A new method for constructing small-bias spaces from Hermitian codes

Olav Geil, Stefano Martin, Ryutaroh Matsumoto

University of Aalborg, Tokyo Institute of Technology

WAIFI, Bochum 2012

ϵ-Bias Spaces

The idea is to have a test set that is much smaller than $\mathbb{F}_2^k$ having statistical properties close to it.

Definition

A multiset $\mathcal{X} \subseteq \mathbb{F}_2^k$ non-empty is called an ϵ-bias space if

$$\left| \mathbb{P}\left[\sum_{i \in S} x_i = 1\right] - \mathbb{P}\left[\sum_{i \in S} x_i = 0\right] \right| \leq \epsilon,$$

$$X = (x_1, \ldots, x_k) \in \mathcal{X}$$

holds for every non-empty index set $S \subseteq \{1, \ldots, k\}$.

ϵ-Bias Spaces

The idea is to have a test set that is much smaller than $\mathbb{F}_2^k$ having statistical properties close to it.

Definition

A multiset $\mathcal{X} \subseteq \mathbb{F}_2^k$ non-empty is called an ϵ-bias space if

$$\left| \mathbb{P}\left[\sum_{i \in S} x_i = 1\right] - \mathbb{P}\left[\sum_{i \in S} x_i = 0\right] \right| \leq \epsilon,$$

$$X = (x_1, \ldots, x_k) \in \mathcal{X}$$

holds for every non-empty index set $S \subseteq \{1, \ldots, k\}$.

ϵ-Bias Spaces

$$\mathcal{X} = \{(0,0,1),(1,0,1),(0,1,1),(1,1,1),(0,0,1),(1,0,1),$$

$$(0,1,1),(1,1,1),(0,0,0),(0,0,0),(0,0,0),(0,0,0)\}$$

is $\frac{1}{3}$-bias space.

If we assume for example $S = \{1\}$ we obtain $|\frac{4}{12} - \frac{8}{12}| = \frac{1}{3}$.
If we assume for example $S = \{1,2\}$ we obtain again :
$|\frac{4}{12} - \frac{8}{12}| = \frac{1}{3}$. Instead treating the columns as a set we derive:

$$\mathcal{X}' = \{(0,0,1),(1,0,1),(0,1,1),(1,1,1),(0,0,0)\}.$$

The smallest value of ϵ for which $\mathcal{X}'$ is ϵ-biased is $\epsilon = \frac{3}{5}$.

ϵ-Bias Spaces

$$\mathcal{X} = \{(0,0,1),(1,0,1),(0,1,1),(1,1,1),(0,0,1),(1,0,1),$$

$$(0,1,1),(1,1,1),(0,0,0),(0,0,0),(0,0,0),(0,0,0)\}$$

is $\frac{1}{3}$-bias space.
If we assume for example $S = \{1\}$ we obtain $|\frac{4}{12} - \frac{8}{12}| = \frac{1}{3}$.
If we assume for example $S = \{1,2\}$ we obtain again :
$|\frac{4}{12} - \frac{8}{12}| = \frac{1}{3}$. Instead treating the columns as a set we derive:

$$\mathcal{X}' = \{(0,0,1),(1,0,1),(0,1,1),(1,1,1),(0,0,0)\}.$$

The smallest value of ϵ for which $\mathcal{X}'$ is ϵ-biased is $\epsilon = \frac{3}{5}$.

ϵ-Bias Spaces

$$\mathcal{X} = \{(0,0,1),(1,0,1),(0,1,1),(1,1,1),(0,0,1),(1,0,1),$$

$$(0,1,1),(1,1,1),(0,0,0),(0,0,0),(0,0,0),(0,0,0)\}$$

is $\frac{1}{3}$-bias space.
If we assume for example $S = \{1\}$ we obtain $|\frac{4}{12} - \frac{8}{12}| = \frac{1}{3}$.
If we assume for example $S = \{1,2\}$ we obtain again :
$|\frac{4}{12} - \frac{8}{12}| = \frac{1}{3}$. Instead treating the columns as a set we derive:

$$\mathcal{X}' = \{(0,0,1),(1,0,1),(0,1,1),(1,1,1),(0,0,0)\}.$$

The smallest value of ϵ for which $\mathcal{X}'$ is ϵ-biased is $\epsilon = \frac{3}{5}$.

ϵ-Bias Spaces

$$\mathcal{X} = \{(0,0,1),(1,0,1),(0,1,1),(1,1,1),(0,0,1),(1,0,1),$$

$$(0,1,1),(1,1,1),(0,0,0),(0,0,0),(0,0,0),(0,0,0)\}$$

is $\frac{1}{3}$-bias space.
If we assume for example $S = \{1\}$ we obtain $|\frac{4}{12} - \frac{8}{12}| = \frac{1}{3}$.
If we assume for example $S = \{1,2\}$ we obtain again :
$|\frac{4}{12} - \frac{8}{12}| = \frac{1}{3}$. Instead treating the columns as a set we derive:

$$\mathcal{X}' = \{(0,0,1),(1,0,1),(0,1,1),(1,1,1),(0,0,0)\}.$$

The smallest value of ϵ for which $\mathcal{X}'$ is ϵ-biased is $\epsilon = \frac{3}{5}$.

ϵ-Balanced Code

Definition

A binary $[n, k]$ code $\mathcal{C}$ is said to be ϵ-balanced if every nonzero $c \in \mathcal{C}$ satisfy:

$$\frac{1-\epsilon}{2} \leq \frac{\mathrm{w}(c)}{n} \leq \frac{1+\epsilon}{2}.$$

$$G = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

is $\frac{1}{3}$-balanced.

ϵ-Balanced Code

Definition

A binary $[n, k]$ code $\mathcal{C}$ is said to be ϵ-balanced if every nonzero $c \in \mathcal{C}$ satisfy:

$$\frac{1-\epsilon}{2} \leq \frac{\mathrm{w}(c)}{n} \leq \frac{1+\epsilon}{2}.$$

$$G = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

is $\frac{1}{3}$-balanced.

ϵ-Balanced Codes

Theorem ([Alon *et al.*, 1992])

Let G be a generator matrix for an ϵ-balanced binary $[n, k]$ code. The columns of G constitute an ϵ-bias space $\mathcal{X} \subseteq \mathbb{F}_2^k$ of size n. Similarly, using the elements of an ϵ-bias space $\mathcal{X}$ as columns of a generator matrix an ϵ-balanced code is derived.

Example:

$$G = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

is $\frac{1}{3}$-balanced with the multiset

$$\mathcal{X} = \{(0,0,1),(1,0,1),(0,1,1),(1,1,1),(0,0,1),(1,0,1),$$

$$(0,1,1),(1,1,1),(0,0,0),(0,0,0),(0,0,0),(0,0,0)\}.$$

Walsh-Hadamard Codes

Definition

Let $s \in \mathbb{N}$, the Walsh-Hadamard code $\mathcal{C}_s$ is a linear code over $\mathbb{F}_2$ with $s \times 2^s$ generator matrix G such that $\mathrm{col}_i(v_i) = v_i \in (\mathbb{F}_2)^s$ and $\{v_1, \ldots, v_{2^s}\} = (\mathbb{F}_2)^s$.

For example with $s = 3$,

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

is a generator matrix.

Proposition

Let $s \in \mathbb{N}$, the Walsh-Hadamard code $\mathcal{C}_s$ is a 0-balanced $[2^s, s, 2^{s-1}]$ code.

Walsh-Hadamard Codes

Definition

Let $s \in \mathbb{N}$, the Walsh-Hadamard code $\mathcal{C}_s$ is a linear code over $\mathbb{F}_2$ with $s \times 2^s$ generator matrix G such that $\mathrm{col}_i(v_i) = v_i \in (\mathbb{F}_2)^s$ and $\{v_1, \ldots, v_{2^s}\} = (\mathbb{F}_2)^s$.

For example with $s = 3$,

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

is a generator matrix.

Proposition

Let $s \in \mathbb{N}$, the Walsh-Hadamard code $\mathcal{C}_s$ is a 0-balanced $[2^s, s, 2^{s-1}]$ code.

Concatenated Codes

Definition

Let $\mathcal{A}$ be an $[\mathcal{N}, \mathcal{K}, \mathcal{D}]_q$ code. Let $Q = q^k$ and define $\psi : \mathbb{F}_Q \to \mathcal{A}$ to be a one-to-one $\mathbb{F}_q$-linear map. Let $\mathcal{B}$ be an $[N, K, D]_Q$ code.
The concatenation of $\mathcal{A}$ and $\mathcal{B}$ is the code:

$$\mathcal{C} = \{\psi(b_1, \ldots, b_N) : (b_1, \ldots, b_N) \in \mathcal{B}\}$$

where $\psi(b_1, \ldots, b_N) = (\psi(b_1), \ldots, \psi(b_N))$.
$\mathcal{C}$ is said to be concatenated code with inner code $\mathcal{A}$ and outer code $\mathcal{B}$.

Theorem ([Alon *et al.*, 1992])

Let $\mathcal{A}, \mathcal{B}$, and $\mathcal{C}$ be as above. Then C is a linear code over $\mathbb{F}_q$ with length $n = N\mathcal{N}$, dimension $k = K\mathcal{K}$ and minimum distance at least $d = D\mathcal{D}$.

Concatenated Codes

Definition

Let $\mathcal{A}$ be an $[\mathcal{N}, \mathcal{K}, \mathcal{D}]_q$ code. Let $Q = q^k$ and define $\psi : \mathbb{F}_Q \to \mathcal{A}$ to be a one-to-one $\mathbb{F}_q$-linear map. Let $\mathcal{B}$ be an $[N, K, D]_Q$ code.
The concatenation of $\mathcal{A}$ and $\mathcal{B}$ is the code:

$$\mathcal{C} = \{\psi(b_1, \ldots, b_N) : (b_1, \ldots, b_N) \in \mathcal{B}\}$$

where $\psi(b_1, \ldots, b_N) = (\psi(b_1), \ldots, \psi(b_N))$.
$\mathcal{C}$ is said to be concatenated code with inner code $\mathcal{A}$ and outer code $\mathcal{B}$.

Theorem ([Alon *et al.*, 1992])

Let $\mathcal{A}, \mathcal{B}$, and $\mathcal{C}$ be as above. Then $\mathcal{C}$ is a linear code over $\mathbb{F}_q$ with length $n = N\mathcal{N}$, dimension $k = K\mathcal{K}$ and minimum distance at least $d = D\mathcal{D}$.

ϵ-Balanced Concatenated Codes

Theorem

Let $q = 2^s$ for some integer $s \geq 1$ and consider a q-ary $[N, K, D]$ code $\mathcal{C}$. Let $\mathcal{C}_s$ be the $[2^s, s]_2$ Walsh-Hadamard code. The concatenated code derived by using $\mathcal{C}$ as outer code and $\mathcal{C}_s$ as inner code is an $\epsilon = \frac{N-D}{N}$-balanced binary code of length $n = N2^s$ and dimension $k = Ks$.

RS-codes, AG-codes, Hermitian codes, GV Bound

Using various outer codes in previous Theorem, one achieves the following formulas for all possible choices of ϵ and k [Alon *et al.*, 1992],[Ben-Aroya & Ta-Shma, 2009]. For $\mathcal{X} \subseteq \mathbb{F}_2^{\Omega(k)}$ we obtain;

Reed-Solomon codes	$\lvert\mathcal{X}\rvert = \mathcal{O}\left(\frac{k^2}{\epsilon^2 \log^2\left(\frac{k}{\epsilon}\right)}\right)$
AG codes of high dimension	$\lvert\mathcal{X}\rvert = \mathcal{O}\left(\frac{k}{\epsilon^3 \log\left(\frac{1}{\epsilon}\right)}\right)$
Hermitian codes $m < g$, $\epsilon \geq k^{-\frac{1}{2}}$	$\lvert\mathcal{X}\rvert = \mathcal{O}\left(\left(\frac{k}{\epsilon^2 \log\left(\frac{1}{\epsilon}\right)}\right)^{\frac{5}{4}}\right)$
Norm-Trace codes for $l = 4, 5, \ldots$, $\epsilon \geq k^{-\frac{1}{\sqrt{l}}}$	$\lvert\mathcal{X}\rvert = \mathcal{O}\left(\left(\frac{k}{\epsilon^{l-\sqrt{l}} \log\left(\frac{1}{\epsilon}\right)}\right)^{\frac{l+1}{l}}\right)$
Gilbert-Varshamov bound	$\lvert\mathcal{X}\rvert = \mathcal{O}\left(\frac{k}{\epsilon^2}\right)$
Linear programming bound	$\lvert\mathcal{X}\rvert = \mathcal{O}\left(\frac{k}{\epsilon^2 \log\left(\frac{1}{\epsilon}\right)}\right)$

RS-codes, AG-codes, Hermitian Codes, GV Bound

One way of comparing the previous results is to choose $\epsilon = k^{-\alpha}, \alpha \in \mathbb{R}^+$...

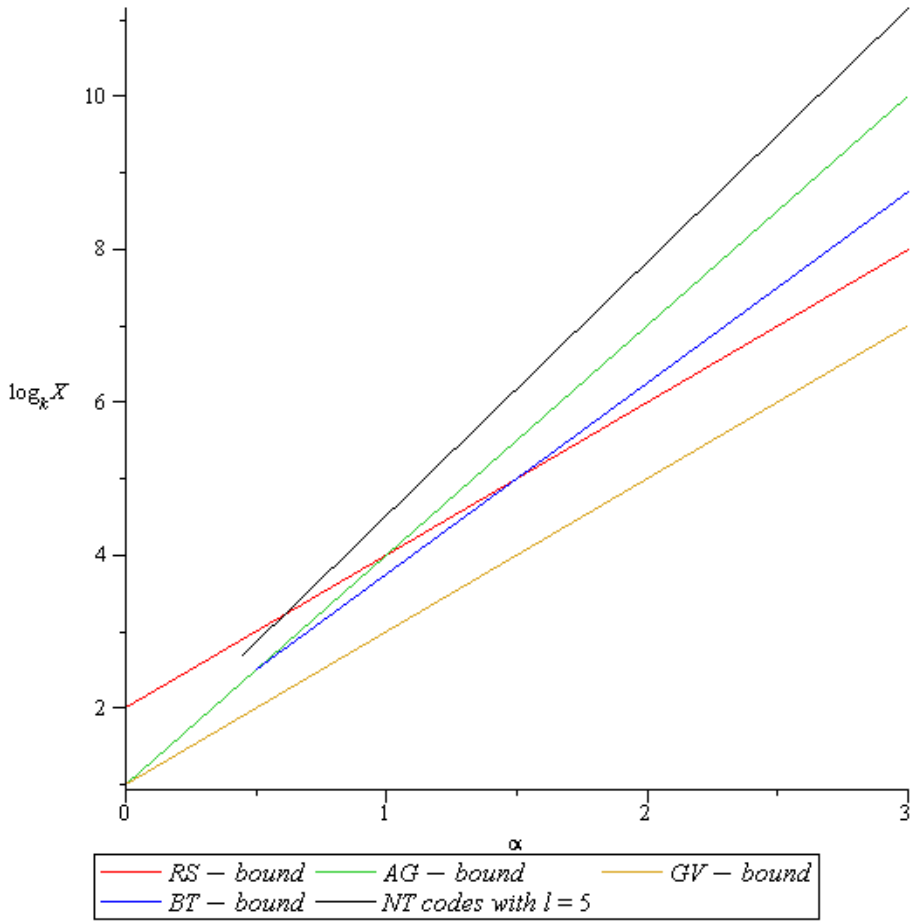
Reed-Solomon codes	$\lvert\mathcal{X}\rvert = \mathcal{O}\left(\frac{k^{2+\alpha}}{\log^2\left(k^{1+\alpha}\right)}\right)$
AG codes of high dimension	$\lvert\mathcal{X}\rvert = \mathcal{O}\left(\frac{k^{1+3\alpha}}{\log(k^{\alpha})}\right)$
Hermitian codes $m < g$, $\epsilon \geq k^{-\frac{1}{2}}$	$\lvert\mathcal{X}\rvert = \mathcal{O}\left(\left(\frac{k^{1+2\alpha}}{\log(k^{\alpha})}\right)^{\frac{5}{4}}\right)$
Norm-Trace codes for $l = 4, 5, \ldots$, $\epsilon \geq k^{-\frac{1}{\sqrt{l}}}$	$\lvert\mathcal{X}\rvert = \mathcal{O}\left(\left(\frac{k^{1+(l-\sqrt{l})\alpha}}{\log(k^{\alpha})}\right)^{\frac{l+1}{l}}\right)$
Gilbert-Varshamov bound	$\lvert\mathcal{X}\rvert = \mathcal{O}\left(k^{1+2\alpha}\right)$
Linear programming bound	$\lvert\mathcal{X}\rvert = \mathcal{O}\left(\frac{k^{1+2\alpha}}{\log(k^{\alpha})}\right)$

RS-codes, AG-codes, Hermitian Codes, GV Bound

...and then to take the logarithm with base k.

Reed-Solomon codes	$\log_k(\lvert\mathcal{X}\rvert) = 2 + 2\alpha + o(1)$
AG codes of high dimension	$\log_k(\lvert\mathcal{X}\rvert) = 1 + 3\alpha + o(1)$
Hermitian codes $m < g$, $\epsilon \geq k^{-\frac{1}{2}}$	$\log_k(\lvert\mathcal{X}\rvert) = \frac{5}{4} + \frac{5}{2}\alpha + o(1)$
Norm-Trace codes for $l = 4, 5, \ldots$, $\epsilon \geq k^{-\frac{1}{\sqrt{l}}}$	$\log_k(\lvert\mathcal{X}\rvert) = \frac{l+1}{l}(1 + \alpha(l - \sqrt{l}) + o(1)$
Gilbert-Varshamov bound	$\log_k(\lvert\mathcal{X}\rvert) = 1 + 2\alpha + o(1)$
Linear programming bound	$\log_k(\lvert\mathcal{X}\rvert) = 1 + 2\alpha + o(1)$

RS-codes, AG-codes, Hermitian Codes, GV Bound



In this presentation we shall introduce a new family of small-bias spaces using a combination of Hermitian codes as outer code. This family gives

$$\log_k(|\mathcal{X}|) = \frac{4}{3} + \frac{8}{3}\alpha + o(1).$$

Footprint of an Ideal

Definition

Given a monomial ordering $\prec$ and an ideal $I \subseteq \mathbb{F}[X_1, \ldots, X_m]$ the footprint is

$$\Delta_\prec(I) := \{X_1^{\alpha_1} \cdots X_m^{\alpha_m} \text{ is not a leading monomial}$$

$$\text{of any polynomial in } I\}$$

Theorem ([Geil & Hoholdt, 2000], [Høholdt, 1998])

Assume I is zero-dimensional (meaning that $\Delta_\prec(I)$ is finite). The variety $\mathbb{V}_{\bar{\mathbb{F}}}(I)$ satisfies $|\mathbb{V}_{\bar{\mathbb{F}}}(I)| \leq |\Delta_\prec(I)|$.

Footprint of an Ideal

Definition

Given a monomial ordering $\prec$ and an ideal $I \subseteq \mathbb{F}[X_1, \ldots, X_m]$ the footprint is

$$\Delta_\prec(I) := \{X_1^{\alpha_1} \cdots X_m^{\alpha_m} \text{ is not a leading monomial of any polynomial in } I\}$$

Theorem ([Geil & Hoholdt, 2000], [Høholdt, 1998])

Assume I is zero-dimensional (meaning that $\Delta_\prec(I)$ is finite). The variety $\mathbb{V}_{\bar{\mathbb{F}}}(I)$ satisfies $|\mathbb{V}_{\bar{\mathbb{F}}}(I)| \leq |\Delta_\prec(I)|$.

The Monomial Function w

Consider the Hermitian polynomial $X^{q+1} - Y^q - Y$ and the corresponing ideal $I = \langle X^{q+1} - Y^q - Y \rangle \subseteq \mathbb{F}_{q^2}[X, Y]$.
Define a monomial function w by $w(X^\alpha Y^\beta) = q\alpha + (q+1)\beta$ and consider the weighted degree monomial ordering $\prec_w$ given by $X^{\alpha_1} Y^{\beta_1} \prec_w X^{\alpha_2} Y^{\beta_2}$ if:

1. $w(X^{\alpha_1} Y^{\beta^1}) < w(X^{\alpha_2} Y^{\beta_2})$,
2. $w(X^{\alpha_1} Y^{\beta^1}) = w(X^{\alpha_2} Y^{\beta_2})$ but $\beta_1 < \beta_2$.

In this way: $w : \Delta_w(I) \to \langle q, q+1 \rangle$ is a bijection.

The Monomial Function w

Consider the Hermitian polynomial $X^{q+1} - Y^q - Y$ and the corresponing ideal $I = \langle X^{q+1} - Y^q - Y \rangle \subseteq \mathbb{F}_{q^2}[X, Y]$.
Define a monomial function w by $w(X^\alpha Y^\beta) = q\alpha + (q+1)\beta$ and consider the weighted degree monomial ordering $\prec_w$ given by $X^{\alpha_1} Y^{\beta_1} \prec_w X^{\alpha_2} Y^{\beta_2}$ if:

1. $w(X^{\alpha_1} Y^{\beta^1}) < w(X^{\alpha_2} Y^{\beta_2})$,
2. $w(X^{\alpha_1} Y^{\beta^1}) = w(X^{\alpha_2} Y^{\beta_2})$ but $\beta_1 < \beta_2$.

In this way: $w : \Delta_w(I) \to \langle q, q+1 \rangle$ is a bijection.

Evaluation Map

Consider next the ideal: $I_{q^2} := \langle X^{q^2} - X, Y^{q^2} - Y \rangle + I$. The variety $\mathbb{V}_{\bar{\mathbb{F}}_{q^2}}(I_{q^2})$ consists of $n = q^3$ different points $\{P_1, \ldots, P_n\}$.

The code construction relies on the bijective evaluation map:

$$\mathrm{ev} : \mathbb{F}_{q^2}[X, Y]/I_{q^2} \to \mathbb{F}_{q^2}^n$$

$$\mathrm{ev}(F(X, Y) + I_{q^2}) = (F(P_1), \ldots, F(P_n))$$

Evaluation Map

Consider next the ideal: $I_{q^2} := \langle X^{q^2} - X, Y^{q^2} - Y \rangle + I$. The variety $\mathbb{V}_{\bar{\mathbb{F}}_{q^2}}(I_{q^2})$ consists of $n = q^3$ different points $\{P_1, \ldots, P_n\}$. The code construction relies on the bijective evaluation map:

$$\mathrm{ev} : \mathbb{F}_{q^2}[X, Y]/I_{q^2} \to \mathbb{F}_{q^2}^n$$

$$\mathrm{ev}(F(X, Y) + I_{q^2}) = (F(P_1), \ldots, F(P_n))$$

Ideal and Variety

Having described the Hermitian codes as affine variety codes we are now ready to introduce the combination of codes on which our construction of small-bias space rely. Consider the ideal:

$$I^{(2)} := \langle X_1^{q+1} - Y_1^q - Y_1, X_2^{q+1} - Y_2^q - Y_2 \rangle \subset \mathbb{F}[X_1, Y_1, X_2, Y_2]$$

Ideal and Variety

Having described the Hermitian codes as affine variety codes we are now ready to introduce the combination of codes on which our construction of small-bias space rely. Consider the ideal:

$$I^{(2)} := \langle X_1^{q+1} - Y_1^q - Y_1, X_2^{q+1} - Y_2^q - Y_2 \rangle \subset \mathbb{F}[X_1, Y_1, X_2, Y_2]$$

The Monomial Function $w^{(2)}$

Assume $X_1 \prec_{\text{lex}} Y_1 \prec_{\text{lex}} X_2 \prec_{\text{lex}} Y_2$. Define a monomial function $w^{(2)}$ given by $w^{(2)}(X_1) = (q, 0)$, $w^{(2)}(Y_1) = (q+1, 0)$, $w^{(2)}(X_2) = (0, q)$ and $w^{(2)}(Y_2) = (0, q+1)$.

Let $\prec_{\mathbb{N}_0^2}$ be any monomial ordering on $\mathbb{N}_0^2$ and define $\prec_{w^2}$ by

$$X_1^{\alpha_1^{(1)}} Y_1^{\beta_1^{(1)}} X_2^{\alpha_1^{(2)}} Y_2^{\beta_1^{(2)}} \prec_{w^{(2)}} X_1^{\alpha_2^{(1)}} Y_1^{\beta_2^{(1)}} X_2^{\alpha_2^{(2)}} Y_2^{\beta_2^{(2)}}$$

if:

1. $w^{(2)}(X_1^{\alpha_1^{(1)}} Y_1^{\beta_1^{(1)}} X_2^{\alpha_1^{(2)}} Y_2^{\beta_1^{(2)}}) \prec_{\mathbb{N}_0^2} w^{(2)}(X_1^{\alpha_2^{(1)}} Y_1^{\beta_2^{(1)}} X_2^{\alpha_2^{(2)}} Y_2^{\beta_2^{(2)}})$,
2. $w^{(2)}(X_1^{\alpha_1^{(1)}} Y_1^{\beta_1^{(1)}} X_2^{\alpha_1^{(2)}} Y_2^{\beta_1^{(2)}}) = w^{(2)}(X_1^{\alpha_2^{(1)}} Y_1^{\beta_2^{(1)}} X_2^{\alpha_2^{(2)}} Y_2^{\beta_2^{(2)}})$ but $X_1^{\alpha_1^{(1)}} Y_1^{\beta_1^{(1)}} X_2^{\alpha_1^{(2)}} Y_2^{\beta_1^{(2)}} \prec_{\text{lex}} X_1^{\alpha_2^{(1)}} Y_1^{\beta_2^{(1)}} X_2^{\alpha_2^{(2)}} Y_2^{\beta_2^{(2)}}$

In this way: $w : \Delta_w(I^{(2)}) \to \langle q, q+1\rangle \times \langle q, q+1\rangle$ is a bijection.

The Monomial Function $w^{(2)}$

Assume $X_1 \prec_{\text{lex}} Y_1 \prec_{\text{lex}} X_2 \prec_{\text{lex}} Y_2$. Define a monomial function $w^{(2)}$ given by $w^{(2)}(X_1) = (q, 0)$, $w^{(2)}(Y_1) = (q+1, 0)$, $w^{(2)}(X_2) = (0, q)$ and $w^{(2)}(Y_2) = (0, q+1)$.
Let $\prec_{\mathbb{N}_0^2}$ be any monomial ordering on $\mathbb{N}_0^2$ and define $\prec_{w^2}$ by

$$X_1^{\alpha_1^{(1)}} Y_1^{\beta_1^{(1)}} X_2^{\alpha_1^{(2)}} Y_2^{\beta_1^{(2)}} \prec_{w^{(2)}} X_1^{\alpha_2^{(1)}} Y_1^{\beta_2^{(1)}} X_2^{\alpha_2^{(2)}} Y_2^{\beta_2^{(2)}}$$

if:

1. $w^{(2)}(X_1^{\alpha_1^{(1)}} Y_1^{\beta_1^{(1)}} X_2^{\alpha_1^{(2)}} Y_2^{\beta_1^{(2)}}) \prec_{\mathbb{N}_0^2} w^{(2)}(X_1^{\alpha_2^{(1)}} Y_1^{\beta_2^{(1)}} X_2^{\alpha_2^{(2)}} Y_2^{\beta_2^{(2)}})$,
2. $w^{(2)}(X_1^{\alpha_1^{(1)}} Y_1^{\beta_1^{(1)}} X_2^{\alpha_1^{(2)}} Y_2^{\beta_1^{(2)}}) = w^{(2)}(X_1^{\alpha_2^{(1)}} Y_1^{\beta_2^{(1)}} X_2^{\alpha_2^{(2)}} Y_2^{\beta_2^{(2)}})$ but $X_1^{\alpha_1^{(1)}} Y_1^{\beta_1^{(1)}} X_2^{\alpha_1^{(2)}} Y_2^{\beta_1^{(2)}} \prec_{\text{lex}} X_1^{\alpha_2^{(1)}} Y_1^{\beta_2^{(1)}} X_2^{\alpha_2^{(2)}} Y_2^{\beta_2^{(2)}}$

In this way: $w : \Delta_w(I^{(2)}) \to \langle q, q+1 \rangle \times \langle q, q+1 \rangle$ is a bijection.

The Monomial Function $w^{(2)}$

Assume $X_1 \prec_{\text{lex}} Y_1 \prec_{\text{lex}} X_2 \prec_{\text{lex}} Y_2$. Define a monomial function $w^{(2)}$ given by $w^{(2)}(X_1) = (q, 0)$, $w^{(2)}(Y_1) = (q+1, 0)$, $w^{(2)}(X_2) = (0, q)$ and $w^{(2)}(Y_2) = (0, q+1)$.
Let $\prec_{\mathbb{N}_0^2}$ be any monomial ordering on $\mathbb{N}_0^2$ and define $\prec_{w^2}$ by

$$X_1^{\alpha_1^{(1)}} Y_1^{\beta_1^{(1)}} X_2^{\alpha_1^{(2)}} Y_2^{\beta_1^{(2)}} \prec_{w^{(2)}} X_1^{\alpha_2^{(1)}} Y_1^{\beta_2^{(1)}} X_2^{\alpha_2^{(2)}} Y_2^{\beta_2^{(2)}}$$

if:

1. $w^{(2)}(X_1^{\alpha_1^{(1)}} Y_1^{\beta_1^{(1)}} X_2^{\alpha_1^{(2)}} Y_2^{\beta_1^{(2)}}) \prec_{\mathbb{N}_0^2} w^{(2)}(X_1^{\alpha_2^{(1)}} Y_1^{\beta_2^{(1)}} X_2^{\alpha_2^{(2)}} Y_2^{\beta_2^{(2)}})$,
2. $w^{(2)}(X_1^{\alpha_1^{(1)}} Y_1^{\beta_1^{(1)}} X_2^{\alpha_1^{(2)}} Y_2^{\beta_1^{(2)}}) = w^{(2)}(X_1^{\alpha_2^{(1)}} Y_1^{\beta_2^{(1)}} X_2^{\alpha_2^{(2)}} Y_2^{\beta_2^{(2)}})$ but $X_1^{\alpha_1^{(1)}} Y_1^{\beta_1^{(1)}} X_2^{\alpha_1^{(2)}} Y_2^{\beta_1^{(2)}} \prec_{\text{lex}} X_1^{\alpha_2^{(1)}} Y_1^{\beta_2^{(1)}} X_2^{\alpha_2^{(2)}} Y_2^{\beta_2^{(2)}}$

In this way: $w : \Delta_w(I^{(2)}) \to \langle q, q+1\rangle \times \langle q, q+1\rangle$ is a bijection.

Evaluation Map and Hermitian Product Code

Consider next the ideal:

$$I_{q^2}^{(2)} := \langle X_1^{q^2} - X_1, X_2^{q^2} - X_2, Y_1^{q^2} - Y_1, Y_2^{q^2} - Y_2 \rangle + I^{(2)}$$

and the corresponing variety:

$$\mathbb{V}_{\mathbb{F}_{q^2}}(I_{q^2}^{(2)}) = \mathbb{V}_{\mathbb{F}_{q^2}}(I_{q^2}) \times \mathbb{V}_{\mathbb{F}_{q^2}}(I_{q^2}) = \{Q_1, \ldots, Q_{q^6}\}.$$

For the code construction we need the following bijective evaluation map:

$$\mathrm{EV} : F_{q^2}[X_1, Y_1, X_2, Y_2]/I_{q^2}^{(2)} \to \mathbb{F}_{q^2}^{q^6}$$

$$EV(F(X_1, Y_1, X_2, Y_2) + I_{q^2}^{(2)}) = (F(Q_1), \ldots, F(Q_{q^6})).$$

Evaluation Map and Hermitian Product Code

Consider next the ideal:

$$I_{q^2}^{(2)} := \langle X_1^{q^2} - X_1, X_2^{q^2} - X_2, Y_1^{q^2} - Y_1, Y_2^{q^2} - Y_2 \rangle + I^{(2)}$$

and the corresponing variety:

$$\mathbb{V}_{\mathbb{F}_{q^2}}(I_{q^2}^{(2)}) = \mathbb{V}_{\mathbb{F}_{q^2}}(I_{q^2}) \times \mathbb{V}_{\mathbb{F}_{q^2}}(I_{q^2}) = \{Q_1, \ldots, Q_{q^6}\}.$$

For the code construction we need the following bijective evaluation map:

$$\mathrm{EV} : F_{q^2}[X_1, Y_1, X_2, Y_2]/I_{q^2}^{(2)} \to \mathbb{F}_{q^2}^{q^6}$$

$$EV(F(X_1, Y_1, X_2, Y_2) + I_{q^2}^{(2)}) = (F(Q_1), \ldots, F(Q_{q^6})).$$

Evaluation Map and Hermitian Product Code

We can define:

$$\tilde{E}(\delta) := \mathrm{Span}_{\mathbb{F}_{q^2}} \left\{ EV(X_1^{i_1} Y_1^{j_1} X_2^{i_2} Y_2^{j_2} + I_{q^2}^{(2)}) | 0 \leq i_1, i_2 \leq q^2, \right.$$

$$\left. 0 \leq j_1, j_2 < q, (q^3 - w(X_1^{i_1} Y_1^{j_1}))(q^3 - w(X_2^{i_2} Y_2^{j_2})) \geq \delta \right\}$$

Parameters of Hermitian Product Code

Proposition

Assume $\delta \geq T$ where $T = q^3 - g$. The parameters of $\tilde{E}(\delta)$ are $\left[n = q^6, k \geq T^2 - \delta + \delta \log\left(\frac{\delta}{T^2}\right), d \geq \delta\right]$.

Conc. Code with Herm. Product Code as Outer Code

Theorem

For any $\epsilon \in (0,1)$, using codes $\tilde{E}(\delta)$ as outer code in the construction of Theorem 8 one can construct ϵ-bias spaces with

$$\mathcal{X} \subseteq \mathbb{F}_2^{\Omega(k)}, \quad |\mathcal{X}| = \mathcal{O}\left(\left(\frac{k}{\epsilon + (1-\epsilon)\ln(1-\epsilon)}\right)^{\frac{4}{3}}\right).$$

Theorem

Consider the family of ϵ-bias spaces in Theorem 12. Given $\alpha \in \mathbb{R}^+$ choose $\epsilon = k^{-\alpha}$ and let $k \to \infty$. We have:

$$\log_k(|\mathcal{X}|) = \frac{4}{3} + \frac{8}{3}\alpha + o(1).$$

Conc. Code with Herm. Product Code as Outer Code

Theorem

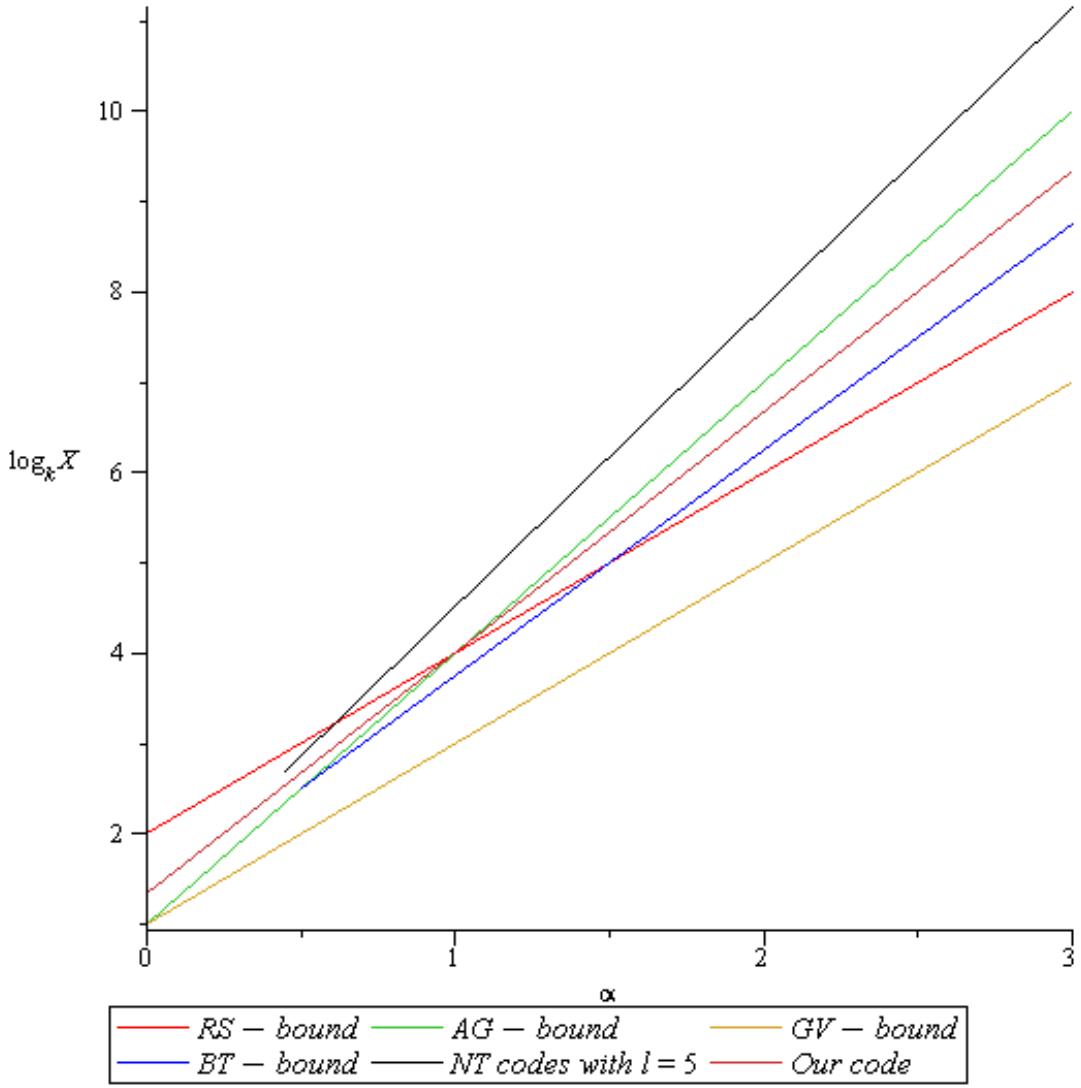
For any $\epsilon \in (0,1)$, using codes $\tilde{E}(\delta)$ as outer code in the construction of Theorem 8 one can construct ϵ-bias spaces with

$$\mathcal{X} \subseteq \mathbb{F}_2^{\Omega(k)}, \quad |\mathcal{X}| = \mathcal{O}\left(\left(\frac{k}{\epsilon + (1-\epsilon)\ln(1-\epsilon)}\right)^{\frac{4}{3}}\right).$$

Theorem

Consider the family of ϵ-bias spaces in Theorem 12. Given $\alpha \in \mathbb{R}^+$ choose $\epsilon = k^{-\alpha}$ and let $k \to \infty$. We have:

$$\log_k(|\mathcal{X}|) = \frac{4}{3} + \frac{8}{3}\alpha + o(1).$$


10
8
6
4
2
0
1
2
3
$\log_k X$
α
RS − bound
AG − bound
GV − bound
BT − bound
NT codes with l = 5
Our code

For $\alpha < \frac{1}{2}$, the complexity of the AG construction is much higher than the complexity of the new construction that we propose.

Norm-Trace Codes

The method developed by Ben-Aroya and Ta-Shma for Hermitian codes in [Ben-Aroya & Ta-Shma, 2009] were generalized to norm-trace codes by Matthew and Peachey in [Matthews & Peachey, 2011]. Given $r \geq 2$ consider the $\mathcal{C}_{ab}$ curve [Miura & Kamiya, 1993]

$$X^{\frac{q^r-1}{q-1}} - Y^{q^{r-1}} - Y^{q^{r-2}} - \ldots - Y^q - Y$$

known as the norm-trace curve over $\mathbb{F}_{q^r}$ [Geil, 2003].

Norm-Trace Codes

Theorem ([Matthews & Peachey, 2011])

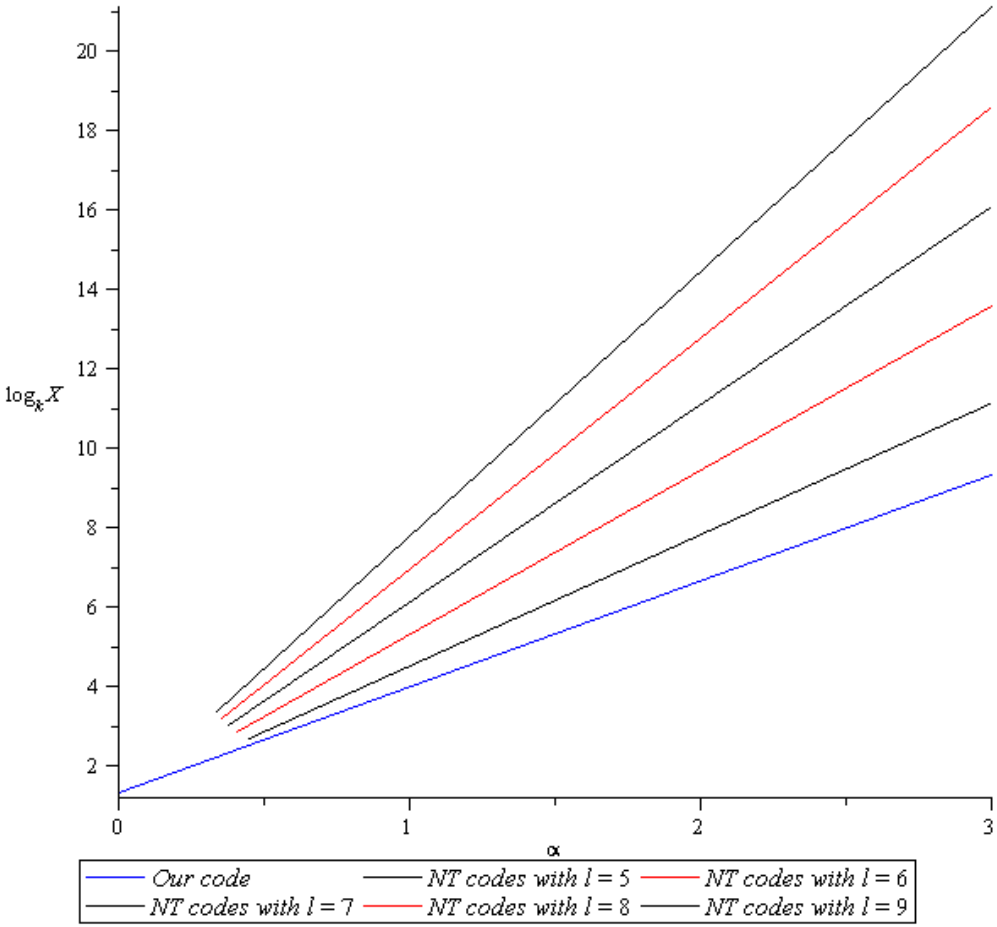
Given an integer $l \geq 4$, define $r = \left\lfloor \frac{l+2}{3} \right\rfloor$. Let k be a positive integer and ϵ a real number, $0 < \epsilon < 1$ such that

$$\frac{\epsilon}{\left(\log_v\left(\frac{1}{\epsilon}\right)\right)^{\frac{1}{\sqrt{l}}}} \leq k^{-\frac{1}{\sqrt{l}}}$$

holds. Here, v is any fixed real number larger than 1. Using the norm-trace function field over $\mathbb{F}_{q^r}$ one can construct an ϵ-bias space $\mathcal{X} \subseteq \mathbb{F}_2^{\Omega(k)}$ with

$$|\mathcal{X}| = \mathcal{O}\left(\left(\frac{k}{\epsilon^{l-\sqrt{l}}\log_v\left(\frac{1}{\epsilon}\right)}\right)^{\frac{l+1}{l}}\right).$$

Our Codes VS Norm-Trace Codes as Outer Codes




Alon, N., Goldreich, O., Håstad, J., & Peralta, R. 1992.
Simple Constructions of Almost k-wise Independent Random Variables.
Random Structures & Algorithms, **3**(3), 289–304.


Ben-Aroya, A., & Ta-Shma, A. 2009.
Constructing small-bias sets from algebraic-geometric codes.
191–197.


Geil, O. 2003.
On codes from norm-trace curves.
Finite fields and their Applications, **9**(3), 351–371.


Geil, O., & Hoholdt, T. 2000.
Footprints or generalized Bezout's theorem.
Information Theory, IEEE Transactions on, **46**(2), 635–641.


Høholdt, T. 1998.
On (or in) Dick Blahuts footprint, in Codes, Curves and Signals,(A. Vardy, ed.).


Matthews, G. L., & Peachey, J. D. 2011.
Small-bias sets from extended norm-trace codes.


Miura, S., & Kamiya, N. 1993.
Geometric-Goppa codes on some maximal curves and their minimum distance.
Pages 85–86 of: Proc. 1993, IEEE Inform. Theory Workshop.

Thank you for your attention!