Can. J. Math., Vol. XXVII, No. 2, 1975, pp. 271–275

SOME RESULTS ON TOTALLY ISOTROPIC SUBSPACES AND FIVE-DIMENSIONAL QUADRATIC FORMS OVER $GF(q)$

CRAIG M. CORDES

1. Introduction. In [**5**] Pall defined a partitioning of a quadratic space over a field of characteristic not 2 to be a collection of disjoint (except for $\{0\}$) maximal totally isotropic subspaces whose union formed the set of isotropic vectors. Clearly isometric quadratic spaces simultaneously do or do not have partitionings. Pall exhibited the existence of partitionings for the spaces associated with

$$\psi_n = \sum_{i=1}^{n} x_i^2 - \sum_{i=1}^{n} x_{n+i}^2$$

over formally real fields for $n = 1, 2, 4, 8$ and over $Z/(p)$, p prime, for $n = 1, 2$. Using the latter, he was able to find a new proof for Jacobi's formula for the number of representations of a positive integer as the sum of four integral squares. It should be noted that Pall's methods also show the existence of partitionings for ψ_4, ψ_8 over fields with level (Stufe) greater than 2, 4 respectively.

In his thesis, Pall's student, L. Couvillon showed ψ_2 had a partitioning over any field (characteristic not 2). He also proved the non-existence for ψ_n over formally real and finite fields when $n > 1$ is odd. In this paper we will obtain some general results on totally isotropic subspaces and will show that five-dimensional quadratic spaces over $GF(q)$ do not admit partitionings. This is the first case over $GF(q)$ which was not covered by Couvillon.

2. Totally isotropic subspaces. Given a regular quadratic form φ over the finite field $GF(q)$, $2 \nmid q$, we want to find the number of totally isotropic subspaces for every dimension. There are essentially three possibilities for φ:

(1) $\varphi_1 = (1, -1, \ldots, 1, -1)$ with dimension $\varphi_1 = 2n$,

(2) $\varphi_2 = (1, -1, \ldots, 1, -1, d)$ with dim $\varphi_2 = 2n + 1$, and

(3) $\varphi_3 = (1, -1, \ldots, 1, -1, 1, d)$ where $-d$ is not a square and dim $\varphi_3 = 2n + 2$.

By Artin [**1**, p. 146] the number of isotropic vectors for each case is given respectively by $(q^n - 1)(q^{n-1} + 1)$, $q^{2n} - 1$, and $(q^n - 1)(q^{n+1} + 1)$. Denote by $r_k(\varphi)$ the number of distinct totally isotropic subspaces of dimension $n - k + 1$ containing a specified one of dimension $n - k$. Moreover, denote

Received August 14, 1973 and in revised form, March 25, 1974.

https://doi.org/10.4153/CJM-1975-033-8 Published online by Cambridge University Press

by $t_k(\varphi)$ the number of distinct totally isotropic subspaces of dimension $n - k + 1$.

PROPOSITION 1. *Let φ be a regular quadratic form over $GF(q)$ as above. Then*

$$r_k(\varphi) = \frac{(q^k - 1)(q^{k-1} + 1)}{q - 1}, \quad \frac{q^{2k} - 1}{q - 1}, \quad \frac{(q^k - 1)(q^{k+1} + 1)}{q - 1}$$

in cases (1), (2), (3) *respectively. Also*

$$t_k(\varphi) = \frac{t_{k+1} r_k}{(q^{n-k+1} - 1)/(q - 1)}, \quad 1 \leqq k \leqq n$$

where $t_{n+1} = 1$.

Proof. All the cases are similar, so we will just give the proof for case (2). Let U be a fixed totally isotropic subspace with dim $U = n - k$. Then there is subspace U' such that $U \oplus U'$ is an orthogonal sum of $n - k$ hyperbolic planes. So if V is the quadratic space associated with φ, then

$$V = (U \oplus U') \perp H_1 \perp \ldots \perp H_k \perp \langle v \rangle$$

where the H_i are hyperbolic planes and $\varphi(v) = d$. Any $n - k + 1$ dimensional totally isotropic subspace containing U can be written as $U \perp \langle u \rangle$ where $u \in H_1 \perp \ldots \perp H_k \perp \langle v \rangle$ and is isotropic. Furthermore different isotropic lines $\langle u \rangle$ give different $U \perp \langle u \rangle$. The result for r_k now follows by counting the isotropic lines of $H_1 \perp \ldots \perp H_n \perp \langle v \rangle$.

For each of the t_{k+1} subspaces of dimension $n - k$ there are r_k extensions to an $(n - k + 1)$-dimensional one. But the larger spaces could have been extended from any of its $(q^{n-k+1} - 1)/(q - 1)$ $(n - k)$-dimensional subspaces. Thus the result for $t_k(\varphi)$ follows.

COROLLARY. *The number of maximal totally isotropic subspaces is*

$$t_1 = \prod_{i=0}^{n-1} (q^i + 1), \quad \prod_{i=1}^{n} (q^i + 1), \quad \prod_{i=1}^{n} (q^{i+1} + 1)$$

in cases (1), (2), (3) *respectively.*

It is immediate from Witt's Theorem [**4**, p. 98] that the orthogonal group is transitive on any set of totally isotropic subspaces of the same dimension. It is also true that this can be extended to double transitivity with some restrictions. The following lemma is an immediate consequence of a remark by Dieudonné [**3**, p. 21].

LEMMA A. *Let V be a quadratic space and V_1, V_2, W_1, W_2 be totally isotropic subspaces satisfying the following:*

(1) dim V_i = dim W_j, $i, j = 1, 2$,

(2) $V_1 \cap V_2 = W_1 \cap W_2 = \{0\}$,

(3) $V_1 \oplus V_2$ *and* $W_1 \oplus W_2$ *are regular.*

Then there is an isometry σ in the orthogonal group of V such that $\sigma V_i = W_i$, $i = 1, 2$.

This lemma will be applied to partitionings, but first we need a result about maximal totally isotropic subspaces.

PROPOSITION 2. *Let U, W be disjoint maximal totally isotropic subspaces of a regular quadratic space V. Then $U \oplus W$ is regular.*

Proof. If $U \oplus W$ is not regular, then there are $u \in U$, $w \in W$ such that $u + w \neq 0$ is orthogonal to $U \oplus W$. But then $U \oplus \langle w \rangle$, $W \oplus \langle u \rangle$ are both totally isotropic. The maximality of U, W shows $u = w = 0$. This contradicts $u + w \neq 0$. So $U \oplus W$ is regular.

If $\{W_i\}_{i \in I}$ is a partitioning of V and if $\sigma \in O(V)$, then clearly $\{\sigma W_i\}_{i \in I}$ is also a partitioning. So it follows from this, Lemma A, and Proposition 2 that if a partitioning with at least two elements exists, we can assume any two particular disjoint maximal totally isotropic spaces belong to one.

3. Partitionings for five-dimensional spaces over $GF(q)$**.** All regular quadratic forms of dimension five over $GF(q)$ are equivalent to $d\varphi$ where $\varphi = \sum_{i=1}^{5} x_i^2$ and d is the determinant. Since $d\varphi$ has a partitioning if and only if φ does, we need to consider just φ. Note also that $\varphi = (1, 1, 1, 1, 1) \cong (1, -1, 1, -1, 1)$ over $GF(q)$. The quadratic space associated with φ will be called V. Notice that maximal totally isotropic subspaces of V have dimension 2.

PROPOSITION 3. *Let W be the quadratic space over $GF(q)$ associated with $\psi = (1, 1, 1, 1)$. Consider W embedded in V by*

$$W = \{(x_1, x_2, x_3, x_4, 0) | x_i \in GF(q)\}.$$

Then any partitioning of V contains exactly two subspaces of W.

Proof. Let U be a maximal totally isotropic subspace of V which is not contained in W. Then $U + W = V$, and, hence $\dim U \cap W = \dim U + \dim W - \dim(U + W) = 1$. So U contains exactly one line of W.

The number of non-zero isotropic vectors in W is $(q^2 - 1)(q + 1)$ and so W contains $(q + 1)^2$ isotropic lines. These lines must be covered in any partitioning for V. This can be accomplished in two ways: (1) the lines lie in spaces contained in W, or (2) they lie in spaces not contained in W. Suppose there are r subspaces of W in a particular partitioning of V. By the above comment spaces in (2) contain only one line of W while spaces in (1) contain $q + 1$ lines of W. Hence there must be $(q + 1)^2 - r(q + 1)$ spaces not contained in W. V has $q^4 - 1$ non-zero isotropic vectors and so there must be $q^2 + 1$ spaces in a partitioning. Consequently, $q^2 + 1 = (q + 1)^2 - r(q + 1) + r$ or $r = 2$. This completes the proof.

COROLLARY. *Suppose U_1, U_2, U_3 are spaces in a partitioning of V. Then U_3 is not contained in $U_1 \oplus U_2$.*

Proof. Couvillon [**2**, p. 11] showed that W has a partitioning. So in particular there exist two maximal totally isotropic subspaces W_1, W_2 in W such that $W_1 \cap W_2 = \{0\}$. By Lemma A, we can find a $\sigma \in O(V)$ satisfying $\sigma U_i = W_i$, $i = 1, 2$. If $U_3 \subseteq U_1 \oplus U_2$, then $\sigma U_3 \subseteq W_1 \oplus W_2 = W$. But this means there is a partitioning of V with three spaces in W, a contradiction.

As we have seen, if there is a partitioning of V, it must have $q^2 + 1$ elements. By the Corollary to Proposition 1, V contains $(q + 1)(q^2 + 1)$ maximal totally isotropic spaces. If U is one of these spaces not in the partitioning, then each of its $q + 1$ lines must lie in a different member of the partitioning. Denote them by $U_1, \ldots, U_{q+1}$. Since U intersects these U_i, it follows that $U \subseteq U_i \oplus U_j$ for $1 \leqq i \neq j \leqq q + 1$. By the Corollary, $U_i \nsubseteq U_j \oplus U_k$. Our goal is to show that such a situation cannot exist and, hence, neither can a partitioning.

LEMMA. *Let V be the quadratic space associated with* $(1, 1, 1, 1, 1)$. *Suppose V_1, V_2, V_3 are maximal totally isotropic subspaces of V with the properties $V_1 \cap V_i = \{0\}$, $i = 2, 3$ and $V_j \nsubseteq V_1 \oplus V_i$ for $\{i, j\} = \{2, 3\}$. Then $V_1 \oplus V_2$ and $V_1 \oplus V_3$ have in common exactly two maximal totally isotropic subspaces of V, one of which is V_1.*

Proof. Since $V_1 \oplus V_2 \neq V_1 \oplus V_3$, $(V_1 \oplus V_2) + (V_1 \oplus V_3) = V$ and dim $[(V_1 \oplus V_2) \cap (V_1 \oplus V_3)] = 3$. Clearly V_1 is in the intersection so $(V_1 \oplus V_2) \cap (V_1 \oplus V_3) = V_1 \oplus \langle v \rangle$. By Proposition 2, $V_1 \oplus V_2$ is regular so the orthogonal complement of V_1 in $V_1 \oplus V_2$ has dimension 2. In fact $V_1^* = V_1$. So there is a $v_0 \in V_1$ with v_0 not orthogonal to v. If v is not isotropic, then $v + \alpha v_0$ will be for appropriate α. Since $V_1 \oplus \langle v \rangle = V_1 \oplus \langle v + \alpha v_0 \rangle$, this allows us to assume v is isotropic. It is easy to see v is orthogonal to a unique line $\langle v_1 \rangle \subseteq V_1$. Let $V_1 = \langle v_1, v_2 \rangle$. Since v, v_2 are not orthogonal, the isotropic vectors in $V_1 \oplus \langle v \rangle$ are of the form $\alpha v_1 + \beta v_2$ and $\gamma v_1 + \delta v$. But these are orthogonal if and only if $\beta\delta = 0$. So the only two-dimensional totally isotropic subspaces of $V_1 \oplus \langle v \rangle$ are V_1 and $\langle v_1, v \rangle$.

PROPOSITION 4. *Let V be the quadratic space associated with* $(1, 1, 1, 1, 1)$. *Suppose $U_1, \ldots, U_n$ are mutually disjoint* (except for $\{0\}$) *maximal totally isotropic subspaces of V with the property $U_i \nsubseteq U_j \oplus U_k$, $1 \leqq i, j, k \leqq n$. Furthermore, suppose that a two-dimensional subspace U intersects each U_i in a line and that there is a vector u satisfying $u \in U - U_i$, $1 \leqq i \leqq n$. Then, for n odd and $3 \leqq n \leqq q$, there are at most $q - n$ maximal totally isotropic subspaces W of V which contain u and such that $W \nsubseteq U_i \oplus U_j$, $1 \leqq i, j, \leqq n$.*

Proof. U must be totally isotropic, and clearly $U \subseteq U_i \oplus U_j$, $1 \leqq i \neq j \leqq n$. By Proposition 1, there are $q + 1$ maximal totally isotropic subspaces of V containing u and two such spaces in each $U_i \oplus U_j$ (one of which is always U).

Consider the set $\{U_1 \oplus U_j\}_{j=2}^n$. By the lemma, then, the subspaces containing u which are not U must all be different. Thus there are at most $(q + 1) - (n - 1) - 1 = q - n + 1$ possible W. The same technique can be applied to $U_2 \oplus U_j$, $1 \leqq j \leqq n$, $j \neq 2$. If a different set of subspaces are eliminated by this new collection, then the proposition holds. The only problem occurs when exactly the same set of n spaces is eliminated from every collection $\{U_i \oplus U_j\}_{j \neq i}$, $1 \leqq i \leqq n$. Consider just the $n - 1$ non-U spaces. By the lemma, these spaces eliminated by $U_i \oplus U_j$ and $U_i \oplus U_k$ are the same if and only if $j = k$. So if $\{U_1 \oplus U_j\}$ and $\{U_2 \oplus U_j\}$ eliminate the same $n - 1$ non-U-spaces, there must be a correspondence $U_1 \oplus U_j \leftrightarrow U_2 \oplus U_{i_j}$ where $j = 2 \Leftrightarrow i_j = 1$ and otherwise $j \neq i_j$ with $\{i_j\} = \{j\}$, $3 \leqq j \leqq n$. The same holds for every pair of sets $\{U_{i_1} \oplus U_j\}_j$, $\{U_{i_2} \oplus U_j\}_j$. What this means is that there exists an $(n - 1) \times n$ array of ordered pairs (i, j) with $i \neq j$ and the kth column consisting of all (k, j) with j taking on all values from 1 to n (except k) subject to the following conditions: (1) if (k, l) appears in a given row, then so does (l, k), and (2) if (i, j), (k, l) appear in the same row, then either $i = l, j = k$ or $\{i, j\} \cap \{k, l\} = \emptyset$. The rows of this array correspond to the $n - 1$ spaces eliminated and the columns to the sets $\{U_i \oplus U_j\}_j$. But condition (1) and the fact that (i, i) is not in the array is impossible if n is odd since there would have to be an even number of columns. This shows every set $\{U_i \oplus U_j\}_j$ cannot eliminate exactly the same set of spaces so at least one more is removable than the n from $\{U_1 \oplus U_j\}_j$. This completes the proof.

In particular, if $n = q$, there are no spaces that will work. Thus the situation mentioned just before the lemma is impossible, and we can record the following result.

THEOREM. *Let V be any regular five-dimensional quaadratic space over $GF(q)$, $2 \nmid q$. Then V does not have a partitioning.*

References

1. E. Artin, *Geometric algebra* (Interscience, New York, 1957).
2. L. Couvillon, *Partitionings by means of maximal isotropic spaces*, Ph.D. Thesis, Louisiana State University, 1971.
3. J. Dieudonné, *La géometrie des groupes classiques* (Springer-Verlag, Berlin, 1971).
4. O. T. O'Meara, *Introduction to quadratic forms* (Springer-Verlag, New York, 1963).
5. G. Pall, *Partitioning by means of maximal isotropic subspaces*, Linear Algebra and Appl. *5* (1972), 173–180.

Louisiana State University,
Baton Rouge, Louisiana