On Weight Spectrum of Linear Codes

Vladimir N. Potapov

Sobolev Institute of Mathematics, Novosibirsk, Russia

online seminar: "Problems and Methods Related to Coding Theory",

December 14, 2021

Definitions

Let F_q^n be a vector space of dimension n over the Galois field F_q.
The weight $\mathrm{wt}(x)$ of a vector $x = (x_1, \ldots, x_n) \in F_q^n$ is the number of nonzero coordinates x_i of x.
The support of a function f is the set of arguments x such that $f(x) \neq 0$.
A linear (affine) code is a linear (affine) subspace of F_q^n.

Definitions

Denote by $\mathcal{A}_i(V) = \{x \in V : \mathrm{wt}(x) = i\}$ the subset of $V \subset F_q^n$ which consists of the vectors with weight i.
A finite sequence $|\mathcal{A}_i(V)|$, $i = 0, \ldots, n$, is called the weight distribution of V.
A code V is called t-weight if $\mathcal{A}_i(V) \neq \varnothing$ only for t different weights.
For a linear code $V \subseteq F_q^n$ we introduce the notation $\alpha'(V) = \max\limits_i \frac{|\mathcal{A}_i(V)|}{|V|}$.

Main definition

We will say that a sequence (V_n) of linear codes $V_n \subseteq F_q^{m_n}$ has a uniform weight spectrum if $\alpha'(V_n) \to 0$ as $n \to \infty$.

Note that $\dim V_n \to \infty$ if a sequence (V_n) has a uniform weight spectrum.

Examples

1. If $\Gamma_n \subseteq F_q^{m_n}$ is a sequence of n-dimensional faces (axis-aligned planes) and $n \to \infty$ then (Γ_n) has a uniform weight spectrum.

2. If (H_n) is a sequence of Hamming codes and $n \to \infty$ then (H_n) has a uniform weight spectrum.

3. If (C_n) is a sequence of t-weight codes then (C_n) has not uniform weight spectrum.

4. Random linear codes (V.M.Sidel'nikov and V.K.Leont'ev)

V.M. Sidelnikov, *Teoriya kodirovaniya*, 2008 (in Russian).

V.K. Leont'ev, "On spectra of linear codes", *Probl. Peredachi Inf.*, 2017.

Main problem

What is sufficient conditions for uniform weight spectrum?

Let us generalize the definition of a uniform weight spectrum sequences to affine codes.
For affine code $C \subseteq F_q^n$ define $\alpha(C) = \max\limits_{i,x} \frac{|\mathcal{A}_i(C+x)|}{|C|}$ where $x \in F_q^n$.

Definition

A sequence of affine codes $C_n \subseteq F_q^{m_n}$ has a strong uniform weight spectrum (SUWS) if $\alpha(C_n) \to 0$ as $n \to \infty$.

Suppose $C = W + y$ where W is a linear code and $y \in F_q^n$.
It is clear that $\alpha'(W) \leq \alpha(C)$.
Let $\alpha(C) = \frac{|\mathcal{A}_i(C+x)|}{|C|} = \frac{|\mathcal{A}_i(W+y+x)|}{|W|}$. Let V be a linear span of $\{x + y, W\}$. Then $\alpha(C) \leq q\alpha'(V)$.
Therefore sufficient conditions for strong or don't strong uniform weight spectrum should be analogous.

Theorem

Let (V_n) and (U_n) be sequences of subspaces of $F_2^{m_n}$ and $U_n \subset V_n$. If (U_n) has SUWS then (V_n) has SUWS.

Proof. Consider a bipartite graph G with parts $D_1 = \mathcal{A}_i(V_n \oplus w)$ and $D_2 = (\mathcal{A}_i(V_n \oplus w) \oplus U_n) \setminus D_1$ for some weight i and a vector w. Without lost of generality, let $w = \overline{0}$.

Vertices $v_1 \in D_1$ and $v_2 \in D_2$ are adjacent if and only if $v_2 = v_1 \oplus u$ where $u \in U_n$.

The degree of $v \in D_1$ in G is not less than $|U_n|(1 - \alpha(U_n))$. Indeed if $v \oplus u \in D_1$ then $\mathrm{wt}(v \oplus u) = i$ and, consequently, $u \in \mathcal{A}_i(U_n \oplus v)$. By the definition of SUWS we obtain that $|\mathcal{A}_i(U_n \oplus v)| \leq \alpha(U_n)|U_n|$. In other case $v \oplus u \in D_2$.

In the same way we can prove that the degree of $v \in D_2$ in G is not greater than $\alpha(U_n)|U_n|$. Indeed if $v \oplus u \in D_1$ then $\mathrm{wt}(v \oplus u) = i$ and, consequently, $u \in \mathcal{A}_i(U_n \oplus v)$. By the definition of SUWS we obtain that $|\mathcal{A}_i(U_n \oplus v)| \leq \alpha(U_n)|U_n|$.

By double counting edges we obtain that $|E| \leq \alpha(U_n)|U_n||D_2|$ and $|E| \geq |D_1||U_n|(1 - \alpha(U_n))$.
Then $|D_1|(1 - \alpha(U_n)) \leq \alpha(U_n)|D_2|$.

$$\frac{|\mathcal{A}_i(V_n)|}{|V_n|} \leq \frac{|D_1|}{|D_2|} \leq \frac{\alpha(U_n)}{1 - \alpha(U_n)}.$$

By the hypothesis (U_n) has SUWS. Then $\alpha(U_n) \to 0$.
Consequently, $\alpha(V_n) = \max \frac{|\mathcal{A}_i(V_n)|}{|V_n|} \to 0$ and (V_n) has SUWS.

Corollary

If $|\mathcal{A}_1(V_n)| \to \infty$ then a sequence (V_n) has SUWS.

If $|\mathcal{A}_1(V_n)| = k$ then V_n contains k-dimensional subcube F_q^k.

question 1

Has a sequence (V_n) SUWS if $|\mathcal{A}_t(V_n)| \to \infty$ for fixed t?

It is well known the following

Delsarte's theorem

If $f : F_q^n \to \mathbb{R}$ is a function such that $\widehat{f}(0) \neq 0$ and $\mathrm{supp}(\widehat{f}) \subseteq \mathcal{A}_{i_1} \cup \cdots \cup \mathcal{A}_{i_k}$, then $|\mathrm{supp}(f)| \geq q^n / b(n, q, k)$ where $b(n, q, k) = |\mathcal{A}_0 \cup \cdots \cup \mathcal{A}_k|$.

There $\widehat{f}(z) = \frac{1}{q^{n/2}} \sum_{x \in F_n^q} f(x) \left(e^{\frac{2\pi i}{q}} \right)^{(x,z)}$ are coefficients of the Fourier transform of f.

Corollary

If $C \subset F_q^n$ is a t-weight linear code then $|C| \leq b(n, q, t) = O(n^t)$.

P. Delsarte, "Four fundamental parameters of a code and their combinatorial significance", *Information and Control*, 1973.

How large may be linear codes from a nonuniform weight spectrum sequence?

question 2

Consider a sequence (C_n), $C_n \subset F_q^n$, which has a nonuniform weight spectrum. Does inequality $|C_n| << q^{\varepsilon n}$ holds for $\varepsilon > 0$?

Counterexamples

Answers to questions 1 and 2 are "No".

Let $q = 2$. Consider affine spaces
$M_{n,i} = \{(x, x \oplus \bar{1}, \bar{0}) : x \in F_2^{(n-i)/2}\}$ where $i = n - 2k$.
$\mathcal{A}_{(n-i)/2}(M_{n,i}) = M_{n,i}$.
$|M_{n,i}| = 2^{(n-i)/2}$.
$V_{n,0} = \{(x, x) : x \in F_2^{n/2}\}$ where n is even.
$M_{n,0} = V_{n,0} \oplus (\bar{0}, \bar{1})$.
$|\mathcal{A}_2(V_{n,0})| = n/2 \to \infty$.

Below we will show that this counterexamples are useful.

Eigenspaces

Definition

Introduce the notation $L(n, q, i_1, \ldots, i_k) = \min |\mathrm{supp}(f)|$, where $\mathrm{supp}(\widehat{f}) \subseteq \mathcal{A}_{i_1} \cup \cdots \cup \mathcal{A}_{i_k}$.

The values of $L(n, q, i, i+1, \ldots, j)$ for $q \geq 4$ and $q = 3$, $i + j \leq n$ are calculated by Valuzhenich and Vorob'ev.

A. Valyuzhenich and K. Vorob'ev, "Minimum supports of functions on the Hamming graphs with spectral constraints", *Discrete Math.*, 2019.

The values of $L(n, 2, k)$ were known early $L(n, 2, k) = 2^{(n+|\theta_k|)/2}$ where $\theta_k = n - 2k$.

D.S. Krotov, "Traids in the combinatorial configurations", XII International Seminar "Discrete Mathematics and its Applications"(Moscow, 20-25 June 2016)

Eigenspaces

Proposition

If $C \subset F_q^n$ is an affine code and $C \subseteq \mathcal{A}_{i_1} \cup \cdots \cup \mathcal{A}_{i_k}$ then $|C| \leq q^n / L(n, q, i_1, \ldots, i_k)$.

Proof. Since $\operatorname{supp}(\widehat{\widehat{\mathbf{1}_C}}) = C$ for any affine code C,
$L(n, q, i_1, \ldots, i_k) \leq |\operatorname{supp}(\widehat{\mathbf{1}_C})|$.
For any affine code C the equations $|C||\operatorname{supp}(\widehat{\mathbf{1}_C})| = q^n$ then
$|C| = q^n / |\operatorname{supp}(\widehat{\mathbf{1}_C})| \leq q^n / L(n, q, i_1, \ldots, i_k)$.

Corollary

If $C \subset F_2^n$ is an affine code and $C \subseteq \mathcal{A}_k$ then $|C| \leq 2^{(n - |\theta_k|)/2}$.

Affine codes $M_{n,i}$ reached this bound.
$\mathcal{A}_{(n-i)/2}(M_{n,i}) = M_{n,i}$, $k = (n-i)/2$, $\theta_k = n - 2k = i$.
$|M_{n,i}| = 2^{(n-i)/2}$.

Eigenfunctions of Fourier transform

It is well known that eigenvalues of the Fourier transform on F_2^n are equal to ± 1. Known examples of eigenfunctions of the Fourier transform are functions of type $(-1)^b$ where b is a self-dual bent function. Functions of type $(-1)^b$ have maximum supports. Let us find eigenfunctions with a minimum support.

$|\mathrm{supp}(f)| \cdot |\mathrm{supp}(\widehat{f})| \geq 2^n$.
Therefore we obtain that $|\mathrm{supp}(f)| \geq 2^{n/2}$ if $\widehat{f} = \pm f$.

T. Tao, "An uncertainty principle for cyclic groups of prime order", *Math. Res. Lett.*, 2005

For even n consider the function $g : F_2^n \to \{0, \pm 1\}$ defined as

$$g(y) = \begin{cases} (-1)^{\mathrm{wt}(x)}, & \text{if } y = (x, x \oplus \overline{1}); \\ 0, & \text{otherwise.} \end{cases}$$

It is not difficult to calculate that $g = \widehat{g}$, $\mathrm{supp}(g) \subset \mathcal{A}_{n/2}$ and $|\mathrm{supp}(g)| = 2^{n/2}$.

Potapov V. N. On Weight Spectrum of Linear Codes // 2021 XVII International Symposium on Problems of Redundancy in Information and Control Systems (25-29 October 2021 Moscow, Russia)
DOI:10.1109/REDUNDANCY52534.2021.9606478
https://arxiv.org/abs/2107.14576