Critical Pairs for the Product Singleton Bound

Diego Mirandola, Gilles Zémor

Critical pairs for the Product Singleton Bound

Diego Mirandola[*], Gilles Zémor[†]

March 4, 2015

Abstract

We characterize Product-MDS pairs of linear codes, i.e. pairs of codes C, D whose product under coordinatewise multiplication has maximum possible minimum distance as a function of the code length and the dimensions $\dim C, \dim D$. We prove in particular, for $C = D$, that if the square of the code C has minimum distance at least 2, and (C, C) is a Product-MDS pair, then either C is a generalized Reed-Solomon code, or C is a direct sum of self-dual codes. In passing we establish coding-theory analogues of classical theorems of additive combinatorics.
Keywords: Error-correcting codes, Schur-product codes, Product Singleton Bound.

1 Introduction

Let F be a finite field. Given vectors $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$ of F^n, let us denote by xy the componentwise product of x and y,

$$xy = (x_1y_1, \ldots, x_ny_n).$$

Given two linear codes $C, D \subseteq F^n$, let us denote by CD the F-linear subspace of F^n generated by all products xy, $x \in C$, $y \in D$. This product, sometimes called the Schur product, has usually been denoted by $C * D$, but we wish to lighten notation. Likewise we shall denote the Schur square (henceforth square) of a code C by C^2: context should prevent confusion with cartesian products.

Products of codes turn up in a variety of situations and are applied to algebraic error correction, secret sharing and multiparty computation, algebraic complexity theory, lattice constructions, and lately cryptanalysis. For a review of these applications, we refer to the introduction of the paper [3]. A number of efforts have gone into describing the code-theoretic structure of code products, see [10] for an extensive review of the current state of the art. In particular the following bound on the minimum distance of products was proved in [9].

THEOREM 1.1 (Product Singleton Bound [9]). *Let $C, D \subseteq F^n$ be linear codes. Then*

$$d_{\min}(CD) \leq \max\{1, n - (\dim C + \dim D) + 2\}. \tag{1}$$

A slightly stronger version of Theorem 1.1 is actually proved in [9], as is a version involving the product of more than two codes, but the above statement is really what motivates our discussion. We shall call the upper bound (1) the *Product Singleton Bound* (PSB), that can be thought of as a generalization of the classical Singleton Bound. Indeed, the classical

[*]CWI Amsterdam and Mathematical Institute, Leiden University, The Netherlands, and Mathematical Institute, Bordeaux University, France. Email: diego@cwi.nl.

[†]Mathematical Institute, Bordeaux University, France. Email: zemor@math.u-bordeaux.fr.

Singleton Bound for a single code C is recovered by taking the code D in Theorem 1.1 to be of dimension 1 and minimum distance n.

Our goal in this paper is to characterize pairs (C, D) of codes that achieve equality in (1). We make the remark that if $d_{\min}(CD)$ is allowed to be equal to 1, then pairs achieving equality in (1) can be almost anything, since typical pairs of codes will have a product equal to the whole space F^n. For a study of this phenomenon see [3]. So we shall disregard the situation when $d_{\min}(CD) = 1$ and call (C, D) a *Product-MDS (PMDS)* pair if it achieves equality in (1) and $d_{\min}(CD) \geq 2$.

As mentioned above, a PMDS pair can consist of an ordinary MDS code and a code of dimension 1. It is a natural question to ask what other PMDS pairs exist. It turns out that there is a surprisingly complete answer to this question. We shall show in particular that if (C, D) is a PMDS pair such that $\dim C \geq 2$, $\dim D \geq 2$, and $d_{\min}(CD) \geq 3$, then C and D can only be Reed-Solomon codes. By this we mean Reed-Solomon code in the widest sense, i.e. generalized, possibly extended or doubly extended in the terminology of [7], or Cauchy codes as in [4]. PMDS pairs with $d_{\min}(CD) = 2$ will also be described quite precisely. To be more specific, in the symmetric case $C = D$ we shall prove:

THEOREM 1.2. *If (C, C) is a PMDS pair, then either C is a Reed-Solomon code or C is a direct sum of self-dual codes.*

Self-duality in the above statement should be understood to be relative to a non-degenerate bilinear form which is not necessarily the standard inner product.

To establish these results we shall import methods from additive combinatorics and establish coding-theoretic analogues of the classical theorems of Kneser [6] and Vosper [12]. For background on and proofs of Kneser and Vosper's Theorems we refer to [11]. Kneser's Theorem implies in particular that if A, B are pairs of subsets of an abelian group such that

$$|A + B| < |A| + |B| - 1$$

then $A + B$ must be periodic, i.e. there exists a non-zero element g of the abelian group that stabilises $A+B$ so that we have $A+B+g = A+B$. Our coding-theoretic variant of Kneser's Theorem will imply that if C and D are two codes such that

$$\dim CD < \dim C + \dim D - 1,$$

then the code C is necessarily the direct sum of two non-zero codes with disjoint supports, which is equivalent to the existence of a non-constant vector x of F^n such that $CD = CDx$.

Vosper's Theorem is a characterization of pairs of subsets A, B of the integers modulo a prime p with the property that $|A + B| = |A| + |B| - 1$. It states that, excluding some degenerate cases, A, B must be arithmetic progressions with the same difference. We make the remark that if a code C has a generator matrix with rows $v, v\alpha, \ldots, v\alpha^{k-1}$, i.e. has a basis of elements in "geometric" progression then, provided v is of weight n and α has distinct coordinates, C must be a Reed-Solomon code. This is why a code-theoretic version of Vosper's Theorem forces the appearance of Reed-Solomon codes. There will be some twists to the analogy however that we shall discuss in the paper.

All proofs are omitted and postponed to the full version of the paper[1].

2 Main result

Throughout the paper F will denote a finite field. We shall need, in a couple of occasions, to deal with fields that may be infinite in which case we will use the notation K.

[1]Available on arxiv: `http://arxiv.org/abs/1501.06419`

Given a vector $x \in K^n$, we denote by $\mathrm{supp}(x)$ its support and by $\mathrm{wt}(x)$ its weight. The support of a subvector space of K^n is defined as the union of the supports of all its vectors, and we shall say that a vector space in K^n has *full support* if its support is $\{1, \ldots, n\}$.

In this paper all codes will be linear. We will call them simply "codes" when the ambient space is F^n, and use the terminology of vector spaces in the general setting of K^n.

Given a code $C \subseteq F^n$, we denote by $C^\perp$ its dual with respect to the standard inner product in F^n and by $d_{\min}(C)$ its minimum distance.

The classical Singleton Bound states

$$\dim C + d_{\min}(C) \leq n + 1.$$

A code which attains this bound is said to be Maximum Distance Separable (MDS). We recall the following well-known property and characterizations of MDS codes [7].

Among MDS codes, Reed-Solomon (RS) codes, in the widest possible sense, will be prominent. An RS code of length n and dimension k is a code of the form

$$\{(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)) : f \in F[X]_{<k}\},$$

where $F[X]_{<k}$ denotes the space of polynomials of degree less than k, $v_1, \ldots, v_n$ are non-zero elements of F, and $\alpha_1, \ldots, \alpha_n$ are pairwise disjoint and belong to $F \cup \{\infty\}$, with the convention that for any $f \in F[X]_{<k}$, $f(\infty)$ equals the coefficient of X^{k-1} in f. We shall call $(\alpha_1, \ldots, \alpha_n)$ an *evaluation-point sequence* for the Reed-Solomon code.

This code family includes the codes called generalized, extended, and doubly-extended Reed-Solomon codes. From the geometric point of view, they may be thought of as the projective version of Reed-Solomon codes. In [4] they are named "Cauchy codes" and have also been called "Cauchy Reed-Solomon codes". We shall simply refer to them as "Reed-Solomon codes".

REMARK 2.1. If C and D are two Reed-Solomon codes with a common evaluation-point sequence α, then the product CD is also Reed-Solomon with evaluation-point sequence α and we have $\dim CD = \min\{n, \dim C + \dim D - 1\}$. Theorem 2.2 below implies that $\min\{n, \dim C + \dim D - 1\}$ is the minimum possible dimension of the product of MDS codes.

For an arbitrary field K, the space K^n is, with the coordinatewise product, a commutative unitary K-algebra. Its unit-element is the all-one vector, denoted by $\mathbf{1}$. The multiplicative group of its invertible elements is $(K^n)^\times = (K^\times)^n$, meaning that $x \in K^n$ is invertible if and only if all entries of x are non-zero. Given $x \in (K^n)^\times$, its inverse is denoted by x^{-1}.

The two results below relate the dimension of the product of two codes with the MDS property. The first one is taken from [10, §3.5].

THEOREM 2.2. *Let $C, D \subseteq F^n$ be full-support codes. If (at least) one of them is MDS, then*

$$\dim CD \geq \min\{n, \dim C + \dim D - 1\}.$$

We also observe the following.

LEMMA 2.3. *Let $C, D \subseteq F^n$ be MDS codes such that*

$$\dim CD = \dim C + \dim D - 1.$$

Then CD is MDS.

Lemma 2.4 below classifies all subalgebras of K^n. For all $i = 1, \ldots, n$, let e_i denote the i-th unit vector in K^n. We call a vector of the form $\sum_{i \in I} e_i$ for some $I \subseteq \{1, \ldots, n\}$ a *projector*. In particular, $\mathbf{1}$ is the projector with support $\{1, \ldots, n\}$. A family of projectors is *disjoint* if the projectors have pairwise disjoint supports.

LEMMA 2.4. *Any K-subalgebra of K^n admits a K-basis of disjoint projectors.*

REMARK 2.5. Lemma 2.4 implies in particular that the number of subalgebras of K^n is finite. This fact will be useful later.

Let $C \subseteq F^n$ be a code. We define $\mathrm{St}(C) := \{x \in F^n : xC \subseteq C\}$, the *stabilizer* of C in F^n. As C is linear, $\mathrm{St}(C)$ is an F-algebra, hence Lemma 2.4 applies and $\mathrm{St}(C)$ admits an F-basis $\{\pi_1, \ldots, \pi_h\}$ of disjoint projectors, with $h := \dim \mathrm{St}(C)$. When $h = 1$ we say that C has trivial stabilizer. We have the following lemma, whose proof is straightforward.

LEMMA 2.6. *Any full-support code C decomposes as*

$$C = \pi_1 C \oplus \cdots \oplus \pi_h C$$

where $\{\pi_1, \ldots, \pi_h\}$ is a basis of disjoint projectors of $\mathrm{St}(C)$. Moreover, each summand $\pi_i C$, viewed as a code in $F^{|\operatorname{supp}(\pi_i)|}$, has trivial stabilizer and has full support.

Facts on stabilizers, including Lemma 2.6, can be found in [10, from §2.6 onwards]. Following [10], let us say that a code is *indecomposable* if it has trivial stabilizer.

Lemma 2.6 states in particular that a full-support code has non-trivial stabilizer if and only if it decomposes as a direct sum of codes, and the dimension of the stabilizer equals the number of indecomposable components. It follows that all MDS codes that are not equal to F^n have trivial stabilizer.

Our main result takes the following form.

THEOREM 2.7. *Let $C, D \subseteq F^n$ be codes such that the pair (C, D) is Product MDS. Then one of the following situations occurs.*

(i) C and D are MDS and, if none of them has dimension 1, they are Reed-Solomon codes with a common evaluation-point sequence.

(ii) There is a partition of the coordinate set into non-empty subsets

$$\{1, 2, \ldots, n\} = I_1 \cup \cdots \cup I_h$$

and there exist h pairs $(C_1, D_1), \ldots, (C_h, D_h)$ of codes of F^n, such that $\operatorname{supp}(C_i) = \operatorname{supp}(D_i) = I_i$, $i = 1, \ldots, h$, and such that C and D decompose as:

$$C = C_1 \oplus \cdots \oplus C_h,$$
$$D = D_1 \oplus \cdots \oplus D_h.$$

Furthermore, for $i = 1, ..., h$, when C_i and D_i are identified with codes of $F^{|I_i|}$ through the natural projection on their support, then $C_i = (g_i D_i)^\perp$ for some $g_i \in (F^\times)^{|I_i|}$.

REMARK 2.8. The codes C_i and D_i are mutually orthogonal relative to the bilinear form $(x, y) \mapsto (x \,|\, g_i y) = (g_i x \,|\, y)$, where $(\cdot \,|\, \cdot)$ denotes the standard inner product. Hence the wording of Theorem 1.2 in the case $C = D$.

3 Kneser's Theorem

Kneser's Addition Theorem below involves the stabilizer $\mathrm{St}(X) = \{g \in G,\ g + X = X\}$ of a subset X of an abelian group G. The (Minkowski) sum $A + B$ of two subsets A, B of G is defined as the set of sums $a + b$ when a, b range over A and B respectively.

THEOREM 3.1 (Kneser [6]). *Let G be an abelian group. Let $A, B \subseteq G$ be non-empty, finite subsets. Then*

$$|A+B| \geq |A| + |B| - |\operatorname{St}(A+B)|.$$

Kneser's original Theorem was transposed to the extension field setting by Hou, Leung and Xiang in [5]. Let L/K be a field extension. For K-linear subspaces $S, T \subseteq L$, we may consider the product of subspaces ST defined as the K-linear span of the set of elements of the form $st, s \in S, t \in T$. Hou et al.'s Theorem is concerned with the structure of pairs of subspaces whose product has small dimension. Again, the stabilizer of a K-subspace $X \subseteq L$ is involved and is defined in the expected way $\operatorname{St}(X) = \{z \in L, zX \subseteq X\}$.

THEOREM 3.2 (Generalized Kneser Theorem [5]). *Let L/K be a separable field extension. Let $S, T \subseteq L$ be non-zero, finite-dimensional K-vector spaces. Then*

$$\dim ST \geq \dim S + \dim T - \dim \operatorname{St}(ST).$$

Remarkably, Kneser's original theorem for groups can be recovered easily from Hou et al.'s version.

We will show that there is a variant of Kneser's Theorem for the algebra induced by coordinatewise multiplication.

THEOREM 3.3. *Let $S, T \subseteq K^n$ be non-zero K-vector spaces. Then*

$$\dim ST \geq \dim S + \dim T - \dim \operatorname{St}(ST).$$

REMARK 3.4. The products ST in Theorems 3.2 and 3.3 are in different algebras.

Our proof is strongly inspired by Hou et al.'s proof of Theorem 3.2 [5], itself drawing upon the e-transform technique of additive combinatorics (see e.g. [11]).

Theorem 3.3 implies in particular that if C and D are two codes such that CD has trivial stabilizer, i.e. is indecomposable, then we must have

$$\dim CD \geq \dim C + \dim D - 1. \tag{2}$$

We turn next to the study of pairs of codes C, D such that CD is indecomposable and achieves equality in (2).

4 Vosper's Theorem and classification of PMDS pairs

We recall Vosper's Addition Theorem.

THEOREM 4.1 (Vosper [12]). *Let G be an abelian group of prime order p. Let $A, B \subseteq G$ be subsets, with $|A|, |B| \geq 2$. If*

$$|A+B| = |A| + |B| - 1 \leq p - 2$$

then A and B are arithmetic progressions with the same difference.

We point out that an extension field version of Vosper's Theorem for finite fields was recently proved in [1].

Since the stabilizer of a subset of a group G must be a subgroup, when G is of prime order and has no proper subgroup, Kneser's Addition Theorem 3.1 implies that subsets A, B of G such that $A + B \neq G$ must satisfy

$$|A+B| \geq |A| + |B| - 1.$$

This result is known as the Cauchy-Davenport Inequality, see [8, 11]. Vosper's Theorem is therefore concerned with characterizing pairs of sets achieving equality in the Cauchy-Davenport Inequality.

In the algebra setting, the inequality (2) may be thought of as a code-product version of the Cauchy-Davenport Inequality. But contrary to the group case, the algebra F^n always has proper subalgebras (for $n > 1$) so we cannot hope to ensure (2) purely by a condition on F^n. However, we have seen that (2) holds when (at least one of) the codes involved is MDS (Theorem 2.2). The following theorem may be seen as a version of Vosper's Theorem for MDS codes.

THEOREM 4.2. *Let $C, D \subseteq F^n$ be MDS codes, with $\dim C, \dim D \geq 2$. If*

$$\dim CD = \dim C + \dim D - 1 \leq n - 2$$

then C and D are Reed-Solomon codes with a common evaluation-point sequence.

REMARK 4.3. The hypotheses $\dim C, \dim D \geq 2$ clearly cannot be removed. The value $n-2$ is also best possible in the hypothesis $\dim CD \leq n-2$, since by taking C to be an arbitrary MDS (non Reed-Solomon) code, and taking $D = C^\perp$, we will have a pair of MDS codes such that $\dim CD = \dim C + \dim D - 1 = n - 1$.

An interesting consequence of Theorem 4.2 is the following characterization of Reed-Solomon codes among MDS codes. Applying Theorem 4.2 in the case $C = D$ yields:

COROLLARY 4.4. *Let $C \subseteq F^n$ be an MDS code, with $\dim C \leq (n-1)/2$. The code C is Reed-Solomon if and only if*

$$\dim C^2 = 2 \dim C - 1 = n - 1. \tag{3}$$

REMARK 4.5. If $\dim C \geq (n+1)/2$, then C being MDS we must have $C^2 = F^n$ and the dimension of the square cannot yield any information on the structure of C. However in that case, whether C is Reed-Solomon is betrayed by the dimension of the square of the dual code $C^\perp$. The remaining case in which Corollary 4.4 does not say anything is the case $\dim C = n/2$. One may wonder whether it still holds that C is Reed-Solomon if and only if $\dim C^2 = 2 \dim C - 1$, and possibly Theorem 4.2 and Corollary 4.4 have not managed to capture this fact.

The answer to this question is negative, indeed there exist plenty of MDS codes of dimension $n/2$ satisfying (3) which are not Reed-Solomon. For instance, the codes denoted $C_{11,8,8}$ and $C_{13,8,21}$ in [2], of length 8 over the fields on 11 and 13 elements respectively are self-dual, therefore satisfy (3), and can be shown not to be Reed-Solomon.

The link between Kneser's Theorem and the characterization of PMDS pairs is expressed by the following proposition.

PROPOSITION 4.6. *Let $C, D \subseteq F^n$ be codes such that the pair (C, D) is PMDS. Then the following holds.*

1. *The pair (C, D) attains the bound of Kneser's Theorem, i.e.*

$$\dim CD = \dim C + \dim D - \dim \mathrm{St}(CD).$$

2. *Either CD is MDS or $d_{\min}(CD) = 2$.*

When CD is MDS, we shall prove that C and D have to be MDS codes as well. Theorem 4.2 can then be invoked to show that C and D cannot be any MDS codes but have to be Reed-Solomon. Case 2 of Proposition 4.6 leads eventually to case 2 of Theorem 2.7.

References

[1] C. Bachoc, O. Serra, and G. Zémor. An analogue of Vosper's Theorem for extension fields, 2015. Preprint: `http://arxiv.org/abs/1501.00602`

[2] K. Betsumiya, S. Georgiou, T. Gulliver, M. Harada, and C. Koukouvinos. On self-dual codes over some prime fields. *Discrete Mathematics*, 262(13):37 – 58, 2003.

[3] I. Cascudo, R. Cramer, D. Mirandola and G. Zémor. Squares of Random Linear Codes. *IEEE Transactions on Information Theory*, vol. 61, no. 3, pp. 1159-1173, March 2015.

[4] A. Dür. The automorphism groups of Reed-Solomon codes. *Journal of Combinatorial Theory*, Series A, Vol. 44, Issue 1, January 1987, Pages 69-82, ISSN 0097-3165.

[5] X.-D. Hou, K. H. Leung, and Q. Xiang. A Generalization of an Addition Theorem of Kneser. *Journal of Number Theory*, 97:1–9, 2002.

[6] M. Kneser. Abschätzung der asymptotischen dichte von summenmengen. *Mathematische Zeitschrift*, 58(1):459–484, 1953.

[7] F. J. McWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, 1977.

[8] M. Nathanson. *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*. Springer, 1996.

[9] H. Randriambololona. An upper bound of Singleton type for componentwise products of linear codes. *IEEE Transactions on Information Theory*, 59(12):7936–7939, Dec 2013.

[10] H. Randriambololona. On products and powers of linear codes under componentwise multiplication, to appear in vol. 637 of Contemporary Math., AMS, Apr. 2015. `http://arxiv.org/abs/1312.0022`

[11] T. Tao and V. H. Vu, *Additive Combinatorics*, Cambridge studies in advanced mathematics 105, Cambridge University Press 2006.

[12] A. G. Vosper. The Critical Pairs of Subsets of a Group of Prime Order. *Journal of The London Mathematical Society-second Series*, s1-31:200–205, 1956.