AN ANALOGUE OF VOSPER'S THEOREM FOR EXTENSION FIELDS

CHRISTINE BACHOC, ORIOL SERRA, AND GILLES ZÉMOR

ABSTRACT. We are interested in characterising pairs S, T of F-linear subspaces in a field extension L/F such that the linear span ST of the set of products of elements of S and of elements of T has small dimension. Our central result is a linear analogue of Vosper's Theorem, which gives the structure of vector spaces S, T in a prime extension L of a finite field F for which
$$\dim_F(ST) = \dim_F(S) + \dim_F(T) - 1,$$
when $\dim_F(S), \dim_F(T) \geq 2$ and $\dim_F(ST) \leq [L : F] - 2$.

1. INTRODUCTION

Inverse problems in additive theory aim to provide structural results of sets in an additive group which have a small subset sum. Motivated by a problem on difference sets, Hou, Cheng and Xiang [15] obtained a linear analogue of one of the central results in the area, the theorem of Kneser [17], in which cardinalities of sets in an abelian group are substituted by dimensions of subspaces over a field. To be specific, Let F be a field and let L be an extension field of F. If S and T are F-subvector spaces of L, we shall denote by ST the F-linear span of the set of products st, $s \in S$, $t \in T$. The linear analogue of Kneser's theorem can be stated as follows.

Theorem 1 (Hou, Cheng and Xiang)**.** *Let $F \subset L$ be fields and let S, T be F-subvectorspaces of L of finite dimension. Suppose that every algebraic element in L is separable over F. Then*

$$\dim(ST) \geq \dim(S) + \dim(T) - \dim H(ST),$$

where $H(ST) = \{x \in L : xST = ST\}$ denotes the stabilizer of ST in L.

One of the remarkable features of the above theorem is that the original theorem of Kneser can be obtained as a corollary. It can therefore be viewed not only as a transposition of an additive result, but as a generalization. This gives extra motivation for studying the translation of additive theory to its linear counterpart, since we may obtain insight on the original additive results and methods.

Eliahou and Lecouvey [6] obtained similar linear analogues of classical additive theorems including theorems of Olson [24] and Kemperman [16] in nonabelian groups. Lecouvey [20] pursued this direction by obtaining, among other extensions, linear versions of the Plünecke–Ruzsa [26] inequalities.

Going back to the statement of Theorem 1, since the stabilizer $H(X)$ of a finite dimensional subspace is a subfield of L of finite dimension, if L/F is an extension with no proper finite

1

intermediate extension, then either $H(X) = F$ or, if $\dim_F(L)$ is finite, $H(X) = L$. Hence one obtains a linear analogue of the Cauchy–Davenport inequality, which states that in an extension without a proper finite intermediate extension (in particular in finite extensions of prime degree), the dimension of the product of two subspaces S and T is either the whole extension, or has dimension at least $\dim(S) + \dim(T) - 1$. Strictly speaking, if we derive this result from Theorem 1 we need to suppose the extension to be separable. However the linear analogue of the Cauchy-Davenport Theorem is obtained in full generality, without the separability hypothesis by Eliahou and Lecouvey (see [6] Theorem 6.2). Let us state it formally:

Theorem 2. *Let L/F be an extension with no proper finite intermediate extension. For every pair of subspaces $S, T \subset L$ of finite dimension,*

$$\dim(ST) \geq \min\{\dim(L), \dim(S) + \dim(T) - 1\}.$$

One of the first inverse statements of additive theory is the theorem of Vosper [31] which states that, in a group of prime order, a pair of sets attaining equality in the Cauchy–Davenport inequality are, except for some degenerate cases, arithmetic progressions. In the present paper, our main result is a transposition of Vosper's theorem to the linear setting which reads:

Theorem 3. *Let F be a finite field and let L be an extension of prime degree p of F. Let S, T be subspaces of L such that $2 \leq \dim(S), \dim(T)$ and $\dim(ST) \leq p - 2$. If*

$$\dim(ST) = \dim(S) + \dim(T) - 1, \tag{1}$$

then there are bases of S and T of the form $\{g, ga, \ldots ga^{\dim(S)-1}\}$ and $\{g', g'a, \ldots, g'a^{\dim(T)-1}\}$ for some $g, g', a \in L$.

We shall see that the conclusion of Theorem 3 continues to hold if L is replaced by an infinite-dimensional extension of the finite field F containing no algebraic extension of F besides F. This last result will be seen to result from Theorem 3 through a valuation argument, and can also be derived by the same methodology that leads to Theorem 3.

The question naturally arises whether the conclusion of Theorem 3 holds for *any* extension L/F with no finite intermediate extensions, not just when F is a finite field. The answer turns out to be negative, and we shall give a counter-example for some infinite extension L/F, and also for a finite extension. We shall obtain some partial results in the case of arbitrary fields F, but the complete picture remains very much unclear. In particular, crucial to our method in the finite extension case is the hypothesis that the extension is separable.

The proof of Theorem 3 will import ideas from additive combinatorics, and also use results on quadratic forms and what has become known as the linear programming method in the theory of error-correcting codes. Since the route to Theorem 3 is fairly long and devious we give an overview.

Overview of the proof of Theorem 3. Given the hypothesis of Theorem 3, we shall consider subspaces A of L of *minimum dimension* (but at least equal to 2) such that

$$\dim(SA) = \dim(S) + \dim(A) - 1. \tag{2}$$

We shall first remark that if we can prove that such a subspace has dimension exactly 2, and has a basis of the form $1, a$, then the conclusion of Theorem 3 follows fairly straightforwardly. From then on we work towards showing that such a subspace A must have dimension 2.

With this objective, we shall transpose to the linear setting the so–called isoperimetric method in additive combinatorics, a method largely due to the late Hamidoune [9], which has proved to be a particularly useful tool in dealing with additive problems. We shall show that the subspaces A of (2), that we call *atoms* by analogy with the classical additive setting, must satisfy intersection properties. In particular we shall show that an atom A must satisfy the following:

$$\text{If } x, y, z, t \in A, \quad \text{and} \quad xy = zt \quad \text{then} \quad \{Fx, Fy\} = \{Fz, Ft\}$$

We call a subspace with this property a *Sidon space* by analogy with Sidon sets of integers which are sets such that, for any x, y, z, t in the set,

$$x + y = z + t \quad \text{implies} \quad \{x, y\} = \{z, t\}.$$

Furthermore, we shall arrive at the conclusion that atoms must have a product of small dimension, namely:

$$\dim(A^2) = 2\dim(A) - 1. \tag{3}$$

It remains to prove that this last property is incompatible with the Sidon property for any subspace A of dimension n greater than 2. To obtain this we shall need more tools: we shall consider the space of quadratic forms over the base field F in the variables $x_1, \ldots, x_n$ together with the natural mapping Φ into A^2 deduced from the correspondence:

$$x_1 \mapsto a_1, \ldots, x_n \mapsto a_n$$

where $a_1, \ldots a_n$ is a basis of A. We make the observation that any non-zero quadratic form that is of the form $\ell_1 \ell_1' + \ell_2 \ell_2'$ where $\ell_1, \ell_1', \ell_2, \ell_2'$ are F-linear expressions in $x_1, \ldots, x_n$ can not map to zero by Φ: this is a reformulation of the Sidon property. This motivates introducing the notion of *weight* of a quadratic form Q.

We shall say that the zero quadratic form has weight 0, that Q has weight 1 if it is the product of two non-zero linear forms, and inductively for $t > 1$ that it has weight t if it is the sum of t quadratic forms of weight 1 and is not of weight $< t$. This slightly non-standard notion is related to the quadratic form's rank, but behaves somewhat differently. The Sidon property of A means therefore that the kernel of the mapping Φ is a subspace $\mathcal{C}$ of the space of quadratic forms with minimum non-zero weight at least 3. On the other hand property (3) implies that $\mathcal{C}$ must be a space of large dimension. The rest of the proof of Theorem 3 consists in showing that such a large set $\mathcal{C}$ of quadratic forms of weight at least 3 can not exist.

Specifically, we shall show that if F is the finite field with q elements and $\mathcal{C}$ is a set of quadratic forms over F^n, any two of which differ by a quadratic form of weight at least 3, then the

cardinality $|\mathcal{C}|$ of $\mathcal{C}$ must satisfy:

$$|\mathcal{C}| < q^{(n-1)(n-2)/2}. \tag{4}$$

This is the minimal result that we need to finish the proof of Theorem 3. To the best of our knowledge, packing problems in the space of quadratic forms endowed with the aforementioned weight distance have not been considered before, making (4) of possibly independent interest. Loosely connected packing problems have been studied before for the related rank distance, in the space of bilinear forms [3], in the space of alternating bilinear forms [4], and more recently in the space of symmetric bilinear forms [27, 28]. The above papers have all applied what has become known as the Delsarte linear programming method, a powerful approach for deriving upper bounds on the size of codes (packings) initiated in [2] (see also [5]) in the framework of association schemes. The results obtained in [3, 4, 27, 28] can not be made to yield (4) directly however, and we have needed to work on the problem from scratch, also applying the Delsarte methodology.

The paper is organized as follows. Section 2 sets up matters by reducing Theorem 3 to the existence of critical spaces of dimension 2. Section 3 develops an extension field analogue of Hamidoune's isoperimetric method: in particular the intersection theorem for atoms (Theorem 9) is proved. Section 4 derives further properties of atoms and proves Theorem 16 which can be seen as a weak version of Theorem 3 in the sense that it is valid only for extensions of degree n such that $n - 2$ is prime. It places no restriction on the base field F however, and requires only the extension to be finite separable, with no intermediate extensions. Section 5 introduces Sidon spaces, makes the point that under the hypothesis of Theorem 3 atoms must be Sidon spaces, and connects them to packings in spaces of quadratic forms. Theorem 3 is reduced to a lower bound (Theorem 18) on the dimension of the square of Sidon space. Section 6 develops the study of packings of quadratic forms necessary to prove Theorem 18 and hence conclude a proof of Theorem 3. Section 7 is devoted to extensions of Theorem 3 to the case of infinite-dimensional extensions. Finally Section 8 concludes with some comments.

2. Deriving Theorem 3 from the existence of critical spaces of dimension 2

In this section we reduce Theorem 3 to showing the existence of a subspace A of dimension 2 satisfying (2). Note that if such a space exists, then without loss of generality we may suppose that it contains the field unit element 1, by multiplying A by an appropriate element of L if necessary.

Lemma 4. *Let L be an extension of F with no proper finite intermediate extension. Suppose that S is an F–subspace of dimension s of L, and that A is a subspace of dimension 2 generated by $\{1, a\}$ such that $\dim(AS) = \dim(S) + 1 \leq \dim(L) - 1$. Then there exists $g \in S$ such that $\{g, ga, \ldots, ga^{s-1}\}$ is a basis for S.*

Proof. We have $\dim(AS) = \dim(S + aS) = 2\dim(S) - \dim(S \cap aS)$ so

$$\dim(S \cap aS) = s - 1. \tag{5}$$

We next show the result by induction on $s \geq 2$.

If $\dim(S) = 2$, let g' generate $S \cap aS$, i.e. $S \cap aS = Fg'$. Then, $g' = ag$ with $g \in S$. Moreover $g \notin aS$ otherwise $g = \lambda g' = \lambda ag$ for some $\lambda \in F^*$ which would mean $a \in F$, so $\{g, ag\}$ is a basis of S.

In the general case $\dim(S) = s$, let $S' = S \cap aS$. Then, from (5), $\dim(S') = s - 1$; moreover S' also satisfies $\dim(AS') = \dim(S') + 1$. Indeed, we have

$$\dim(S') + 1 \leq \dim(AS') \leq \dim(aS) = \dim(S') + 1$$

where Theorem 2 gives the first inequality while the second follows from $AS' = S' + aS' \subset aS$. By induction, S' has a basis of the form $\{g', g'a, \ldots, g'a^{s-2}\}$. Since $g' \in aS$, for some $g \in S$, $g' = ga$. Moreover $g \notin S'$ otherwise $g = \sum_{i=1}^{s-1} \lambda_i ga^i$ for some $\lambda_i \in F$ but this would mean that $\deg_F(a) \leq s - 1 < \dim(L)$. So, $\{g, ga, \ldots, ga^{s-1}\}$ is a basis of S. $\square$

Lemma 5. *Let L/F be an extension with no proper finite intermediate extension. Let S, T be subspaces of L with $\dim(S), \dim(T) \geq 2$. Suppose that there exists a basis of S of the form $\{g, ga, \ldots, ga^{s-1}\}$ for $a, g \in L$ and that we have*

$$\dim(ST) = \dim(S) + \dim(T) - 1 \leq \dim(L) - 1.$$

Then there is a basis of T of the form $\{g', g'a, \ldots, g'a^{t-1}\}$ for some $g' \in L$.

Proof. Without loss of generality we will assume that S has a basis of the form $\{1, a, \ldots, a^{s-1}\}$ and we will proceed by induction on $s = \dim(S) \geq 2$. The case $s = 2$ is treated in Lemma 4.

Let S' be the subspace generated by $a, \ldots, a^{s-1}$: because $ST = T + S'T$, we have

$$\dim(T) + \dim(S'T) - \dim(T \cap S'T) = \dim(ST) = \dim(S) + \dim(T) - 1$$

thus

$$\dim(S'T) = \dim(S') + \dim(T \cap S'T). \tag{6}$$

Since

$$\dim(S') + \dim(T) - 1 \leq \dim(S'T) \leq \dim(ST) = \dim(S) + \dim(T) - 1,$$

the leftmost inequality coming from Theorem 2, we have that (6) leaves two possibilities: either $\dim(T \cap S'T) = \dim(T) - 1$ or $\dim(T \cap S'T) = \dim(T)$. Let us rule out the latter: indeed, it would mean that $ST = S'T$, therefore, setting $W = T + aT + \cdots + a^{s-2}T$ we get $W \subset ST = S'T = aW$. But W and aW have the same dimension, so we would have $W = aW$, which is impossible, given that $0 < \dim(W) < \dim(L)$ and $F(a)$ is either infinite-dimensional or equal to L.

So $\dim(S'T) = \dim(S') + \dim(T) - 1$ and $\dim(S') = s - 1$ so by induction T has a basis of the required form. $\square$

3. Connectivity in Field Extensions

We now transpose to the context of field extensions the basic notions of the isoperimetric method as introduced in [11] and developed in a number of later papers, see [25]. We borrow the terminology of [12, 13] and other papers with some adaptation to the linear case.

Recall that in a finite separable field extension the symmetric bilinear form

$$(x, y) \mapsto (x \,|\, y) = \mathrm{Tr}_{L/F}(xy)$$

where $\mathrm{Tr}_{L/F}()$ denotes the trace map, is non-degenerate. Crucial to the developments below will be the property:

$$(xy \,|\, z) = (x \,|\, yz) \ \text{ for all } x, y, z \in L. \tag{7}$$

We make the remark that the statements of this section rely mostly on (7) and as such could be stated in the general context of algebras over F in which a non-degenerate symmetric bilinear form satisfying (7) exists, namely symmetric Frobenius algebras. Since our applications will only concern extension fields, we do not pursue this generalization.

The next proposition is valid for any field extension L/F. Let S be a subspace of L of finite dimension.

For every subvectorspace X of L with non-zero, finite dimension we denote by

$$\partial_S X = \dim(XS) - \dim(X),$$

the increment of dimension of X when multiplied by S. We have the submodularity relation:

Proposition 6. *Let X, Y be finite-dimensional subspaces of L. We have*

$$\partial_S(X + Y) + \partial_S(X \cap Y) \leq \partial_S(X) + \partial_S(Y).$$

Proof. We have $(X + Y)S \subset XS + YS$ and $(X \cap Y)S \subset XS \cap YS$. Therefore,

$$
\begin{aligned}
\partial_S(X + Y) + \partial_S(X \cap Y) \ =\ & \dim((X + Y)S) - \dim(X + Y) + \dim((X \cap Y)S) \\
& - \dim(X \cap Y) \\
\leq\ & \dim(XS) + \dim(YS) - \dim(XS \cap YS) - \dim(X + Y) \\
& + \dim(XS \cap YS) - \dim(X \cap Y) \\
\leq\ & \dim(XS) + \dim(YS) - \dim(X) - \dim(Y) \\
=\ & \partial_S X + \partial_S Y.
\end{aligned}
$$

$\square$

Let $\mathfrak{X}_k$ be the set of subvectorspaces X of L such that

$$k \leq \dim(X) < \infty \text{ and } \dim(XS) + k \leq \dim(L).$$

If the set $\mathfrak{X}_k$ is non-empty, we define the *k–th connectivity* of S by

$$\kappa_k(S) = \min_{X \in \mathfrak{X}_k} \partial_S X.$$

If the set $\mathfrak{X}_k$ is empty we set $\kappa_k(S) = -\infty$. When $\kappa_k(S) \neq -\infty$, we define a *k–fragment of* S to be a subspace M of $\mathfrak{X}_k$ with $\partial_S M = \kappa_k(S)$. A *k–fragment* with minimum dimension is called a *k–atom*.

Suppose henceforth that the extension L/F is either infinite or finite separable in which case let $(\,|\,)$ denote the trace inner product (7). For a subspace $X < L$ we denote by

$$X^\perp = \{y \in L : \forall x \in X, (x\,|\,y) = 0\},$$

The following Lemma is crucial to the development of the isoperimetric method.

Lemma 7. *Let L/F be a finite separable extension. If X is a k-fragment of S, then $X^* = (XS)^\perp$ is also a k-fragment of S.*

Proof. Since

$$0 = (xs\,|\,x^*) = (x\,|\,x^*s),$$

for every $x \in X, s \in S$ and $x^* \in X^*$, we have $(X^*S)^\perp \supseteq X$, so that

$$\dim(X^*S) \le \dim(L) - \dim(X). \tag{8}$$

It follows that

$$
\begin{aligned}
\partial_S(X^*) &= \dim(X^*S) - \dim(X^*) \\
&\le \dim(L) - \dim(X) - \dim(X^*) \\
&= \dim(L) - \dim(X) - (\dim(L) - \dim(XS)) \\
&= \partial_S(X).
\end{aligned}
\tag{9}
$$

Finally, since X satisfies $\dim(XS) \le \dim(L) - k$ we have that $\dim(X^*) \ge k$. Together with (8) and (9) this implies that X^* is a k-fragment of S. $\square$

Corollary 8. *Let L/F be a finite separable extension. Let $S \subset L$ be a subvectorspace. If A is a k-atom of S then*

$$\dim(L) \ge 2\dim(A) + \kappa_k(S). \tag{10}$$

Proof. Let $A^* = (AS)^\perp$. Since $\dim(AS) = \dim(A) + \partial_S(A) = \dim(A) + \kappa_k(S)$ by definition of $\partial_S(A)$ and $\kappa_k(S)$, we have that $\dim(L) = \dim(AS) + \dim(A^*) = \dim(A) + \kappa_k(S) + \dim(A^*)$. Furthermore, by definition of an atom we have $\dim(A) \le \dim(A^*)$ since A^* is a fragment by Lemma 7. Hence the result. $\square$

The cornerstone of the isoperimetric method is the following property.

Theorem 9 (Intersection Theorem)**.** *Let the extension L/F be either infinite or finite separable. Let A, B be two distinct k–atoms of S. Then,*

$$\dim(A \cap B) \le k - 1.$$

Proof. By the submodularity relation one has

$$\partial_S(A + B) + \partial_S(A \cap B) \le \partial_S A + \partial_S B = 2\kappa(S).$$

Suppose that $\dim(A \cap B) \geq k$. By the definition of a k–atom, we have $\partial_S(A \cap B) > \kappa_k(S)$. It follows that $\partial_S(A + B) < \kappa_k(S)$. Hence,

$$
\begin{aligned}
\dim((A+B)S) &= \dim(A+B) + \partial_S(A+B) \\
&< 2\dim(A) - \dim(A \cap B) + \kappa_k(S) \\
&\leq 2\dim(A) - k + \kappa_k(S),
\end{aligned}
$$

from which we get

$$
\dim((A+B)S) + k \leq \dim(L)
$$

trivially if L is infinite dimensional and by Corollary 8 if L is a finite separable extension of F. By the definition of $\kappa_k(S)$, this contradicts $\partial_S(A + B) < \kappa_k(S)$. $\square$

Let A be a k–atom of S. We observe that, from the definitions of ∂_S and of atoms, for each $\alpha \in L \setminus \{0\}$, αA is also a k–atom of S. Therefore there is a k–atom of S containing 1. By the Intersection Theorem, when $k = 1$ the atom containing 1 is unique. The following Theorem is the linear analogue of a theorem of Mann [22, Ch. 1]. It is not as powerful as Kneser's theorem but it is already enough to recover the linear Cauchy-Davenport Theorem 2.

Theorem 10. *Let A be the 1–atom of S containing 1. Then A is a subfield of L. Moreover, if*

$$
\dim(ST) < \dim(S) + \dim(T) - 1 < \dim L,
$$

for some subspace T, then A is a subfield of L properly containing F.

Proof. For each $a \in A \setminus \{0\}$ we have $a \in aA \cap A$. Hence, by the Intersection Theorem $aA = A$. Therefore $a^{-1} \in A$ and A is a subfield of L. Moreover, if $\dim(ST) < \dim(S) + \dim(T) - 1$ for some subspace T then

$$
0 \leq \partial_S(A) = \dim(AS) - \dim(A) \leq \partial_S(T) = \dim(ST) - \dim(T) < \dim(S) - 1,
$$

so that we can not have $\dim(A) = 1$. $\square$

One consequence of Theorem 10 is the linear Cauchy–Davenport inequality of Theorem 2

$$
\dim(ST) \geq \dim(S) + \dim(T) - 1, \tag{11}
$$

when L has no proper finite-dimensional subfields containing F and L/F is either infinite or finite separable.

4. The 2–atom of a Vosper space

We now investigate the properties of 2-atoms of a subspace S, with in particular the goal of showing that under the conditions of Theorem 3 they must be of dimension 2. Note that under the conditions of Theorem 3, 2-atoms of S must exist.

Let L/F be either an infinite dimensional extension with no intermediate subfields of finite dimension, or a finite separable extension that has no intermediate subfields. In the latter

case, if F is a finite field this means that L/K has prime degree, hence the hypothesis of Theorem 3, but the results of this section hold in the more general case.

Let S be an F-vector space of finite dimension in L such that

$$\kappa_2(S) = \dim(S) - 1.$$

Let A be a 2–atom of S. We shall be interested in the sequence of subspaces A^i, $i \geq 1$, where A^i is defined inductively by $A^i = A^{i-1}$. In this section we shall show that A is also a 2–atom of A, that A^i, $i \geq 1$ is a 2–fragment of A as long as $\dim(A^i S) + 2 \leq \dim(L)$, and that in the case when $\dim(L)$ is finite $\dim(L) \equiv 2 \pmod{n-1}$, where $n = \dim(A)$.

Lemma 11. *If A is a 2–atom of S then A is a 2–atom of A.*

Proof. The statement is clear if $\dim(A) = 2$. Suppose that $\dim(A) = n \geq 3$. Note that S is a witness that $\kappa_2(A) = \dim(A) - 1$. Let B be a 2–atom of A. Without loss of generality we assume $1 \in A \cap B$.

Let $b \in B \setminus F$ and $a \in A \setminus F$.

Claim 12. $\dim(A) = \dim(B)$ *and* $AB = A + bA = B + aB$.

Proof. By the Intersection Theorem (Theorem 9),

$$2\dim(A) - 1 \leq \dim(A + bA) \leq \dim(AB) = \dim(A) + \dim(B) - 1,$$

which implies $\dim(B) \geq \dim(A)$. Analogously,

$$2\dim(B) - 1 \leq \dim(B + aB) \leq \dim(AB) = \dim(A) + \dim(B) - 1,$$

so that $\dim(A) = \dim(B) = n$. Moreover

$$AB = A + bA = B + aB.$$

$\square$

Claim 13. $\dim(A^2 B) < \dim(L)$.

Proof. We have

$$A^2 B = A(AB) = A(aB + B) \leq aAB + AB.$$

Hence,

$$
\begin{aligned}
\dim(A^2 B) &\leq 2\dim(AB) - \dim(aAB \cap AB) \\
&\leq 2(\dim(A) + \dim(B) - 1) - \dim(B) \\
&= 2\dim(A) + \dim(B) - 2,
\end{aligned}
\tag{12}
$$

where in the second inequality we use that $aB \subset aAB \cap AB$. On the other hand, by Corollary 8,

$$\dim(L) \geq 2\dim(A) + \kappa_2(A) = 3n - 1.$$

$\square$

Claim 13 allows us to apply the linear Cauchy–Davenport inequality (11) to the spaces A^2 and B, and together with (12) we obtain

$$\dim(A^2) + \dim(B) - 1 \leq \dim(A^2 B) \leq \dim A^2 B \leq 2\dim(A) + \dim(B) - 2,$$

which implies

$$\dim(A^2) \leq 2\dim(A) - 1.$$

This shows that A is its own 2–atom.   □

Lemma 14. *Let A be a 2–atom of S and $t \geq 2$ an integer. We have*

$$\dim(A^t) = \min\{\dim(A^{t-1}) + \dim(A) - 1, \dim(L)\}.$$

Proof. Let $a \in A \setminus F$. By Lemma 11 A is a 2–atom of A and $\dim(A^2) = \dim(A + aA) = 2\dim(A) - 1$, which establishes the result for $t = 2$. In particular, $A^2 = A + aA$, so that we have

$$A^t = A^{t-2}(A + aA) = A^{t-1} + aA^{t-1}.$$

Now, notice that $A^{t-1} \cap aA^{t-1}$ contains aA^{t-2}, therefore

$$\dim(A^t) = \dim(A^{t-1} + aA^{t-1}) \leq \dim(A^{t-1}) + \dim(A^{t-1}) - \dim(A^{t-2}).$$

Suppose that $A^t \neq L$. By induction on t we have that $\dim(A^{t-1}) - \dim(A^{t-2}) = \dim(A) - 1$ therefore

$$\dim(A^t) \leq \dim(A^{t-1}) + \dim(A) - 1.$$

Now since $A^t \neq L$, the linear Cauchy-Davenport inequality (11) gives

$$\dim(A^{t-1}) + \dim(A) - 1 \leq \dim(A^t),$$

which yields $\dim(A^t) = \dim(A^{t-1}) + \dim(A) - 1.$ □

Lemma 15. *Let A be a 2–atom of S with $\dim(A) = n > 2$. Then if $\dim(L)$ is finite we have:*

$$\dim(L) \equiv 2 \bmod (n - 1).$$

Proof. Let t be the largest positive integer such that $\dim(A^t) < \dim(L)$. We recall that $\dim(A^2) \leq \dim(L) - 2$, so that $t \geq 2$. Let $X = A^{t-1}$ and let $X^* = (A^t)^{\perp}$. Since we have supposed $\dim(A^t) < \dim(L)$, we have $\dim(X^*) > 0$. Lemma 14 implies that either $\dim(X^*) = 1$ or $X = A^{t-1}$ is a 2-fragment of A. But if X is a 2-fragment of A then Lemma 7 applied to X and A implies that X^* is also a 2-fragment of A. But then the maximality of t such that $\dim(A^t) < \dim(L)$ and Lemma 14 imply that $\dim(X^*) \leq \dim(A) - 1$, which is in contradiction with A being a 2-atom of A (Lemma 11). Therefore $\dim(A^t) = \dim(L) - 1$. To conclude, observe that Lemma 14 gives $\dim(A^t) = \dim(A) + (t - 1)(\dim(A) - 1)$, hence

$$\dim(L) = 2 + t(\dim(A) - 1).$$

                                                                                          □

As an immediate consequence of Lemma 15, we have that if $\dim(L) - 2 = m - 2$ is prime, then atoms can only have dimension 2 and by Lemmas 4 and 5 the linear version of Vosper's theorem holds for any separable extension of degree m over any field, given that there is no intermediate subfield. This is the case in particular if p and $p - 2$ are a pair of twin primes and if L/F is separable of degree p. Specifically:

Theorem 16. *Let L/F be a finite separable extension with no intermediate proper extension. Suppose furthermore that $[L : F] - 2$ is prime. Let S, T be subspaces of L such that $2 \leq \dim(S), \dim(T)$ and $\dim(ST) \leq \dim(L) - 2$. If*

$$\dim(ST) = \dim(S) + \dim(T) - 1,$$

then there are bases of S and of T respectively of the form

$$\{g, ga, \ldots ga^{\dim(S)-1}\} \quad and \quad \{g', g'a, \ldots, g'a^{\dim(T)-1}\}$$

for some $g, g', a \in L$.

Without the condition that $\dim(L) - 2$ is prime some possible dimensions other than 2 escape Lemma 15. To remove them we introduce more tools.

5. Sidon spaces and quadratic forms

The Intersection Theorem 9 gives a key property of 2–atoms that in infinite or finite separable extensions L/F without proper finite sub-extensions, translates into:

$$\forall x \in L \setminus F, \quad \dim(A \cap xA) \leq 1. \tag{13}$$

We note that (13) implies

$$\forall x, y, z, t \in A \setminus \{0\}, \ xy = zt \Rightarrow \begin{cases} Fx = Fz \text{ and } Fy = Ft \quad \text{or} \\ Fx = Ft \text{ and } Fy = Fz \end{cases}$$

This is because since $x^{-1}A \cap z^{-1}A$ contains F, we deduce that either x and z are F-proportional, from which the conclusion follows, or that $x^{-1}A \cap z^{-1}A = F$ by (13) from which it follows that $x^{-1}t$ and $z^{-1}y$ each generate the constant field F.

This suggests calling a subspace which satisfies (13) a *Sidon space*, by analogy with classical Sidon sets. We make the remark that when a space A has a basis in geometric progression then there exists an $x \in L$ such that $\dim(A \cap xA) = \dim(A) - 1$. Therefore Sidon spaces can be thought of as spaces that are "furthest away" from a space with a basis in geometric progression.

For a Sidon space we clearly have

$$\dim(A^2) \geq \dim(A + aA) \geq 2\dim(A) - 1, \tag{14}$$

for any $a \in A \setminus F$. According to Lemma 11, if A is a 2–atom of some set S satisfying (2) in an infinite of finite separable extension without proper finite sub-extensions, then the inequalities in (14) are actually equalities. To recap we have:

Proposition 17. *Let L/F be either a finite separable extension without proper subfields, or an infinite extension without proper finite intermediate subfields. Let S be a subspace of L with finite dimension ≥ 2 and let A be a 2-atom of S. Then A is a Sidon space. Furthermore if $\dim(SA) = \dim(S) + \dim(A) - 1$ then $\dim(A^2) = 2\dim(A) - 1$.*

Now classical Sidon sets $\mathcal{S}$ of integers (or Sidon sets in abelian groups) have the property that $|\mathcal{S} + \mathcal{S}| = \binom{|\mathcal{S}|+1}{2}$ which implies in particular that $|\mathcal{S} + \mathcal{S}| = 2|\mathcal{S}| - 1$ if and only if $|\mathcal{S}| \leq 2$. If we let ourselves be guided by the additive analogy, we may be led to expect for a moment that for any Sidon space A it is true that $\dim(A) = \binom{\dim(A)+1}{2}$. This would immediately imply that the only Sidon spaces A such that $\dim(A^2) = 2\dim(A) - 1$ are of dimension ≤ 2. It is however *not true* in general that $\dim(A) = \binom{\dim(A)+1}{2}$ for Sidon spaces, even in separable extensions of prime order.

For the sake of explicitness, here is a counter-example: take for F the finite field of size 2, for L the field of size 2^{19}, and let A be the F-vector with basis $(1, \alpha, \alpha^7, \alpha^{12} + \alpha^2 + 1)$ where α is a root of the irreducible polynomial $X^{19} + X^{14} + X^{10} + X^7 + X^2 + X + 1$. Computing dimensions yields $\dim(A^2) = 9 < \binom{\dim(A)+1}{2} = 10$.

However, for the purpose of deriving Theorem 3, we only need to prove that the only Sidon spaces that satisfy (14) with equalities are of dimension ≤ 2. If F is allowed to be any field, again this is not true. After we make the connection between Sidon spaces and quadratic forms, we shall give an example at the end of this section of a Sidon space of dimension 3 that satisfies (14) with equalities.

When F is a finite field it *is* true though that Sidon spaces satisfying (14) with equalities must be of dimension ≤ 2. Specifically:

Theorem 18. *Let F be a finite field and let L be an extension field of F. Let A be a Sidon subspace of L of finite dimension $\dim(A) \geq 3$. Then $\dim(A^2) > 2\dim(A) - 1$.*

Note that we do not need to suppose that L/F is finite and of prime degree.

Theorem 18 together with Proposition 17 will in particular establish that the 2-atom of S in Theorem 3 can only have dimension 2, and Theorem 3 will follow from Lemmas 4 and 5.

To prove Theorem 18 we shall transform our problem into a problem in the space of quadratic forms.

Let $\mathcal{Q}_n$ denote the vector space of homogeneous polynomials of degree 2 in the variables $x_1, \ldots, x_n$ with coefficients in the field F. A typical element of $\mathcal{Q}_n$ will be denoted

$$Q = \sum_{1 \leq i \leq j \leq n} a_{ij} x_i x_j. \tag{15}$$

The F-vector space $\mathcal{Q}_n$ is of dimension $n(n + 1)/2$ and we can identify it with the space of quadratic forms over F^n. Similarly, let $\mathcal{L}_n$ denote the space of linear forms over F^n, identified with the space of homogeneous polynomials of degree 1 in $x_1, \ldots, x_n$. Let us now introduce a notion of *weight* of a quadratic form.

Definition 19. *For a non-zero quadratic form $Q \in \mathcal{Q}_n$, let its* weight *equal the smallest integer k such that Q can be expressed as a sum of k products of linear forms in $x = (x_1, \ldots, x_n)$.*

$$\mathrm{wt}(Q) := \min\{k \ : \ Q = \ell_1(x)\ell_1'(x) + \cdots + \ell_k(x)\ell_k'(x), \ \ell_i, \ell_j' \in \mathcal{L}_n, 1 \leq i, j \leq k\}. \qquad (16)$$

If $\mathcal{C}$ is a set of quadratic forms, we will call the minimum weight of $\mathcal{C}$ the smallest weight of the difference between two distinct quadratic forms of $\mathcal{C}$:

$$\mathrm{wt}(\mathcal{C}) := \min\{\mathrm{wt}(Q - Q') \ : \ (Q, Q') \in \mathcal{C}^2, \ Q \neq Q'\}. \qquad (17)$$

We note that, it $\mathcal{C}$ is a linear subspace of $\mathcal{Q}_n$, then $\mathrm{wt}(\mathcal{C}) = \min\{\mathrm{wt}(Q) \ : \ Q \in \mathcal{C}, \ Q \neq 0\}$.

Now let A be a Sidon space of dimension n in some extension of F. Let $(a_1, \ldots, a_n)$ be a basis of A. Consider the homomorphism Φ of vector spaces $\mathcal{L}_n \to A$ defined by the mapping

$$x_1 \mapsto a_1, \ldots, x_n \mapsto a_n.$$

This homomorphism extends in a natural way to a homomorphism of F-vector spaces

$$\Phi \ : \mathcal{Q}_n \to A^2$$

through the relations $x_i x_j \mapsto a_i a_j$. Note that for any $\ell, \ell' \in \mathcal{L}_n$, the map Φ satisfies $\Phi(\ell\ell') = \Phi(\ell)\Phi(\ell')$. Consider the subspace $\mathcal{C}$ of $\mathcal{Q}_n$, $\mathcal{C} = \ker \Phi$.

Proposition 20. *A is a Sidon space if and only if for any $Q \in \mathcal{C}, Q \neq 0$, we have $\mathrm{wt}(Q) \geq 3$.*

Proof. That $\mathrm{wt}(Q) > 1$ is simply that elements of A^2 live in a field where products of non-zero elements are non-zero. If $\mathrm{wt}(Q) = 2$, meaning that $Q = \ell_1\ell_1' + \ell_2\ell_2'$, then setting $x = \Phi(\ell_1), y = \Phi(\ell_1'), z = \Phi(\ell_2), t = \Phi(\ell_2')$ we have that $xy + zt = 0$ in A^2. But A being a Sidon set implies, according to the remark following (13), that either x is an F-multiple of z and y is an F-multiple of t or x is an F-multiple of t and y is an F-multiple of z. Since the mapping Φ is one-to-one from $\mathcal{L}_n$ to A we deduce from this that Q is F-proportional to $\ell_1\ell_1'$, which contradicts $\mathrm{wt}(Q) = 2$. The reverse implication should be obvious. $\square$

Example of a Sidon Space. Let $\mathbb{Q}$ denote the rational field and consider the extension $L = \mathbb{Q}[x, y]/(x^2 + y^2 + 1)$. The polynomial $x^2 + y^2 + 1$ is absolutely irreducible over $\mathbb{Q}$, meaning that L contains no proper finite intermediate extension of $\mathbb{Q}$. We claim that the subspace A with basis $(1, x, y)$ is a Sidon space such that $\dim(A^2) = 5 = 2\dim(A) - 1$. The statement regarding the dimensions is obvious: to see that A is indeed a Sidon space, suppose the contrary which would mean that four $\mathbb{Q}$-linear combinations a, b, c, d of $1, x, y$ are such that $ab + cd = x^2 + y^2 + 1$. Switching to projective coordinates, this would mean exactly that the quadratic form $x^2 + y^2 + z^2$ is of weight 2 over $\mathbb{Q}$. But it is readily seen that this form is actually of weight 3 over $\mathbb{Q}$, therefore A can only be a Sidon space.

As remarked at the beginning of the section, the definition of a Sidon space contradicts, for dimensions at least 3, having a basis in geometric progression. Therefore the above example is also an example of a space A satisfying $\dim(A^2) = 2\dim(A) - 1$ which does not have a basis in geometric progression. The setting is that of an infinite extension but this Sidon space can be transplanted as follows into a finite separable extension without intermediate subfields.

Example of a Sidon Space in a finite extension. Let $L = \mathbb{Q}(a)$ where a is a root of the irreducible polynomial $P(x) = 2 + 2x + 2x^2 + 2x^4 + 2x^5 + x^8 = 1 + x^2 + (1 + x + x^4)^2$. It can be checked that the Galois group of this polynomial is the full symmetric group S_8 which implies that the extension $L/\mathbb{Q}$ has no intermediate extension. Setting A to be the subspace of L generated by $1, a, b = 1 + a + a^4$, we again have $\dim(A^2) = 5$ since $1 + a^2 + b^2 = 0$. We also have that if Φ is the mapping from the space of quadratic forms in the variables x, y, z over $\mathbb{Q}$ into A defined by $x \mapsto a$, $y \mapsto b$, $z \mapsto 1$, then $\ker \Phi$ has dimension 1 and is generated by the quadratic form $x^2 + y^2 + z^2$ which is of weight 3 as mentioned above. Therefore A is a Sidon set in L.

We remark that the quadratic form $x^2 + y^2 + z^2$ is anisotropic over $\mathbb{Q}$, and that this makes it of weight 3. Similar examples can be constructed whenever we have such a quadratic form: these forms do not exist over finite fields however, which motivates our quest for Theorem 3 and our study of packings of quadratic forms of minimum weight 3 in the next section.

We remark that if $\dim(A^2) = 2\dim(A) - 1 = 2n - 1$, we have that $\dim(\ker \Phi) = n(n+1)/2 - (2n - 1) = (n-1)(n-2)/2$. Theorem 18 will follow if we can prove that for every $n \geq 3$, a subspace of $\mathcal{Q}_n$ of dimension $(n-1)(n-2)/2$ and of minimum weight 3 does not exist.

6. Codes in the space of quadratic forms over finite fields

In this section, q is a power of a prime and $F = \mathbb{F}_q$ is the finite field with q elements. As mentioned in the previous section, we will prove the following theorem, which will enable us to conclude the proof of Theorem 3.

Theorem 21. *Let $n \geq 3$, and let $\mathcal{C} \subset \mathcal{Q}_n$, with $\mathrm{wt}(\mathcal{C}) \geq 3$. Then, $|\mathcal{C}| < q^{(n-1)(n-2)/2}$.*

The inequality $|\mathcal{C}| \leq q^{(n-1)(n-2)/2}$ follows from a simple packing argument. Indeed, if ℓ_1 and ℓ_2 are two linearly independent elements of $\mathcal{L}_n$, let

$$\mathcal{A}_{\ell_1,\ell_2} := \{Q = \ell_1(x)\ell_1'(x) + \ell_2(x)\ell_2'(x) \ : \ \ell_i' \in \mathcal{L}_n\} \subset \mathcal{Q}_n. \tag{18}$$

$\mathcal{A}_{\ell_1,\ell_2}$ is a subspace of $\mathcal{Q}_n$, of dimension $2n - 1$: if $\ell_3, \ldots, \ell_n$ are such that $\{\ell_1, \ell_2, \ldots, \ell_n\}$ is a basis of $\mathcal{L}_n$, then $\{\ell_1(x)\ell_i(x), \ell_2(x)\ell_j(x), 1 \leq i \leq n, 2 \leq j \leq n\}$ is a basis of $\mathcal{A}_{\ell_1,\ell_2}$. Moreover, for all $Q \in \mathcal{A}_{\ell_1,\ell_2}$, $\mathrm{wt}(Q) \leq 2$. So, if $\mathcal{C}$ has minimum weight at least 3, and if $(Q, Q') \in \mathcal{C}^2$, then $Q - Q' \notin \mathcal{A}_{\ell_1,\ell_2}$ unless $Q = Q'$. Said differently, the elements of $\mathcal{C}$ are pairwise distinct in the quotient space $\mathcal{Q}_n/\mathcal{A}_{\ell_1,\ell_2}$. As a consequence, their cardinalities satisfy

$$|\mathcal{C}| \leq |\mathcal{Q}_n/\mathcal{A}_{\ell_1,\ell_2}| = q^{(n-1)(n-2)/2}. \tag{19}$$

The bound (19) is an instance of an *anticode* bound in coding theory terminology [21, Ch 17]: the set $\mathcal{A}_{\ell_1,\ell_2}$ is an anticode, i.e. a set of diameter 2. Henceforth we refer to $\mathcal{C}$ as a *code*, i.e. a set $\mathcal{C} \subset \mathcal{Q}_n$ with a minimum weight condition.

The claim in Theorem 21 is therefore that the inequality in (19) is not attained when $n \geq 3$. Improving upon (19) seems out of reach by elementary packing arguments and we shall need

to involve group actions. As mentioned in the introduction, we shall derive Theorem 21 by applying the Delsarte "linear programming" method.

Let us first give a short sketch of the proof. The space $\mathcal{Q}_n$ affords the action of the group $G := \mathbb{F}_q^* \times \mathrm{Gl}(n, q)$, where $\mathbb{F}_q^*$ acts by scalar multiplication on quadratic forms and the linear group $\mathrm{Gl}(n, q)$ acts linearly on the variables. This action preserves $\mathcal{L}_n$, and hence the weight of a quadratic form. The orbits of the action of G on $\mathcal{Q}_n$ will be denoted $\{\mathcal{O}_t, \ t \in \mathcal{T}_n\}$, where the index set $\mathcal{T}_n$ will be specified later. For a code of quadratic forms $\mathcal{C}$, let $X_t := |\mathcal{C} \cap \mathcal{O}_t|$. In a first step, we will prove that, under the assumptions $\mathrm{wt}(\mathcal{C}) \geq 3$ and $|\mathcal{C}| = q^{(n-1)(n-2)/2}$, these numbers satisfy a certain system of linear equations (Proposition 29). Some of the equations are straightforward translations of the assumptions, but the most interesting ones arise from an application of Delsarte linear programming method [2], that focuses on an appropriate test function with non negative Fourier coefficients. In a second step, we will prove that this system doesn't have any real solutions when $n \geq 3$. To this end, we will work on a much smaller linear system (Proposition 30) satisfied by certain variables related to the Fourier coefficients of the characteristic function of $\mathcal{C}$. When the code $\mathcal{C}$ is linear, these new variables can be interpreted in terms of the dual code of $\mathcal{C}$. The duality notion that we shall rely on is somewhat non-standard and associates to a code of quadratic forms a dual code of symmetric bilinear forms.

We start by recalling some classical results on the classification of quadratic forms and symmetric bilinear forms over finite fields.

6.1. Group actions on quadratic forms and symmetric bilinear forms over finite fields. Let $x = (x_1, \ldots, x_n)$, and $u = (u_{i,j})_{1 \leq i,j \leq n} \in \mathrm{Gl}(n, q)$. Denoting by u^t the transpose matrix of u, to any quadratic form $Q : x \mapsto Q(x)$ we can associate the form $Q^u : x \mapsto Q(xu^t)$,

$$Q^u(x) = Q\left(\sum_{k=1}^{n} u_{1,k} x_k, \ldots, \sum_{k=1}^{n} u_{n,k} x_k\right).$$

For $g = (a, u) \in G = \mathbb{F}_q^* \times \mathrm{Gl}(n, q)$, a (right) group action is thus defined on elements Q of $\mathcal{Q}_n$ by $Q^g = aQ^u$. The orbits of $\mathcal{Q}_n$ under this action are straightforwardly obtained from the well known description of the orbits of $\mathcal{Q}_n$ under $\mathrm{Gl}(n, q)$ ([30, Chapter 11]). We use the notation $Q \sim Q'$ for two G-equivalent quadratic forms. We recall that a symmetric bilinear form B_Q, defined by $B_Q(x, y) = Q(x+y) - Q(x) - Q(y)$, is naturally associated to $Q \in \mathcal{Q}_n$. The radical Rad_Q of Q is the linear space of elements of $\mathbb{F}_q^n$ such that $Q(x) = 0$ and $B_Q(x, y) = 0$ for all $y \in \mathbb{F}_q^n$. The rank $\mathrm{rk}(Q)$ of Q is the codimension of its radical, and Q is said to be non degenerate if $\mathrm{rk}(Q) = n$. The set of quadratic forms of given rank r makes up one orbit if r is odd, and splits into two orbits if r is even:

Proposition 22. *If $Q \in \mathcal{Q}_n$ is a quadratic form over $\mathbb{F}_q$ in n variables of rank $r = \mathrm{rk}(Q) > 0$, then one of the following holds:*

(1) r *is odd and* $Q \sim \sum_{i=1}^{(r-1)/2} x_{2i-1} x_{2i} + x_r^2$.
(2) r *is even and* $Q \sim \sum_{i=1}^{r/2} x_{2i-1} x_{2i}$.

(3) r is even and $Q \sim \sum_{i=1}^{r/2-1} x_{2i-1} x_{2i} + Q_0(x_{r-1}, x_r)$, where

$$Q_0(x_1, x_2) = \begin{cases} x_1^2 - bx_2^2 \ if \ p \neq 2 \\ x_1^2 + x_1 x_2 + bx_2^2 \ if \ p = 2. \end{cases}$$

In the above, $b \in \mathbb{F}_q$ is such that $b \in \mathbb{F}_q \setminus \mathbb{F}_q^2$ if $p \neq 2$, and $b \in \mathbb{F}_q \setminus \sigma(\mathbb{F}_q)$ if $p = 2$, where $\sigma(\mathbb{F}_q) = \{\lambda^2 + \lambda, \ \lambda \in \mathbb{F}_q\}$.

The space $\mathcal{S}_n$ of symmetric bilinear forms over $\mathbb{F}_q$ is also equipped with a natural action of G, given by $B^g = au^t Bu$, where we identify symmetric bilinear forms and symmetric matrices. We note that the $\mathbb{F}_q$-vector spaces $\mathcal{Q}_n$ and $\mathcal{S}_n$ have the same dimension $n(n+1)/2$. Moreover, the correspondence $Q \mapsto B_Q$ defines an isomorphism of G-spaces when q is odd, because Q can be recovered from B_Q thanks to the formula $B_Q(x, x) = 2Q(x)$. When q is even, B_Q is alternating and the correspondence $Q \mapsto B_Q$ is not one to one. However, for all q, there exists a *pairing* between $\mathcal{Q}_n$ and $\mathcal{S}_n$ that behaves well with respect to the action of G (the duality between the association schemes of quadratic forms and of symmetric bilinear forms derived from this pairing was already observed in [32]).

Lemma 23. *Let $\alpha : (\mathbb{F}_q, +) \to (\mathbb{C}^*, \times)$ be a fixed non trivial character. Let, for $Q \in \mathcal{Q}_n$, $Q = \sum_{1 \leq i \leq j \leq n} a_{i,j} x_i x_j$ and $B \in \mathcal{S}_n$, $B = (b_{i,j})_{1 \leq i, j \leq n}$,*

$$(Q, B) := \alpha\Big(\sum_{1 \leq i \leq j \leq n} a_{i,j} b_{i,j} \Big). \tag{20}$$

Then, this expression defines a non degenerate pairing between $\mathcal{Q}_n$ and $\mathcal{S}_n$, i.e. it satisfies:

- $(Q + Q', B) = (Q, B)(Q', B)$ *for all* $Q, Q' \in \mathcal{Q}_n$, $B \in \mathcal{S}_n$.
- $(Q, B + B') = (Q, B)(Q, B')$ *for all* $Q \in \mathcal{Q}_n$, $B, B' \in \mathcal{S}_n$.
- $(Q, B) = 1$ *for all* $B \in \mathcal{S}_n$ *if and only if* $Q = 0$.
- $(Q, B) = 1$ *for all* $Q \in \mathcal{Q}_n$ *if and only if* $B = 0$.

For $g = (a, u) \in G$, let $g^t = (a, u^t)$. We have:

$$(Q^g, B) = (Q, B^{g^t}) \ for \ all \ Q \in \mathcal{Q}_n, \ B \in \mathcal{S}_n, \ g \in G. \tag{21}$$

Proof. It is a straightforward verification. □

The pairing introduced above allows for a convenient description of the multiplicative characters of the additive group $(\mathcal{Q}_n, +)$ and of the way the group G acts on them. Indeed, the characters of $(\mathcal{Q}_n, +)$ are in one to one correspondence with $\mathcal{S}_n$ and for every $B \in \mathcal{S}_n$ the associated character is given by:

$$\chi_B(Q) = (Q, B) \tag{22}$$

where $B \in \mathcal{S}_n$. Furthermore, if we define the action of G on characters by $(g.\chi)(Q) := \chi(Q^g)$, then Lemma 23 translates into:

$$g.\chi_B = \chi_{B^{g^t}}.$$

In the next proposition, we recall the description of the orbits of $\mathcal{S}_n$ under the action of G. If q is even, and $B \in \mathcal{S}_n$ is non degenerate, $W := \{x \in \mathbb{F}_q^n \ : \ B(x,x) = 0\}$ is a hyperplane, and the restriction of B to W is alternating, so the description of the $\mathrm{Gl}(n,q)$-orbits of $\mathcal{S}_n$ follows easily from the classification of alternating forms [30, Chapter 8]. A matrix with a diagonal block structure $\left(\begin{smallmatrix} A & 0 \\ 0 & B \end{smallmatrix}\right)$ is denoted below by $A \oplus B$.

Proposition 24. *If $B \in \mathcal{S}_n$ is a symmetric bilinear form over $\mathbb{F}_q$ in n variables of rank* $\mathrm{rk}(B) = r > 0$, *then one of the following holds:*

(1) *r is odd and $B \sim \oplus_{i=1}^{(r-1)/2} \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \oplus (1)$.*
(2) *r is even and $B \sim \oplus_{i=1}^{r/2} \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.*
(3) *r is even and $B \sim \oplus_{i=1}^{r/2-1} \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \oplus B_0$ where $B_0 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ if $p = 2$, and $B_0 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -b \end{smallmatrix}\right)$, $b \in \mathbb{F}_q \setminus \mathbb{F}_q^2$, if $p \neq 2$.*

From Propositions 22 and 24, we see that the orbits of $\mathcal{Q}_n$ and of $\mathcal{S}_n$ under the action of G can be parametrized by the same set $\mathcal{T}_n$, where

$$\mathcal{T}_n = \{0\} \cup \{(r,e) \ : \ 1 \leq r \leq n, \ e = 0 \text{ if } r \text{ is odd }, \quad e = \pm 1 \text{ if } r \text{ is even}\}, \qquad (23)$$

as follows:

Notation 25. *For a non-zero quadratic form $Q \in \mathcal{Q}_n$ (respectively a non-zero symmetric bilinear form $B \in \mathcal{S}_n$), of rank r, let $e = 0$ in case (1), $e = 1$ in case (2), $e = -1$ in case (3). The pair $(r,e) \in \mathcal{T}_n$ will be called* the type *of the quadratic form or of the symmetric bilinear form. The type of $Q = 0$, or of $B = 0$, will by definition be 0.*

If Q is of type $t \in \mathcal{T}_n$, we will use the notation $Q \sim t$. The orbit of $Q \sim t$ will be denoted by $\mathcal{O}_Q$ or $\mathcal{O}_t$, and G_Q will denote the stabilizer of Q in G.

When dealing with types, orbits and stabilizers, we will use the same set of notations whether we are speaking of quadratic forms or of symmetric bilinear forms. However, to avoid confusion, we will preferentially reserve the letter t for types of elements of $\mathcal{Q}_n$ and the letter s for types of elements of $\mathcal{S}_n$.

Let us now make the connection between the weight and the type of a quadratic form. Since the weight of a quadratic form is left unchanged under the action of G, it should be expressible in terms of its type. Indeed, we have:

Lemma 26. *If $Q \sim (r,e)$, $\mathrm{wt}(Q) = (r - e + 1)/2$.*

Proof. This formula can be put in a more general context as follows: over an arbitrary field F, it is well known that a non degenerate quadratic form $Q \in \mathcal{Q}_n$ can be decomposed up to G-equivalence into the direct sum of a hyperbolic form $H_{hyp}(x_1,\ldots,x_{2h}) := x_1 x_2 + x_3 x_4 + \cdots + x_{2h-1}x_{2h}$ of rank $2h$ and of an anisotropic form $Q_{an}(x_{2h+1},\ldots,x_n)$ of rank $n - 2h$. Then, it is not difficult to verify that $\mathrm{wt}(H_{hyp}) = h$, $\mathrm{wt}(Q_{an}) = n - 2h$ and $\mathrm{wt}(Q) = h + (n - 2h) = n - h$. $\qquad\square$

6.2. **The equations satisfied by** $\{X_t, \ t \in \mathcal{T}_n\}$. Let $\mathcal{C} \subset \mathcal{Q}_n$ denote a (not necessarily linear) subset of $\mathcal{Q}_n$, such that $\mathrm{wt}(\mathcal{C}) \geq 3$. Without loss of generality, we will assume that $0 \in \mathcal{C}$. We have already introduced, for $t \in \mathcal{T}_n$,

$$X_t := |\mathcal{C} \cap \mathcal{O}_t| = |\{Q \in \mathcal{C} \ : \ Q \sim t\}|. \tag{24}$$

These numbers satisfy a few trivial equations:

$$\begin{cases} X_0 = 1 \\ \sum_{t \in \mathcal{T}_n} X_t = |\mathcal{C}| \\ X_t = 0 \text{ for } t = (1,0), (2,1), (2,-1), (3,0), (4,1). \end{cases} \tag{25}$$

The last set of conditions follow from the assumption $\mathrm{wt}(\mathcal{C}) \geq 3$ and Lemma 26. We will prove that, if $\mathcal{C}$ is a hypothetical optimal code, i.e. if it satisfies equality in (19), then there are more equations for $\{X_t\}$:

Proposition 27. *For $s \in \mathcal{T}_n$, the expression $\sum_{B \in \mathcal{O}_s} \chi_B(Q) = \sum_{B \in \mathcal{O}_s} (Q, B)$ only depends on the type of Q. Let*

$$\chi_s(t) := \sum_{B \in \mathcal{O}_s} (Q, B) \qquad (Q \sim t). \tag{26}$$

If $\mathcal{C} \subset \mathcal{Q}_n$, $0 \in \mathcal{C}$, $\mathrm{wt}(\mathcal{C}) \geq 3$ and $|\mathcal{C}| = q^{(n-1)(n-2)/2}$, for all $s = (r,e)$ such that $1 \leq r \leq n-2$, we have

$$\sum_{t \in \mathcal{T}_n} \chi_s(t) X_t = 0. \tag{27}$$

Proof. We consider the function on $\mathcal{Q}_n$ defined by:

$$F(Q) := \sum_{g \in G} 1_{\mathcal{A}^g}(Q) \tag{28}$$

where $\mathcal{A} := \mathcal{A}_{x_1, x_2}$. We note that $\mathcal{A}^g$ runs over the set $\{\mathcal{A}_{\ell_1, \ell_2} \ : \ (\ell_1, \ell_2) \text{ independent}\}$. We will compute in two different ways the expression:

$$\Sigma := \sum_{(Q, Q') \in \mathcal{C}^2} F(Q - Q'). \tag{29}$$

The first way is straightforward; taking account of the fact that, if $Q \neq Q'$, $\mathrm{wt}(Q - Q') \geq 3$, so that $Q - Q'$ cannot belong to $\mathcal{A}^g$, we have

$$\Sigma = \sum_{Q \in \mathcal{C}} F(0) = |G||\mathcal{C}|. \tag{30}$$

The second method uses the expansion of F over the characters of $\mathcal{Q}_n$, in other words its Fourier expansion. We introduce the complex vector space

$$L(\mathcal{Q}_n) := \{f \ : \ \mathcal{Q}_n \to \mathbb{C}\}$$

The multiplicative characters $\chi_B : (\mathcal{Q}_n, +) \to \mathbb{C}^*$, for $B \in \mathcal{S}_n$, form a basis of $L(\mathcal{Q}_n)$, which is orthonormal for the standard inner product

$$\langle f_1, f_2 \rangle := \frac{1}{|\mathcal{Q}_n|} \sum_{Q \in \mathcal{Q}_n} f_1(Q) \overline{f_2(Q)} \qquad f_1, f_2 \in L(\mathcal{Q}_n).$$

So, F can be written $F = \sum_{B \in \mathcal{S}_n} f_B \chi_B$. It will be essential in what follows that $f_B \geq 0$, and we will also need to know when $f_B > 0$. The next lemma clarifies this.

Lemma 28. *With the above notation, $f_B \geq 0$ for all $B \in \mathcal{S}_n$, and $f_B > 0$ if and only if $\mathrm{rk}(B) \leq n - 2$. Moreover, $f_0 = |G||\mathcal{A}|/|\mathcal{Q}_n|$.*

Proof. We have

$$f_B = \langle F, \chi_B \rangle = \frac{1}{|\mathcal{Q}_n|} \sum_{Q \in \mathcal{Q}_n} F(Q) \overline{\chi_B(Q)}$$

$$= \frac{1}{|\mathcal{Q}_n|} \sum_{Q \in \mathcal{Q}_n} \left(\sum_{g \in G} 1_{\mathcal{A}^g}(Q) \overline{\chi_B(Q)} \right)$$

$$= \frac{1}{|\mathcal{Q}_n|} \sum_{g \in G} \left(\sum_{Q \in \mathcal{A}^g} \overline{\chi_B(Q)} \right).$$

Let $\mathcal{A}^\perp = \{B \in \mathcal{S}_n : (Q, B) = 1 \text{ for all } Q \in \mathcal{A}\}$. Then, from the property (21) of the pairing, $(\mathcal{A}^g)^\perp = (\mathcal{A}^\perp)^{g^{-t}}$ (where g^{-t} denotes the transpose of the inverse of g), and, because $\mathcal{A}^g$ is a subgroup of $\mathcal{Q}_n$,

$$\sum_{Q \in \mathcal{A}^g} \chi_B(Q) = \begin{cases} 0 & \text{if } B \notin (\mathcal{A}^\perp)^{g^{-t}} \\ |\mathcal{A}^g| = |\mathcal{A}| & \text{if } B \in (\mathcal{A}^\perp)^{g^{-t}}. \end{cases}$$

So, we find

$$f_B = \frac{|\mathcal{A}|}{|\mathcal{Q}_n|} |\{g \in G : B^{g^t} \in \mathcal{A}^\perp\}|. \tag{31}$$

From (31), it is clear that $f_B \geq 0$. Moreover, we see that $f_B > 0$ if and only if the orbit of B intersects $\mathcal{A}^\perp$. Going back to the definitions of $\mathcal{A}$ (18) and of the pairing (20), we see that $\mathcal{A}^\perp = \{B' \in \mathcal{S}_n : B'_{1,j} = B'_{2,j} = 0 \text{ for all } 1 \leq j \leq n\}$. So, the orbit of B intersects $\mathcal{A}^\perp$ if and only if $\mathrm{rk}(B) \leq n - 2$. The expression for f_0 follows from (31). $\square$

Going back to Σ in (29), we have:

$$\Sigma = \sum_{B \in \mathcal{S}_n} f_B \Big(\sum_{(Q,Q') \in \mathcal{C}^2} \chi_B(Q - Q') \Big) = \sum_{B \in \mathcal{S}_n} f_B \Big| \sum_{Q \in \mathcal{C}} \chi_B(Q) \Big|^2 \geq f_0 |\mathcal{C}|^2 \tag{32}$$

where, in the last inequality, we have neglected the contributions of all the characters except that of the trivial one; the non negativity of the coefficients f_B is crucial in this step.

Now we recap our findings: from (30), (32) and Lemma 28,

$$|G||\mathcal{C}| = \Sigma \geq \frac{|G||\mathcal{A}|}{|\mathcal{Q}_n|} |\mathcal{C}|^2.$$

So, we obtain after simplification, the inequality $1 \geq (|\mathcal{A}|/|\mathcal{Q}_n|)|\mathcal{C}|$; this inequality is nothing more than (19). The interesting point here is that the equality $1 = (|\mathcal{A}|/|\mathcal{Q}_n|)|\mathcal{C}|$ holds if and only if the neglected terms in (32) are equal to zero, leading, in the case of a hypothetical optimal code, to the conditions

$$\sum_{Q \in \mathcal{C}} \chi_B(Q) = 0 \qquad \text{if } f_B > 0, \ B \neq 0. \tag{33}$$

From Lemma 28, we know that $f_B > 0$ if and only if $\mathrm{rk}(B) \leq n - 2$. Let $s = (r, e)$ where $1 \leq r \leq n-2$; observing that the condition $f_B > 0$ holds simultaneously for all the elements of the orbit $\mathcal{O}_s$ allows us to sum up the equations (33) over $B \in \mathcal{O}_s$. The expression $\sum_{B \in \mathcal{O}_s} \chi_B(Q) = \sum_{B \in \mathcal{O}_s}(Q, B)$ only depends on the type of Q, since

$$\sum_{B \in \mathcal{O}_s} (Q^g, B) = \sum_{B \in \mathcal{O}_s} (Q, B^{g^t}) = \sum_{B' \in \mathcal{O}_s} (Q, B'),$$

so the definition (26) of $\chi_s(t)$ is consistent and we obtain that

$$\sum_{t \in \mathcal{T}_n} \chi_s(t) X_t = \sum_{B \in \mathcal{O}_s} \Big(\sum_{Q \in \mathcal{C}} \chi_B(Q) \Big) = 0.$$

$\square$

6.3. **A change of variables.** Let us recapitulate what we have achieved by now:

Proposition 29. *Suppose $\mathcal{C} \subset \mathcal{Q}_n$ is such that $0 \in \mathcal{C}$, $\mathrm{wt}(\mathcal{C}) \geq 3$ and $|\mathcal{C}| = q^{(n-1)(n-2)/2}$. Then,*

$$X_t := |\mathcal{C} \cap \mathcal{O}_t| \quad (t \in \mathcal{T}_n)$$

satisfy the following equations:

$$\begin{cases} (i) & X_0 = 1 \\ (ii) & X_t = 0 \quad \text{for } t = (1,0), (2,1), (2,-1), (3,0), (4,1) \\ (iii) & \sum_{t \in \mathcal{T}_n} X_t = q^{(n-1)(n-2)/2} \\ (iv) & \sum_{t \in \mathcal{T}_n} \chi_s(t) X_t = 0 \quad \text{for all } s = (r, e), \ 1 \leq r \leq n-2 \end{cases} \tag{34}$$

(34) is a linear system of equations with $|\mathcal{T}_n|$ unknowns (the variables X_t) and $|\mathcal{T}_n| + 3$ equations. So, if we are reasonably lucky, this linear system has no solutions, which in turn proves the non existence of the code $\mathcal{C}$. Unfortunately, only a few of the unknowns are equal to zero so we cannot easily reduce the size of this system, and moreover, we so far have no closed expression for the coefficients $\chi_s(t)$. In order to overcome these issues, we will introduce a change of variables, whose effect will be to 'exchange' variables and equations, the end result yielding a very small linear system.

Proposition 30. *Suppose $\mathcal{C} \subset \mathcal{Q}_n$ is such that $0 \in \mathcal{C}$, $\mathrm{wt}(\mathcal{C}) \geq 3$ and $|\mathcal{C}| = q^{(n-1)(n-2)/2}$. Let*

$$X_t := |\mathcal{C} \cap \mathcal{O}_t| \quad (t \in \mathcal{T}_n)$$

and let

$$Y_s := \frac{1}{|\mathcal{C}|} \sum_{t \in \mathcal{T}_n} \chi_s(t) X_t \quad (s \in \mathcal{T}_n).$$

The numbers Y_s satisfy the following equations:

$$
\begin{cases}
(i') & Y_0 = 1 \\
(ii') & Y_s = 0 \quad \text{for all } s = (r, e), \ 1 \leq r \leq n - 2 \\
(iii') & \sum_{s \in \mathcal{T}_n} Y_s = q^{2n-1} \\
(iv') & \sum_{s \in \mathcal{T}_n} \frac{\chi_s(t)}{|\mathcal{O}_s|} Y_s = 0 \quad t = (1,0), (2,1), (2,-1), (3,0), (4,1)
\end{cases}
\tag{35}
$$

Proof. The new variables Y_t are related to the coefficients $\{\lambda_B, \ B \in \mathcal{S}_n\}$ of the characteristic function $1_\mathcal{C}$ of $\mathcal{C}$ on the basis of characters:

$$1_\mathcal{C} = \sum_{B \in \mathcal{S}_n} \lambda_B \chi_B. \tag{36}$$

Indeed, we have

$$\lambda_B = \langle 1_\mathcal{C}, \chi_B \rangle = \frac{1}{|\mathcal{Q}_n|} \sum_{Q \in \mathcal{C}} \overline{\chi_B(Q)}, \tag{37}$$

so

$$\sum_{B \in \mathcal{O}_s} \lambda_B = \frac{1}{|\mathcal{Q}_n|} \sum_{Q \in \mathcal{C}} \left(\sum_{B \in \mathcal{O}_s} (Q, -B) \right) = \frac{1}{|\mathcal{Q}_n|} \sum_{t \in \mathcal{T}_n} \chi_s(t) X_t$$

and thus

$$Y_s = \frac{|\mathcal{Q}_n|}{|\mathcal{C}|} \sum_{B \in \mathcal{O}_s} \lambda_B. \tag{38}$$

Let us verify the equations $(i') - (iv')$. From (38), $Y_0 = \frac{|\mathcal{Q}_n|}{|\mathcal{C}|} \lambda_0$ and from (37), $\lambda_0 = \frac{|\mathcal{C}|}{|\mathcal{Q}_n|}$ so we find (i'). The equations (ii') follow immediately from (iv). From (37) and (36), we obtain (iii'):

$$\sum_{s \in \mathcal{T}_n} Y_s = \frac{|\mathcal{Q}_n|}{|\mathcal{C}|} \sum_{B \in \mathcal{S}_n} \lambda_B = \frac{|\mathcal{Q}_n|}{|\mathcal{C}|} 1_\mathcal{C}(0) = q^{2n-1}.$$

It remains to prove $(iv)'$. To this end, we introduce the characteristic function $1_{\mathcal{O}_t}$ of the orbit $\mathcal{O}_t$ of quadratic forms of type t and its decomposition as a linear combination of characters:

$$1_{\mathcal{O}_t} = \sum_{B \in \mathcal{S}_n} \mu_{t,B} \chi_B$$

where

$$\mu_{t,B} = \langle 1_{\mathcal{O}_t}, \chi_B \rangle = \frac{1}{|\mathcal{Q}_n|} \sum_{Q \in \mathcal{O}_t} \overline{\chi_B(Q)} = \frac{1}{|\mathcal{Q}_n|} \sum_{Q \in \mathcal{O}_t} \chi_B(Q)$$

the last equality being because for any $Q \in \mathcal{O}_t$ we have $-Q \in \mathcal{O}_t$ and $\chi_B(-Q) = (-Q, B) = \overline{(Q, B)}$ by definition (20) of (Q, B). Now the expression $\sum_{Q \in \mathcal{O}_t} \chi_B(Q)$ only depends on the

type s of B, and

$$|\mathcal{O}_s|(\sum_{Q\in\mathcal{O}_t}\chi_B(Q)) = \sum_{B\in\mathcal{O}_s}(\sum_{Q\in\mathcal{O}_t}\chi_B(Q))$$

$$= \sum_{Q\in\mathcal{O}_t}(\sum_{B\in\mathcal{O}_s}\chi_B(Q)) = \sum_{Q\in\mathcal{O}_t}\chi_s(t) = |\mathcal{O}_t|\chi_s(t)$$

so

$$\mu_{t,B} = \frac{|\mathcal{O}_t|\chi_s(t)}{|\mathcal{Q}_n||\mathcal{O}_s|}. \tag{39}$$

Then,

$$X_t = |\mathcal{Q}_n|\langle 1_{\mathcal{O}_t}, 1_{\mathcal{C}}\rangle = |\mathcal{Q}_n|\sum_{B\in\mathcal{S}_n}\mu_{t,B}\lambda_B.$$

Taking account of (39) and of (38), we find

$$X_t = |\mathcal{O}_t|\sum_{B\in\mathcal{S}_n}\frac{\chi_s(t)}{|\mathcal{O}_s|}\lambda_B = |\mathcal{O}_t|\sum_{s\in\mathcal{T}_n}\frac{\chi_s(t)}{|\mathcal{O}_s|}(\sum_{B\in\mathcal{O}_s}\lambda_B)$$

$$= \frac{|\mathcal{O}_t||\mathcal{C}|}{|\mathcal{Q}_n|}\sum_{s\in\mathcal{T}_n}\frac{\chi_s(t)}{|\mathcal{O}_s|}Y_s.$$

The above relation between X_t and Y_s shows that (ii) is equivalent to (iv'). $\qquad\square$

If the code $\mathcal{C}$ is a linear subspace of $\mathcal{Q}_n$, the numbers Y_s have a combinatorial interpretation in terms of the dual code

$$\mathcal{C}^\perp = \{B\in\mathcal{S}_n \ : \ (Q,B) = 1 \text{ for all } Q\in\mathcal{C}\}.$$

Indeed, it follows from the Poisson summation formula that $Y_s = |\mathcal{C}^\perp\cap\mathcal{O}_s|$. Moreover, it now follows from Proposition 30 that we have a remarkable connection between linear codes of quadratic forms endowed with the weight distance, and linear codes of symmetric bilinear forms endowed with the rank distance, namely:

Corollary 31. *If $\mathcal{C}$ is a linear subspace of $\mathcal{Q}_n$ of dimension $(n-1)(n-2)/2$ and minimum weight 3, then $\mathcal{C}^\perp$ is a linear subspace of $\mathcal{S}_n$ of dimension $2n-1$ and minimum rank $n-1$.*

Codes of symmetric bilinear forms for the rank distance have been studied in [27] and [28]. In particular, the tight upper bound of q^{n+1} is proved for a linear code of minimum rank at least $n-1$, if q is even and n is even ([27]), and if q is odd ([28]). Noting that $n+1 < 2n-1$ if and only if $n\geq 3$, we have therefore that Corollary 31 together with [28] proves Theorem 18 for q odd and hence Theorem 3 for q odd. For even q, the results of [27] together with Corollary 31 yield Theorem 18 with the additional hypothesis that $\dim(A)$ is even. If we remark that Lemma 15 proves that under the hypothesis of Theorem 3 the 2-atom A can not have odd dimension, then we obtain a proof of Theorem 3 for finite fields with q even.

In the next section we shall nevertheless give a self-contained proof that the system (35) has no solutions over the real numbers. This will give us a complete proof of Theorem 18 which is of independent interest besides being a stepping stone towards Theorem 3.[1]

6.4. **Solving the linear system satisfied by** $\{Y_s, \ s \in \mathcal{T}_n\}$**.** The linear system (35) is much more friendly than (34) because it can be re-written as a linear system in only three variables (depending on the parity of n, $\{Y_{(n-1,0)}, Y_{(n,-1)}, Y_{(n,1)}\}$ or $\{Y_{(n-1,-1)}, Y_{(n-1,1)}, Y_{(n,0)}\}$) and six equations. In order to prove that this linear system doesn't have any solutions when $n \geq 3$, it will be enough to take account of the equations (iv') associated to the types $t = (1,0), (2,1), (2,-1)$, and thus to compute the values of $\chi_s(t)$ for $s = (n,e), (n-1,e)$ and $t = (1,0), (2,1), (2,-1)$. These numbers are the so-called P-*numbers* of the association scheme defined by the action of G on $\mathcal{Q}_n$ ([1]) and they could be derived from [7] and [28]. In order to keep this paper self-contained, we offer a direct computation in the appendix. We obtain the following systems of equations:

Lemma 32. *With the notation of Proposition 30, let* $Y = (Y_{(n-1,0)}, Y_{(n,1)}, Y_{(n,-1)})$ *if* n *is even, and* $Y = (Y_{(n-1,1)}, Y_{(n-1,-1)}, Y_{(n,0)})$ *if* n *is odd, then*

$$MY^t = (q^{2n-1} - 1, -1, -1, -1)^t$$

where:

(1) *If* n *is even and* $p = 2$,

$$M = \begin{bmatrix} 1 & 1 & 1 \\ \frac{-1}{q^n-1} & 1 & \frac{-1}{q^n-1} \\ \frac{q^n-2q^{n-1}+1}{(q^n-1)(q^{n-1}-1)} & \frac{-1}{q^{n-1}-1} & \frac{-1}{q^n-1} \\ \frac{-1}{q^{n-1}-1} & \frac{-1}{q^{n-1}-1} & \frac{q^{n-1}+1}{(q^n-1)(q^{n-1}-1)} \end{bmatrix}$$

(2) *If* n *is odd and* $p = 2$,

$$M = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \frac{-1}{q^n-1} & \frac{-1}{q^n-1} \\ \frac{-1}{q^n-1} & \frac{q^n-2q^{n-1}+1}{(q^n-1)(q^{n-1}-1)} & \frac{-1}{q^n-1} \\ \frac{-1}{q^n-1} & \frac{q^n+1}{(q^n-1)(q^{n-1}-1)} & \frac{-1}{q^n-1} \end{bmatrix}$$

(3) *If* n *is even and* $p \neq 2$,

$$M = \begin{bmatrix} 1 & 1 & 1 \\ \frac{-1}{q^n-1} & \frac{q^{n/2}-1}{q^n-1} & \frac{-q^{n/2}-1}{q^n-1} \\ \frac{q^n-2q^{n-1}+1}{(q^n-1)(q^{n-1}-1)} & \frac{-q^{n-1}-q^{n/2-1}(q-1)+1}{(q^n-1)(q^{n-1}-1)} & \frac{-q^{n-1}+q^{n/2-1}(q-1)+1}{(q^n-1)(q^{n-1}-1)} \\ \frac{-1}{q^{n-1}-1} & \frac{q^{n-1}-q^{n/2-1}(q+1)+1}{(q^n-1)(q^{n-1}-1)} & \frac{q^{n-1}+q^{n/2-1}(q+1)+1}{(q^n-1)(q^{n-1}-1)} \end{bmatrix}$$

---

[1]Additionally, this will enable us to derive a proof of Theorem 3 that avoids relying on the preprint [28] which at the time of writing is as yet unpublished.

(4) *If n is odd and $p \neq 2$,*

$$M = \begin{bmatrix} 1 & 1 & 1 \\ \dfrac{q^{(n+1)/2}-1}{q^n-1} & \dfrac{-q^{(n+1)/2}-1}{q^n-1} & \dfrac{-1}{q^n-1} \\ \dfrac{q^n-2q^{n-1}+1-q^{(n-1)/2}(q-1)}{(q^n-1)(q^{n-1}-1)} & \dfrac{q^n-2q^{n-1}+1+q^{(n-1)/2}(q-1)}{(q^n-1)(q^{n-1}-1)} & \dfrac{-1}{q^n-1} \\ \dfrac{q^n+1-q^{(n-1)/2}(q+1)}{(q^n-1)(q^{n-1}-1)} & \dfrac{q^n+1+q^{(n-1)/2}(q-1)}{(q^n-1)(q^{n-1}-1)} & \dfrac{-1}{q^n-1} \end{bmatrix}$$

The following proposition will conclude the proof of Theorem 21.

Proposition 33. *The linear systems defined in Lemma 32 have no solutions if $n \geq 3$.*

Proof. By brute force: we solve for the first three equations; it turns out that there is a unique solution Y^*, and then we evaluate the left hand side of the last equation at Y^*, and observe that it cannot be equal to -1 unless $n = 1, 2$. We skip the details.

(1) If n is even and $p = 2$,

$$Y^* = \left(\frac{(q^n - 1)(q^{n-1} - 1)}{q - 1}, q^{n-1} - 1, \frac{(q^n - 1)(q^n - 2q^{n-1} + 1)}{q - 1} \right)$$

and the LHS of the last equation evaluated at Y^* is equal to

$$-1 - 2\frac{q^n(q^{n-2} - 1)}{(q - 1)(q^{n-1} - 1)}.$$

(2) If n is odd and $p = 2$,

$$Y^* = \left(q^{n-1} - 1, \frac{q(q^{n-1} - 1)^2}{q - 1}, (q^{2n-1} - 1) - \frac{(q^{n-1} - 1)}{q - 1} \right)$$

and the LHS of the last equation evaluated at Y^* is equal to

$$-1 + 2\frac{q^n(q^{n-1} - 1)}{(q - 1)(q^n - 1)}.$$

(3) If n is even and $p \neq 2$,

$$Y^* = \left(\frac{(q^n - 1)(q^{n-1} - 1)}{q - 1}, \frac{(q^{2n-1} - 1)}{2} + \frac{(q^{n/2}(q - 1) - 1)(q^{n-1} - 1)}{2(q - 1)}, \right.$$
$$\left. \frac{(q^{2n-1} - 1)}{2} + \frac{(-q^{n/2}(q - 1) - 1)(q^{n-1} - 1)}{2(q - 1)} \right)$$

and the LHS of the last equation evaluated at Y^* is equal to

$$-1 - 2\frac{q^n(q^{n-2} - 1)}{(q - 1)(q^{n-1} - 1)}.$$

(4) If n is odd and $p \neq 2$,

$$Y^* = \Big(\frac{(q^{n-1}-1)(q^{(n-1)/2}+1)(q^{(n+1)/2}-1)}{2(q-1)},$$

$$\frac{(q^{n-1}-1)(q^{(n-1)/2}-1)(q^{(n+1)/2}-1)}{2(q-1)},$$

$$(q^{2n-1}-1) - \frac{(q^{n-1}-1)}{q-1} \Big)$$

and the LHS of the last one at Y^* is equal to

$$-1 + 2\frac{q^n(q^{n-1}-1)}{(q-1)(q^n-1)}.$$

$\square$

7. Transcendental extensions

We now suppose that the two finite-dimensional subspaces S and T are such that $\dim_F(ST) = \dim_F(S) + \dim_F(T) - 1$ but that they live in an infinite dimensional extension L/F, with no element of $L \setminus F$ algebraic over F. When $\dim(S), \dim(T) \geq 2$, can we conclude that S and T have bases in geometric progression as in Theorem 3 ? It is natural to search for guidance in the classical additive setting: it is much easier to prove in the set $\mathbb{Z}$ of integers than in $\mathbb{Z}/p\mathbb{Z}$, that if $|S|, |T| \geq 2$ and $|S+T| = |S| + |T| - 1$, then S and T must be arithmetic progressions. This leads us to think that the case of infinite extensions should be easier than the case of finite extensions. This turns out to be true, but only in part. Transcendental extensions have valuation rings which allow us to transfer the structure of spaces with small products to sets with small sumsets in totally ordered abelian groups. This method has limitations however as we develop below.

We first deal with the case when F is algebraically closed: in this case the valuation approach is straightforward.

Theorem 34. *Let F be an algebraically closed field and let L/F be a non-trivial extension of F. Let S, T be subspaces of L such that $\dim(S) \geq 2, \dim(T) \geq 2$ and*

$$\dim(ST) = \dim(S) + \dim(T) - 1.$$

Then there are bases of S and T of the form $\{g, ga, \ldots ga^{\dim(S)-1}\}$ and $\{g', g'a, \ldots, g'a^{\dim(T)-1}\}$ for some $g, g', a \in L$.

Proof. From Section 2 it suffices to show that there exists a space A of dimension 2 such that $\dim(SA) = \dim(S) + 1$. The result will therefore follow by induction if we can show that when $\dim(T) > 2$, there exists a subspace of T' such that $\dim(T') = \dim(T) - 1$ and $\dim(ST') \leq \dim(S) + \dim(T') - 1$. Without loss of generality we may suppose that L is the subfield generated by S and T, hence its transcendence degree is finite, in other words L is a function field. Since there always exists a place of L, by composition of places we

may choose a place with values in an algebraic extension of F which is F because F is algebraically closed. This place is equivalent to a valuation ring with residual field equal to F (e.g. Lang [18, Ch. 7]). We may now choose a basis $(\tau_1, \tau_2, \ldots, \tau_t)$ of T such that $v(\tau_1) > v(\tau_2) > \cdots > v(\tau_t)$ where v is the valuation function. Setting T' to be the subspace generated by $\tau_1, \ldots, \tau_{t-1}$, we see that elements of ST of minimum valuation can not exist in ST'. Therefore $\dim(ST') < \dim(ST)$ so that $\dim(ST') \leq \dim(S) + \dim(T') - 1$ and we are done. $\qquad\square$

The above approach extends to every case when we can guarantee the existence of a place of L with values in F. However when F is not algebraically closed, it may happen that L has no F-valued places in which case we can only guarantee the existence of places with values in an algebraic extension of F. In this type of situation we can hope to obtain a result through the valuation approach only if we already have a version of Vosper's Theorem for finite extensions. We illustrate this below by extending Theorem 3 to transcendental extensions of finite fields.

Theorem 35. *Let F be the finite field $\mathbb{F}_q$ with q elements and let L/F be an infinite extension such that no element of $L \setminus F$ is algebraic over F. Let S, T be subspaces of L such that $\dim(S) \geq 2, \dim(T) \geq 2$ and*

$$\dim(ST) = \dim(S) + \dim(T) - 1.$$

Then there are bases of S and T of the form $\{g, ga, \ldots ga^{\dim(S)-1}\}$ and $\{g', g'a, \ldots, g'a^{\dim(T)-1}\}$ for some $g, g', a \in L$.

Proof. As in the proof of Theorem 34, we are done if we can exhibit a subspace T' of codimension 1 in T such that $\dim(ST') \leq \dim(S) + \dim(T') - 1$.

By the Lang-Weil estimation of the number of rational points of an algebraic variety, for any sufficiently large m there exists a place of L with values in the finite extension $\mathbb{F}_{q^m}$ of $F = \mathbb{F}_q$ [19, Cor 4]. From this we have a valuation v from L into an ordered abelian group, together with a valuation ring $\mathcal{O}$ in L made up of all elements of non-negative valuation. If P is the maximal ideal of $\mathcal{O}$ made up of all elements of positive valuation, we have the isomorphism $\mathcal{O}/P \xrightarrow{\sim} \mathbb{F}_{q^m}$. We chose m to be prime and such that $m \geq \dim(ST) + 2$.

Without loss of generality, translating T if need be, we may suppose that the minimum valuation of elements of T is 0. Let $T_P = T \cap P$ and decompose T as $T = T_0 \oplus T_P$ where T_0 is any subspace of T in direct sum with T_P. Note that since 0 is the minimum valuation in T, we have that $T_0 \neq \{0\}$ and all non-zero elements of T_0 are of valuation 0. Let $S = S_0 + S_P$ be a similar decomposition.

We clearly have $ST \supset S_0 T_0 + S_P T_P$. Now let E be a maximal subspace of $S_0 T_0$ all of whose non-zero elements have valuation zero. We therefore have

$$ST \supset E \oplus S_P T_P.$$

We make the remark that if $s \in S_0$ and if τ is an element of T_P of minimum valuation, then the valuation of $s\tau$ equals the valuation of τ and does not belong to the set of valuations of

the space $E + S_P T_P$. Therefore $s\tau \notin E + S_P T_P$ and

$$\dim(ST) \geq \dim(E) + \dim(S_P T_P) + 1. \tag{40}$$

The map $\pi : \mathcal{O} \to \mathcal{O}/P$ is injective on E and we have

$$\dim(E) = \dim(\pi(E)) = \dim(\pi(S_0)\pi(T_0)).$$

By the Cauchy-Davenport inequality (Theorem 2) applied in the extension $\mathcal{O}/P$ of F, i.e. in $\mathbb{F}_{q^m}/\mathbb{F}_q$, we have that $\dim(E) \geq \dim(S_0) + \dim(T_0) - 1$. From the Cauchy-Davenport inequality applied in L we have that $\dim(S_P T_P) \geq \dim(S_P) + \dim(T_P) - 1$. Since $\dim(ST) = \dim(S) + \dim(T) - 1$ by the hypothesis of the Theorem, (40) implies that both the above inequalities must be equalities so that we have

$$\dim(\pi(S_0 T_0)) = \dim(E) = \dim(S_0) + \dim(T_0) - 1.$$

Now if $\dim(S_0) \geq 2$ and $\dim(T_0) \geq 2$, because we have chosen the extension $\mathbb{F}_{q^m}$ sufficiently large, Theorem 3 applies in $\mathbb{F}_{q^m}/\mathbb{F}_q$ and there exists a subspace T_0' of T_0 of codimension 1 such that $\dim(\pi(S_0)\pi(T_0')) < \dim(\pi(S_0)\pi(T_0))$ and $T' = T_0' \oplus T_P$ is the required subspace of T of codimension 1. If either $\dim(S_0) = 1$ or $\dim(T_0) = 1$, then $T' = T_0' + T_P$ for any subspace T_0' of codimension 1 of T_0 again yields the required subspace of T. $\square$

8. Concluding Comments

- An alternative proof of Theorem 34 follows from a version of Theorem 18 for algebraically closed fields F. To obtain this, we need the equivalent of Theorem 21. We actually have a stricter upper bound. We only deal with odd characteristic:

Theorem 36. *If F is algebraically closed of odd characteristic, and if $\mathcal{C} \subset \mathcal{Q}_n$ is a linear space, such that $\mathrm{wt}(\mathcal{C}) \geq 3$, then $\dim(\mathcal{C}) \leq n(n+1)/2 - (4n-6)$.*

Proof. If F is algebraically closed, up to $F^* \times \mathrm{Gl}(n, F)$-equivalence, x_1^2 is the only anisotropic form, from which it follows fairly easily that for a quadratic form Q,

$$\mathrm{wt}(Q) \geq 3 \iff \mathrm{rk}(Q) \geq 5.$$

We identify $\mathcal{Q}_n$ with the space $\mathcal{S}_n$ of symmetric matrices over F. We introduce $\mathcal{R}_4 := \{S \in \mathcal{S}_n : \mathrm{rk}(S) \leq 4\}$, which is an algebraic variety over F (because the rank condition is equivalent to the condition that the minors of order 5 vanish, and the minors are polynomials in the matrix coefficients). The assumption $\mathrm{wt}(\mathcal{C}) \geq 3$ translates to $\mathcal{C} \cap \mathcal{R}_4 = \{0\}$ which implies that $\dim(\mathcal{C}) + \dim(\mathcal{R}_4) \leq \dim(\mathcal{S}_n) = n(n+1)/2$ (see [14]) so it remains to compute $\dim(\mathcal{R}_4)$. The variety $\mathcal{R}_4$ splits into 5 orbits under the action of $\mathrm{Gl}(n, F)$, with representatives of the form

$$\left(\begin{array}{c|c} S_0 & 0 \\ \hline 0 & 0 \end{array} \right)$$

where

$$S_0 \in \left\{ (0), (1), \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \right\}.$$

Each of these orbits can be identified with the quotient space $\mathrm{Gl}(n, F)/O((\begin{smallmatrix} S_0 & 0 \\ 0 & 0 \end{smallmatrix}))$ where $O((\begin{smallmatrix} S_0 & 0 \\ 0 & 0 \end{smallmatrix}))$ denotes the orthogonal group of the form $S := (\begin{smallmatrix} S_0 & 0 \\ 0 & 0 \end{smallmatrix})$. We assume $S_0 \neq (0)$ since in this case the orbit is reduced to one point. Let $U \in O(S)$, and let us write $U = (\begin{smallmatrix} U_{1,1} & U_{1,2} \\ U_{2,1} & U_{2,2} \end{smallmatrix})$ according to the block structure of S. Then, a straightforward verification shows that the condition $U^t S U = S$ translates to: $U_2 = 0$ and $U_1 \in O(S_0)$. There are no constraints on U_3; the only condition on U_4 is $U_4 \in \mathrm{Gl}(n - n_0, F)$ where $n_0 = \mathrm{rk}(S_0)$ (so that $U \in \mathrm{Gl}(n, F)$). Putting everything together, we find that $\dim(O(S)) = \dim(O(S_0)) + n_0(n - n_0) + \dim(\mathrm{Gl}(n - n_0)) = \dim(O(S_0)) + n(n - n_0)$, and the corresponding orbit in $\mathcal{R}_4$ has dimension $nn_0 - \dim(O(s_0)) = nn_0 - n_0(n_0 - 1)/2$. $\qquad\square$

- Theorem 35 follows also from Proposition 17 and Theorem 18. However the alternative proof given in Section 7 serves to illustrate that versions of Vosper's theorem for an infinite dimensional extension will require a finite-dimensional theorem as a stepping stone.
- What is the minimum dimension of the square of a Sidon space ? This question is quite intriguing and very much open even in the case of finite fields. It is likely that the upper bound claimed in Theorem 21 is far from tight, and that it would be possible to greatly improve it by pursuing the Delsarte methodology further. For finite fields this would yield a lower bound on the minimum dimension of the square of a Sidon space that improves upon Theorem 18.
- The central question left open is that of a complete characterisation of the critical spaces achieving equality in the Cauchy-Davenport inequality of Theorem 2. The example at the end of section 5 shows that it is not true for all base fields that all such pairs $\{S, T\}$ of spaces have bases in geometric progression whenever $\dim(S), \dim(T), \mathrm{codim}(ST) \geq 2$. We also note that for finite non-separable extensions, the methods of this paper break down completely.

References

[1] E. Bannai and T. Ito, *Algebraic Combinatorics I: association schemes*, Benjamin/Cummings Pub. Co., 1984.

[2] P. Delsarte, An algebraic approach to the association schemes of coding theory, *Philips Research Repts Suppl.* 10, 1 97, 1973.

[3] P. Delsarte, Bilinear forms over a finite field, with applications to coding theory, *J. Combin. Theory Ser. A*, 25(3) (1978.), 226-241.

[4] P. DELSARTE AND J. M. GOETHALS, Alternating bilinear forms over $GF(q)$, *J. Combin. Theory Ser. A*, 19(1) (1975), 26–50.

[5] P. DELSARTE AND V. LEVENSHTEIN, Association schemes and coding theory, *IEEE Transactions on Information Theory*, vol. 44(6) (1998), 2477–2504.

[6] S. ELIAHOU AND C. LECOUVEY, On linear versions of some additive theorems. *Linear and multilinear algebra.* 57 (2009) 759–775.

[7] R. FENG, Y. WANG, C. MA AND J. MA, Eigenvalues of association schemes of quadratic forms, *Discrete Mathematics.* 308 (2008), 3023 3047.

[8] G. A. FREIMAN, *Foundations of a structural theory of set addition*, Transl. Math. Monographs 37, Amer. Math. Soc., Providence, RI, 1973.

[9] In memory of Yahya Ould Hamidoune, special issue of European Journal of Combinatorics, Plagne, Serra and Zémor Eds., Vol. 34, 2013.

[10] Y. O. HAMIDOUNE, On the connectivity of Cayley digraphs, *Europ. J. Combinatorics*, 5 (1984), 309–312.

[11] Y. O. HAMIDOUNE, An isoperimetric method in Additive Theory, *J. Algebra* 179 (1996), 622–630.

[12] Y. O. HAMIDOUNE, Some results in Additive Number Theory I: The critical pair Theory, *Acta Arithmetica* 96 (2000) 97–119.

[13] Y. O. HAMIDOUNE, Some additive applications of the isoperimetric approach, Annales de l'Institut Fourier 58(2008), fasc. 6, 2007-2036.

[14] R. HARTSHORNE, *Algebraic Geometry*, GTM 52, Springer.

[15] X. HOU, K.H. LEUNG, AND Q. XIANG, A generalization of an addition theorem of Kneser. *Journal of Number Theory* 97 (2002) 1–9.

[16] J.H.B. KEMPERMAN, On complexes in a semigroup. *Idag. Math.* 18 (1956) 247–254.

[17] M. KNESER, Summenmengen in lokalkompakten abelesche Gruppen, *Math. Zeit.* 66 (1956), 88–110

[18] S. LANG, *Algebra*, Springer, 3rd Edition, 2005.

[19] S. LANG AND A. WEIL, Number of points of varieties over finite fields, *Amer. J. Math.* 76 (1954), 819-827.

[20] C. LECOUVEY, Plünnecke and Kneser type theorems for dimension estimates. *Combinatorica.* 34 (3) (2014) 331–358.

[21] F.J. MACWILLIAMS AND N.J.A. SLOANE *The theory of error-correcting codes*, North-Holland 1977.

[22] H. B. MANN, *Addition Theorems: The Addition Theorems of Group Theory and Number Theory.* Krieger Publishing Company, 1976.

[23] M.B. NATHANSON, *Additive Number Theory. Inverse problems and the geometry of sumsets*, Grad. Texts in Math. 165, Springer, 1996.

[24] J.E. OLSON, On the sum of two sets in a group. *J. Number Theory* 18 (1984) 110–120.

[25] A. PLAGNE, O. SERRA AND G. ZÉMOR, Yahya Ould Hamidoune's mathematical journey: A critical review of his work, *European Journal of Combinatorics*, Vol. 34 (2013) 1207–1222.

[26] I.Z. RUZSA, An application of graph theory to additive number theory, *Scientia, Ser. A* **3** (1989), 97–109.

[27] K.-U. SCHMIDT, Symmetric bilinear forms over finite fields of even characteristic, *Journal of Combinatorial Theory Ser. A*, 117(8) (2010), 1011-1026.

[28] K.-U. SCHMIDT, Symmetric bilinear forms over finite fields with applications to coding theory, `arXiv:1410.7184`

[29] T. TAO AND V. VU, *Additive Combinatorics*, Cambridge University Press, 2006.

[30] D. E. TAYLOR, *The geometry of the classical groups*, Berlin: Heldermann, 1992 (Sigma series on pure mathematics; 9).

[31] G. VOSPER, The critical pairs of subsets of a group of prime order,*J. London Math. Soc.* 31 (1956), 200–205.

[32] Y. WANG, C. WANG, C. MA AND J. MA, Association Schemes of Quadratic Forms and Symmetric Bilinear Forms, *Journal of Algebraic Combinatorics*, 17 (2003), 149 161.

9. APPENDIX: THE COMPUTATION OF THE NEEDED VALUES OF $\frac{\chi_s(t)}{|\mathcal{O}_s|}$

We compute explicit expressions for $\chi_s(t)/|\mathcal{O}_s|$ when $t = (1,0), (2,1), (2,-1)$. It turns out that the formulas are slightly different depending on the parity of q. We start by recalling

the formulas for the number of elements on which a quadratic form vanishes, in terms of its type (see [30, Theorem 11.5]).

Lemma 37. *For $Q \in \mathcal{Q}_n$, let*

$$Z_Q = |\{x \in \mathbb{F}_q^n \ : \ Q(x) = 0\}|.$$

The value of Z_Q only depends on the dimension n and the type $t = (r, e)$ of Q, and will be denoted $Z_{n,t}$. We have:

$$Z_{n,t} = q^{n-1} + eq^{n-r/2-1}(q-1).$$

Proposition 38. *We have, for $s = (r, e)$,*

(1) *Case $t = (1, 0)$*
   (a) *If $p = 2$*

$$\frac{\chi_s(t)}{|\mathcal{O}_s|} = \begin{cases} \dfrac{-1}{q^n - 1} & \text{if } e = 0, -1 \\ 1 & \text{if } e = 1 \end{cases}$$

   (b) *If $p \neq 2$*

$$\frac{\chi_s(t)}{|\mathcal{O}_s|} = \frac{eq^{n-r/2} - 1}{q^n - 1}$$

(2) *Case $t = (2, 1)$*
   (a) *If $p = 2$*

$$\frac{\chi_s(t)}{|\mathcal{O}_s|} = \begin{cases} \dfrac{q^{2n-r-1} - 2q^{n-1} + 1}{(q^n - 1)(q^{n-1} - 1)} & \text{if } e = 0, -1 \\ \dfrac{q^{2n-r-1} - q^n - q^{n-1} + 1}{(q^n - 1)(q^{n-1} - 1)} & \text{if } e = 1 \end{cases}$$

   (b) *If $p \neq 2$*

$$\frac{\chi_s(t)}{|\mathcal{O}_s|} = \frac{q^{2n-r-1} - 2q^{n-1} + 1 - eq^{n-r/2-1}(q-1)}{(q^n - 1)(q^{n-1} - 1)}$$

(3) *Case $t = (2, -1)$*
   (a) *If $p = 2$*

$$\frac{\chi_s(t)}{|\mathcal{O}_s|} = \begin{cases} \dfrac{-q^{2n-r-1} + 1}{(q^n - 1)(q^{n-1} - 1)} & \text{if } e = 0 \\ \dfrac{q^{2n-r-1} - q^n - q^{n-1} + 1}{(q^n - 1)(q^{n-1} - 1)} & \text{if } e = 1 \\ \dfrac{q^{2n-r-1} + 1}{(q^n - 1)(q^{n-1} - 1)} & \text{if } e = -1 \end{cases}$$

   (b) *If $p \neq 2$*

$$\frac{\chi_s(t)}{|\mathcal{O}_s|} = \begin{cases} \dfrac{-q^{2n-r-1} + 1}{(q^n - 1)(q^{n-1} - 1)} & \text{if } e = 0 \\ \dfrac{q^{2n-r-1} + 1 - eq^{n-r/2-1}(q+1)}{(q^n - 1)(q^{n-1} - 1)} & \text{if } e = \pm 1 \end{cases}$$

Proof. In the following, $Q_t = \sum_{i \leq j} a_{i,j}^t x_i x_j$ denotes the representative of the orbit of quadratic forms of type t given in Proposition 22, and analogously $B_s = (b_{i,j}^s)$ denotes the representative of the orbit of symmetric bilinear forms of type s from Proposition 24. We introduce the following notation: if $Q = \sum_{i \leq j} a_{i,j} x_i x_j$ and $B = (b_{i,j})$, we let $b(Q,B) := \sum_{i \leq j} a_{i,j} b_{i,j}$. We recall that $(Q,B) = \alpha(b(Q,B))$, where $\alpha : (\mathbb{F}_q, +) \to (\mathbb{C}^*, \times)$ is a fixed non trivial character. Then,

$$\chi_s(t) = \sum_{B \in \mathcal{O}_s} (Q_t, B) = \frac{1}{|G_s|} \sum_{g \in G} (Q_t, B_s^g)$$

$$= \frac{1}{|G_s|} \sum_{u \in \mathrm{Gl}(n,q)} \left(\sum_{a \in \mathbb{F}_q^*} (Q_t, B_s^{(a,u)}) \right).$$

Due to the standard properties of characters,

$$\sum_{a \in \mathbb{F}_q^*} (Q_t, B_s^{(a,u)}) = \begin{cases} -1 & b(Q_t, B_s^u) \neq 0 \\ q-1 & b(Q_t, B_s^u) = 0 \end{cases}$$

We introduce:

$$N_{s,t} := |\{u \in \mathrm{Gl}(n,q) : b(Q_t, B_s^u) = 0\}|$$

and we have:

$$\chi_s(t) = \frac{1}{|G_s|} (qN_{s,t} - |\mathrm{Gl}(n,q)|) = \frac{|\mathcal{O}_s|}{q-1} \left(\frac{qN_{s,t}}{|\mathrm{Gl}(n,q)|} - 1 \right). \tag{41}$$

Let $\{v_1, \ldots, v_n\}$ denote the column vectors of the matrix $u \in \mathrm{Gl}(n,q)$. We have

$$b(Q_t, B_s^u) = \sum_{i \leq j} a_{i,j}^t (v_i^t B_s v_j). \tag{42}$$

We introduce the quadratic form $Q(x) := x^t B_s x$ and will denote its type by t'; it can be readily verified that, if $p \neq 2$, $t' = s$, and if $p = 2$, $t' = (1,0)$ for $e = 0, -1$ and $t' = 0$ for $e = 1$.

<u>Case 1:</u> $t = (1,0)$. Then, $Q_t = x_1^2$ and $b(Q_t, B_s^u) = v_1^t B_s v_1$. So, with the notation above and that of Proposition 37,

$$N_{s,t} = (Z_{n,t'} - 1)(q^n - q) \ldots (q^n - q^{n-1})$$

$$= (Z_{n,t'} - 1) \frac{|\mathrm{Gl}(n,q)|}{q^n - 1}.$$

The expressions for $\chi_s(t)/|\mathcal{O}_s|$ follow then immediately from the formulas for $Z_{n,t'}$ in Proposition 37 and from (41).

<u>Case 2:</u> $t = (2,1)$. In this case, $Q_t = x_1 x_2$ and $b(Q_t, B_s^u) = v_1^t B_s v_2$. For $w = (v_1, v_2) \in \mathbb{F}_q^{2n}$, $Q(w) := v_1^t B_s v_2$ defines a quadratic form which can be easily seen to be of type $(2r, 1)$. So, the number of $w = (v_1, v_2)$ such that $Q(w) = 0$ is equal to $Z_{2n,(2r,1)}$. Because v_1, v_2 are the two first column vectors of $u \in \mathrm{Gl}(n,q)$, they should not be linearly dependent. The number of (v_1, v_2) such that $Q(w) = 0$ and $\{v_1, v_2\}$ are linearly dependent is: $2q^n - 1 + (q-1)(Z_{n,t'} - 1)$

so we obtain:

$$N_{s,t} = (Z_{2n,(2r,1)} - (q-1)(Z_{n,t'} - 1) - 2q^n + 1)\frac{|\operatorname{Gl}(n,q)|}{(q^n-1)(q^n-q)}.$$

Case 3: $t = (2,-1)$. In this case, Q_t depends on the parity of p. If $p = 2$, $Q_t = x_1^2 + x_1 x_2 + b x_2^2$ and $b(Q_t, B_s^u) = v_1^t B_s v_1 + v_1^t B_s v_2 + b v_2^t B_s v_2$. For $w = (v_1, v_2) \in \mathbb{F}_q^{2n}$, let $Q(w) := v_1^t B_s v_1 + v_1^t B_s v_2 + b v_2^t B_s v_2$. Again, we count the number of (v_1, v_2) such that $Q(w) = 0$ and $\{v_1, v_2\}$ are linearly dependent, and find $1 + (q+1)(Z_{n,t'} - 1)$. We need to determine the type t'' of Q. With some work, we find:

$$\text{If } s = (r,1),\ t'' = (2r,1)$$
$$\text{If } s = (r,0),\ t'' = (2r,-1)$$
$$\text{If } s = (r,-1),\ t'' = (2r,1)$$

so

$$N_{s,t} = (Z_{2n,t''} - (q+1)(Z_{n,t'} - 1) - 1)\frac{|\operatorname{Gl}(n,q)|}{(q^n-1)(q^n-q)}.$$

If $p \neq 2$, $Q_t = x_1^2 - b x_2^2$ and $b(Q_t, B_s^u) = v_1^t B_s v_1 - b v_2^t B_s v_2$. For $w = (v_1, v_2) \in \mathbb{F}_q^{2n}$, let $Q(w) := v_1^t B_s v_1 - b v_2^t B_s v_2$. The number of (v_1, v_2) such that $Q(w) = 0$ and $\{v_1, v_2\}$ are linearly dependent is as in the previous case of $p = 2$ equal to $1 + (q+1)(Z_{n,t'} - 1)$. Also, we find the same type t'' for Q so again

$$N_{s,t} = (Z_{2n,t''} - (q+1)(Z_{n,t'} - 1) - 1)\frac{|\operatorname{Gl}(n,q)|}{(q^n-1)(q^n-q)}.$$

$\square$

Institut de Mathématiques de Bordeaux, UMR 5251, université de Bordeaux, 351 cours de la Libération, 33400 Talence, France.

E-mail address: `Christine.Bachoc@math.u-bordeaux.fr`

Universitat Politècnica de Catalunya, Matemàtica Aplicada IV, Mòdul C3, Campus Nord, Jordi Girona, 1, 08034 Barcelona, Spain.

E-mail address: `oserra@ma4.upc.edu`

Institut de Mathématiques de Bordeaux, UMR 5251, université de Bordeaux, 351 cours de la Libération, 33400 Talence, France.

E-mail address: `zemor@math.u-bordeaux.fr`