

Bounds on ordered codes and ordered orthogonal arrays

Punarbasu Purkayastha
Joint work with Alexander Barg

University of Maryland, College Park

November 28, 2007

Outline

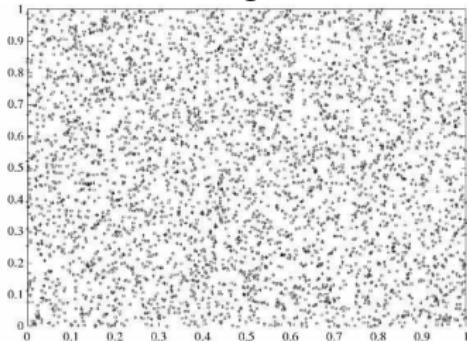
- Introduction to (t, m, s) – nets and Ordered Orthogonal Arrays
- Introduction to NRT-space
- Previous work
- Properties of r -variate Krawtchouk Polynomials
- Upper Bounds on the size of codes in NRT-space

Introduction

Numerical integration of functions on the unit cube

Introduction

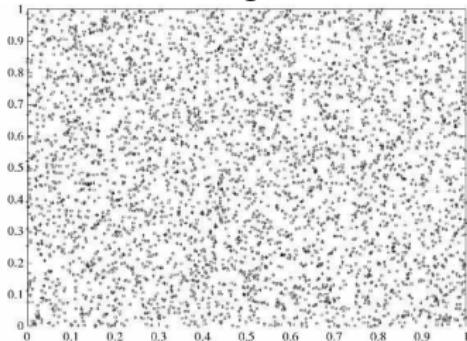
Numerical integration of functions on the unit cube



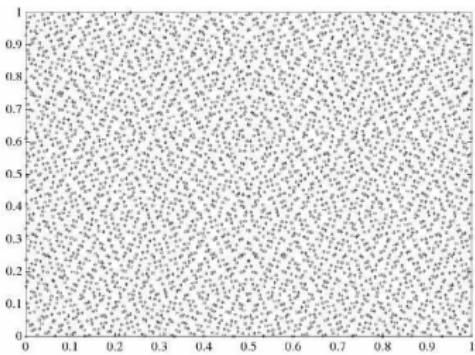
- Monte-Carlo Method
- Randomly generated set of points
- From Uniform distribution
- Not very uniformly distributed

Introduction

Numerical integration of functions on the unit cube



- Monte-Carlo Method
- Randomly generated set of points
- From Uniform distribution
- Not very uniformly distributed

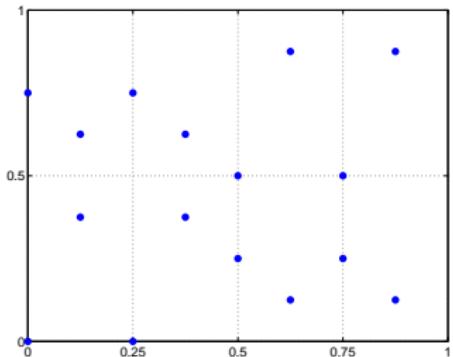


- Quasi Monte-Carlo Method
- Deterministic set of points
- More uniformly distributed

Images from Morokoff & Caflisch (1994)

(t, m, s) -nets

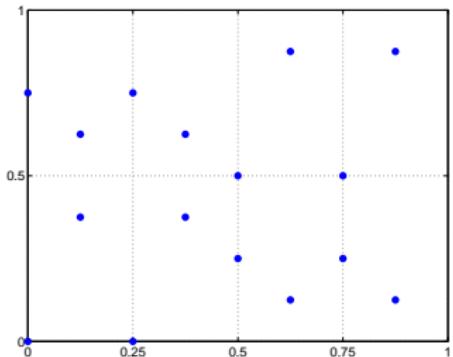
- Sobol (1967) introduced the notion of uniformly distributed point sets for numerical integration
- Further developed by Niederreiter (1987) into the notion of (t, m, s) -nets



- (t, m, s) -net in base q is a set of q^m points in $[0, 1]^s$ such that every interval of the form $\prod_{i=1}^s [\frac{a_i}{q^{d_i}}, \frac{a_i+1}{q^{d_i}})$, where $d_i \geq 0, a_i < q^{d_i}$ are integers, of volume $q^{-\sum d_i} = q^{-(m-t)}$ contains exactly q^t points.

(t, m, s) -nets

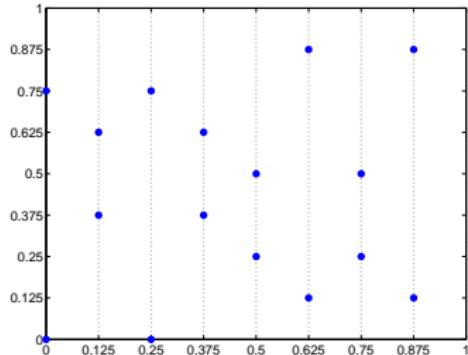
- Sobol (1967) introduced the notion of uniformly distributed point sets for numerical integration
- Further developed by Niederreiter (1987) into the notion of (t, m, s) -nets



- (t, m, s) -net in base q is a set of q^m points in $[0, 1]^s$ such that every interval of the form $\prod_{i=1}^s [\frac{a_i}{q^{d_i}}, \frac{a_i+1}{q^{d_i}})$, where $d_i \geq 0, a_i < q^{d_i}$ are integers, of volume $q^{-\sum d_i} = q^{-(m-t)}$ contains exactly q^t points.
- $(1, 4, 2)$ -net in base 2
- Every interval of above form and volume $1/2^3$ contains 2 points

(t, m, s) -nets

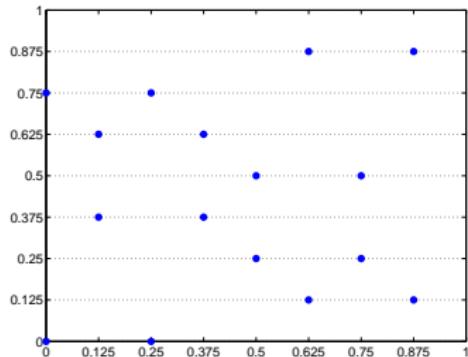
- Sobol (1967) introduced the notion of uniformly distributed point sets for numerical integration
- Further developed by Niederreiter (1987) into the notion of (t, m, s) -nets



- (t, m, s) -net in base q is a set of q^m points in $[0, 1]^s$ such that every interval of the form $\prod_{i=1}^s [\frac{a_i}{q^{d_i}}, \frac{a_i+1}{q^{d_i}}]$, where $d_i \geq 0, a_i < q^{d_i}$ are integers, of volume $q^{-\sum d_i} = q^{-(m-t)}$ contains exactly q^t points.
- $(1, 4, 2)$ -net in base 2
- Every interval of above form and volume $1/2^3$ contains 2 points

(t, m, s) -nets

- Sobol (1967) introduced the notion of uniformly distributed point sets for numerical integration
- Further developed by Niederreiter (1987) into the notion of (t, m, s) -nets



- (t, m, s) -net in base q is a set of q^m points in $[0, 1]^s$ such that every interval of the form $\prod_{i=1}^s [\frac{a_i}{q^{d_i}}, \frac{a_i+1}{q^{d_i}}]$, where $d_i \geq 0, a_i < q^{d_i}$ are integers, of volume $q^{-\sum d_i} = q^{-(m-t)}$ contains exactly q^t points.
- $(1, 4, 2)$ -net in base 2
- Every interval of above form and volume $1/2^3$ contains 2 points

Ordered Orthogonal Arrays

- **Left-justified columns:** Consider an array of sl columns, labeled $\{(i, j) : 1 \leq i \leq s, 1 \leq j \leq l\}$. Called a set T of columns left-justified if (i, j) included $\Rightarrow (i, j - 1)$ also included.

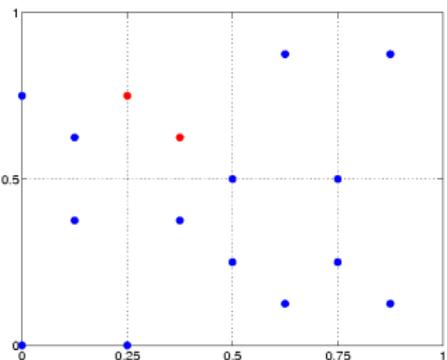
0	0	0	0	0	0
0	0	1	1	0	1
0	1	0	1	1	0
0	1	1	0	1	1
1	0	0	0	1	0
1	0	1	1	1	1
1	1	0	1	0	0
1	1	1	0	0	1
0	0	0	1	1	0
0	0	1	0	1	1
0	1	0	0	0	0
0	1	1	1	0	1
1	0	0	1	0	0
1	0	1	0	0	1
1	1	0	0	1	0
1	1	1	1	1	1

Ordered Orthogonal Arrays

0	0	0	0	0	0
0	0	1	1	0	1
0	1	0	1	1	0
0	1	1	0	1	1
1	0	0	0	1	0
1	0	1	1	1	1
1	1	0	1	0	0
1	1	1	0	0	1
0	0	0	1	1	0
0	0	1	0	1	1
0	1	0	0	0	0
0	1	1	1	0	1
1	0	0	1	0	0
1	0	0	0	1	0
1	0	1	0	0	0
0	1	1	0	1	0
1	0	0	1	0	0
1	0	0	0	0	1
1	0	1	1	1	1
1	1	0	1	1	1
1	1	1	1	0	0

- **Left-justified columns:** Consider an array of sl columns, labeled $\{(i, j) : 1 \leq i \leq s, 1 \leq j \leq l\}$. Called a set T of columns left-justified if (i, j) included $\Rightarrow (i, j - 1)$ also included.
- An $OOA_\lambda(t, s, l, q)$ is an $\lambda q^t \times sl$ array, with columns indexed by (i, j) and elements from \mathbb{F}_q , such that in every left-justified set T of t columns each t -tuple occurs exactly λ times as a row.
- $OOA_2(3, 2, 3, 2)$: for every left-justified 3 columns each row repeats 2 times.

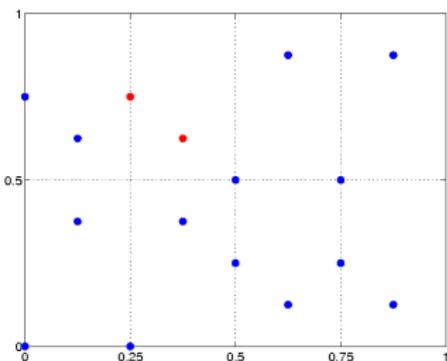
Ordered Orthogonal Arrays



Binary
representation:

.000	.000
.001	.101
.010	.110
.011	.011
.100	.010
.101	.111
.110	.100
.111	.001
.000	.110
.001	.011
.010	.000
.011	.101
.100	.100
.101	.001
.110	.010
.111	.111

Ordered Orthogonal Arrays



Theorem

Lawrence (1996), Mullen & Schmid (1996): There exists a (t, m, s) -net in base q iff there exists a $OOA_{q^t}(m - t, s, m - t, q)$ of size q^m .

This example: $q = 2, m = 4, t = 1, s = 2$

$(1, 4, 2)$ -net exists iff $OOA_2(4 - 1, 2, 4 - 1, 2)$ of size 2^4 exists

Binary representation:	
.000	.000
.001	.101
.010	.110
.011	.011
.100	.010
.101	.111
.110	.100
.111	.001
.000	.110
.001	.011
.010	.000
.011	.101
.100	.100
.101	.001
.110	.010
.111	.111

Ordered Hamming Space (Rosenbloom & Tsfasman (1997))

- Field \mathbb{F}_q
- Write $\mathbf{x} \in \mathbb{F}_q^{r,n}$ as $\mathbf{x} = (x_{11}, \dots, x_{1r} | \dots | x_{n1}, \dots, x_{nr})$. (n blocks of r elements each)
- Weight of one block, say $wt(x_{11}, \dots, x_{1r})$ is the **maximum value of index j** for which $x_{1j} \neq 0$. Weight is 0 if there is no such index j .
- $r = 3, n = 4, q = 2$: $\mathbf{x} = (0, 1, 0 | 0, 0, 0 | 1, 1, 0 | 1, 0, 0)$.
$$\begin{matrix} 2 & 0 & 2 & 1 \end{matrix}$$

Ordered Hamming Space (Rosenbloom & Tsfasman (1997))

- Field \mathbb{F}_q
- Write $\mathbf{x} \in \mathbb{F}_q^{r,n}$ as $\mathbf{x} = (x_{11}, \dots, x_{1r} | \dots | x_{n1}, \dots, x_{nr})$. (n blocks of r elements each)
- Weight of one block, say $wt(x_{11}, \dots, x_{1r})$ is the **maximum value of index j** for which $x_{1j} \neq 0$. Weight is 0 if there is no such index j .
- Let $e_i = \#$ blocks of weight i . Then $wt(\mathbf{x}) \triangleq \sum_{i=1}^r ie_i$.
- Distance $d(\mathbf{x}, \mathbf{y}) = wt(\mathbf{x} - \mathbf{y})$.
- $r = 3, n = 4, q = 2$: $\mathbf{x} = (0, 1, 0 | 0, 0, 0 | 1, 1, 0 | 1, 0, 0)$.
$$\begin{matrix} 2 & 0 & 2 & 1 \end{matrix}$$

In this case, $e_1 = 1, e_2 = 2, e_3 = 0, e_0 = n - \sum_{i=1}^r e_i = 1$.
Hence, $wt(\mathbf{x}) = 5$.

Niederreiter-Rosenbloom-Tsfasman space (NRT-space)

Other contexts

- Günther weight in the theory of linear complexity of sequences [Massey & Serconek (1996)]
- A communication system for a type of slow fading channel [Tavildar & Viswanath (2006)]
- List Decoding algorithms for Reed-Solomon Codes [Nielsen (2000)]

Main Problem

Consider a set \mathcal{C} of M points such that $d(\mathbf{x}, \mathbf{y}) \geq d$, $\forall \mathbf{x} \neq \mathbf{y}$ in \mathcal{C}

Determine **universal upper bounds** on the size of codes \mathcal{C} in the NRT-space.

Selected previous work on bounds in NRT-space or (t, m, s) -nets

- (Martin, Stinson (1999)) Association Scheme for OOA and (t, m, s) -nets,- showed that **OOA and ordered codes are dual concepts** in the context of Delsarte's Theory, Generalized Rao bound for (t, m, s) -nets
- (Martin (2000)) LP Bounds for OOA and (t, m, s) -nets
- (Martin, Visentin (2007)) Dual Plotkin Bound for (t, m, s) -nets
- (Rosenbloom-Tsfasman (1997)) **Gilbert Bound, Plotkin Bound**, Hamming Bound, Singleton Bound, Algebraic-Geometry Bound, Code constructions (Reed-Solomon, Reed-Muller, Algebraic-Geometry)
- (Bierbrauer, Schmid, Edel (2002,2005)) Gilbert-Varshamov Bound,
- (Bierbrauer (2007)) Plotkin Bound, Sphere-Packing Bound, Quadratic Bound, **explicit expression of Generalized Krawtchouk Polynomials.**

Bassalygo-Elias Bound

- $e_i = \#$ blocks of weight i .
- Shape: $e = (e_1, \dots, e_r)$
- Degree: $|e| \triangleq \sum_{i=1}^r e_i$ (Number of non-zero blocks)
- Weight: $|e|' \triangleq \sum_i i e_i$ (Weight of x with shape e)

Bassalygo-Elias Bound

- $e_i = \#$ blocks of weight i .
- Shape: $e = (e_1, \dots, e_r)$
- Degree: $|e| \triangleq \sum_{i=1}^r e_i$ (Number of non-zero blocks)
- Weight: $|e|' \triangleq \sum_i i e_i$ (Weight of \mathbf{x} with shape e)
- Number of vectors of shape e is

$$v_e = \binom{n}{e_0, e_1, \dots, e_r} (q-1)^{|e|} q^{|e|' - |e|}$$

- Cardinality of the sphere of weight w is

$$S_w = \sum_{e:|e|'=w} v_e$$

Bassalygo-Elias Bound

Theorem

Let \mathcal{C} be an (n, M, d) code. Let $\delta_{\text{crit}} = 1 - \frac{1}{rq^r} \frac{q^r - 1}{q - 1}$. For any $w \leq nr\delta_{\text{crit}}(1 - \sqrt{1 - d/(nr\delta_{\text{crit}})})$,

$$|\mathcal{C}| = M \leq \frac{q^{rn}}{S_w} \frac{dn}{(dn - 2wn + w^2/r\delta_{\text{crit}})}.$$

For any *linear OOA* $(d - 1, n, r, q)$, \mathcal{C} of size M ,

$$|\mathcal{C}| = M \geq \frac{1}{dn} S_w \left(dn - 2wn + \frac{w^2}{r\delta_{\text{crit}}} \right).$$

Bassalygo-Elias Bound

Theorem

Let \mathcal{C} be an (n, M, d) code. Let $\delta_{\text{crit}} = 1 - \frac{1}{rq^r} \frac{q^r - 1}{q - 1}$. For any $w \leq nr\delta_{\text{crit}}(1 - \sqrt{1 - d/(nr\delta_{\text{crit}})})$,

$$|\mathcal{C}| = M \leq \frac{q^{rn}}{S_w} \frac{dn}{(dn - 2wn + w^2/r\delta_{\text{crit}})}.$$

For any linear OOA($d - 1, n, r, q$), \mathcal{C} of size M ,

$$|\mathcal{C}| = M \geq \frac{1}{dn} S_w (dn - 2wn + \frac{w^2}{r\delta_{\text{crit}}}).$$

Proof relies on:

1. Lemma (Johnson-type bound): Let C , $|C| = M'$ be a code all of whose vectors have weight w and are at least distance d apart. Then for $d \geq 2w - w^2/(nr\delta_{\text{crit}})$,

$$M' \leq \frac{dn}{dn - 2wn + w^2/r\delta_{\text{crit}}}.$$

2. Inequality: $MS_w = \sum_{\mathbf{x} \in \mathbb{F}_q^{r,n}} (\mathcal{C} - \mathbf{x}) \cap \{\mathcal{S}_w\} \leq q^{rn} M'$

Bassalygo-Elias Bound: Asymptotics

Let r be fixed, $n \rightarrow \infty$, $d/nr \rightarrow \delta$, $\frac{1}{nr} \log_q M \rightarrow R$, then

$$R \leq 1 - H_{q,r} \left(\delta_{\text{crit}} \left(1 - \sqrt{1 - \delta/\delta_{\text{crit}}} \right) \right).$$

$q^{nrH_{q,r}(\delta)}$ is the asymptotic volume of the ball of radius δnr in $\mathbb{F}_q^{r,n}$.

Generalized Krawtchouk Polynomials

- $K_f(x)$: r -variate polynomials, indexed by the shapes $f \in \Delta_{r,n}$ where $\Delta_{r,n}$ is the set of all partitions of $N \leq n$ into r parts
- Let F, G be r -variate polynomials, and define the inner product on $L_2(\Delta_{r,n})$:

$$\langle F, G \rangle \triangleq \sum_e F(e)G(e)v_e q^{-rn}$$

- **Orthogonality**: $\langle K_f, K_g \rangle = v_f \delta_{f,g}$

Linear Programming Bound (Delsarte 1973)

Theorem

Let $F(x) = F_0 + \sum_{e \neq 0} F_e K_e(x)$ be a polynomial that satisfies

$$F_0 > 0, \quad F_e \geq 0 (e \neq 0); \quad F(e) \leq 0 \quad \text{for all } e \text{ such that } |e|' \geq d.$$

Then any (n, M, d) code satisfies

$$M \leq F(0)/F_0.$$

Any OOA of strength $t = d - 1$ and size M' satisfies

$$M' \geq q^{nr} F_0 / F(0).$$

Generalized Krawtchouk Polynomials: Properties

- Orthogonality: $\langle K_f, K_g \rangle = v_f \delta_{f,g}$
- Using shapes $F_i = (0^{i-1}, 1, 0^{r-i-1})$, linear polynomials are

$$K_{F_i}(e) = q^{i-1}(q-1)(n - e_r - \cdots - e_{r-i+2}) - q^i e_{r-i+1}$$

(Can be derived using Gram-Schmidt on $\{1, e_1, \dots, e_r\}$)



- Can express e_i in terms of the degree-1 polynomials to get:

$$e_i = q^{i-r-1}((q-1)(n + K_{F_1} + \cdots + K_{F_{r-i}}) - K_{F_{r-i+1}}), \quad \text{and}$$

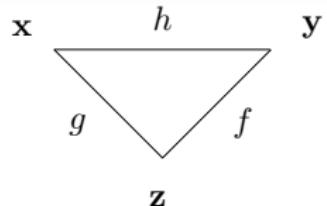
$$P(e) = \delta_{\text{crit}} rn - \sum_i i e_i = \sum_i L_i K_{F_i}(e)$$

where $L_i = \frac{q^{r-i+1}-1}{q^r(q-1)}$.

Generalized Krawtchouk Polynomials: Properties

Intersection numbers:

$$K_g(e)K_f(e) = \sum_h p_{g,f}^h K_h(e), \quad \text{where}$$

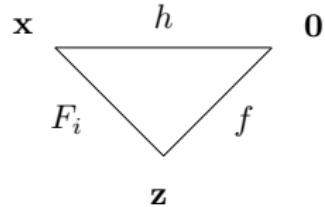


$p_{g,f}^h = |\{\mathbf{z} \in \mathbb{F}_q^{r,n} : \text{shape}(\mathbf{z} - \mathbf{x}) = g; \text{shape}(\mathbf{z} - \mathbf{y}) = f; \text{shape}(\mathbf{x} - \mathbf{y}) = h\}|$
are the intersection numbers

Generalized Krawtchouk Polynomials: Properties

Intersection numbers:

$$K_g(e)K_f(e) = \sum_h p_{g,f}^h K_h(e), \quad \text{where}$$



$$p_{g,f}^h = |\{\mathbf{z} \in \mathbb{F}_q^{r,n} : \text{shape}(\mathbf{z} - \mathbf{x}) = g; \text{shape}(\mathbf{z} - \mathbf{y}) = f; \text{shape}(\mathbf{x} - \mathbf{y}) = h\}|$$

are the intersection numbers

Values of $p_{F_i,f}^h$ can be explicitly computed.

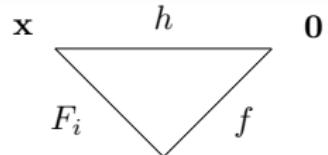
$$\mathbf{z} - \mathbf{x} = (0^r | 0^r | \cdots | u_1, \dots, u_i, 0, \dots, 0 | 0^r | \cdots | 0^r)$$

$$p_{F_i,f}^h = \begin{cases} (n - |f| + 1)q^{i-1}(q-1) & h = (f_1, \dots, f_i - 1, \dots, f_r), \ |h| = |f| - 1 \\ 0 & \text{otherwise} \end{cases}$$

Generalized Krawtchouk Polynomials: Properties

Intersection numbers:

$$K_g(e)K_f(e) = \sum_h p_{g,f}^h K_h(e), \quad \text{where}$$



$p_{g,f}^h = |\{\mathbf{z} \in \mathbb{F}_q^{r,n} : \text{shape}(\mathbf{z} - \mathbf{x}) = g; \text{shape}(\mathbf{z} - \mathbf{y}) = f; \text{shape}(\mathbf{x} - \mathbf{y}) = h\}|$
are the intersection numbers

Values of $p_{F_i,f}^h$ can be explicitly computed.

$$\mathbf{z} - \mathbf{x} = (0^r | 0^r | \cdots | u_1, \dots, u_i, 0, \dots, 0 | 0^r | \cdots | 0^r)$$

$$p_{F_i,f}^h = \begin{cases} (n - |f| + 1)q^{i-1}(q-1) & h = (f_1, \dots, f_i - 1, \dots, f_r), |h| = |f| - 1 \\ f_i + 1, & h = (f_1, \dots, f_i + 1, \dots, f_r), |h| = |f| + 1 \\ f_i(q-2)q^{i-1}, & h = f \\ (f_k + 1)(q-1)q^{i-1}, & h = (f_1, \dots, f_k + 1, \dots, f_i - 1, \dots, f_r), \\ & 1 \leq k < i, |h| = |f| \\ (f_i + 1)(q-1)q^{k-1}, & h = (f_1, \dots, f_k - 1, \dots, f_i + 1, \dots, f_r), \\ & 1 \leq k < i, |h| = |f| \\ 0, & \text{otherwise} \end{cases}$$

Generalized Krawtchouk Polynomials: Properties

- Three-term relation:

Let $\mathbb{K}_\kappa(e)$ be the column vector $(K_f(e))_{|f|=\kappa}$, $P(e) = \sum_i L_i K_{F_i}(e)$.

$$P(e)\mathbb{K}_\kappa(e) = a_\kappa \mathbb{K}_{\kappa+1}(e) + b_\kappa \mathbb{K}_\kappa(e) + c_\kappa \mathbb{K}_{\kappa-1}(e)$$

$$a_\kappa[f, h] = L_i(f_i + 1) \quad h = (f_1, \dots, f_i + 1, \dots, f_r)$$

$$c_\kappa[f, h] = L_i(n - \kappa + 1)q^{i-1}(q - 1) \quad h = (f_1, \dots, f_i - 1, \dots, f_r)$$

$$b_\kappa[f, h] = \begin{cases} L_i f_i (q - 2) q^{i-1} & h = f \\ L_i (f_k + 1) (q - 1) q^{i-1} & h = (f_1, \dots, f_k + 1, \dots, f_i - 1, \dots, f_r) \\ & 1 \leq k < i \\ L_i (f_i + 1) (q - 1) q^{k-1} & h = (f_1, \dots, f_k - 1, \dots, f_i + 1, \dots, f_r) \\ & 1 \leq k < i \end{cases}$$

Generalized Krawtchouk Polynomials: Properties

- Three-term relation:

Let $\mathbb{K}_\kappa(e)$ be the column vector $(K_f(e))_{|f|=\kappa}$, $P(e) = \sum_i L_i K_{F_i}(e)$.

$$P(e)\mathbb{K}_\kappa(e) = a_\kappa \mathbb{K}_{\kappa+1}(e) + b_\kappa \mathbb{K}_\kappa(e) + c_\kappa \mathbb{K}_{\kappa-1}(e)$$

$$a_\kappa[f, h] = L_i(f_i + 1) \quad h = (f_1, \dots, f_i + 1, \dots, f_r)$$

$$c_\kappa[f, h] = L_i(n - \kappa + 1)q^{i-1}(q - 1) \quad h = (f_1, \dots, f_i - 1, \dots, f_r)$$

$$b_\kappa[f, h] = \begin{cases} L_i f_i (q-2) q^{i-1} & h = f \\ L_i (f_k + 1) (q-1) q^{i-1} & h = (f_1, \dots, f_k + 1, \dots, f_i - 1, \dots, f_r) \\ & 1 \leq k < i \\ L_i (f_i + 1) (q-1) q^{k-1} & h = (f_1, \dots, f_k - 1, \dots, f_i + 1, \dots, f_r) \\ & 1 \leq k < i \end{cases}$$

- Three-term relation with normalized polynomials $\langle \tilde{K}_f, \tilde{K}_g \rangle = \delta_{f,g}$:

$$P(e)\tilde{\mathbb{K}}_\kappa(e) = A_\kappa \tilde{\mathbb{K}}_{\kappa+1}(e) + B_\kappa \tilde{\mathbb{K}}_\kappa(e) + C_\kappa \tilde{\mathbb{K}}_{\kappa-1}(e)$$



Generalized Krawtchouk Polynomials

- Explicit expression (Bierbrauer, 2007):

$$K_f(x) = q^{|f|' - |f|} \prod_{i=1}^r k_{f_i}(n_i, x_{r-i+1}), \quad n_i = n - \sum_{j=r-i}^r x_j - \sum_{j=i+1}^r f_j$$

$$k_l(n, y) = \sum_{i=0}^l (-1)^i (q-1)^{l-i} \binom{y}{i} \binom{n-y}{l-i}$$

Linear Programming Bound

- In Hamming space, the LP Bound relies on the asymptotic estimate of the first root of the Krawtchouk Polynomial $k_l(y)$.
- Difficult to work with roots of the Generalized Krawtchouk Polynomials.
- Instead we rely on a linear algebraic, "Spectral Method"
Bachoc (2006), Barg & Nogin (2006)

Linear Programming Bound

Let λ_κ be the maximum eigenvalue of

$$\tilde{\mathbf{S}}_\kappa = \begin{bmatrix} B_0 & A_0 & 0 & \dots & 0 \\ C_1 & B_1 & A_1 & \dots & 0 \\ 0 & C_2 & B_2 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & C_\kappa & B_\kappa \end{bmatrix}$$

Theorem

Let \mathcal{C} be a (n, M, d) code. Let κ be such that $P(e) \leq \lambda_{\kappa-1}$, $\forall e : |e|' \geq d$. Then

$$M \leq \frac{4r\delta_{\text{crit}}(n - \kappa)}{\delta_{\text{crit}}rn - \lambda_\kappa} (q^r - 1)^\kappa \binom{n}{\kappa}.$$

Let \mathcal{C} be a $(t = d - 1, n, r, q)$ OOA of size M . Then

$$M \geq \frac{q^{nr}}{\binom{n}{\kappa}} \frac{(\delta_{\text{crit}}rn - \lambda_\kappa)}{4r\delta_{\text{crit}}(n - \kappa)(q^r - 1)^\kappa}.$$

Linear Programming Bound

Let λ_κ be the maximum eigenvalue of

$$\tilde{\mathbf{S}}_\kappa = \begin{bmatrix} B_0 & A_0 & 0 & \dots & 0 \\ C_1 & B_1 & A_1 & \dots & 0 \\ 0 & C_2 & B_2 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & C_\kappa & B_\kappa \end{bmatrix}$$

Theorem

Let \mathcal{C} be a (n, M, d) code. Let κ be such that $P(e) \leq \lambda_{\kappa-1}$, $\forall e : |e|' \geq d$. Then

$$M \leq \frac{4r\delta_{\text{crit}}(n - \kappa)}{\delta_{\text{crit}}rn - \lambda_\kappa} (q^r - 1)^\kappa \binom{n}{\kappa}.$$

Let \mathcal{C} be a $(t = d - 1, n, r, q)$ OOA of size M . Then

$$M \geq \frac{q^{nr}}{\binom{n}{\kappa}} \frac{(\delta_{\text{crit}}rn - \lambda_\kappa)}{4r\delta_{\text{crit}}(n - \kappa)(q^r - 1)^\kappa}.$$

Linear Programming Bound

- Choice of polynomial $F(e)$: $F(e) = (P(e) - \lambda_\kappa)G(e)^2$ where $G(e)$ is (almost) an eigenfunction of

$$Proj_{\deg \leq \kappa} \circ P(e) = \tilde{\mathbf{S}}_\kappa$$

$\tilde{\mathbf{S}}_\kappa$ is **symmetric, irreducible and non-negative**

\Rightarrow (Perron-Frobenius)

- λ_κ is the unique maximum eigenvalue with a positive eigenvector G .
- $\lambda_{\kappa-1} \leq \lambda_\kappa$.
- Need above to show $F_0 > 0$, $F_e \geq 0$ and $F(e) \leq 0 \ \forall e : |e|' \geq d$.

Asymptotic Bound

Theorem

Let $\kappa/n \rightarrow \tau$, $f_i/n \rightarrow \tau_i$. Then

$$\lim_{\substack{n \rightarrow \infty \\ \frac{\kappa}{n} \rightarrow \tau}} \frac{\lambda_\kappa}{n} \geq \max_{\substack{\tau_i \geq 0 \\ \sum_{i=1}^r \tau_i = \tau}} \Lambda(\tau_1, \dots, \tau_r)$$

where

$$\begin{aligned} \Lambda(\tau_1, \dots, \tau_r) &= \sum_{i=1}^r L_i \left(2\sqrt{(1-\tau)\tau_i(q-1)q^{i-1}} \right. \\ &\quad \left. + (q-2)\tau_i(q^r - q^{i-1}) + 2\frac{(q-1)}{q} \sum_{k=1}^{i-1} \sqrt{\tau_k \tau_i q^{i+k}} \right). \end{aligned}$$

Asymptotic Bound

Theorem

Let $\kappa/n \rightarrow \tau$, $f_i/n \rightarrow \tau_i$. Then

$$\lim_{\substack{n \rightarrow \infty \\ \frac{\kappa}{n} \rightarrow \tau}} \frac{\lambda_\kappa}{n} \geq \max_{\substack{\tau_i \geq 0 \\ \sum_{i=1}^r \tau_i = \tau}} \Lambda(\tau_1, \dots, \tau_r)$$

where

$$\begin{aligned} \Lambda(\tau_1, \dots, \tau_r) &= \sum_{i=1}^r L_i \left(2\sqrt{(1-\tau)\tau_i(q-1)q^{i-1}} \right. \\ &\quad \left. + (q-2)\tau_i(q^r - q^{i-1}) + 2\frac{(q-1)}{q} \sum_{k=1}^{i-1} \sqrt{\tau_k \tau_i q^{i+k}} \right). \end{aligned}$$

Proof.

Use $\lambda_\kappa \geq \frac{\langle y, \tilde{S}_\kappa y \rangle}{\langle y, y \rangle}$, and take y as a $\{0, 1\}$ vector with 1's placed selectively.



Asymptotic Bound

Theorem

Let $R_{\text{LP}}(\delta)$ be the function defined by

$$R(\tau) = \frac{1}{r} \left(H_{q,1}(\tau) + \tau \log_q \frac{q^r - 1}{q - 1} \right)$$

$$\delta(\tau) = \delta_{\text{crit}} - \frac{1}{r} \max_{\substack{\tau_i \geq 0 \\ \sum_{i=1}^r \tau_i = \tau}} \Lambda(\tau_1, \dots, \tau_r), \quad 0 \leq \tau \leq 1.$$

Then the asymptotic rate of any code family of relative distance δ satisfies $R \leq R_{\text{LP}}(\delta)$ and the rate of any family of OOAs of relative strength δ satisfies $R \geq 1 - R_{\text{LP}}(\delta)$.

(For $|e|' = d, P(e) = \delta_{\text{crit}}rn - |e|' = \delta_{\text{crit}}rn - d \leq \lambda_{\kappa-1}$)

Improved LP Bound for $r = 2$

- 1. Use explicit expression of the Krawtchouk Polynomial for $r = 2$
$$K_{(f_1, f_2)}(e) = q^{f_2} k_{f_2}(n - e_2, e_1) k_{f_1}(n - f_2, e_2)$$
- 2. Estimate of the 1st root of $k_l(n, x)$. Let $l/n \rightarrow y$
$$\lim_{n \rightarrow \infty} x_1(n, l)/n = \gamma(y) \triangleq \frac{q-1}{q} - \frac{q-2}{q}y - \frac{2}{q}\sqrt{(q-1)y(1-y)}.$$
- Similar method in Aaltonen (1990)

Improved LP Bound for $r = 2$

- 1. Use explicit expression of the Krawtchouk Polynomial for $r = 2$
$$K_{(f_1, f_2)}(e) = q^{f_2} k_{f_2}(n - e_2, e_1) k_{f_1}(n - f_2, e_2)$$
- 2. Estimate of the 1st root of $k_l(n, x)$. Let $l/n \rightarrow y$
$$\lim_{n \rightarrow \infty} x_1(n, l)/n = \gamma(y) \triangleq \frac{q-1}{q} - \frac{q-2}{q}y - \frac{2}{q}\sqrt{(q-1)y(1-y)}.$$
- Similar method in Aaltonen (1990)

Theorem

The asymptotic rate of any family of codes of relative distance δ satisfies $R \leq \Phi(\delta)$, where

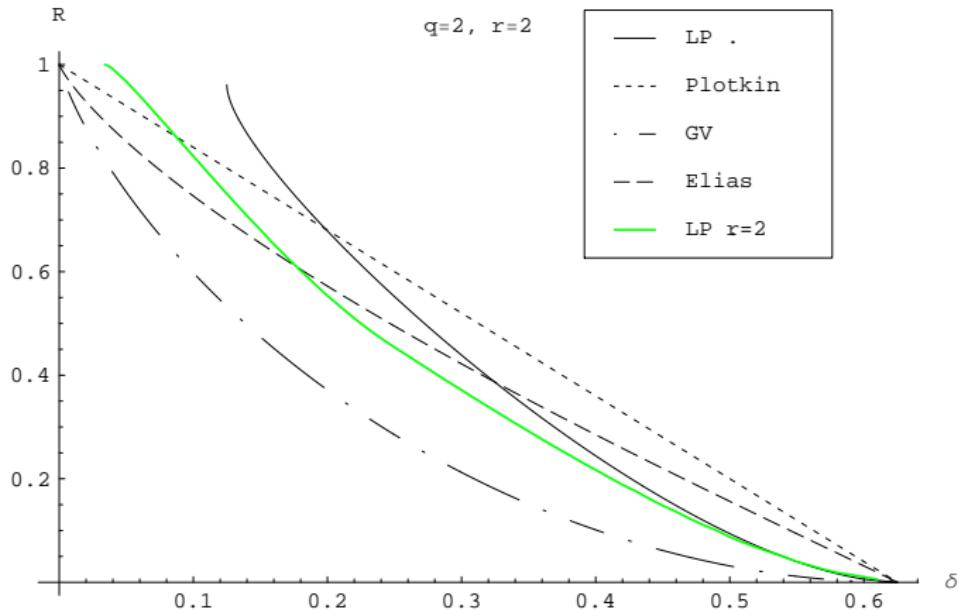
$$\Phi(\delta) = \min_{\tau_1, \tau_2} \frac{1}{2} \left\{ \tau_2 + H_{q,1}(\tau_1) + (1 - \tau_1)H_{q,1}\left(\frac{\tau_2}{1 - \tau_1}\right) \right\},$$

where the minimum is taken over all τ_1, τ_2 that satisfy

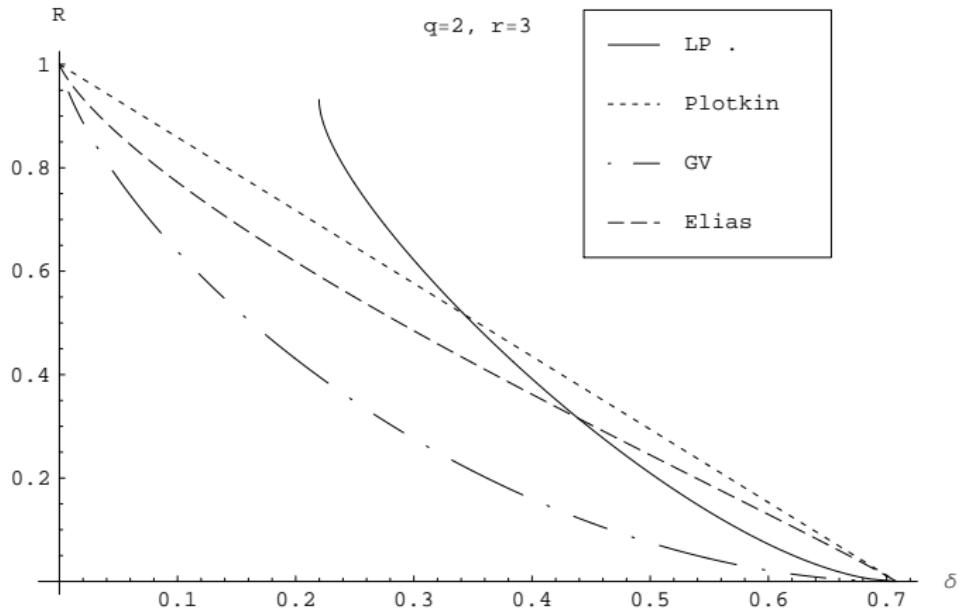
$$0 \leq \tau_1 \leq (q-1)/q^2, \quad 0 \leq \tau_2 \leq (q-1)/q$$
$$\gamma(\tau_2) + (2 - \gamma(\tau_2))(1 - \tau_2)\gamma(\tau_1) \leq 2\delta.$$

The asymptotic rate of any family of OOAs of relative strength δ satisfies $R \geq 1 - \Phi(\delta)$.

Numerical Results: $q = 2, r = 2$



Numerical Results: $q = 2, r = 3$



Thank You!

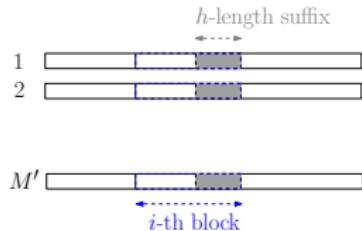
Extra Slides

Bassalygo-Elias Bound: Proof

Proof.

(Proof of lemma):

For $i = 1, \dots, n; h = 1, \dots, r; c \in \mathbb{F}_q^h$ let
 $\lambda_{i,c}^h = |\{\mathbf{x}^i \in C^i : \mathbf{x}^{i,h} = c\}|$.



$$\begin{matrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{matrix}$$

$$\lambda_{i,11}^2 = 2, \quad \lambda_{i,1}^1 = 4$$

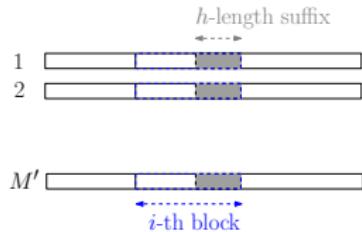


Bassalygo-Elias Bound: Proof

Proof.

(Proof of lemma):

For $i = 1, \dots, n; h = 1, \dots, r; c \in \mathbb{F}_q^h$ let
 $\lambda_{i,c}^h = |\{\mathbf{x}^i \in C^i : \mathbf{x}^{i,h} = c\}|$.



$$dM'(M' - 1) \leq \sum_{\mathbf{x}, \mathbf{y} \in C} d_r(\mathbf{x}, \mathbf{y}) = nrM'^2 - \sum_{i=1}^n \sum_{h=1}^r \sum_{c \in \mathbb{F}_q^h} (\lambda_{i,c}^h)^2.$$

Solve the minimization:

$$\text{minimize } \sum_{i=1}^n \sum_{h=1}^r \sum_{c \in \mathbb{F}_q^h} (\lambda_{i,c}^h)^2$$

such that $\sum_{c \in \mathbb{F}_q^h} \lambda_{i,c}^h = M'$ and $\sum_{i=1}^n \sum_{h=1}^r \lambda_{i,0}^h = M'(nr - w)$

$$\Rightarrow dM'(M' - 1) \leq \frac{M'^2}{n} \left(2wn - \frac{w^2}{r\delta_{\text{crit}}} \right)$$



Linear Krawtchouk Polynomials

Take $K_{0,\dots,0} = 1$. For some constant c

$$K_{F_1}(x) = c(x_r - \langle x_r, 1 \rangle) = c(x_r - n(q-1)/q)$$

c is obtained from $\|K_{F_i}\|^2 = v_{F_i} = n(q-1)q^{i-1}$; we get

$$c = \pm q;$$

We take $c = -q$ to ensure $K_{F_i}(0) > 0$.

(Back)

Asymptotic volume of the ball (Rosenbloom-Tsfasman, 1997)

Let $A(z) = (q - 1)z(z^r - 1)/(q(z - 1))$ and let $z_0 = z_0(x)$ be the unique positive root of the equation

$$xr(1 + A(z)) = \frac{q - 1}{q} \sum_{i=1}^r iz^i.$$

Define the function

$$H_{q,r}(x) = x(1 - \log_q z_0) + \frac{1}{r} \log_q (1 + A(z_0)).$$

Then

$$\lim_{n \rightarrow \infty} (nr)^{-1} \log_q S_{\delta nr} = \begin{cases} H_{q,r}(\delta) & 0 \leq \delta \leq \delta_{\text{crit}} \\ 1 & \delta_{\text{crit}} < \delta \leq 1. \end{cases}$$



Three-term for normalized polynomials

$$A_\kappa[f, h] = L_i \sqrt{(f_i + 1)(n - \kappa)q^{i-1}(q - 1)} \quad \text{if } h = (f_1, \dots, f_i + 1, \dots, f_r)$$

$$C_\kappa[f, h] = L_i \sqrt{(n - \kappa + 1)f_i q^{i-1}(q - 1)} \quad \text{if } h = (f_1, \dots, f_i - 1, \dots, f_r)$$

$$B_\kappa[f, h] = \begin{cases} L_i f_i q^{i-1}(q - 2) & \text{if } h = f \\ L_i \frac{q - 1}{q} \sqrt{(f_k + 1)f_i q^{k+i}} & \text{if } h = (f_1, \dots, f_k + 1, \dots, f_i - 1, \dots, f_r), \\ & 1 \leq k < i \\ L_i \frac{q - 1}{q} \sqrt{f_k(f_i + 1)q^{k+i}} & \text{if } h = (f_1, \dots, f_k - 1, \dots, f_i + 1, \dots, f_r), \\ & 1 \leq k < i \end{cases}$$

(Back to 3-term)
(Back to Λ)