Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory
September 7–13, 2014, Svetlogorsk (Kaliningrad region), Russia *pp. 169–174*

On Linear Rigidity of Codes

Gorkunov E. V. gorkunov@math.nsc.ru
Sobolev Institute of Mathematics, Novosibirsk State University
Sotnikova E. V. jennies@list.ru
Sobolev Institute of Mathematics

Abstract. In this paper a notion of linear rigidity of codes is discussed. We point several examples of codes those are linearly rigid as well as those are not. Also, some conditions for a linear code to be linearly rigid are obtained.

1 Introduction

Let q be a positive power of a prime p. Denote by $\mathbb{F}_q$ a finite field of order q and let $\mathbb{F}_q^*$ be its multiplicative subgroup. Any subset C of the n-dimensional vector space $\mathbb{F}_q^n$ over the field $\mathbb{F}_q$ is called a *code* of length n. If C forms a subspace in $\mathbb{F}_q^n$, then the code is said to be *linear*. The *Hamming distance* between vectors $x, y \in \mathbb{F}_q^n$ equals the number of positions where they differ. The set $\operatorname{supp}(x) = \{i \colon x_i \neq 0\}$ is called the *support* of $x \in \mathbb{F}_q^n$. The *weight* of x is the number $w(x) = |\operatorname{supp}(x)|$.

Two codes in $\mathbb{F}_q^n$ are called *equivalent* if there exists an isometry of the space $\mathbb{F}_q^n$ mapping one of the codes onto the other one. In 1956 Markov [1] showed that every isometry of $\mathbb{F}_q^n$ can be represented as a pair $(\pi;\sigma)$, where the permutation $\pi \in S_n$ permutes positions of each vector, and $\sigma = (\sigma_1, \ldots, \sigma_n)$ is a tuple of permutations from S_q acting on elements of $\mathbb{F}_q$. In other words, the isometry group of $\mathbb{F}_q^n$ is the semidirect product

$$\operatorname{Aut}\left(\mathbb{F}_q^n\right) = S_n \leftthreetimes S_q^n = \left\{(\pi;\sigma) \colon \pi \in S_n,\, \sigma \in S_q^n\right\}$$

with the multiplication $(\pi;\sigma)(\tau;\delta) = (\pi\tau;\sigma\tau\cdot\delta)$, where $\sigma\tau = (\sigma_{1\tau^{-1}}, \ldots, \sigma_{n\tau^{-1}})$.

The action of an isometry $(\pi;\sigma) \in \operatorname{Aut}\left(\mathbb{F}_q^n\right)$ on a vector $x \in \mathbb{F}_q^n$ is given by the following equalities:

$$x(\pi;\sigma) = (x\pi)\sigma,\ y = x\pi = \left(x_{1\pi^{-1}}, \ldots, x_{n\pi^{-1}}\right),$$
$$y\sigma = (y_1\sigma_1, \ldots, y_n\sigma_n).$$

Isometries of $\mathbb{F}_q^n$ mapping a code C onto itself form the group $\operatorname{Aut}(C)$ called the *automorphism group* of C. By the *symmetry group* of C we mean the group $\operatorname{Sym}(C)$ of automorphisms $(\pi;\sigma) \in \operatorname{Aut}(C)$ such that $0(\pi;\sigma) = 0$ (despite whether or not the all-zero vector 0 belongs to C). As a known proposition states, for a linear code the symmetry group is a significant part of its automorphism group.

Proposition 1. *For a linear code* $C \subseteq \mathbb{F}_q^n$ *it holds* $\mathrm{Aut}(C) \cong \mathrm{Sym}(C) \leftthreetimes C$.

Multiplying all vectors of $\mathbb{F}_q^n$ by a monomial $n \times n$ matrix, we obtain a *monomial automorphism* of $\mathbb{F}_q^n$. The *monomial automorphism group* of C is denoted by $\mathrm{MAut}(C)$. Let us call codes C_1 and C_2 *monomially equivalent* if $C_2 = \{xM \colon x \in C_1\}$ for some monomial $n \times n$ matrix M. MacWilliams [2] established that two linear codes are monomially equivalent iff there exists an isomorphism between them preserving the weight of each vector. Here the term *isomorphism* means an isomorphism between linear spaces.

From MacWilliams' theorem it follows that the monomial automorphism group $\mathrm{MAut}(C)$ of a linear code C consists of all its linear symmetries. Given a field automorphism $\gamma \in \mathrm{Gal}(\mathbb{F})$, a function $f \colon \mathbb{F}_q^n \to \mathbb{F}_q^n$ is called *semilinear* if for any $x, y \in \mathbb{F}_q^n$ and $\alpha, \beta \in \mathbb{F}_q$ it holds $f(\alpha x + \beta y) = \gamma(\alpha) f(x) + \gamma(\beta) f(y)$. The semidirect product $\Gamma L_n(q) = \mathrm{Gal}(\mathbb{F}) \leftthreetimes GL_n(q)$ is called the general semilinear group. So, all semilinear symmetries of $\mathbb{F}_q^n$ is exhausted by elements of the semidirect product $\mathrm{Gal}(\mathbb{F}) \leftthreetimes \mathrm{MAut}(\mathbb{F}_q^n)$.

All symmetries of $\mathbb{F}_2^n$ and $\mathbb{F}_3^n$ are linear. In case $q \geq 4$ semilinear symmetries of $\mathbb{F}_q^n$ generate a proper subgroup of $\mathrm{Sym}(\mathbb{F}_q^n)$ and there are a lot of symmetries which are not semilinear. In later case, let us say that a symmetry is *nonsemilinear*.

A linear code will be referred to as *linearly rigid* if every its symmetry is semilinear. This definition can be generalized on nonlinear codes in the following way. A code $C \subseteq \mathbb{F}_q^n$ will be called *linearly rigid* if there exists another code $C' \subseteq \mathbb{F}_q^n$ such that C' is equivalent to C, contains the all-zero vector, and all symmetries of its span are semilinear.

In [3] it is proved that the Hamming code is linearly rigid. In this paper several examples of linearly nonrigid codes are listed. At the same time, for a linear code with the automorphism group of a specified kind, some conditions sufficient for the code to be linearly rigid are obtained. Since $\mathbb{F}_2^n$ and $\mathbb{F}_3^n$ are linearly rigid spaces, hereinafter we have in mind $q \geq 4$.

2 Examples of linearly nonrigid codes

While $\mathbb{F}_q^n$ has nonsemilinear symmetries, it interesting to understand how many codes in the space are linearly rigid and how many ones are not.

Example 1. *Codes with nonessential positions.* If all codewords of a code C have the same symbol at some fixed position, we call the position *nonessential* for the code C. Let us remark that if a linear code has a nonessential position, then the codewords can have only 0 at this position. The sets of essential and nonessential positions of a code are invariant with respect to automorphisms of the code. The proof of this fact is trivial.

Proposition 2. *An arbitrary automorphism of any code takes an essential position of the code to an essential one, while each nonessential position is mapped to a nonessential one.*

If a permutation $\sigma \in S_q$ represents multiplication on some element from $\mathbb{F}_q^*$, we will call it a *multiplying permutation*.

Proposition 3. *A code with nonessential positions is linearly nonrigid.*

Proof. We may assume that the code given is linear. Indeed, by the definition of linear rigidity, given a nonlinear code C, we should consider the span of a code C' equivalent to C such that C' contains the all-zero vector. Since C and C' are equivalent, C' has nonessential positions as much as C has. Further, because of $0 \in C'$ all codewords of C' have 0 at each nonessential position.

In any case, we have to find a nonsemilinear symmetry of a linear code C with at least one nonessential position. Let the i-th position of C is nonessential. Take any permutation $\sigma_i \in S_q$ that fix 0 but is not multiplying. Denote by id the identity permutation and put $\sigma = (\mathrm{id}, \ldots, \mathrm{id}, \sigma_i, \mathrm{id}, \ldots, \mathrm{id})$. Obviously, $(\mathrm{id}; \sigma) \in \mathrm{Aut}(C)$ but it is a nonsemilinear symmetry of C. Therefore, the code is linearly nonrigid. □

Example 2. *Codes of minimum distance* 1 give us another class of linearly nonrigid codes.

Proposition 4. *A code of minimum distance* 1 *is linearly nonrigid.*

Proof. Consider a code $C \subseteq \mathbb{F}_q^n$ of minimum distance 1. Again we may assume C to be linear. By definition, there are codewords $x, y \in C$ such that $d(x, y) = 1$. Let x and y differ in the i-th position. Then the code C contains the vector e_i, which has zeroes at all positions except 1 at the i-th position. Consequently, we can partition C into subsets of q codewords each such that all vectors of one subset are pairwise at distance 1 and differ at the i-th position.

Now we easily get a nonsemilinear symmetry of C. As before, take any permutation $\sigma_i \in S_q$ that fix 0 but is not multiplying. Clearly, $(\mathrm{id}; \sigma) \in \mathrm{Aut}(C)$ in case $\sigma = (\mathrm{id}, \ldots, \mathrm{id}, \sigma_i, \mathrm{id}, \ldots, \mathrm{id})$, but it is a nonsemilinear symmetry of C. This concludes the proof. □

Example 3. *A q-ary code with a parity check matrix all entries of which are in a subfield of $\mathbb{F}_q$.* Finally, we recall a well-known method to construct one more infinite set of linearly nonrigid codes. Consider a parity check matrix H such that all of its entries are in a proper subfield $\mathbb{F}$ of $\mathbb{F}_q$. To be definite, let $\mathbb{F}$ be the prime subfield $\mathbb{F}_p < \mathbb{F}_q$. Denote by C the code with the matrix H.

From the theory of finite fields it is known that in case $q = p^r$ and $r > 1$ the field $\mathbb{F}_q$ forms a linear space of dimension r over $\mathbb{F}_p$. Take a permutation $\sigma \in S_q$ that is a linear transformation of $\mathbb{F}_q$ over $\mathbb{F}_p$. Provided σ is linear, for any $x \in \mathbb{F}_q^n$ we get

$$H(x^{\mathsf{T}}\sigma) = (Hx^{\mathsf{T}})\sigma,$$

where σ acts on each position of the vector-columns x^{T} and Hx^{T}. Furthermore, $0\sigma = 0$. This implies that the vectors x and $(x_1\sigma, \ldots, x_n\sigma)$ belongs to C or do not simultaneously. So, $(\mathrm{id}; (\sigma, \ldots, \sigma)) \in \mathrm{Sym}(C)$.

If $q \geq 8$, the permutation σ can be chosen such that it is neither a multiplying permutation nor a field automorphism from the Galois group $\mathrm{Gal}(\mathbb{F}_q)$. Then the symmetry of C pointed above is a nonsemilinear. This makes C to be linearly nonrigid.

3 Sufficient conditions for linear rigidity

In this section we describe some conditions which are sufficient for a linear code to be linearly rigid. To present further, we need some notation. For a code $C \subseteq \mathbb{F}_q^n$ designate the following subgroups of its automorphism group:

$\mathrm{PAut}(C) = \{(\pi; \mathrm{id}) \in \mathrm{Aut}(C)\}$, the *permutation automorphism group* of C;
$\mathrm{Atp}(C) = \{(\mathrm{id}; \sigma) \in \mathrm{Aut}(C)\}$, the *autotopy group* of C;
$\mathrm{SAtp}(C) = \mathrm{Sym}(C) \cap \mathrm{Atp}(C)$, the *symmetric autotopy group* of C.

Instead of $(\pi; \mathrm{id}) \in \mathrm{PAut}(C)$ and $(\mathrm{id}; \sigma) \in \mathrm{Atp}(C)$ we write briefly $\pi \in \mathrm{PAut}(C)$ and $\sigma \in \mathrm{Atp}(C)$.

The conditions we are going to present include a restriction on the automorphism group of a code. Namely every symmetry $(\pi; \sigma) \in \mathrm{Sym}(C)$ should be decomposable into symmetries of C, that is $\pi, \sigma \in \mathrm{Sym}(C)$. The theory of groups gives us a criterion for determining if a group is the semidirect product of some their subgroups (see, e. g., [4, Ch. 6]). Being employed, it makes possible to get another form for the restriction on the automorphism group.

Proposition 5. *Given a code $C \subseteq \mathbb{F}_q^n$, for each symmetry $(\pi; \sigma) \in \mathrm{Sym}(C)$, its parts π and σ are symmetries of C iff $\mathrm{Sym}(C) \cong \mathrm{PAut}(C) \leftthreetimes \mathrm{SAtp}(C)$.*

Let $[n] = \{1, 2, \ldots, n\}$. For a pair of vectors $x, y \in \mathbb{F}_q^n$ such that positions $i, j \in \mathrm{supp}(x) \cap \mathrm{supp}(y)$, define the *mutual coefficient* $\omega_{ij}(x, y)$ of x and y with respect to i and j by

$$\omega_{ij}(x, y) = \frac{y_j}{x_j} \Big/ \frac{y_i}{x_i} = \frac{x_i y_j}{x_j y_i}.$$

Remark some trivial properties of a mutual coefficient:

1) $\omega_{ij}(x, y) = \dfrac{y_j}{x_j}$ in case of $x_i = y_i$;
2) $\omega_{ij}(y, x) = \omega_{ji}(x, y) = \omega_{ij}^{-1}(x, y)$;
3) $\omega_{ij}(x, \mu x) = 1$ for any $i, j \in \mathrm{supp}(x)$ and any $\mu \in \mathbb{F}_q^*$;
4) $\omega_{ij}(\lambda x, \mu y) = \omega_{ij}(x, y)$ for any $\lambda, \mu \in \mathbb{F}_q^*$;
5) $\omega_{i\pi, j\pi}(x\pi, y\pi) = \omega_{ij}(x, y)$ for any $\pi \in S_n$.

We say that vectors $x, y \in \mathbb{F}_q^n$ form a *link* for positions $i, j \in [n]$, or briefly, an (i,j)*-link,* if the mutual coefficient $\omega_{ij}(x,y)$ is a primitive element of $\mathbb{F}_q$.

Consider a linear code $C \subseteq \mathbb{F}_q^n$ of minimum distance d and the subcode $D_C \subseteq C$ formed by the minimum-weight codewords of C. In other words, $D_C = \{x \in C \colon w(x) = d\}$. We will refer to D_C as the *minimum-weight subcode* of the code C. Since $\mathrm{Sym}(C) \le \mathrm{Sym}(D_C)$, the following is obvious.

Proposition 6. *A linear code is linearly rigid whenever its minimum-weight subcode is linearly rigid.*

Let us recall a useful lemma, which can be found, e. g., in [2]. This lemma is crucial while we try to prove that one or another automorphism of a code is monomial or semilinear.

Lemma 1. *Suppose $C \subseteq \mathbb{F}_q^n$ is a linear code of minimum distance d and codewords $x, y \in C$ have the same support and weight $w(x) = w(y) = d$. Then there exists $\mu \in \mathbb{F}_q^*$ such that $y = \mu x$.*

An (i,j)-link, if there is any one in a linear code $C \subseteq \mathbb{F}_q^n$, binds components σ_i and σ_j of every symmetric autotopy $\sigma \in \mathrm{SAtp}(C)$.

Lemma 2. *Let $C \subseteq \mathbb{F}_q^n$ be a linear code of minimum distance $d \ge 2$. If its minimum-weight subcode contains an (i,j)-link, then, for every symmetric autotopy $\sigma \in \mathrm{SAtp}(C)$, components σ_i and σ_j are multiplying permutations.*

Proof. For simplicity, put $i = 1$ and $j = 2$. Suppose D_C is the minimum-weight subcode of C and vectors $x, y \in D_C$ form an (i,j)-link. Since C is linear, we may assume $x_1 = y_1 = 1$. Denote $x_2 = \alpha$, $y_2 = \beta$, and $\omega = \omega_{12}(x,y) = \beta\alpha^{-1}$. Because ω is a primitive element of $\mathbb{F}_q$, we have $\alpha \ne \beta$.

Let $\sigma \in \mathrm{SAtp}(C)$ and $\nu\sigma_1 = \lambda_\nu$ for each $\nu \in \mathbb{F}_q^*$. The arguments below remain valid for any $\nu \in \mathbb{F}_q^*$. Clearly, $\mathrm{supp}(\nu x) = \mathrm{supp}((\nu x)\sigma)$. By Lemma 1, vectors νx and $(\nu x)\sigma$ are collinear. Therefore,

$$\nu x = (\nu, \nu\alpha, \ldots) \quad \overset{\sigma}{\longmapsto} \quad (\nu x)\sigma = (\lambda_\nu, \lambda_\nu\alpha, \ldots).$$

That is $(\nu\alpha)\sigma_2 = \lambda_\nu\alpha$. In particular, $(\omega\alpha)\sigma_2 = \beta\sigma_2 = \lambda_\omega\alpha$.

On the other hand, from Lemma 1 we derive

$$\nu y = (\nu, \nu\beta, \ldots) \quad \overset{\sigma}{\longmapsto} \quad (\nu y)\sigma = (\lambda_\nu, \lambda_\nu\beta, \ldots).$$

This implies that $\beta\sigma_2 = \lambda_1\beta$. Comparing with $\beta\sigma_2 = \lambda_\omega\alpha$, we get

$$\lambda_\omega = \lambda_1\beta\alpha^{-1} = \lambda_1\omega.$$

Similarly, it holds

$$\lambda_\nu\beta = (\nu\beta)\sigma_2 = (\nu\omega\alpha)\sigma_2 = \lambda_{\nu\omega}\alpha.$$

So, $\lambda_{\nu\omega} = \lambda_\nu \omega$ for any $\nu \in \mathbb{F}_q^*$. Then $\lambda_{\omega^2} = \lambda_\omega \omega = \lambda_1 \omega^2$ and, by induction, $\lambda_{\omega^k} = \lambda_1 \omega^k$ for any integer k. Because ω is a primitive element of $\mathbb{F}_q$, it follows that σ_1 is the permutation multiplying on $\lambda_1 = 1\sigma_1$.

Since $\omega_{ji}(x, y) = \omega_{ij}^{-1}(x, y)$, we can interchange i and j in the reasoning above and conclude that σ_2 is a multiplying permutation too. □

Now, given a code $C \subseteq \mathbb{F}_q^n$, we define a *link graph* $L(C)$ on $[n]$ as a vertex set. Put that the edge (i, j) belongs to the edge set of $L(C)$ if there exists an (i, j)-link in the code C.

Theorem 1. *Let $C \subseteq \mathbb{F}_q^n$ be a linear code of minimum distance $d \geq 2$. Suppose the code C satisfies the following conditions:*
1) $\mathrm{Sym}(C) \cong \mathrm{PAut}(C) \leftthreetimes \mathrm{SAtp}(C)$*;*
2) the link graph $L(D_C)$ is connected.
Then all symmetries of C are monomial, that is $\mathrm{Sym}(C) = \mathrm{MAut}(C)$.

From Theorem 1 it follows the main result of the paper.

Corollary 1. *Let $C \subseteq \mathbb{F}_q^n$ be a linear code of minimum distance $d \geq 2$. Suppose the code C satisfies the following conditions:*
1) $\mathrm{Sym}(C) \cong \mathrm{PAut}(C) \leftthreetimes \mathrm{SAtp}(C)$*;*
2) the link graph $L(D_C)$ is connected.
Then the code C is linearly rigid.

As we can see the sufficient conditions for linear rigidity of a code obtained in this paper are rather strong. So, there is a subject to investigate whether each of them is necessary or not.

References

[1] A. A. Markov, On Transformations without Error Propagation, *Izbrannye trudy* (Selected Works), vol. II: *Teoriya algorifmov i konstruktivnaya matematika. Matematicheskaya logika. Informatika i smezhnye voprosy* (Theory of Algorithms and Constructive Mathematics. Mathematical Logic. Information Science and Related Topics), N. M. Nagornyi, Ed., Moscow: MCCME, 2003, 70–93 (in Russian).

[2] F. J. MacWilliams, *Combinatorial Problems of Elementary Abelian Groups,* Doctoral thesis, Harvard University, Harvard, 1962.

[3] E. V. Gorkunov, The Automorphism Group of a q-ary Hamming Code, *Diskretn. Anal. Issled. Oper.,* **17** (6), 50–55, 2010 (in Russian).

[4] M. Hall, Jr., *The Theory of Groups,* AMS Chelsea Publishing, Providence, 1998.