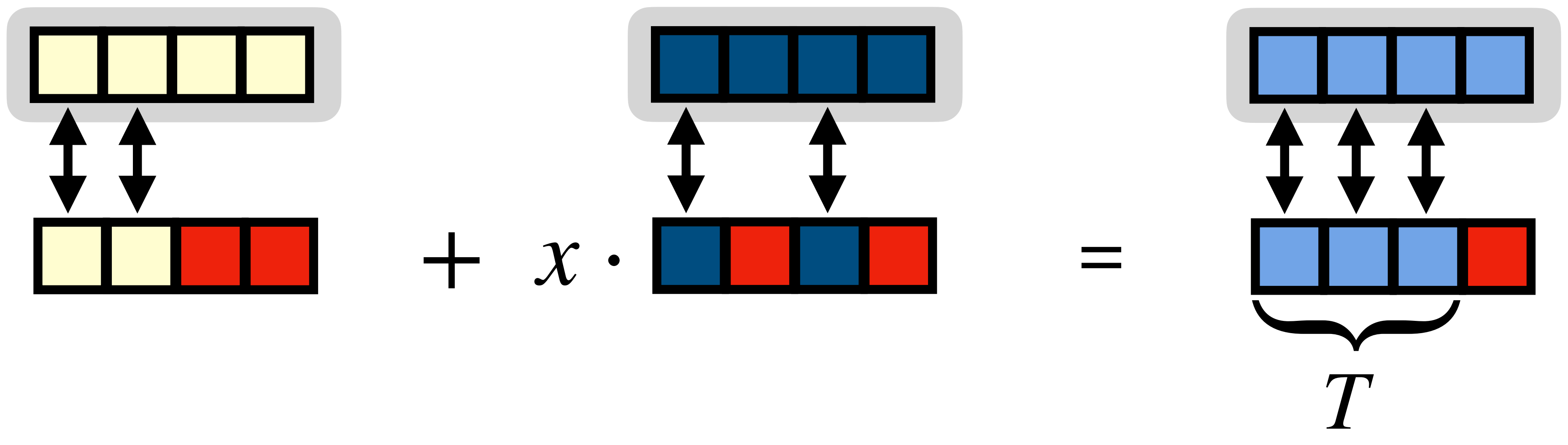
MCA for Univariate Powers

Theorem (UDR): $G : S \to \mathbb{F}^{d+1}$ defined as $x \mapsto (1, x, \ldots, x^d)$ has MCA for any linear code $\mathscr{C} \subseteq \mathbb{F}^n$, with error

$$\epsilon_{MCA}(\gamma) = n \cdot d / |S| \quad \text{for} \quad 1/n \leq \gamma < \delta_{\mathscr{C}}/(\ell + 1)$$

pf (sketch): Define the set of *bad seeds*:

$$B := \left\{ x \in S : \begin{array}{c} \exists T \subseteq [n] \\ |T| \geq n \cdot (1 - \gamma) \\ (G(x) \cdot \mathbf{U})|_T \in \mathscr{C}|_T \\ \vee_{j \in [\ell]} \mathbf{u}_j|_T \notin \mathscr{C}|_T \end{array} \right\}$$



Invertibility
+triangle inequality
+UDR

Assume $|B| > n \cdot d$. We find $\mathbf{c}_1^\star, \ldots, \mathbf{c}_\ell^\star \in \mathscr{C}$:

For all $x \in S$, the closest codeword to $G(x) \cdot \mathbf{U}$ is $\sum_{j \in [\ell]} G(x)_j \cdot \mathbf{c}_j^\star$

MCA for Univariate Powers

MCA for Univariate Powers

pf (sketch): We have $\mathbf{c}_1^\star, \ldots, \mathbf{c}_\ell^\star \in \mathscr{C}$ s.t. for all $x \in S$, the closest codeword to $G(x) \cdot \mathbf{U}$ is $\sum_{j \in [\ell]} G(x)_j \cdot \mathbf{c}_j^\star$.

$\blacksquare$

MCA for Univariate Powers

pf (sketch): We have $\mathbf{c}_1^\star, \ldots, \mathbf{c}_\ell^\star \in \mathscr{C}$ s.t. for all $x \in S$, the closest codeword to $G(x) \cdot \mathbf{U}$ is $\sum_{j \in [\ell]} G(x)_j \cdot \mathbf{c}_j^\star$.

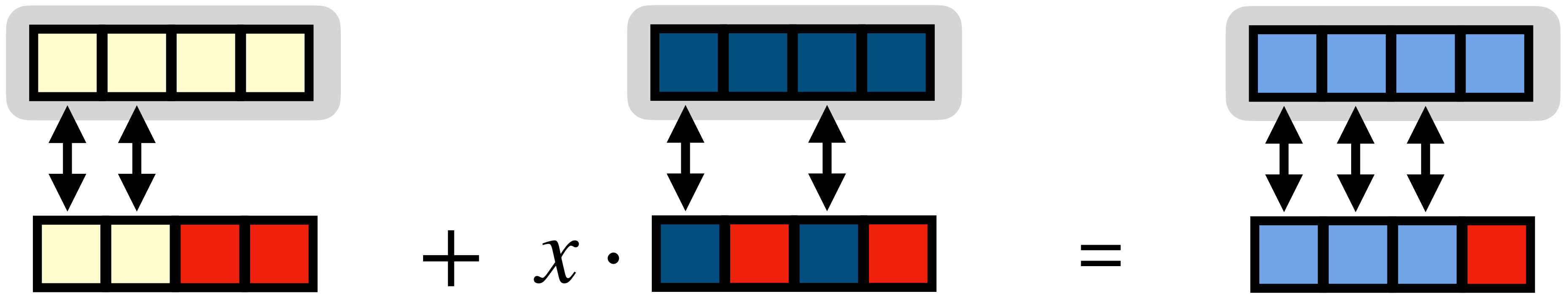
For any $x \in B$, let T_x be a set like in the definition of B.

$\blacksquare$

MCA for Univariate Powers

pf (sketch): We have $\mathbf{c}_1^\star, \ldots, \mathbf{c}_\ell^\star \in \mathscr{C}$ s.t. for all $x \in S$, the closest codeword to $G(x) \cdot \mathbf{U}$ is $\sum_{j \in [\ell]} G(x)_j \cdot \mathbf{c}_j^\star$.

For any $x \in B$, let T_x be a set like in the definition of B.

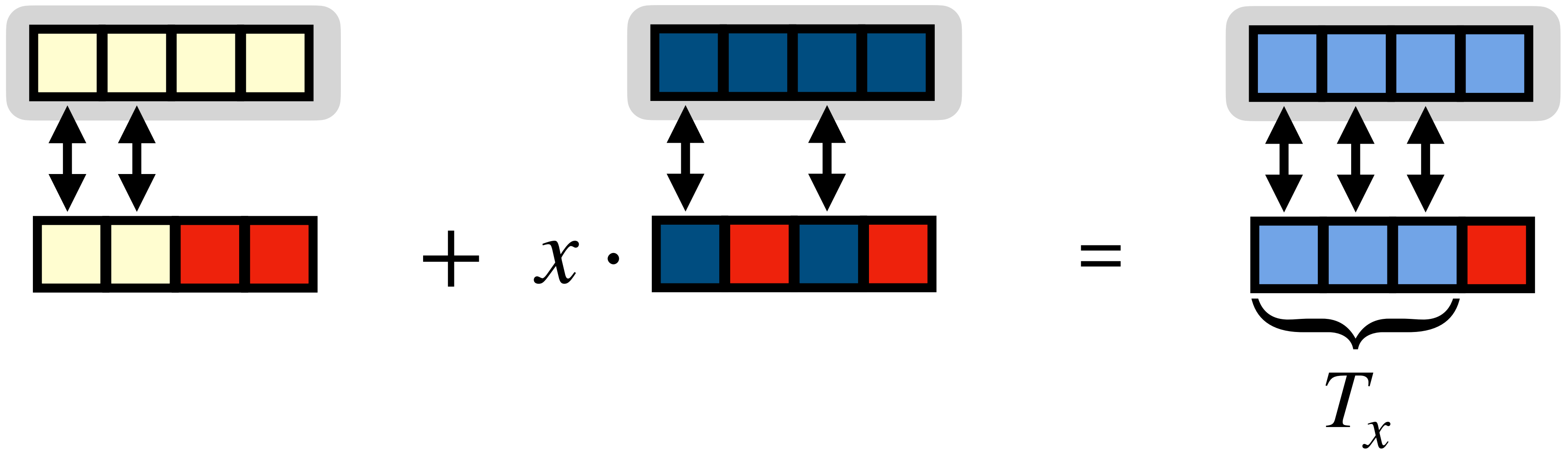


■

MCA for Univariate Powers

pf (sketch): We have $\mathbf{c}_1^\star, \ldots, \mathbf{c}_\ell^\star \in \mathscr{C}$ s.t. for all $x \in S$, the closest codeword to $G(x) \cdot \mathbf{U}$ is $\sum_{j \in [\ell]} G(x)_j \cdot \mathbf{c}_j^\star$.

For any $x \in B$, let T_x be a set like in the definition of B.



■

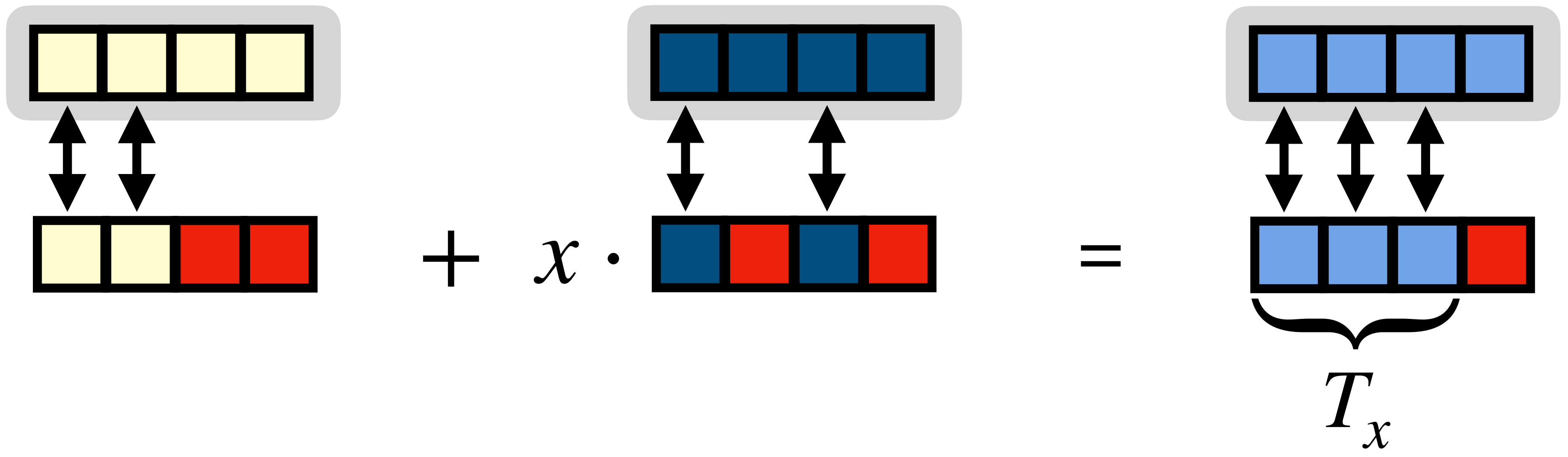
MCA for Univariate Powers

pf (sketch): We have $\mathbf{c}_1^\star, \ldots, \mathbf{c}_\ell^\star \in \mathscr{C}$ s.t. for all $x \in S$, the closest codeword to $G(x) \cdot \mathbf{U}$ is $\sum_{j \in [\ell]} G(x)_j \cdot \mathbf{c}_j^\star$.

For any $x \in B$, let T_x be a set like in the definition of B.

It must be that $T \subsetneq T_x$.

The correlated agreement set between the $\mathbf{u}_j$'s and the $\mathbf{c}_j^\star$'s



■

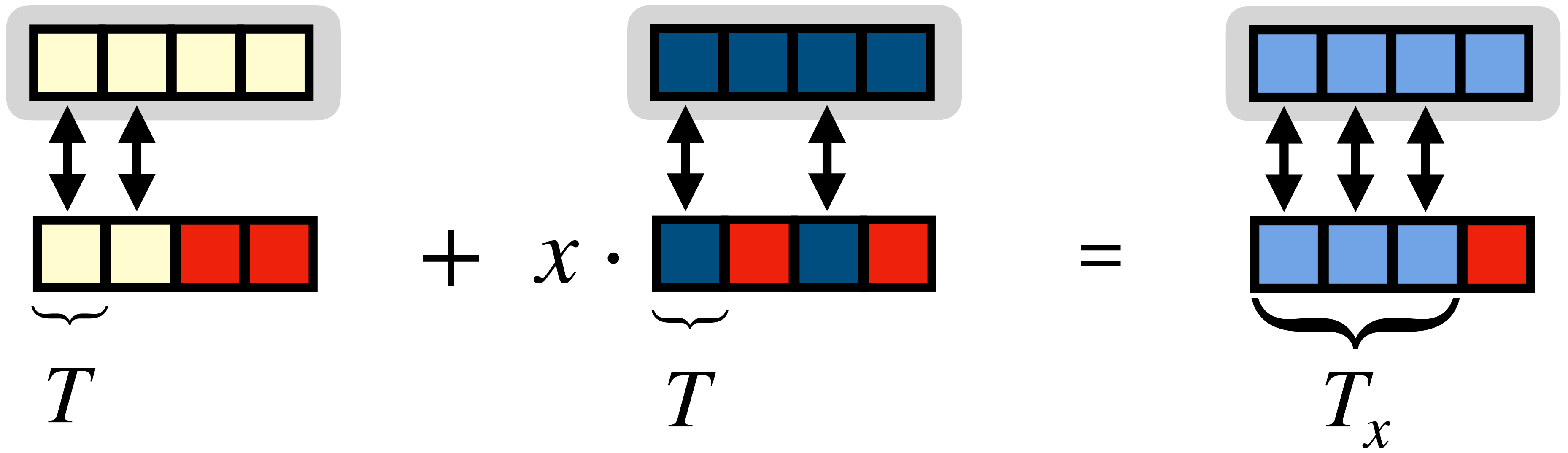
MCA for Univariate Powers

pf (sketch): We have $\mathbf{c}_1^\star, \ldots, \mathbf{c}_\ell^\star \in \mathscr{C}$ s.t. for all $x \in S$, the closest codeword to $G(x) \cdot \mathbf{U}$ is $\sum_{j\in[\ell]} G(x)_j \cdot \mathbf{c}_j^\star$.

For any $x \in B$, let T_x be a set like in the definition of B.

It must be that $T \subsetneq T_x$.

The correlated agreement set between the $\mathbf{u}_j$'s and the $\mathbf{c}_j^\star$'s



∎

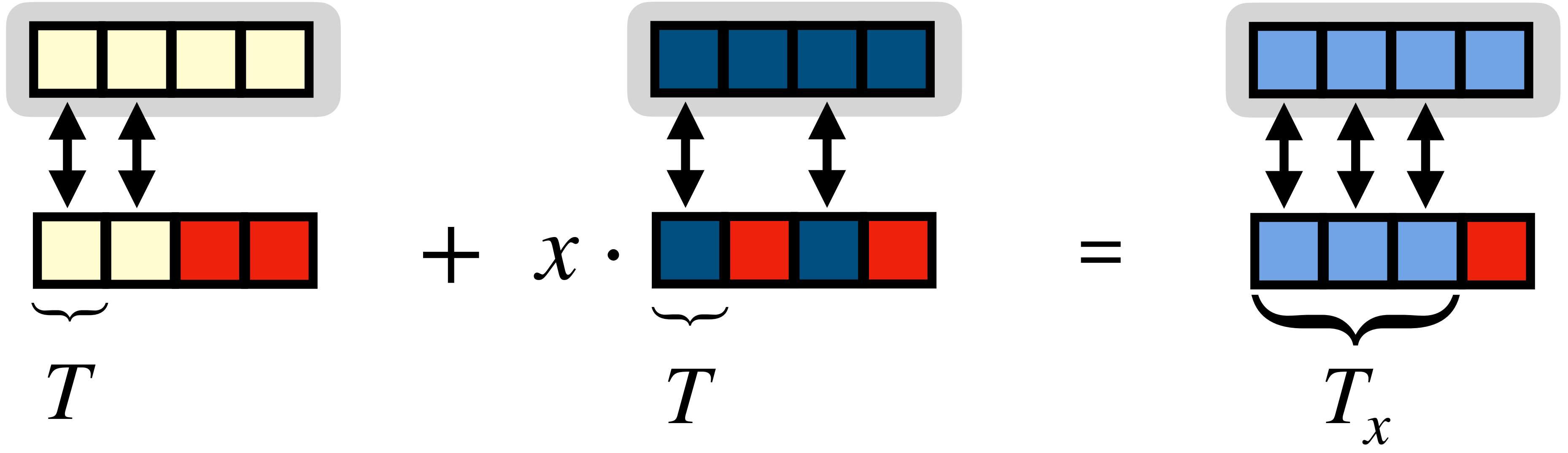
MCA for Univariate Powers

pf (sketch): We have $\mathbf{c}_1^\star, \ldots, \mathbf{c}_\ell^\star \in \mathscr{C}$ s.t. for all $x \in S$, the closest codeword to $G(x) \cdot \mathbf{U}$ is $\sum_{j \in [\ell]} G(x)_j \cdot \mathbf{c}_j^\star$.

For any $x \in B$, let T_x be a set like in the definition of B.

It must be that $T \subsetneq T_x$.

The correlated agreement set between the $\mathbf{u}_j$'s and the $\mathbf{c}_j^\star$'s



The number of such T_x is at most $(n - |T|) \cdot \epsilon_{ZE} \cdot |S| \leq n \cdot d$ $\blacksquare$

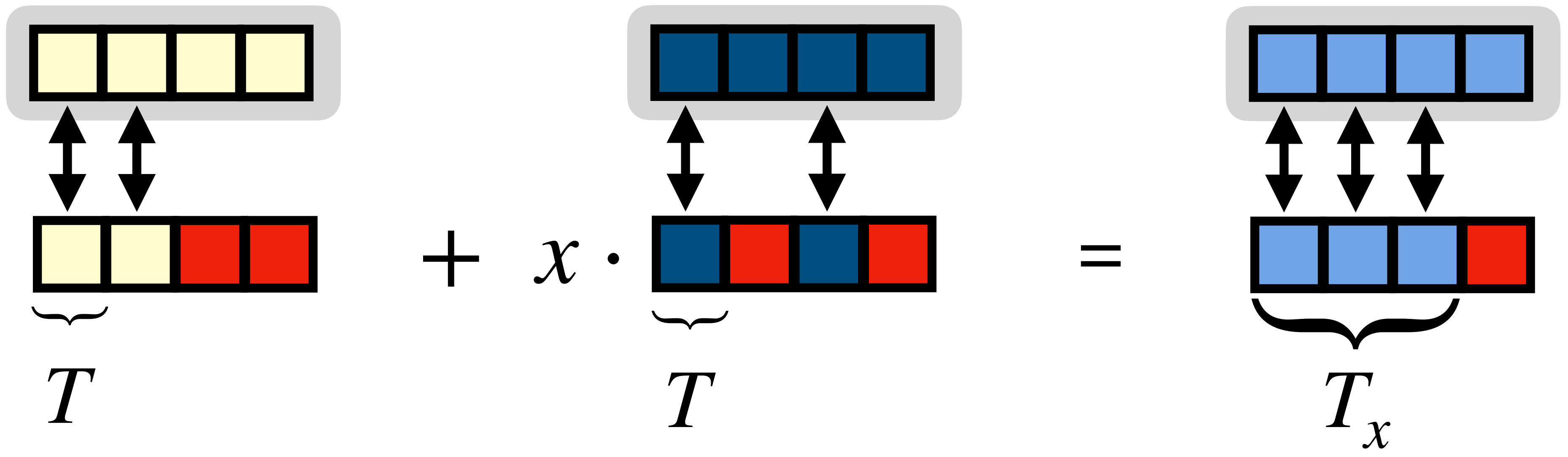
MCA for Univariate Powers

pf (sketch): We have $\mathbf{c}_1^\star, \ldots, \mathbf{c}_\ell^\star \in \mathscr{C}$ s.t. for all $x \in S$, the closest codeword to $G(x) \cdot \mathbf{U}$ is $\sum_{j \in [\ell]} G(x)_j \cdot \mathbf{c}_j^\star$.

For any $x \in B$, let T_x be a set like in the definition of B.

It must be that $T \subsetneq T_x$.

The correlated agreement set between the $\mathbf{u}_j$'s and the $\mathbf{c}_j^\star$'s



The number of such T_x is at most $(n - |T|) \cdot \epsilon_{ZE} \cdot |S| \leq n \cdot d$ ■

Can show $|T| \geq n \cdot (1 - \gamma)$

Extending to list-decoding

Theorem (List-decoding): If $G: S \to \mathbb{F}^{\ell}$ is MDS (of dim. ℓ), then it has MCA for any linear code $\mathscr{C} \subseteq \mathbb{F}^n$, with error

$$\epsilon_{MCA}(\gamma) = O\left(\frac{n}{\eta}\right) \cdot \epsilon_{ZE} \ \text{ for } \ \gamma \leq 1 - (1 - \delta_{\mathscr{C}} + \eta)^{\frac{1}{\ell+1}}$$

Extending to list-decoding

Theorem (List-decoding): If $G: S \to \mathbb{F}^{\ell}$ is MDS (of dim. ℓ), then it has MCA for any linear code $\mathscr{C} \subseteq \mathbb{F}^n$, with error

$$\epsilon_{MCA}(\gamma) = O\left(\frac{n}{\eta}\right) \cdot \epsilon_{ZE} \quad \text{for} \quad \gamma \leq 1 - (1 - \delta_{\mathscr{C}} + \eta)^{\frac{1}{\ell+1}}$$

Fancier counting argument to restrict the # of possible $T's$

Extending to list-decoding

Theorem (List-decoding): If $G\colon S \to \mathbb{F}^{\ell}$ is MDS (of dim. ℓ), then it has MCA for any linear code $\mathscr{C} \subseteq \mathbb{F}^n$, with error

$$\epsilon_{MCA}(\gamma) = O\left(\frac{n}{\eta}\right) \cdot \epsilon_{ZE} \quad \text{for} \quad \gamma \leq 1 - (1 - \delta_{\mathscr{C}} + \eta)^{\frac{1}{\ell+1}}$$

Fancier counting argument to restrict the # of possible T's

Counting x's such that $T \subsetneq T_x$

Beyond polynomial generators

Beyond polynomial generators

[AGHP92] generator: $\mathbb{F}_q \subseteq \mathbb{F}_{q^k}$ with $\phi\colon \mathbb{F}_{q^k} \xrightarrow{\cong} \mathbb{F}_q^k$, and $G\colon \mathbb{F}_{q^k} \times \mathbb{F}_q^k \to \mathbb{F}_q^\ell$ s.t.

$$G(x, \vec{v}) = ((\phi(x^i))_{i\in[\ell]} \cdot \vec{v}^\intercal)$$

Beyond polynomial generators

[AGHP92] generator: $\mathbb{F}_q \subseteq \mathbb{F}_{q^k}$ with $\phi : \mathbb{F}_{q^k} \xrightarrow{\cong} \mathbb{F}_q^k$, and $G : \mathbb{F}_{q^k} \times \mathbb{F}_q^k \to \mathbb{F}_q^\ell$ s.t.

$$G(x, \vec{v}) = ((\phi(x^i))_{i \in [\ell]} \cdot \vec{v}^\intercal)$$

$$G(x) = (x, \ldots, x^\ell)$$

Beyond polynomial generators

[AGHP92] generator: $\mathbb{F}_q \subseteq \mathbb{F}_{q^k}$ with $\phi \colon \mathbb{F}_{q^k} \xrightarrow{\simeq} \mathbb{F}_q^k$, and $G \colon \mathbb{F}_{q^k} \times \mathbb{F}_q^k \to \mathbb{F}_q^\ell$ s.t.

$$G(x, \vec{v}) = ((\phi(x^i))_{i \in [\ell]} \cdot \vec{v}^\intercal)$$

$G(x) = (x, \ldots, x^\ell)$

$G(\vec{v}) = \vec{v}$

Beyond polynomial generators

[AGHP92] generator: $\mathbb{F}_q \subseteq \mathbb{F}_{q^k}$ with $\phi\colon \mathbb{F}_{q^k} \xrightarrow{\simeq} \mathbb{F}_q^k$, and $G\colon \mathbb{F}_{q^k} \times \mathbb{F}_q^k \to \mathbb{F}_q^\ell$ s.t.

$$G(x, \vec{v}) = ((\phi(x^i))_{i \in [\ell]} \cdot \vec{v}^\intercal)$$

$G(x) = (x, \ldots, x^\ell)$

$G(\vec{v}) = \vec{v}$

Lemma: this transformation (matrix-vector product) sums MCA errors