Linear nearMDS codes in the poset metric

Alexander Barg and Punarbasu Purkayastha

ECE/Institute for Systems Research
University of Maryland

Linear MDS codes in the Hamming space $\mathbb{F}_q^n$

$\mathscr{C}$ - k-dimensional linear subspace (code) in $\mathbb{F}_q^n$ with distance d=n-k+1

Fix a basis $G=(g_1,g_2,\ldots,g_k) \subset \mathbb{F}_q^n$

$E \subset [n]=\{1,2,\ldots,n\}$ is ***independent*** if the projection of G on E is a basis

$\mathscr{C}$ is MDS iff every F, |F|=k is independent

$U_{u,v}=\left|F \subset [n]: |F|=u, \mathrm{rank}(F)=v\right|$

$$U_{u,v} = \binom{n}{u}\delta_{u,v}, \quad 0 \le v \le u \le k$$

$$U_{u,v} = \binom{n}{u}\delta_{k,v}, \quad k < u \le n$$

Rank function $$U(x,y) \triangleq \sum_{u=0}^{n}\sum_{v=0}^{u} U_{u,v}x^u y^v = \sum_{u=0}^{k}\binom{n}{u}(xy)^u + \sum_{u=k+1}^{n}\binom{n}{u}x^u v^k$$

Linear MDS codes in the Hamming space $\mathbb{F}_q^n$

Let $A_s=\{x\in\mathscr{C} : |x|=s\}$, then

$$A_{(n-k)+\ell} = \binom{n}{k-\ell} \sum_{j=0}^{\ell-1} (-1)^j \binom{n-k+\ell}{j} (q^{\ell-j}-1), \quad \ell = 1,2,\ldots,k$$

Poset metrics

Example (Niederreiter ‘86; Rosenbloom-Tsfasman ’97)

1. $\mathbf{x}=(********x_j00000000) \in \mathbb{F}_q^r$

   $(x_j \neq 0 \ \& \ x_{j+1}=\ldots=x_r=0) \Leftrightarrow |\mathbf{x}|_{NRT}=j$

2. $\mathbf{x}=(\mathbf{x}_1,\mathbf{x}_2,\ldots,\mathbf{x}_n)$, $\mathbf{x}_i = (x_{11},\ldots,x_{1,r})$, i=1,2,…,n

   $|\mathbf{x}|_{NRT}=\sum_{i=1}^{n} |\mathbf{x}_i|_{NRT}$

q=5,r=3,n=5

x=(0,0,1; 0,4,0; 1,1,0; 2,0,1; 0,1,3) **y**=(1,3,2; 0,3,2; 2,4,0; 0,0,0; 0,0,0)
$d(\mathbf{x},\mathbf{y})=|\mathbf{x}-\mathbf{y}|_{NRT}=|(4,2,4; 0,1,3; 4,2,0; 2,0,1; 0,1,3)|_{NRT}= 14$

Codes in the NRT space are important in the context of Monte-Carlo integration [(t,m,s) nets], list decoding of RS codes, linear complexity of sequences, algebraic combinatorics.

Poset metrics

q=5, r=8, n=….

x=(3,0,1,2,1,0,0,0)

What matters is the rightmost coordinate in each block; so there is a natural domination order within the block $(x_{i,1},\ldots,x_j,\ldots,x_{i,r})$:

$$1<2<\ldots<j<\ldots<r$$

NRT order = $\cup_{i=1}^{n}$ r-chains

Hamming order = an antichain of length n

$|\mathbf{x}|_{NRT}$=length(shortest chain that covers all the nonzeros of **x**)

Now let $\mathbf{z}\in(\mathbb{F}_q)^{n,r}$, then $|\mathbf{z}|=\sum$ length(shortest chains within their blocks)

Chains and their unions are examples of "ideals" in partial orders.

Poset metrics

Let N be a finite set (of code's coordinates) and P a partial order on N

A subset $\mathcal{I}$ is called an ideal in P if $(j\in\mathcal{I})\ \&\ (i<j) \Rightarrow i\in\mathcal{I}$

Definition: (R.A. Brualdi, J.S. Graves, K.M. Lawrence, 1995)
N=finite set; P a partial order

The poset norm of $\mathbf{x}\in\mathbb{F}_q^{|N|}$ equals $|\mathbf{x}|=\min_{\mathcal{I}\subset P:\ \mathcal{I} \text{ covers } \mathbf{x}} |\mathcal{I}|$

Notation: $|\mathbf{x}|=\langle \mathrm{supp}(\mathbf{x})\rangle$

Poset codes were considered in a number of papers

J.Y. Huyn, H.K. Kim, D.Y. Oh, 2002-2009;
S. Dougherty, M. Skriganov, K. Shiromoto, 2002-2008.

Linear MDS codes in a Poset metric

Coordinates N=[n], partial order P

$\mathscr{C}$ - k-dimensional linear code in $\mathbb{F}_q^n$ is called MDS if d=n-k+1
(the Singleton bound is still proved by shortening)

A more convenient definition:
Given a vector $\mathbf{y} \in \mathbb{F}_q^n$, call the set

$$B_{\mathcal{I}}(\mathbf{y})=\{\mathbf{z}\in\mathbb{F}_q^n: |\langle \mathrm{supp}(\mathbf{y}-\mathbf{z})\rangle \subseteq \mathcal{I}\}$$

an $\mathcal{I}$-sphere around **y**. Then $\mathscr{C}$ is MDS if for any $\mathcal{I}$,$|\mathcal{I}|$=n-k the spheres around the codewords tile the space $\mathbb{F}_q^n$.

Example: Hamming space

$\mathcal{I}$ - (n-k)-subset of [n]

There are q^{n-k} vectors in any $B_{\mathcal{I}}(\mathbf{c})$; they are all distinct

Weight distribution of linear MDS poset codes has been found by

M. Skriganov, Coding theory and uniform distributions, 1999 (NRT case)

J.Y. Huyn and H.K. Kim, Maximum distance separable poset codes, *Designs, Codes and Cryptography*, 2008

We consider poset codes that are one away from the Singleton bound
An interesting class among them are NearMDS codes

- Weight distribution

The main example is the NRT metric because ordered codes give rise to “uniform” point allocations (distributions) in the unit cube.

- We characterize distributions that correspond to NMDS codes.

NearMDS codes in a Poset metric

d_t – t^{th} Generalized Hamming Weight

$$d_t = \min \{|\mathrm{supp}(\mathscr{D})|: \mathscr{D} \text{ is a t-dim subcode of } \mathscr{C}\}$$

Properties:

$d_t(\mathscr{C}) \leq$ n-k+t, t=1,…,k

$\forall\, \mathcal{I} \in$ P every (δ-t)-subset$\in \mathcal{I}$ of columns of H have rank $\geq \delta$-t

etc.

(Standard properties)

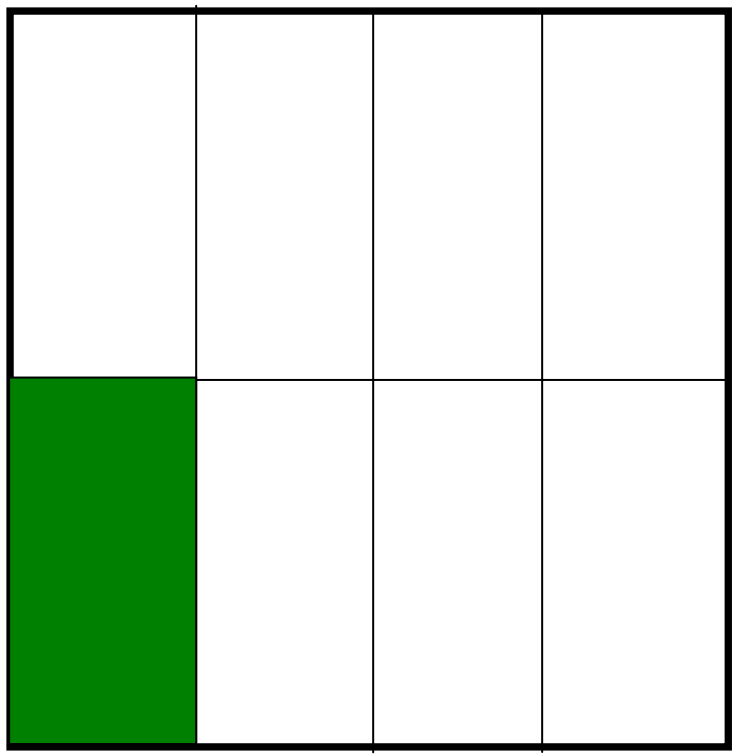
A code with distance d=n-k is called NearMDS if d_2=n-k+2

Distributions

$K^n=[0,1]^n$ unit cube

Partition each axis into q^{m_i} equal segments, $0 \leq m_i \leq r$

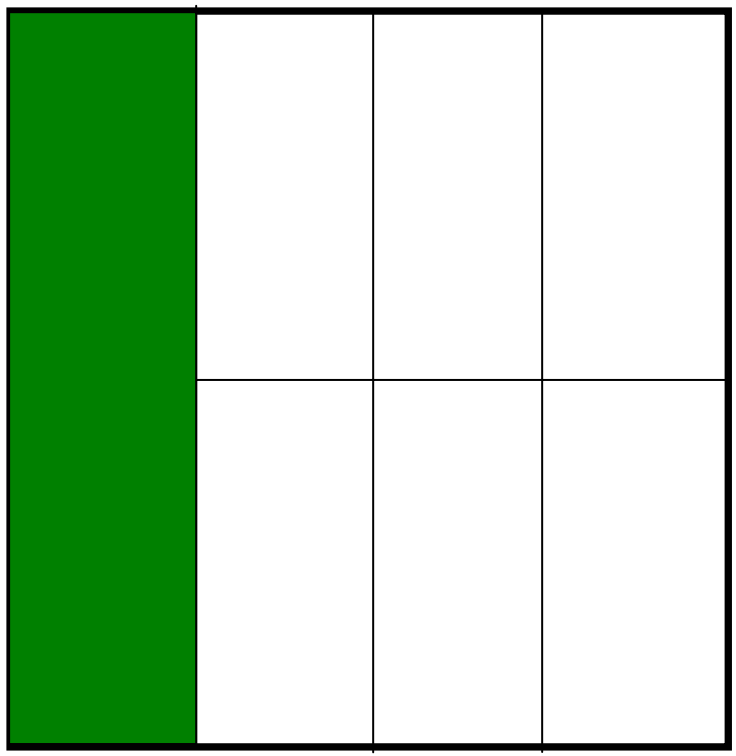
Elementary interval



Distributions

$K^n=[0,1]^n$ unit cube

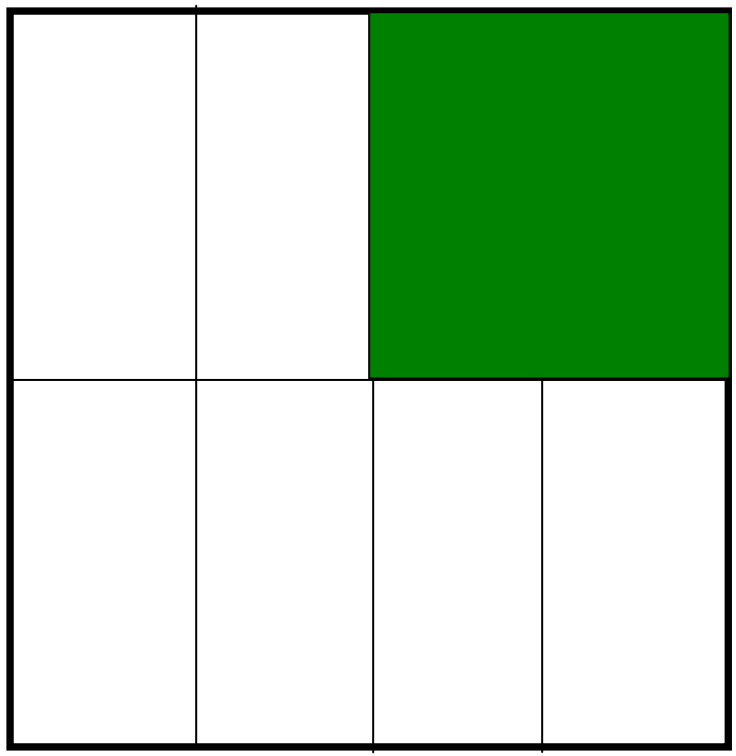
Partition each axis into q^{m_i} equal segments, $0 \leq m_i \leq r$



Distributions

$K^n=[0,1]^n$ unit cube

Partition each axis into q^{m_i} equal segments, $0 \leq m_i \leq r$



Distributions

$K^n=[0,1]^n$ unit cube

Elementary interval: take $0 \le a_i < q^{m_i}$, $0 \le m_i < r$

$$E = \prod_{i=1}^{n} \left[\frac{a_i}{q^{m_i}}, \frac{a_i + 1}{q^{m_i}} \right)$$

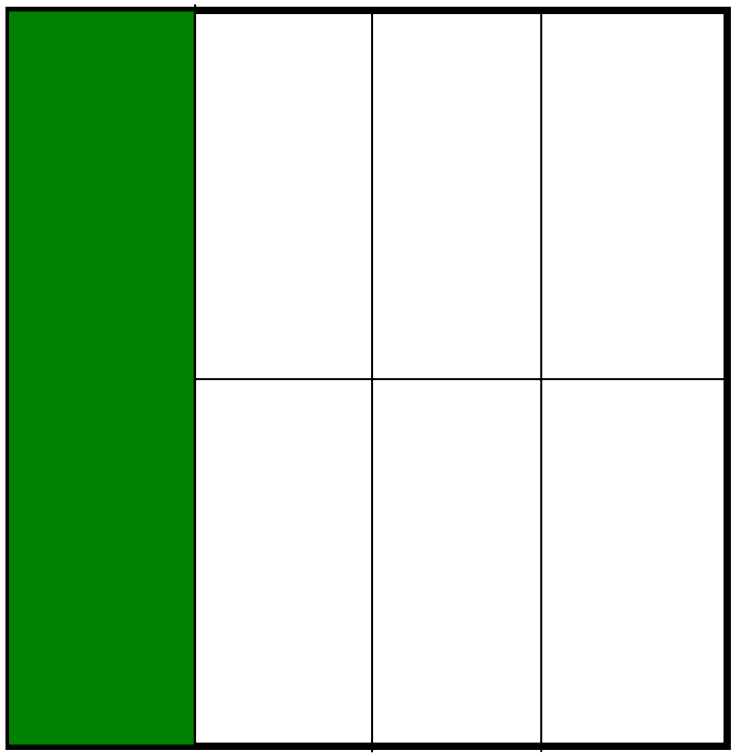
A Distribution is a collection of points in K^n uniformly distributed with respect to a partition into elementary intervals

Kuipers/Niederreiter (1974); Beck/Chen (1987); Matoušek (1998)

M. Skriganov (1999)

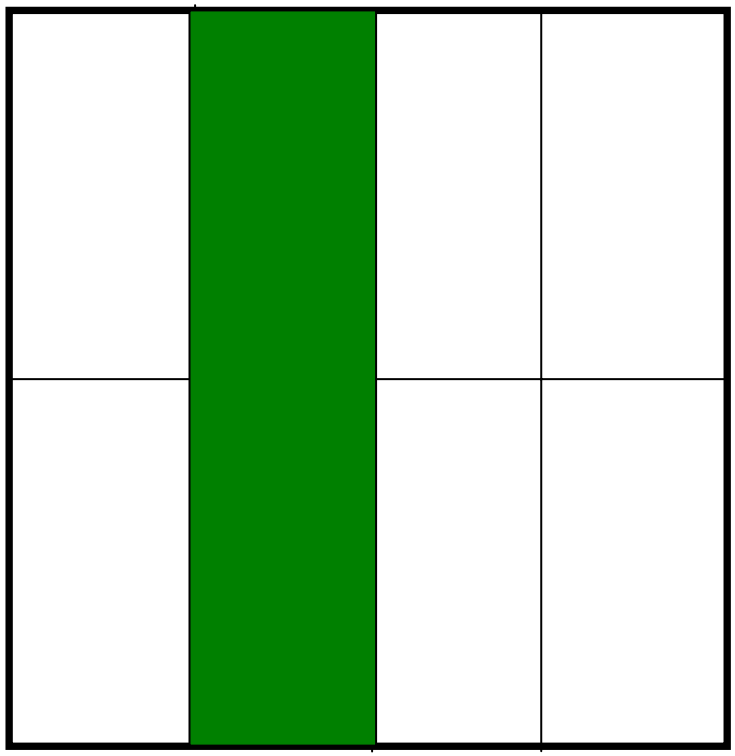
Distributions and uniform sampling

A collection of q^k points in K^n such that *every* cell of a *fixed volume* contains the same number of points



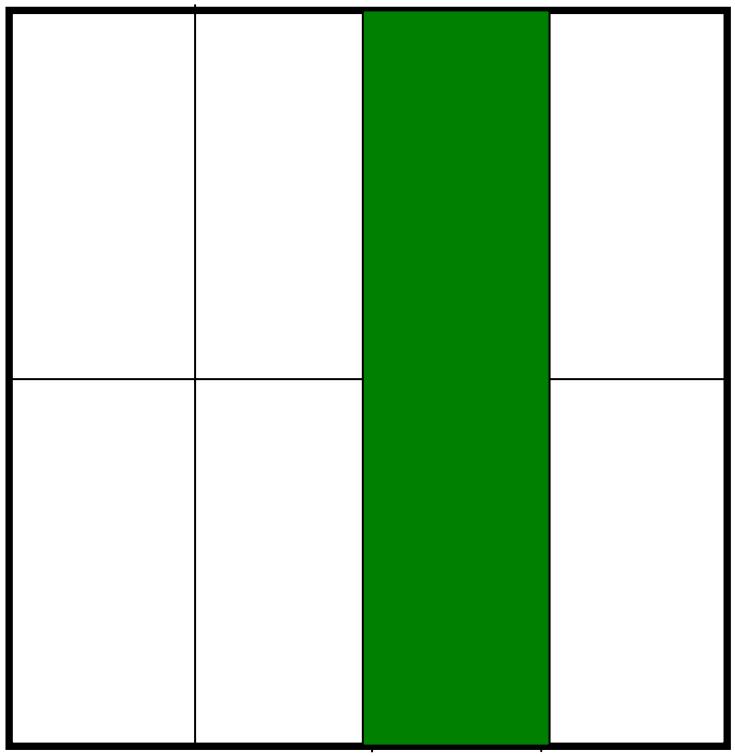
Distributions and uniform sampling

A collection of q^k points in K^n such that *every* cell of a *fixed volume* contains the same number of points



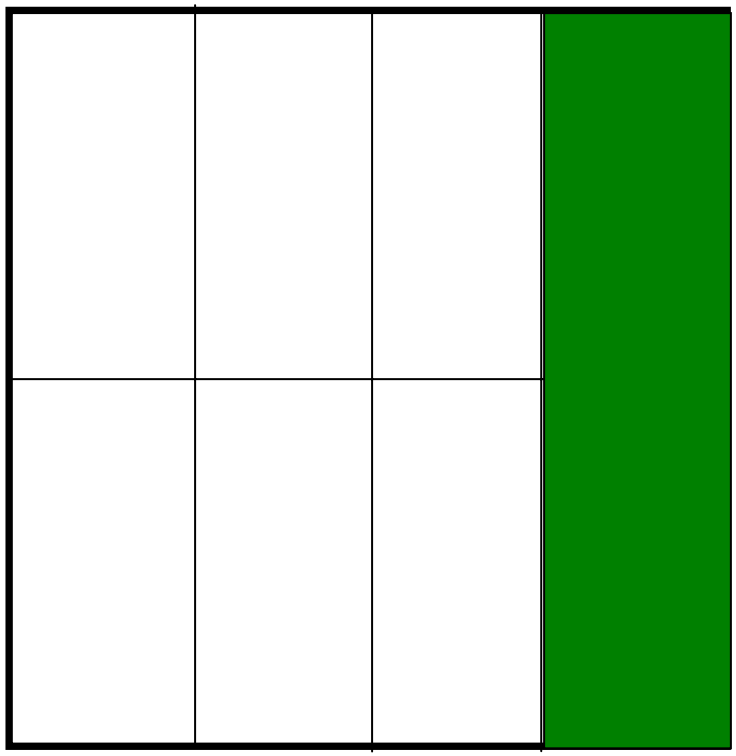
Distributions and uniform sampling

A collection of q^k points in K^n such that *every* cell of a *fixed volume* contains the same number of points



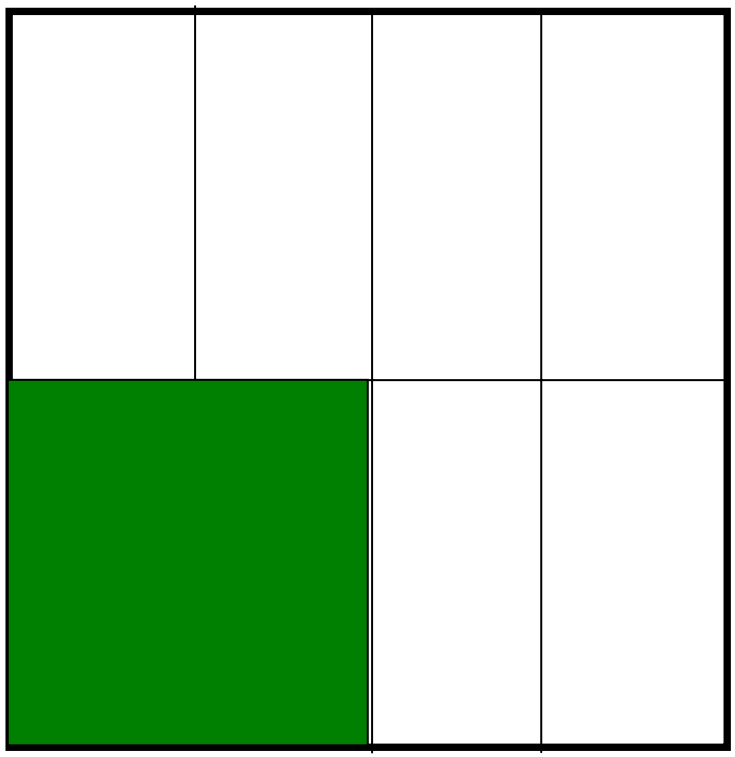
Distributions and uniform sampling

A collection of q^k points in K^n such that *every* cell of a *fixed volume* contains the same number of points



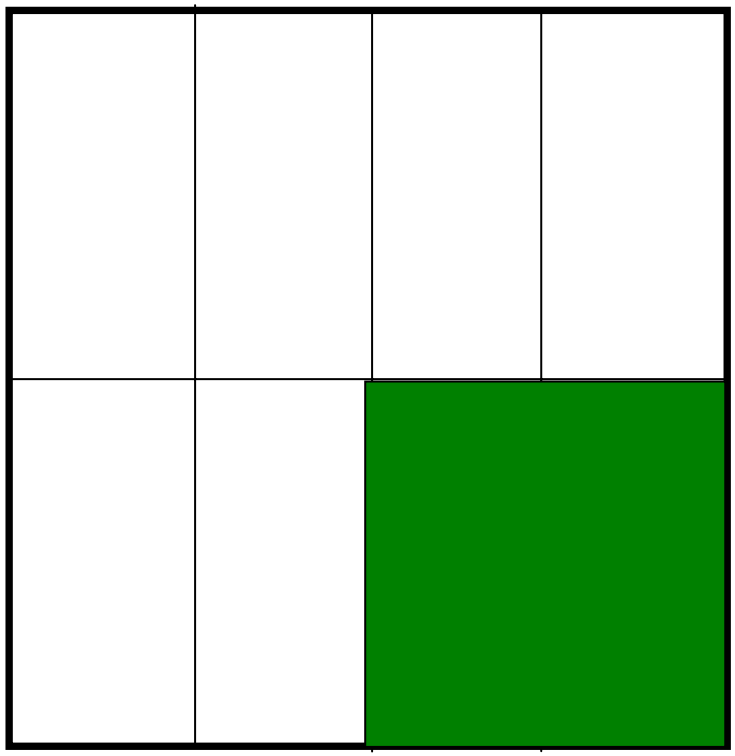
Distributions and uniform sampling

A collection of q^k points in K^n such that *every* cell of a *fixed volume* contains the same number of points



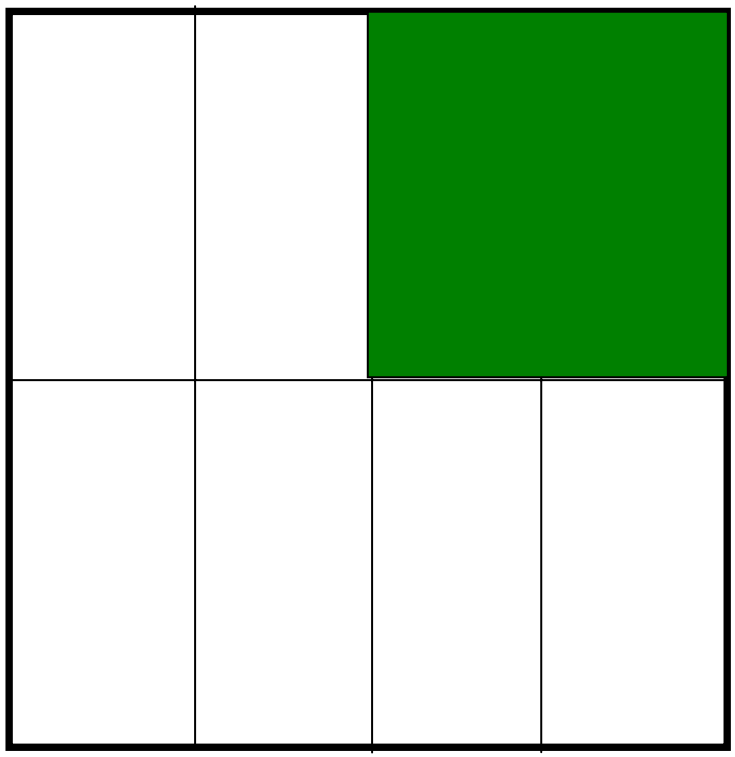
Distributions and uniform sampling

A collection of q^k points in K^n such that *every* cell of a *fixed volume* contains the same number of points



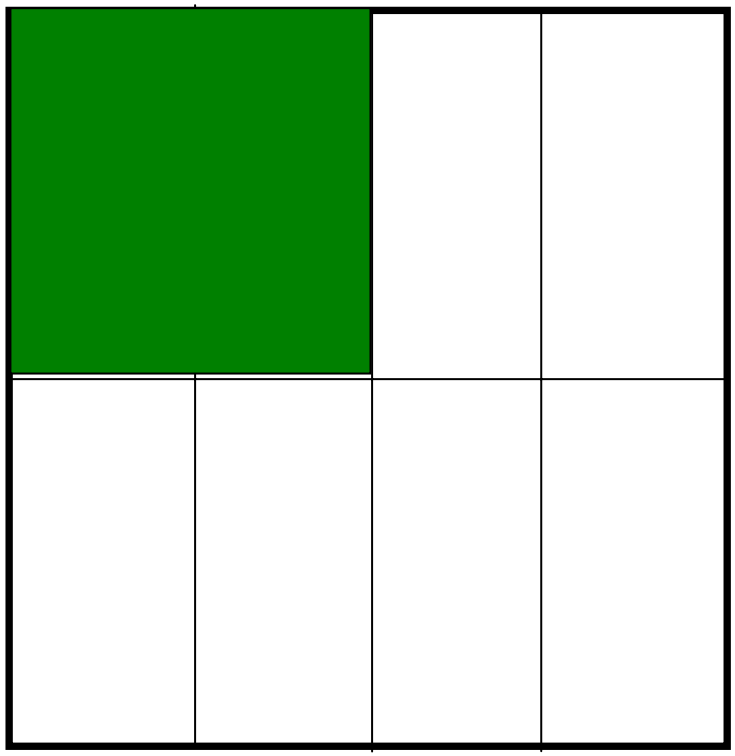
Distributions and uniform sampling

A collection of q^k points in K^n such that *every* cell of a *fixed volume* contains the same number of points



Distributions and uniform sampling

A collection of q^k points in K^n such that *every* cell of a *fixed volume* contains the same number of points



Ordered Codes and Distributions

A linear code $\mathscr{C}$ in the NRT space $(\mathbb{F}_q)^{n,r}$ gives rise to a uniform distribution

0	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
0	0	1	1	0	1	1	1	1
1	0	1	0	1	1	0	1	1
1	1	1	0	0	1	1	0	1
1	1	0	1	0	0	0	1	0
0	1	1	1	1	1	0	0	1
1	0	0	1	1	0	1	0	0
0	1	0	0	1	0	1	1	0

Ordered Codes and Distributions

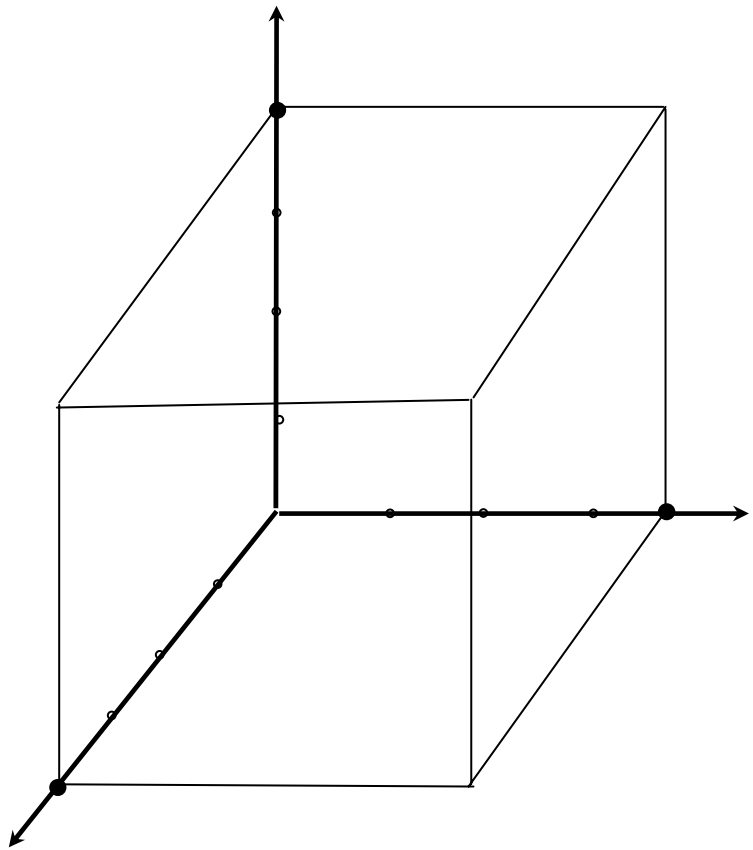
A linear code $\mathscr{C}$ in the NRT space $(\mathbb{F}_q)^{n,r}$ gives rise to a uniform distribution

.0	**0**	**0**	**.0**	**0**	**0**	**.0**	**0**	**0**
.0	0	1	.1	0	1	.1	1	1
.1	0	1	.0	1	1	.0	1	1
.1	1	1	.0	0	1	.1	0	1
.1	1	0	.1	0	0	.0	1	0
.0	1	1	.1	1	1	.0	0	1
.1	0	0	.1	1	0	.1	0	0
.0	1	0	.0	1	0	.1	1	0

Ordered Codes and Distributions

A linear code $\mathscr{C}$ in the NRT space $(\mathbb{F}_q)^{n,r}$ gives rise to a uniform distribution

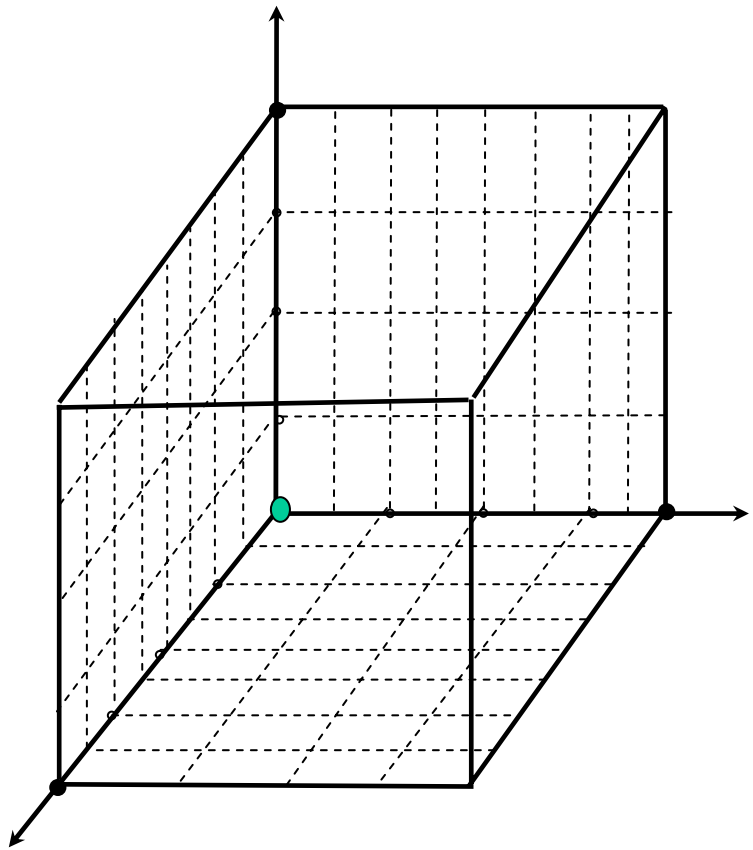
.0	**0**	**0**	**.0**	**0**	**0**	**.0**	**0**	**0**
.0	0	1	.1	0	1	.1	1	1
.1	0	1	.0	1	1	.0	1	1
.1	1	1	.0	0	1	.1	0	1
.1	1	0	.1	0	0	.0	1	0
.0	1	1	.1	1	1	.0	0	1
.1	0	0	.1	1	0	.1	0	0
.0	1	0	.0	1	0	.1	1	0



Ordered Codes and Distributions

A linear code $\mathscr{C}$ in the NRT space $(\mathbb{F}_q)^{n,r}$ gives rise to a uniform distribution

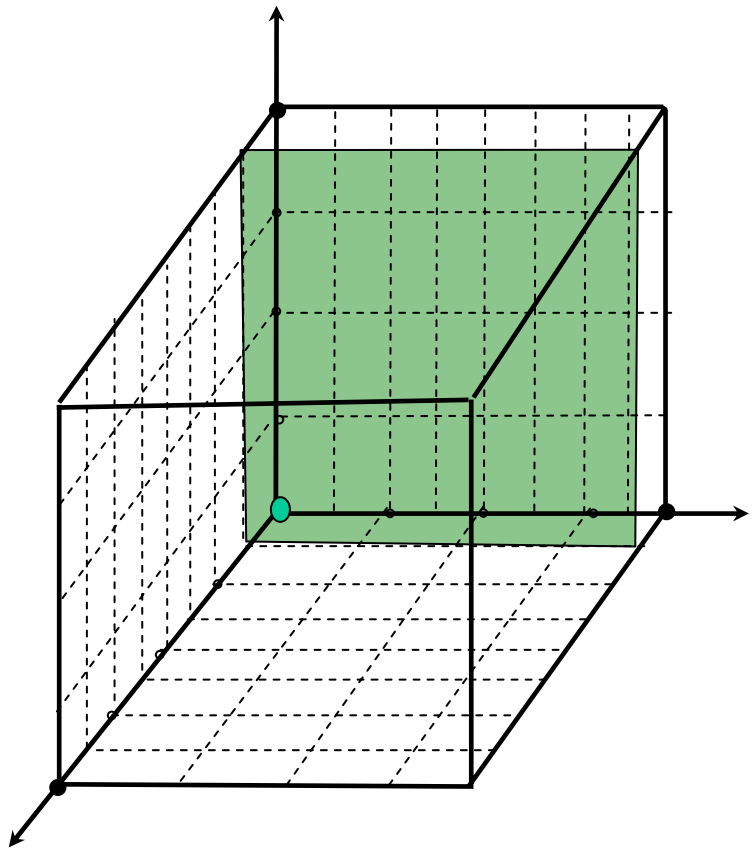
.0	**0**	**0**	**.0**	**0**	**0**	**.0**	**0**	**0**
.0	0	1	.1	0	1	.1	1	1
.1	0	1	.0	1	1	.0	1	1
.1	1	1	.0	0	1	.1	0	1
.1	1	0	.1	0	0	.0	1	0
.0	1	1	.1	1	1	.0	0	1
.1	0	0	.1	1	0	.1	0	0
.0	1	0	.0	1	0	.1	1	0



Ordered Codes and Distributions

A linear code $\mathscr{C}$ in the NRT space $(\mathbb{F}_q)^{n,r}$ gives rise to a uniform distribution

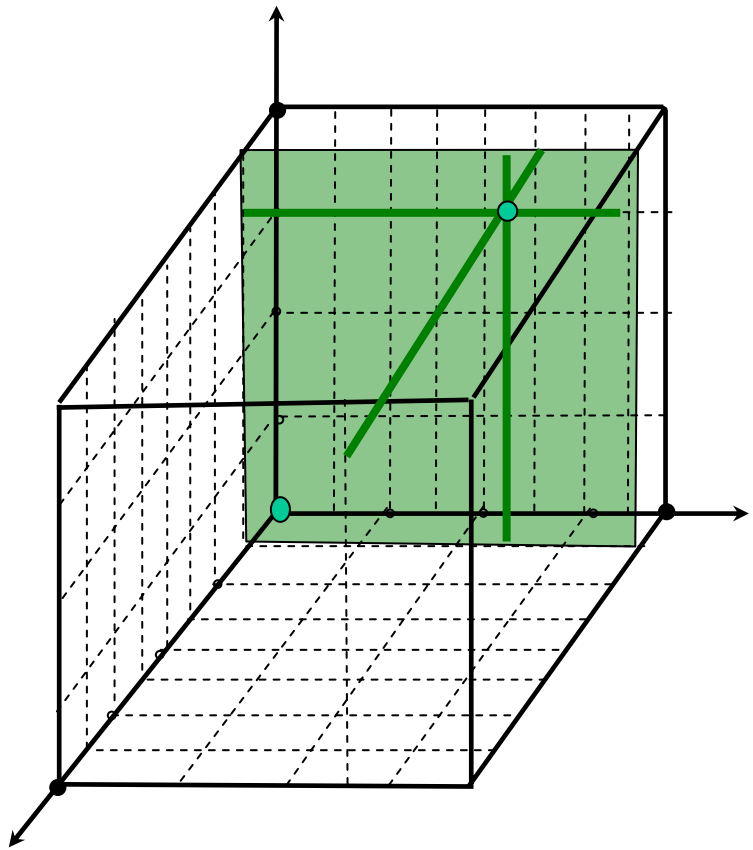
.0	**0**	**0**	**.0**	**0**	**0**	**.0**	**0**	**0**
.0	0	1	.1	0	1	.1	1	1
.1	0	1	.0	1	1	.0	1	1
.1	1	1	.0	0	1	.1	0	1
.1	1	0	.1	0	0	.0	1	0
.0	1	1	.1	1	1	.0	0	1
.1	0	0	.1	1	0	.1	0	0
.0	1	0	.0	1	0	.1	1	0



Ordered Codes and Distributions

A linear code $\mathscr{C}$ in the NRT space $(\mathbb{F}_q)^{n,r}$ gives rise to a uniform distribution

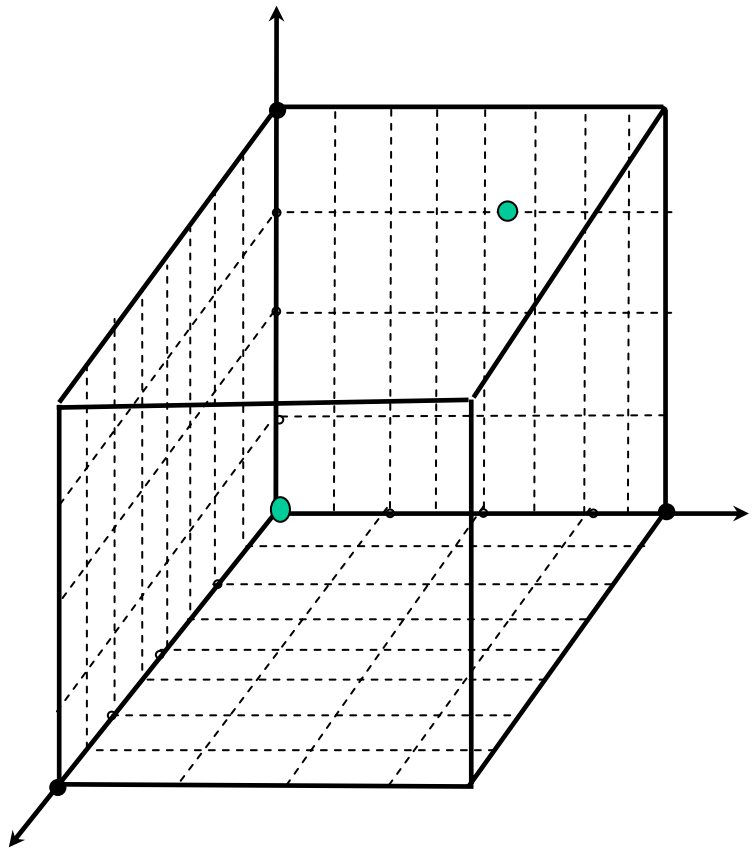
.0	**0**	**0**	**.0**	**0**	**0**	**.0**	**0**	**0**
.0	0	1	.1	0	1	.1	1	1
.1	0	1	.0	1	1	.0	1	1
.1	1	1	.0	0	1	.1	0	1
.1	1	0	.1	0	0	.0	1	0
.0	1	1	.1	1	1	.0	0	1
.1	0	0	.1	1	0	.1	0	0
.0	1	0	.0	1	0	.1	1	0



Ordered Codes and Distributions

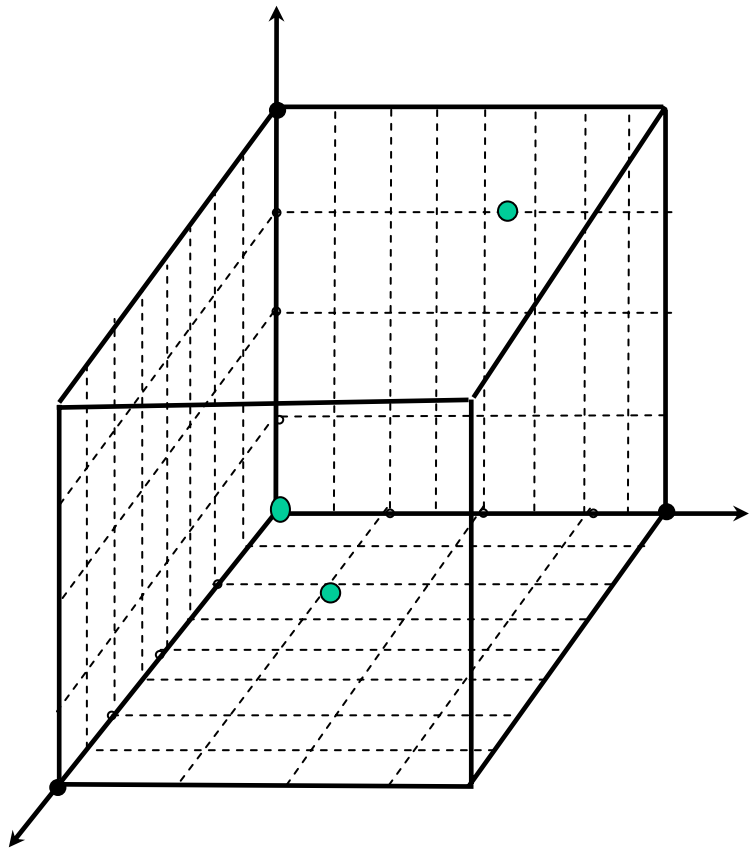
A linear code $\mathscr{C}$ in the NRT space $(\mathbb{F}_q)^{n,r}$ gives rise to a uniform distribution

.0	**0**	**0**	**.0**	**0**	**0**	**.0**	**0**	**0**
.0	0	1	.1	0	1	.1	1	1
.1	0	1	.0	1	1	.0	1	1
.1	1	1	.0	0	1	.1	0	1
.1	1	0	.1	0	0	.0	1	0
.0	1	1	.1	1	1	.0	0	1
.1	0	0	.1	1	0	.1	0	0
.0	1	0	.0	1	0	.1	1	0



Ordered Codes and Distributions

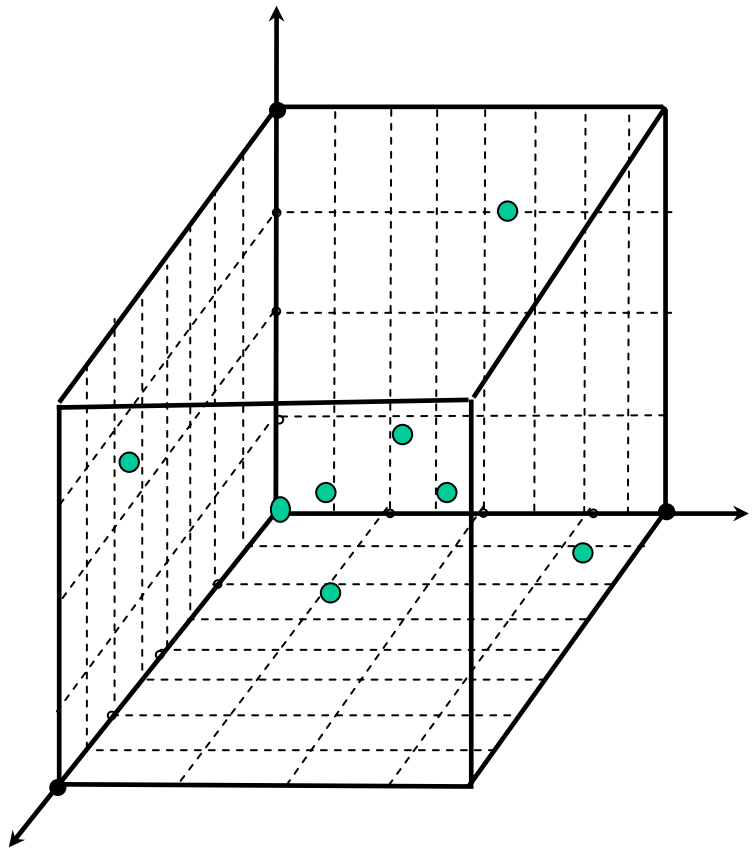
.0	0	0	.0	0	0	.0	0	0
.0	0	1	.1	0	1	.1	1	1
.1	0	1	.0	1	1	.0	1	1
.1	1	1	.0	0	1	.1	0	1
.1	1	0	.1	0	0	.0	1	0
.0	1	1	.1	1	1	.0	0	1
.1	0	0	.1	1	0	.1	0	0
.0	1	0	.0	1	0	.1	1	0



Ordered Codes and Distributions

A linear code $\mathscr{C}$ in the NRT space $(\mathbb{F}_q)^{n,r}$ gives rise to a uniform distribution

.0	**0**	**0**	**.0**	**0**	**0**	**.0**	**0**	**0**
.0	0	1	.1	0	1	.1	1	1
.1	0	1	.0	1	1	.0	1	1
.1	1	1	.0	0	1	.1	0	1
.1	1	0	.1	0	0	.0	1	0
.0	1	1	.1	1	1	.0	0	1
.1	0	0	.1	1	0	.1	0	0
.0	1	0	.0	1	0	.1	1	0



Ordered Codes and Distributions

A linear code $\mathscr{C}$ in the NRT space $(\mathbb{F}_q)^{n,r}$ gives rise to a uniform distribution

.0	**0**	**0**	**.0**	**0**	**0**	**.0**	**0**	**0**
.0	0	1	.1	0	1	.1	1	1
.1	0	1	.0	1	1	.0	1	1
.1	1	1	.0	0	1	.1	0	1
.1	1	0	.1	0	0	.0	1	0
.0	1	1	.1	1	1	.0	0	1
.1	0	0	.1	1	0	.1	0	0
.0	1	0	.0	1	0	.1	1	0

Every 3 left-adjusted columns are surjective, equidistributed!

Ordered Codes and Distributions

A linear code $\mathscr{C}$ in the NRT space $(\mathbb{F}_q)^{n,r}$ gives rise to a uniform distribution

.0	**0**	**0**	**.0**	**0**	**0**	**.0**	**0**	**0**
.0	0	1	.1	0	1	.1	1	1
.1	0	1	.0	1	1	.0	1	1
.1	1	1	.0	0	1	.1	0	1
.1	1	0	.1	0	0	.0	1	0
.0	1	1	.1	1	1	.0	0	1
.1	0	0	.1	1	0	.1	0	0
.0	1	0	.0	1	0	.1	1	0

Every 3 left-adjusted columns are surjective, equidistributed!

Ordered Codes and Distributions

A linear code $\mathscr{C}$ in the NRT space $(\mathbb{F}_q)^{n,r}$ gives rise to a uniform distribution

.0	**0**	**0**	**.0**	**0**	**0**	**.0**	**0**	**0**
.0	0	1	.1	0	1	.1	1	1
.1	0	1	.0	1	1	.0	1	1
.1	1	1	.0	0	1	.1	0	1
.1	1	0	.1	0	0	.0	1	0
.0	1	1	.1	1	1	.0	0	1
.1	0	0	.1	1	0	.1	0	0
.0	1	0	.0	1	0	.1	1	0

Every 3 left-adjusted columns are surjective, equidistributed!

$OOA_{\lambda=1}(t=3,n=3,r=3,q=2)$
Ordered Orthogonal Array

Ordered Codes and Distributions

A linear code $\mathscr{C}$ in the NRT space $(\mathbb{F}_q)^{n,r}$ gives rise to a uniform distribution

.0	**0**	**0**	**.0**	**0**	**0**	**.0**	**0**	**0**
.0	0	1	.1	0	1	.1	1	1
.1	0	1	.0	1	1	.0	1	1
.1	1	1	.0	0	1	.1	0	1
.1	1	0	.1	0	0	.0	1	0
.0	1	1	.1	1	1	.0	0	1
.1	0	0	.1	1	0	.1	0	0
.0	1	0	.0	1	0	.1	1	0

Every 3 left-adjusted columns are surjective, equidistributed!

$OOA_{\lambda=1}(t=3,n=3,r=3,q=2)$
Ordered Orthogonal Array

General results: Lawrence (1996), Mullen/Schmid (1996)

Ordered Codes and Distributions

Definition. A distribution of q^k points is called optimal if every elementary box of volume q^{-k} contains exactly one point.

If $a_1+\ldots+a_n \leq k$, then every box E in K^n contains exactly $q^{k-a_1-\ldots-a_n}$ points of an optimal distribution.

A linear code $\mathscr{C} \in (\mathbb{F}_q)^{n,r}$ (NRT) gives rise to an OOA; to a distribution $\mathscr{D} \in K^n$

Proposition (Skriganov) MDS code $\mathscr{C} \Leftrightarrow$ optimal distribution D

Proposition: $\mathscr{C}$ is NMDS if and only if

(1) Any elementary box of volume $q^{-(k-1)}$ contains exactly q points

(2) There is an elementary box of the form

$$\prod_{i=1}^{n}[0,q^{m_i}]$$

and volume q^{-k} that contains q points, and this is the smallest elementary box with this property

Distributions are related to the concept of (t,m,s) nets (Niederreiter 1986)

Duality

Definition: Let $P_{\prec}$ be a poset on the set N of coordinates. The *dual poset* $P_{\succ}$ on N is obtained by reversing all the chains of $P_{\prec}$.

Example: Ordered Hamming space. $\mathbf{x} \in (\mathbb{F}_q)^{n,r}$

$$\overrightarrow{\mathcal{H}}: \; P_{\prec} = \cup_{i=1}^{n} \Big((i,1) < (i,2) < \cdots < (i,r) \Big)$$

$$\overleftarrow{\mathcal{H}}: \; P_{\succ} = \cup_{i=1}^{n} \Big((i,1) > (i,2) > \cdots > (i,r) \Big)$$

$$\mathbf{x} \in \overrightarrow{\mathcal{H}} : |\mathbf{x}| = \sum_{i=1}^{n} \max_{1 \le j \le r} (j : x_{ij} \neq 0)$$

$$\mathbf{x} \in \overleftarrow{\mathcal{H}} : |\mathbf{x}| = \sum_{i=1}^{n} \min_{1 \le j \le r} (r - j + 1 : x_{ij} \neq 0)$$

Duality

Definition: Let $P_{\prec}$ be a poset on the set N of coordinates. The *dual poset* $P_{\succ}$ on N is obtained by reversing all the chains of $P_{\prec}$.

$\mathscr{C}$ is a code in $\mathbb{F}_q^{|N|}$ w.r.t. $P_{\prec}$. Then the weights of its dual code $\mathscr{C}^{\perp}$ are counted w.r.t. $P_{\succ}$.

Example: Ordered Hamming space. The dual of a linear code is an OOA of strength d-1.

To establish the link of NMDS codes and distributions, we need to work with a linear subspace $\mathscr{C}$ as with a code and an OOA at the same time.

Weight distributions of poset NMDS codes

Weight distribution of an NMDS poset code $\mathscr{C}$ depends on the number of vectors associated with ideals of size d.

$A_{\mathcal{I}} \triangleq |\{\mathbf{x} \in \mathscr{C} : \langle \mathrm{supp}(\mathbf{x}) \rangle = \mathcal{I}\}|$

$A_s = \sum_{\mathcal{I}:\, |\mathcal{I}|=s} A_{\mathcal{I}}$

In an NMDS code $\mathscr{C}$

$$A_s = \sum_{I \in \mathcal{J}_s} \sum_{l=0}^{s-d-1} (-1)^l \binom{|\Omega(I)|}{l} (q^{s-d-l} - 1) + (-1)^{s-d} \sum_{I \in \mathcal{J}_s} \sum_{J \in \mathcal{J}_d(I), J \supseteq I \setminus \Omega(I)} A_J, \quad n \geq s \geq d.$$

$\mathcal{J}_s := \{\mathcal{I} \in P : |\mathcal{I}| = s\}$

$\Omega(\mathcal{I}) = \{\text{maximal elements in } \mathcal{I}\}$

Weight distributions of poset NMDS codes

Case study:

- Ordered Hamming space $(\mathbb{F}_q)^{n,r}$

$$A_s = \sum_{l=0}^{s-d-1} (-1)^l \left(\sum_{e:\sum ie_i=s} \binom{|e|}{l} \binom{n}{e_0, \ldots, e_r} \right) (q^{s-d-l}-1) + (-1)^{s-d} \sum_{e:\sum ie_i=d} N_s(e) A_e,$$

where $N_s(e) \triangleq \sum_{f:\sum if_i=s} \binom{e_{r-1}}{f_r - e_r} \binom{e_{r-2}}{(f_r + f_{r-1}) - (e_r + e_{r-1})} \cdots \binom{e_0}{|f| - |e|}.$

- Hamming space, r=1 $s=d,d+1,\ldots,n$

$$A_s = \sum_{l=0}^{s-d-1} (-1)^l \binom{s}{l} \binom{n}{s} (q^{s-d-l} - 1) + (-1)^{s-d} \binom{n-d}{s-d} A_d.$$

(known, Dodunekov/Landgev 1995)

THE END