On products of linear error correcting codes

Mirandola, D.

Chapter 4

Critical Pairs for the Product Singleton Bound

4.1 Overview

Let $\mathbb{F}$ be a finite field, let n be a positive integer. Our goal in this chapter is to characterize pairs (C, D) of codes that attain the following bound.

THEOREM 4.1.1 (Product Singleton Bound [62]). *Let $C, D \subseteq \mathbb{F}^n$ be linear codes. Then*

$$d_{\min}(CD) \leq \max\{1, n - (\dim C + \dim D) + 2\}. \tag{4.1}$$

A slightly stronger version of Theorem 4.1.1 is actually proved in [62], 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 (4.1) the *Product Singleton Bound*, that can be thought of as a generalization of the classical Singleton Bound. Indeed, the classical Singleton Bound for a single code C is recovered by taking the code D in Theorem 4.1.1 to be of dimension 1 and minimum distance n.

We make the remark that if $d_{\min}(CD)$ is allowed to be equal to 1, then pairs achieving equality in (4.1) can be almost anything, since typical pairs of codes will have a product equal to the whole space $\mathbb{F}^n$. This phenomenon has been studied in Chapter 3 in the case of $C = D$ and in [64] in the general case. 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 (4.1) 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 [48], or Cauchy codes as in [30]. 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 4.1.2. *If (C, C) is a PMDS pair, then C is either a Reed-Solomon code or 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 [42] and Vosper [72]. For background on and proofs of Kneser and Vosper's Theorems we refer to [69]. Kneser's Theorem implies in particular that if A, B are 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 stabilizes $A + B$ 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, which is equivalent to the existence of a non-constant vector x of F^n such that $xCD = CD$.

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 $g, g\alpha, \ldots, g\alpha^{k-1}$, i.e. has a basis of elements in "geometric" progression then, provided g 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 later in the paper.

Our main result takes the following form.

MAIN THEOREM 4.1.3. *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

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

and there exist h pairs $(C_1, D_1), \ldots, (C_h, D_h)$ of codes of F^n, such that $\operatorname{supp} C_i = \operatorname{supp} D_i = I_i$, for all $i = 1, \ldots, h$, 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 all $i = 1, \ldots, h$, when C_i and D_i are identified with codes of $F^{|I_i|}$ through the natural projection on their support, we have that $C_i = (g_i D_i)^\perp$ for some $g_i \in (F^{|I_i|})^\times$.

REMARK 4.1.4. The codes C_i and D_i are mutually orthogonal relative to the non-degenerate 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 4.1.2 in the case $C = D$.

The rest of the chapter is organized as follows. Section 4.2 states and proves the coding-theory equivalent of Kneser's Theorem. Section 4.3 is dedicated to a coding-theory version of Vosper's Theorem. Section 4.4 shows how to recover a version of the Product Singleton Bound as a straightforward consequence of Kneser's Theorem and goes on to derive the proof of Theorem 4.1.3. Section 4.5 concludes with some comments.

4.2 Kneser's Theorem

As usual, $\mathbb{F}$ will denote a finite field, but we shall need, in a couple of occasions, to deal with fields that may be infinite in which case we will use the notation $\mathbb{K}$. All codes will be linear. We will call them simply "codes" when the ambient space is $\mathbb{F}^n$, and use the terminology of vector spaces in the general setting of $\mathbb{K}^n$.

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 and b range over A and B respectively.

THEOREM 4.2.1 (Kneser [42]). *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 [36]. Let $\mathbb{L}/\mathbb{K}$ be a field extension. For $\mathbb{K}$-linear subspaces $S, T \subseteq \mathbb{L}$, we may consider the product of subspaces ST defined as the $\mathbb{K}$-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 $X \subseteq \mathbb{L}$ is involved and is defined in the expected way $\operatorname{St}(X) = \{z \in \mathbb{L} : zX \subseteq X\}$.

THEOREM 4.2.2 (Generalized Kneser Theorem [36]). *Let $\mathbb{L}/\mathbb{K}$ be a separable field extension. Let $S, T \subseteq \mathbb{L}$ be non-zero, finite-dimensional $\mathbb{K}$-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 now proceed to show that there is a variant of Kneser's Theorem for the algebra induced by coordinatewise multiplication.

THEOREM 4.2.3. *Let $S, T \subseteq \mathbb{K}^n$ be non-zero $\mathbb{K}$-vector spaces. Then*

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

REMARK 4.2.4. The products ST in Theorems 4.2.2 and 4.2.3 are in different algebras. The statement of Theorem 4.2.2 is the only instance of the paper where the product ST does not refer to a coordinatewise product.

REMARK 4.2.5. Assuming that Theorem 4.2.3 holds in the case of full-support S and T, the general case can be derived as follows. Let $S_0, T_0 \subseteq \mathbb{K}^{n_0}$ be the projections of S, T respectively on $\operatorname{supp} ST$, where $n_0 := |\operatorname{supp} ST|$. The spaces S_0 and T_0 both have full support, hence

$$\dim S_0T_0 \geq \dim S_0 + \dim T_0 - \dim \operatorname{St}(S_0T_0).$$

Clearly $\dim S_0T_0 = \dim ST$ and $\dim \operatorname{St}(ST) = \dim \operatorname{St}(S_0T_0) + n - n_0$. It remains to prove that

$$\dim S_0 + \dim T_0 \geq \dim S + \dim T - (n - n_0).$$

Let $S_1, T_1 \subseteq \mathbb{K}^{n-n_0}$ be the projections of S, T respectively on the complement of $\operatorname{supp} ST$. Observe that $\operatorname{supp} S_1$ and $\operatorname{supp} T_1$ cannot intersect, hence $\dim S_1 + \dim T_1 \leq n - n_0$. Moreover $\dim S \leq \dim S_0 + \dim S_1$ and $\dim T \leq \dim T_0 + \dim T_1$. Putting everything together we obtain the desired inequality.

From here on "Kneser's Theorem" will refer to Theorem 4.2.3 rather than to the original result. Our proof is strongly inspired by Hou et al.'s proof of Theorem 4.2.2 [36], itself drawing upon the e-transform technique of additive combinatorics (see e.g. [69]).

If V is a $\mathbb{K}$-subspace of $\mathbb{K}^n$, we use the notation $V^\times$ to mean the subset of invertible elements of V.

LEMMA 4.2.6. *Let $S, T \subseteq \mathbb{K}^n$ be non-zero $\mathbb{K}$-vector spaces. Assume that T has a basis of invertible elements. Then, for all $x \in S^\times$, there exist a $\mathbb{K}$-algebra $H_x \subseteq \mathbb{K}^n$ and a $\mathbb{K}$-vector space $V_x \subseteq \mathbb{K}^n$ such that $H_x V_x = V_x$, $xT \subseteq V_x \subseteq ST$ and*

$$\dim V_x + \dim H_x \geq \dim S + \dim T.$$

PROOF. Assume that the lemma is proved for $x = \mathbf{1}$. Then, if $S^\times$ is non-empty, for any $x \in S^\times$ we may apply the result for the case $x = \mathbf{1}$ to $x^{-1}S$ and T. So we only need to prove the Lemma for $\mathbf{1} \in S$ and $x = \mathbf{1}$. Analogously, we may assume that $\mathbf{1} \in T$.

We argue by induction on $k := \dim S$. If $k = 1$, $H := \mathbb{K}\mathbf{1}$ and $V := T$ do the job. So assume that $k > 1$ and the result holds for smaller dimension. For each $e \in T^\times$, define

$$S(e) := S \cap Te^{-1}, \quad T(e) := T + Se.$$

We have $S(e)T \subseteq ST$, $S(e)Se \subseteq TS$, therefore $S(e)T(e) \subseteq ST$. Furthermore,

$$\begin{aligned} \dim T(e) &= \dim T + \dim Se - \dim(T \cap Se) \\ &= \dim T + \dim S - \dim(Te^{-1} \cap S) \end{aligned}$$

by Lemma 2.5.10, hence

$$\dim S(e) + \dim T(e) = \dim S + \dim T.$$

We distinguish two cases.

Assume that $S(e) = S$ for all $e \in T^\times$, i.e. $S \subseteq Te^{-1}$ for all $e \in T^\times$. Then, since T has a basis of invertible elements, we have $ST \subseteq T$. The result then holds with H the subalgebra generated by S and $V := T$.

Assume that there exists $e \in T^\times$ such that $S(e) \subsetneqq S$. Then $0 < \dim S(e) < k$ hence the induction hypothesis applied to $S(e)$ and $T(e)$ gives an algebra H

and a vector space V such that $HV = V$,

$$T \subseteq T(e) \subseteq V \subseteq S(e)T(e) \subseteq ST$$

and

$$\dim V + \dim H \geq \dim S(e) + \dim T(e) = \dim S + \dim T.$$

□

Proof of Theorem 4.2.3. By Remark 4.2.5 we may assume that both S and T have full support. The key to the proof is the following observation. Assume that T has a basis of invertible elements. Recall that, by Lemma 4.2.6, for all $x \in S^\times$ there exist a K-algebra $H_x \subseteq \mathbb{K}^n$ and a $\mathbb{K}$-vector space $V_x \subseteq \mathbb{K}^n$ such that

$$\begin{aligned} H_x V_x &= V_x && (4.2)\\ xT &\subseteq V_x \subseteq ST && (4.3)\\ \dim V_x + \dim H_x &\geq \dim S + \dim T. && (4.4) \end{aligned}$$

Set $k := \dim S$ and assume furthermore that there exists a $\mathbb{K}$-basis $\{x_1, \ldots, x_k\}$ of S contained in $S^\times$ such that

$$H_{x_1} = \cdots = H_{x_k} =: H. \tag{4.5}$$

Then $ST = V_{x_1} + \cdots + V_{x_k}$ by (4.3), and therefore $HST = ST$ by (4.2), in other words $H \subseteq \mathrm{St}(ST)$. From (4.4) it follows therefore that

$$\dim ST + \dim \mathrm{St}(ST) \geq \dim V_{x_1} + \dim H \geq \dim S + \dim T,$$

hence the conclusion.

We shall first prove the Theorem when $\mathbb{K}$ is an infinite field, by showing in that case that T always has a basis of invertible elements and that there always exists a basis $\{x_1, \ldots, x_n\}$ of invertible elements of S satisfying (4.5).

Since T has full support, it should be clear enough that it has a basis of invertible elements for $\mathbb{K}$ infinite. In this case Lemma 4.2.6 applies. Now fix a $\mathbb{K}$-basis $\{s_1, \ldots, s_k\}$ of S and define, for all $\alpha \in \mathbb{K}$, $y_\alpha := \sum_{i=1}^k \alpha^{i-1} s_i \in S$. For any choice of non-zero, pairwise distinct $\alpha_1, \ldots, \alpha_k \in \mathbb{K}$, the matrix transforming $s_1, \ldots, s_k$ into $y_{\alpha_1}, \ldots, y_{\alpha_k}$ is Vandermonde, and therefore $y_{\alpha_1}, \ldots, y_{\alpha_k}$ is also a $\mathbb{K}$-basis of S. We now observe that the set $\{\alpha \in \mathbb{K} : y_\alpha \in S^\times\}$ is infinite: indeed its complement in $\mathbb{K}$ is finite, as it is a finite union of zero-sets of non-zero polynomials. That these polynomials are non-zero is guaranteed by the full-support property of S. On the other hand, the number of subalgebras of $\mathbb{K}^n$ is finite by Remark 2.5.12, in particular the number of subalgebras H_x guaranteed by Lemma 4.2.6 is finite. It follows that there exist $\alpha_1, \ldots, \alpha_k$

such that $\{x_1 = y_{\alpha_1}, \ldots, x_k = y_{\alpha_k}\}$ is a $\mathbb{K}$-basis of S whose elements are all invertible and such that $H_{x_1} = \cdots = H_{x_k}$. This concludes the proof in the case $\mathbb{K}$ infinite.

Assume now that $\mathbb{K}$ is finite, and consider an infinite field extension $\mathbb{K}'$ of $\mathbb{K}$, for example the rational function field $\mathbb{K}' := \mathbb{K}(t)$, where t is transcendental over $\mathbb{K}$. The infinite base-field case applies to $\mathbb{K}'$-vector spaces. Our purpose is to draw our conclusion from this. Define the base-field extensions $S' := S \otimes \mathbb{K}', T' := T \otimes \mathbb{K}'$, where tensor products are taken over $\mathbb{K}$. By construction S' and T' are $\mathbb{K}'$-vector spaces and we have just proved that

$$\dim_{\mathbb{K}'} S'T' \geq \dim_{\mathbb{K}'} S' + \dim_{\mathbb{K}'} T' - \dim_{\mathbb{K}'} \mathrm{St}(S'T').$$

It is clear that $S'T' = ST \otimes \mathbb{K}'$, $\dim_{\mathbb{K}'} S' = \dim S$, $\dim_{\mathbb{K}'} T' = \dim T$ and $\dim_{\mathbb{K}'} S'T' = \dim ST$, where non-indexed dimensions are taken over $\mathbb{K}$. Moreover $\mathrm{St}(S'T') = \mathrm{St}(ST) \otimes \mathbb{K}'$ by Lemma 2.5.13 and the conclusion follows. □

Theorem 4.2.3 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

$$\dim CD \geq \dim C + \dim D - 1. \tag{4.6}$$

The next section studies pairs of codes C, D such that CD is indecomposable and achieves equality in (4.6).

4.3 Vosper's Theorem

We start by recalling Vosper's Addition Theorem.

THEOREM 4.3.1 (Vosper [72]). *Let G be an abelian group of prime order p. Let $A, B \subseteq G$ be subsets, with $|A|, |B| \geq 2$ and $|A + B| \leq p - 2$. If*

$$|A + B| = |A| + |B| - 1$$

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 [2].

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 4.2.1 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 [54, 69]. Vosper's Theorem is therefore concerned with characterizing pairs of sets achieving equality in the Cauchy-Davenport Inequality.

In the algebra setting, the inequality (4.6) may be thought of as a code-product version of the Cauchy-Davenport Inequality. But contrary to the group case, the algebra $\mathbb{F}^n$ always has proper subalgebras (for $n > 1$) so we cannot hope to ensure (4.6) purely by a condition on $\mathbb{F}^n$. However, we have seen that (4.6) holds when (at least one of) the codes involved is MDS (Theorem 2.5.16). The following theorem may be seen as a version of Vosper's Theorem for MDS codes, and is the main result of this section.

THEOREM 4.3.2. *Let $C, D \subseteq \mathbb{F}^n$ be MDS codes, with $\dim C, \dim D \geq 2$ and $\dim CD \leq n-2$. If*

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

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

REMARK 4.3.3. 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 $\dim CD = \dim C + \dim D - 1 = n-1$. A slight relaxation of the MDS hypothesis is presented in [1]: here it is observed that only the projections C_I and D_I of C and D onto a sufficiently large coordinate set $I \subseteq \{1, \ldots, n\}$ are required to be MDS in order to make our argument work.

We introduce the following notation for Vandermonde-type matrices. Given a positive integer k and $\alpha = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{F} \cup \{\infty\})^n$ we denote by $V_k(\alpha)$ the $k \times n$ matrix whose i-th column is $(1, \alpha_i, \ldots, \alpha_i^{k-1})^T$ if $\alpha_i \neq \infty$, $(0, \ldots, 0, 1)^T$ otherwise. Note that the possible presence of this last column makes $V_k(\alpha)$ a Vandermonde matrix in a generalized sense. We remark that if the entries of α are pairwise distinct then $V_k(\alpha)$ has full rank. With this notation, a Reed-Solomon code of length n and dimension k is a code of the form gC, where $g \in (\mathbb{F}^{\times})^n$ (i.e. g has no zero entries) and C is generated by $V_k(\alpha)$ for some $\alpha \in (\mathbb{F} \cup \{\infty\})^n$ with pairwise-distinct entries. The vector α is an evaluation-point sequence of C.

LEMMA 4.3.4. *Let $C \subseteq \mathbb{F}^n$ be a full-support code with $\dim C \geq 2$ and $d_{\min}(C) > 1$. Assume that there exists a 2-dimensional MDS code $A \subseteq \mathbb{F}^n$, generated by $V_2(\alpha)$ for some $\alpha \in \mathbb{F}^n$ with pairwise distinct entries, such that*

$$\dim AC = \dim C + 1 \leq n - 1.$$

Then C is generated by $gV_{\dim C}(\alpha)$ for some $g \in C$.

PROOF. Since α has at most one zero coordinate, $d_{\min}(C) > 1$ implies that $\dim \alpha C = \dim C$. We therefore have

$$\dim AC = \dim(C + \alpha C) = 2 \dim C - \dim(C \cap \alpha C),$$

hence

$$\dim(C \cap \alpha C) = \dim C - 1.$$

Moreover, $C' = C \cap \alpha C$ has support strictly larger than its dimension, otherwise it would have minimum distance 1 and this would imply the existence of a word of weight 1 in C. We prove the lemma by induction on $k := \dim C$.

In the case $k = 2$, pick $g' \in C \cap \alpha C$, which exists as $\dim(C \cap \alpha C) = 1$, and let $g \in C$ be such that $g' = g\alpha$. Then g and $g' = g\alpha$ are linearly independent, as $|\operatorname{supp} g| \geq |\operatorname{supp} g'| \geq 2$ and α has pairwise distinct entries. It follows that C is generated by g and $g\alpha$, i.e. by $gV_2(\alpha)$.

Now assume that $k > 2$. We have

$$k = \dim C' + 1 \leq \dim AC' \leq \dim \alpha C = k,$$

where the right inequality follows from the inclusion $AC' = C' + \alpha C' \subseteq \alpha C$, and the left inequality follows from Theorem 2.5.16 (recall that A is MDS). Strictly speaking, Theorem 2.5.16 only applies to full-support codes and C' may have a support of cardinality $n - 1$ if α has a zero coordinate. But if this happens we may puncture A and C' by deleting this coordinate to obtain full-support codes of the same dimension as A and C and still apply Theorem 2.5.16.

Since $C' \subseteq C$ we have $d_{\min}(C') \geq d_{\min}(C) > 1$, and we have just shown $\dim AC' = \dim C' + 1 \leq (n-1) - 1$, since $\dim C' = \dim C - 1$. Therefore the induction hypothesis applies to C', possibly after puncturing one zero coordinate to make C' full support. Hence C' is generated by $g'V_{k-1}(\alpha)$ for some $g' \in C'$. Let $g \in C$ be such that $g' = g\alpha$. The matrix whose rows are the elements of the set $\{g, g' = g\alpha, \ldots, g'\alpha^{k-2} = g\alpha^{k-1}\} \subseteq C$ is $gV_k(\alpha)$, which has rank k as $|\operatorname{supp} g| \geq |\operatorname{supp} C'| \geq k$. It follows that this set is linearly independent and $gV_k(\alpha)$ generates C. □

LEMMA 4.3.5. *Let $C, D \subseteq \mathbb{F}^n$ be MDS codes satisfying*

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

Assume that there exists an index set $I \subseteq \{1, \ldots, n\}$ with $|I| \geq \dim CD$ such that the punctured codes $C_I, D_I \subseteq \mathbb{F}^{|I|}$ obtained by projecting C and D on the coordinates indexed by I are Reed-Solomon codes with a common evaluation-point sequence. Then C and D are Reed-Solomon codes with a common evaluation-point sequence.

PROOF. Set $k := \dim C$, $\ell := \dim D$. Since $|I| \geq \dim CD$ we have $|I| \geq k$ and $|I| \geq \ell$ and since C and D are MDS we must have $\dim C_I = \dim C = k$, $\dim D_I = \dim D = \ell$. Note that we may suppose $k, \ell \geq 2$, otherwise there is nothing to prove.

Reformulating the hypothesis, there exist $g_I, g'_I \in \mathbb{F}^{|I|}$, $\alpha_I \in (\mathbb{F} \cup \{\infty\})^{|I|}$, where α_I has pairwise-distinct entries, such that C_I and D_I are generated by $g_I V_k(\alpha_I)$ and $g'_I V_\ell(\alpha_I)$ respectively. In other words there are unique generator matrices G_C and G_D of C and D whose I-indexed columns form $g_I V_k(\alpha_I)$ and $g'_I V_\ell(\alpha_I)$ respectively. It also follows that $g_I g'_I V_{k+\ell-1}(\alpha_I)$ generates $C_I D_I$ (as $k + \ell - 1 \leq |I|$), $\dim C_I D_I = k + \ell - 1 = \dim CD$ and there is a unique generator matrix G_{CD} of CD whose I-indexed columns form $g_I g'_I V_{k+\ell-1}(\alpha_I)$.

Let $x_0, \ldots x_{k-1}$ and $y_0, \ldots, y_{\ell-1}$ denote the rows of G_C and G_D respectively.

The key observation is the following: let u, v, s, t be integers, with $0 \leq u, s \leq k-1$ and $0 \leq v, t \leq \ell - 1$, such that

$$u + v = s + t.$$

Since $x_u y_v$ and $x_s y_t$ coincide in the I-indexed coordinates, and $\dim C_I D_I = \dim CD$, the vectors $x_u y_v$ and $x_s y_t$ must coincide in every coordinate of $\{1, \ldots, n\}$. In other words, if $\pi = (\pi_0, \pi_1, \ldots, \pi_{k-1})^T$ and $\tau = (\tau_0, \tau_1 \ldots, \tau_{\ell-1})^T$ are the j-th column of G_C and G_D respectively, for some $j \notin I$, then

$$\pi_u \tau_v = \pi_s \tau_t.$$

We now exploit this property in order to prove the lemma. Pick two columns π, τ of G_C, G_D as above.

First assume that $\pi_0 \neq 0$ and $\tau_0 \neq 0$. Without loss of generality we may assume $\pi_0 = \tau_0 = 1$. It follows from $\pi_0 \tau_1 = \pi_1 \tau_0$ that $\tau_1 = \pi_1 =: \beta \in \mathbb{F}$. For all $i \leq k-1$, it holds that $\pi_i = \pi_i \tau_0 = \pi_{i-1} \tau_1$. Applying this formula recursively we obtain $\pi_i = \beta^i$ for all $i \leq k-1$, i.e. π corresponds to the evaluation point $\beta \in \mathbb{F}$. The same argument applies to τ, which corresponds to the evaluation point $\beta \in \mathbb{F}$ as well.

Now assume that $\pi_0 = 0$. If $\tau_0 \neq 0$, then $\pi_1 \tau_0 = \pi_0 \tau_1 = 0$ implies $\pi_1 = 0$. Continuing in this way, we see that if $\pi_i = 0$, then $\pi_{i+1} \tau_0 = \pi_i \tau_1 = 0$ implies $\pi_{i+1} = 0$ and by induction we obtain $\pi = 0$ which contradicts the full-support property of the MDS code C. Therefore $\tau_0 = 0$. Assume without loss of generality that $k \leq \ell$. If $k = \ell = 2$, then both π_1 and τ_1 are non zero as C and D have full support, hence the columns π and τ correspond to the evaluation point ∞. If $k = 2$ and $\ell \geq 3$ then as $\tau_i \pi_1 = \tau_{i+1} \pi_0 = 0$ for all $i < \ell - 1$ and as $\pi_1 \neq 0$ it follows that $\tau_i = 0$ for all $i < \ell - 1$ and again the full-support property of D implies that the column τ corresponds to the evaluation point

∞. If $k > 2$, then the same procedure that we applied to π_0, τ_0 again yields $\pi_1 = \tau_1 = 0$. Iterating in this way, we obtain that both π and τ correspond to the evaluation point ∞.

We have proved that up to multiplication by vectors g, g', the codes C and D have generator matrices of the form $V_k(\alpha)$ and $V_\ell(\alpha)$. Since C and D are MDS, the evaluation-sequence α must have distinct entries and C and D are Reed-Solomon codes with the same evaluation-point sequence. □

Proof of Theorem 4.3.2. Set $k := \dim C$, $\ell := \dim D$, $k^* := \dim CD = k + \ell - 1$. Let $C_0, D_0 \subseteq \mathbb{F}^{n_0}$ be the punctured codes obtained by projecting C, D on the first $n_0 := k^* + 2$ coordinates. As C_0, D_0 and C_0D_0 are MDS, we have $\dim C_0 = \dim C$, $\dim D_0 = \dim D$, $\dim C_0D_0 = \dim CD$ and

$$k^* = \dim C_0D_0 = \dim C_0 + \dim D_0 - 1 = n_0 - 2. \tag{4.7}$$

Define the code $A \subseteq \mathbb{F}^{n_0}$ by

$$A := (C_0D_0)^\perp.$$

By Lemma 2.5.17 the code C_0D_0 is MDS, therefore A is MDS and furthermore has dimension 2 by (4.7). Now observe that for any $a \in A$, $x \in C_0$, $y \in D_0$, orthogonality of A and C_0D_0 translates into

$$(a \,|\, xy) = 0$$

which is equivalent to

$$(ax \,|\, y) = 0.$$

We have therefore $(AC_0)^\perp \supseteq D_0$, from which we deduce

$$\dim AC_0 \leq n_0 - \dim D_0 = \dim C_0 + 1 \leq n_0 - 1$$

whence

$$\dim AC_0 = \dim C_0 + 1 \tag{4.8}$$

by Theorem 2.5.16. Similarly we also have

$$\dim AD_0 = \dim D_0 + 1. \tag{4.9}$$

Now A is an MDS code of dimension 2 and therefore has a generator matrix with at most two zero entries. By puncturing one coordinate if need be, we obtain a generator matrix with at most one zero entry. The two rows of this matrix are clearly of the form $g, g\alpha$ for some $g \in \mathbb{F}^n$ and $\alpha \in \mathbb{F}^n$ with pairwise distinct coordinates. Finally, consider that $\dim C_0 = n_0 - 1 - \dim D_0 \leq n_0 - 3$, and similarly $\dim D_0 \leq n_0 - 3$. Hence (4.8) and (4.9) imply

$$\dim AC_0 \leq n_0 - 2,$$
$$\dim AD_0 \leq n_0 - 2.$$

Therefore Lemma 4.3.4 applies to A, C_0 and to A, D_0, possibly after puncturing one coordinate. From there we obtain that C_0 and D_0 (possibly punctured on a common coordinate) are Reed-Solomon codes with a common evaluation-point sequence, and Lemma 4.3.5 gives the desired conclusion. □

4.3.1 Consequences of Theorem 4.3.2

A first interesting consequence of Theorem 4.3.2 is the following characterization of Reed-Solomon codes among MDS codes.

COROLLARY 4.3.6. *Let $C \subseteq \mathbb{F}^n$ be an MDS code, with $\dim C \leq (n-1)/2$. The code C is Reed-Solomon if and only if*

$$\dim C^2 = 2\dim C - 1. \tag{4.10}$$

REMARK 4.3.7. If $\dim C \geq (n+1)/2$, then C being MDS we must have $C^2 = \mathbb{F}^n$ 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 4.3.6 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 4.3.2 and Corollary 4.3.6 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 (4.10) which are not Reed-Solomon. For instance, the codes denoted $C_{11,8,8}$ and $C_{13,8,21}$ in [9], of length 8 over the fields with 11 and 13 elements respectively are self-dual, therefore satisfy (4.10), and can be shown not to be Reed-Solomon.

In addition, as our proofs are constructive, they can be used to design an algorithm that, given an MDS code which satisfies (4.10) (and is henceforth a Reed-Solomon code), recovers its defining parameters, i.e. the α_i's and g_i's as in Definition 2.5.7.

A second consequence concerns error correcting pairs, which we defined in Section 2.5.3. Recall that a pair of MDS codes (A, B) with $\dim A = t+1$ and $\dim B = t$ is a t-error correcting pair for $C := (AB)^\perp$, and $\dim C \leq n - 2t$. Moreover, this bound is attained if A and B are Reed-Solomon codes with a common evaluation-point sequence, and in this case C is a Reed-Solomon code as well. The converse also holds.

THEOREM 4.3.8. *Let $2 \leq t < n/2$ be an integer. Let $C \subseteq \mathbb{F}^n$ be a code of dimension $n-2t$ that has a t-error correcting pair (A, B) over a finite extension of $\mathbb{F}$. Then A, B, C are Reed-Solomon codes with a common evaluation-point sequence.*

This results first appeared in [49, Theorem 6.2]. In the original statement, it was further assumed that C is MDS, but this is actually implied by the existence of a t-error correcting pair: as observed in [58, Corollary 2.15] if C can correct t errors, then $d_{\min}(C) \geq 2t+1$, hence $\dim C + d_{\min}(C) \geq n - 2t + 2t + 1 = n + 1$. The paper [49] gives two separate proofs of this result: a first direct one, and a second one based on our Main Theorem 4.1.3. In fact, this second proof can be further simplified by using Theorem 4.3.2 as follows. For simplicity, we assume that the error correcting pair is defined over $\mathbb{F}$ (and not over an extension). For the full proof the reader is referred to [1].

First observe that, as in the original proof, A is MDS of dimension $t+1$, and B, possibly after an extension of the base field, contains a subcode B' which is MDS of dimension t such that (A, B') is a t-error correcting pair for C. We have that

$$2t = n - \dim C \geq \dim AB \geq \dim A + \dim B - 1 \geq \dim A + \dim B' - 1 = 2t,$$

where the dimensions are taken over the field of definition of B', hence $B' = B$, and in particular this field extension was not even necessary. The inequality $\dim AB \geq \dim A + \dim B - 1$ holds because A is MDS. Moreover, we have that $\dim AB = \dim A + \dim B - 1$, hence Theorem 4.3.2 applies and yields that A, B, AB and $C = (AB)^{\perp}$ are Reed-Solomon codes with a common evaluation-point sequence.

Finally we show that a t-strongly multiplicative secret sharing scheme among n players such that $n = 3t+1$, i.e. attains the bound given in Proposition 2.6.9, is necessarily based on a Reed-Solomon code. Recall that given a secret sharing scheme $\Sigma = (\pi_0, \ldots, \pi_n) \subseteq V^*$, where V is an $\mathbb{F}$-vector space, we define the code

$$C(\Sigma) := \{(\pi_0(x), \ldots, \pi_n(x)) : x \in V\}.$$

THEOREM 4.3.9. *Let t be a positive integer. Let Σ be a t-strongly multiplicative secret sharing scheme among n players. If $n = 3t+1$ then $C(\Sigma)$ is a Reed-Solomon code.*

PROOF. By assumption Σ has t-privacy and $(n - t = 2t + 1)$-product reconstruction. By Lemma 2.6.8 it also has $(n - 2t = t + 1)$-reconstruction, hence it is $(t+1)$-threshold. It follows by Corollary 2.6.14 that the associated code $C(\Sigma)$ is MDS of dimension $t+1$. Its square has dimension

$$\dim C(\Sigma)^2 \geq 2 \dim C(\Sigma) - 1 = 2t + 1$$

by Theorem 2.5.16 and

$$\dim C(\Sigma)^2 \leq 2t + 1$$

as the product scheme has $(2t+1)$-reconstruction. The conclusion now follows by our variant of Vosper's Theorem. □

This result was first proved in [1], together with two generalizations. The first one consider secret sharing schemes for a finite extension $\mathbb{L}$ of $\mathbb{F}$, i.e. schemes which allow the secret to be in $\mathbb{L}$. To capture this notion in full generality, one can use the definition of codex introduced in [16]. Alternatively one can adapt Definition 2.6.4 allowing π_0 to be an $\mathbb{F}$-linear map $V \to \mathbb{L}$, or can consider secret sharing schemes associated to $\mathbb{F}$-linear subspaces of $\mathbb{L} \times \mathbb{F}^n$ in the sense of Definition 2.6.15. In this setting, one can prove that a t-strongly multiplicative secret sharing scheme among n players satisfies

$$n \geq 3t + 2k - 1,$$

where k is the degree of the field extension. If $\mathbb{L} = \mathbb{F}$ this is simply Proposition 2.6.9.

THEOREM 4.3.10. *Let t be a positive integer. Let Σ be a t-strongly multiplicative secret sharing scheme for $\mathbb{L}$ among n players. If $n = 3t + 2k - 1$ then $C(\Sigma)$ is a Reed-Solomon code in $\mathbb{L} \times \mathbb{F}^n$.*

By a Reed-Solomon code in $\mathbb{L} \times \mathbb{F}^n$, we mean a code of the form

$$\{(g_0 f(\alpha_0), g_1 f(\alpha_1), \ldots, g_n f(\alpha_n)) : f \in \mathbb{F}[X]_{<k}\},$$

where $\alpha_1, \ldots, \alpha_n \in \mathbb{F} \cup \{\infty\}$ are pairwise distinct and $g_1, \ldots, g_n \in \mathbb{F}$ are non-zero, $\alpha_0 \in \mathbb{L}$ is different from the other α_i's and $g_0 \in \mathbb{L}$ is non-zero.

We only quickly sketch the proof. First, one proves that the $\mathbb{L}$-span of $C(\Sigma)$, which is an $\mathbb{L}$-liner code, defines a secret sharing scheme which has $(t+k-1)$-privacy and $(2t+2k-1)$-product reconstruction, hence $(t+k)$-reconstruction, hence the scheme is $(t+k)$-threshold. It follows that the $\mathbb{L}$-span of $C(\Sigma)$ is an MDS code of dimension $t+k$. Then, one notices that this implies $\dim_{\mathbb{L}} C(\Sigma)^2 = 2\dim_{\mathbb{L}} C(\Sigma) - 1$, hence the $\mathbb{L}$-span of $C(\Sigma)$ is a Reed-Solomon code. The last step consists of proving that $C(\Sigma)$ itself is a Reed-Solomon code in $\mathbb{L} \times \mathbb{F}^n$.

The second generalization allows not only the secret, but also each share to lie in a possibly different field extension of $\mathbb{F}$. For all $i = 1, \ldots, n$, let us denote by $\mathbb{F}_i$ the field where the i-th share lies. The idea is to focus on projections of $C(\Sigma)$: for all sufficiently large subsets $I \subseteq \{1, \ldots, n\}$, we can prove that $C(\Sigma_I)$ is a Reed-Solomon code in $\mathbb{L} \times \mathbb{F}_I^{|I|}$, where $\mathbb{F}_I$ denotes the compositum of the $\mathbb{F}_i$'s with $i \in I$. Then two such projections can be glued together if their supports intersect in at least three points, using the fact that the set of all evaluation-point sequences of a given Reed-Solomon code is an orbit under the action of a triply transitive group. Finally, if i belong to the intersection of two different supports I and J then $\alpha_i \in \mathbb{F}_I \cap \mathbb{F}_J$ and if $\mathbb{F}_I$ and $\mathbb{F}_J$ are "sufficiently different" then it may be the case that $\mathbb{F}_I \cap \mathbb{F}_J = \mathbb{F}_i$ as desired. We refer the reader to [1, Section 7] for a fully detailed discussion and a precise statement of the results.

4.4 Classification of PMDS pairs

We now are finally ready to focus on the chapter's central result, namely Theorem 4.1.3.

First, we show how Randriambololona's Product Singleton Bound can be obtained as a consequence of Theorem 4.2.3. To be precise we obtain:

THEOREM 4.4.1. *Let $C_1, \dots, C_t \subseteq \mathbb{F}^n$ be codes. Assume that their product $C_1 \cdots C_t$ has full support. Then*

$$d_{\min}(C_1 \cdots C_t) \leq \max\{t-1, n - (\dim C_1 + \cdots + \dim C_t) + t\}.$$

REMARK 4.4.2. The full result of [62] is actually stronger than Theorem 4.4.1, as it ensures that an element of weight at most $\max\{t-1, n-(\dim C_1 + \cdots + \dim C_t) + t\}$ can be found in the set

$$\{x_1 \cdots x_t : x_1 \in C_1, \dots, x_t \in C_t\},$$

and not only in its span. The support condition given here is also not the same as the apparently weaker hypothesis given in [62], but the two conditions are really interchangeable, as argued in [62, Remark 3(c)].

PROOF OF THEOREM 4.4.1. For ease of notation, set $k_i := \dim C_i$ for all $i = 1, \dots, t$, $P := C_1 \cdots C_t$, $k^* := \dim P$, $d^* := d_{\min}(P)$. Assume that $d^* \geq t$. The classical Singleton Bound, applied to P, says that

$$k^* \leq n - d^* + 1. \tag{4.11}$$

Repeatedly applying Kneser's Theorem 4.2.3 we obtain

$$k^* \geq k_1 + \cdots + k_t - (t-1)\dim \mathrm{St}(P). \tag{4.12}$$

Combining it with (4.11), we get

$$d^* \leq n - (k_1 + \cdots + k_t) + 1 + (t-1)\dim \mathrm{St}(P), \tag{4.13}$$

which is apparently a weaker statement than Theorem 4.4.1. To improve it, we "correct" (4.11) to transform it into an identity, namely we define $m := n - d^* + 1 - k^*$. Thus, by definition, P is "m-far from being MDS". The combination of this identity with (4.12) gives an improved version of (4.13), namely

$$d^* = n - k^* + 1 - m \leq n - (k_1 + \cdots + k_t) + 1 + (t-1)\dim \mathrm{St}(P) - m. \tag{4.14}$$

In the case of $t = 2$, the first claim of Lemma 2.5.15, rewritten as

$$\dim \mathrm{St}(P) - (n - d^* + 1 - k^*) \leq 1$$

immediately proves the theorem. In the general case, using the second claim of Lemma 2.5.15 instead we obtain

$$\begin{aligned}(t-1)\dim \mathrm{St}(P) - m &\leq (t-1)\ \frac{n-k^*}{d^*-1} - m \\ &= t-1+(t-1)\ \frac{m}{d^*-1} - m \\ &= t-1-\frac{d^*-t}{d^*-1}\ m. \end{aligned} \tag{4.15}$$

As $d^* \geq t$ the conclusion follows. □

From here on we focus on the case of $t = 2$. Recall that a pair of codes $C, D \subseteq \mathbb{F}^n$ is defined to be PMDS if

$$2 \leq d_{\min}(CD) = n - \dim C - \dim D + 2.$$

Observe that for a PMDS pair (C, D) all inequalities in the proof of Theorem 4.4.1 are actually identities. From this simple observation we obtain some corollaries which relate the Product Singleton Bound with Kneser's Theorem and with the classical Singleton Bound.

COROLLARY 4.4.3. *Let $C, D \subseteq \mathbb{F}^n$ be codes such that the pair (C, D) is PMDS. Then the following hold.*

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 $d_{\min}(CD) = 2$.*

PROOF. From the above observation, (4.12) is an identity if (C, D) is PMDS, hence the first claim is immediately proved. From (4.14) and (4.15) we obtain

$$\frac{d_{\min}(CD)-2}{d_{\min}(CD)-1}\ m = 0,$$

where $m := n - d_{\min}(CD) + 1 - \dim CD$, hence either $m = 0$ meaning CD is MDS, or $d_{\min}(CD) = 2$. □

The two possible cases in our main Theorem 4.1.3 arise from the two possible situations given by the second claim of the above corollary. We distinguish the case of $d_{\min}(CD) > 2$, which implies that CD is MDS, and $d_{\min}(CD) = 2$.

PROPOSITION 4.4.4. *Let $C, D \subseteq \mathbb{F}^n$ be codes such that the pair (C, D) is PMDS, and assume $d_{\min}(CD) > 2$. Then C, D and CD are MDS. Moreover, if $\dim C, \dim D \geq 2$ then C, D and CD are Reed-Solomon codes with a common evaluation-point sequence.*

PROOF. By the above corollary CD is MDS. Moreover the PMDS property immediately yields $n > \dim C + \dim D$. We now proceed to prove that C and D are also MDS through Lemma 2.5.6.

Set $k := \dim C, \ell := \dim D$. Without loss of generality, we can choose a generator matrix G_C of C that is systematic in the first k positions. Let G_D be a generator matrix of D. The matrix formed by the last $n-k$ columns of G_D has full rank, otherwise there is a non-zero vector of D that is zero in the last $n-k$ positions, and taking the product with a row of G_C we would obtain a vector of CD of weight 1, contradicting that CD is MDS and not the whole space $\mathbb{F}^n$. So we can now assume that G_C is systematic in the first k positions and G_D is systematic in the subsequent ℓ positions.

Now we focus on G_C. Assume that there is a zero entry in the j-th column of G_C for some $j > k + \ell$, say in position (i, j) of G_C. Then, since the j-th column of G_D is not all-zero (otherwise CD would not be full support and would not be MDS), the product of the i-th row of G_C with some row of G_D yields non-zero vector of CD of weight at most $n - k - \ell + 1 = d_{\min}(CD) - 1$, a contradiction. Therefore, all columns of G_C indexed by $j > k + \ell$, that exist since $n > k + \ell$, have no zero entries. For the same reason, this is also true of G_D, and we obtain that the product of any row of G_C with any row of G_D is non-zero.

From this last fact, we get that G_C cannot have zero entries in the columns indexed by $\{k + 1, \ldots, k + \ell\}$, or again, by taking a product of a row of G_C with a row of G_D, we would have a non-zero vector of CD of weight at most $n - k - \ell + 1$. Now Lemma 2.5.6 allows us to conclude that C is MDS. Analogously, one has that D is MDS as well.

The last statement now follows immediately by Theorem 4.3.2. Note that $n > \dim C + \dim D$ is equivalent to the hypothesis $\dim CD \leq n - 2$. □

The following lemma will be useful to deal with the second case.

LEMMA 4.4.5. *Let $C, D \subseteq \mathbb{F}^n$ be codes such that CD is MDS and*

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

Then there exists $g \in (\mathbb{F}^n)^\times$ such that $C = (gD)^\perp$.

PROOF. Let $g \in \mathbb{F}^n$ be a generator of $(CD)^\perp$, which is invertible as $(CD)^\perp$ is MDS of dimension 1. For any $x \in C$, $y \in D$, we have

$$(x \,|\, gy) = (xy \,|\, g) = 0$$

so that $C \subseteq (gD)^\perp$, and equality follows by comparing dimensions. □

PROPOSITION 4.4.6. *Let $C, D \subseteq \mathbb{F}^n$ be codes such that the pair (C, D) is PMDS. Set $h := \dim \mathrm{St}(CD)$ and let $\{\pi_1, \ldots, \pi_h\}$ be an $\mathbb{F}$-basis of $\mathrm{St}(CD)$ of disjoint projectors with supports $I_1, \ldots, I_h$. Then C, D and CD decompose as*

$$\begin{aligned} C &= \pi_1 C \oplus \cdots \oplus \pi_h C, \\ D &= \pi_1 D \oplus \cdots \oplus \pi_h D, \\ CD &= \pi_1 CD \oplus \cdots \oplus \pi_h CD \end{aligned}$$

and, for all $i = 1, \ldots, h$, we have $\operatorname{supp} \pi_i C = \operatorname{supp} \pi_i D = \operatorname{supp} \pi_i CD = I_i$ and

$$\dim \pi_i CD = \dim \pi_i C + \dim \pi_i D - 1. \tag{4.16}$$

Moreover, if $d_{\min}(CD) = 2$ then, for all $i = 1, \ldots, h$, when $\pi_i C$ and $\pi_i D$ are identified with codes of $\mathbb{F}^{|I_i|}$ through the natural projection on their support, then $\pi_i C = (g_i \pi_i D)^\perp$ for some $g_i \in (\mathbb{F}^{|I_i|})^\times$.

PROOF. By Kneser's Theorem we have, for all $i = 1, \ldots, h$,

$$\dim \pi_i CD \geq \dim \pi_i C + \dim \pi_i D - 1 \tag{4.17}$$

since $\pi_i CD$ has trivial stabilizer. Therefore

$$\dim CD = \sum_{i=1}^{h} \dim \pi_i CD \geq \sum_{i=1}^{h} (\dim \pi_i C + \dim \pi_i D - 1). \tag{4.18}$$

Observing that

$$C \subseteq \pi_1 C \oplus \cdots \oplus \pi_h C, \quad D \subseteq \pi_1 D \oplus \cdots \oplus \pi_h D \tag{4.19}$$

we get

$$\sum_{i=1}^{h} (\dim \pi_i C + \dim \pi_i D - 1) \geq \dim C + \dim D - h,$$

but the right hand side of this inequality equals $\dim CD$ by the first claim of Corollary 4.4.3. From (4.18) we obtain therefore that all inequalities in (4.17) are equalities, i.e. for all $i = 1, \ldots, h$,

$$\dim \pi_i CD = \dim \pi_i C + \dim \pi_i D - 1,$$

and we obtain also

$$\sum_{i=1}^{h} (\dim \pi_i C + \dim \pi_i D) = \dim C + \dim D,$$

hence both inclusions in (4.19) are actually identities.

Now assume that $d_{\min}(CD) = 2$. Observe that $n = \dim C + \dim D$ by the Product Singleton Bound. From here on all codes are identified with full-support codes through the natural projection on their support. For all $i = 1, \ldots, h$, we have $d_{\min}(\pi_i CD) \geq 2$, hence $|I_i| \geq \dim \pi_i CD + 1$ by the classical Singleton Bound applied to $\pi_i CD$. Therefore

$$\begin{aligned} n = \sum_{i=1}^{h} |I_i| &\geq \sum_{i=1}^{h} (\dim \pi_i CD + 1) \\ &= \sum_{i=1}^{h} (\dim \pi_i C + \dim \pi_i D) \\ &= \dim C + \dim D = n. \end{aligned}$$

It follows that

$$\dim \pi_i CD = \dim \pi_i C + \dim \pi_i D - 1 = |I_i| - 1$$

and $d_{\min}(\pi_i CD) \geq 2 = |I_i| - \dim \pi_i CD + 1$ proves that $\pi_i CD$ is MDS. Now the conclusion follows by Lemma 4.4.5. □

Propositions 4.4.4 and 4.4.6 constitute the proof of Theorem 4.1.3.

4.5 Concluding Comments

As mentioned in Section 4.3, Theorem 4.3.2 is arguably a coding-theoretic analogue of Vosper's Addition Theorem. The analogy with its additive counterpart is not as clear-cut however as in the case of Theorem 4.2.3 and Kneser's Addition Theorem. More precisely, the MDS hypothesis in Theorem 4.3.2 is not a very natural analogue of the prime order of the ambient group hypothesis in Vosper's original Theorem, and there may possibly be other coding-theoretic analogues to consider.

The natural question raised by Theorem 4.2.3 and Theorem 4.3.2 is whether there exists a satisfying characterization of pairs C, D such that CD is indecomposable and of codimension at least 2, and $\dim CD = \dim C + \dim D - 1$. Beside pairs of Reed-Solomon codes, one now has Reed-Solomon codes with duplicate coordinates. Beside these, other examples turn up.

THEOREM 4.5.1 ([1, Theorem 4.9]). *For any finite field $\mathbb{F}$ and positive integer ℓ there exists a code C of length n (which in general depends on ℓ) which is not MDS, and whose square is indecomposable and satisfies*

$$\dim C^2 = 2 \dim C - 1 = n - \ell.$$

Such codes are constructed by taking the amalgamated direct sum, defined in the end of Section 2.5, of self-dual codes. Given two self-dual codes $C \subseteq \mathbb{F}^{n_1}$ and $D \subseteq \mathbb{F}^{n_2}$ such that $\dim C^2 = 2\dim C - 1 = n_1 - 1$ and $\dim D^2 = 2\dim D - 1 = n_2 - 1$, we have that

$$\begin{aligned}\dim(C \dot{\oplus} D)^2 &= 2\dim C \dot{\oplus} D - 1 = 2(\dim C + \dim D - 1) - 1 \\ &= (2\dim C + 2\dim D - 1) - 2 = n - 2\end{aligned}$$

where $n = n_1 + n_2 - 1$ is the length of $C \dot{\oplus} D$. The theorem is then proved by iterating this construction.

If the analogy with additive combinatorics is to be trusted, a full characterization may be tractable, though probably difficult, and would be a coding-theory equivalent of Kemperman's Structure Theorem for small sumsets [41].

Finally, it is natural to wonder whether the characterization of PMDS pairs extends to products of more than two codes. Our techniques (Corollary 4.4.3 and Proposition 4.4.4) allow to deal with the analogue of the first case of Theorem 4.1.3 and to prove the following: if $(C_1, \ldots, C_t)$ is a t-PMDS tuple, i.e. satisfies

$$d_{\min}(C_1 \cdots C_t) = n - (\dim C_1 + \cdots + \dim C_t) + t,$$

if none of the C_i's has dimension 1 and

$$d_{\min}(C_1 \cdots C_t) > t,$$

then all C_i's are Reed-Solomon codes with a common evaluation-point sequence. On the other hand the arguments in the paper do not seem quite sufficient to deal with the case of

$$d_{\min}(C_1 \cdots C_t) = t$$

corresponding to the second case of our main theorem. We leave the matter open for further study.

A version of Kneser's Theorem for a family of algebras was independently posted by Beck and Lecouvey [4], and is a more general version of Theorem 4.2.3. The proof follows similar arguments. Moreover, [4, Section 6] shows how Kneser's original Theorem can be recovered from the new variant. The very same argument, which is based on the embedding of the group G into the complex group algebra $\mathbb{C}[G]$ and on the isomorphism $\mathbb{C}[G] \cong \mathbb{C}^{|G|}$, allows one to recover the original theorem from our variant as well.