TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 336, Number 1, March 1993

WITT'S EXTENSION THEOREM FOR MOD FOUR VALUED QUADRATIC FORMS

JAY A. WOOD

ABSTRACT. The mod 4 valued quadratic forms defined by E. H. Brown, Jr. are studied. A classification theorem is proven which states that these forms are determined by two things: whether or not their associated bilinear form is alternating, and the σ-invariant of Brown (which generalizes the Arf invariant of an ordinary quadratic form). Particular attention is paid to a generalization of Witt's extension theorem for quadratic forms. Some applications to self-orthogonal codes are sketched, and an exposition of some unpublished work of E. Prange on Witt's theorem is provided in an appendix.

1. INTRODUCTION

Quadratic forms over fields of characteristic two have a long and distinguished history. Dickson [5] classified nonsingular quadratic forms over the finite fields $GF(2^k)$ of characteristic two. Arf [2], generalizing work of Witt [21], showed that the maximal totally isotropic subspaces for a nonsingular quadratic form have a well-defined dimension. Arf also defined an invariant of quadratic forms which distinguishes inequivalent forms, at least if the field is perfect.

More recently, Quillen used the above information about quadratic forms to help calculate the cohomology rings of extra-special two-groups [18]. In related work, the author has shown that the doubly-even self-orthogonal error-correcting codes can be interpreted as totally isotropic subspaces for the quadratic forms associated to certain extra-special two-groups [23].

One fact of life in dealing with quadratic forms over fields of characteristic two is that the associated bilinear form is necessarily alternating. In certain topological applications involving the cup product on mod 2 cohomology, alternating bilinear forms are unnecessarily restrictive. To remedy this situation, Brown [3] generalized the definition of quadratic forms over $\mathbf{Z}/2$ by allowing the quadratic form to take values in $\mathbf{Z}/4$. Brown then defined a $\mathbf{Z}/8$-invariant σ of $\mathbf{Z}/4$-valued quadratic forms which generalized the Arf invariant.

The purpose of this paper is to prove theorems for Brown's $\mathbf{Z}/4$-valued quadratic forms which are the analogs of the theorems of Dickson and Arf

Received by the editors September 4, 1990 and, in revised form, December 28, 1990.
1991 *Mathematics Subject Classification.* Primary 15A63; Secondary 57R67, 94B05.
Key words and phrases. Quadratic form, Witt's extension theorem, Witt index, self-orthogonal code, isotropic subspace.
Partially supported by NSA grant MDA904-89-H-2041 to Bowdoin College.

mentioned above. In more detail, the contents of this paper are as follows. In §2, we review the basic terminology of quadratic forms, both standard and $\mathbf{Z}/4$-valued, as well as Brown's invariant σ. A classification theorem for $\mathbf{Z}/4$-valued quadratic forms is proved in §3. Nonsingular quadratic forms are characterized by the type of their associated bilinear form (whether alternating or not) and their σ-invariant.

In §4, an extension theorem for isometries is proved which generalizes theorems of Witt and Arf. There are obstructions to extending isometries, and the statement of the extension theorem follows Pless [14, 15] and unpublished work of Prange [17]. Since Prange's proof is of independent interest, we include it in an appendix. Finally, in §5, the dimensions of maximal isotropic subspaces are determined, and some coding theoretic applications are discussed.

Remark. Although ordinary quadratic forms will be defined over any field K of characteristic two, there has been a conscious decision to state most known results only for the case $K = \mathbf{Z}/2$ and to provide a reference for the general case. This is justified: the main topic of the paper is Brown's $\mathbf{Z}/4$-valued quadratic forms, and these forms generalize only the $K = \mathbf{Z}/2$ case. On the other hand, the exposition of the version of the extension theorem due to Prange, which appears in the Appendix, will be over an arbitrary K, since the general version of this work would be otherwise unavailable.

2. Quadratic forms

Throughout this paper, K will denote an arbitrary field of characteristic two. Let V be a finite-dimensional vector space over K, say $n = \dim V$, and let B be a symmetric bilinear form on V with values in K. B is *nonsingular* if, for any nonzero $u \in V$, there exists $v \in V$ with $B(u, v) \neq 0$.

The following definition is standard. A function $Q: V \to K$ is an *ordinary quadratic form* on V associated to B if

$$Q(\lambda u + \mu v) = \lambda^2 Q(u) + \mu^2 Q(v) + \lambda\mu B(u, v),$$

for all $u, v \in V$, $\lambda, \mu \in K$. Q is said to be *nonsingular* if B is nonsingular. Note that $Q(0) = 0$ and that taking $u = v$, $\lambda = \mu = 1$ implies that $B(u, u) = 0$, for all $u \in V$. Consequently, a necessary condition for B to be the bilinear form associated to an ordinary quadratic form Q is that B be alternating.

When Q is nonsingular, V has even dimension $n = 2m$, since B is then a nonsingular symplectic form on V. If the field K is a finite field $GF(2^k)$, Dickson [5, §199] proved that Q is characterized by a normal form. In the case where $K = \mathbf{Z}/2$, a suitable choice of basis for V allows Q to have the form

$$Q(u) = \sum_{i=1}^{m} u_{2i-1}u_{2i}$$

or the form

$$Q(u) = \sum_{i=1}^{m-1} u_{2i-1}u_{2i} + u_{2m-1}^2 + u_{2m-1}u_{2m} + u_{2m}^2,$$

where the u_i are the coefficients of u with respect to the particular basis. These two normal forms can be distinguished by their *Arf invariants* in $\mathbf{Z}/2$, denoted $\operatorname{Arf} Q$, which are 0 and 1, respectively.

Remark. For general K, the Arf invariant is an element of K modulo elements of the form $\lambda + \lambda^2$. Nonsingular quadratic forms over a perfect field K are classified by their Arf invariants. There is the weaker notion of *nondefective* quadratic forms in the literature [7, §I.16], and the Arf invariant actually classifies nondefective quadratic forms. We shall not have occasion to use this more general notion, (see [2; 10, §1.12; 11; 22]).

Brown [3] generalized the definition of a quadratic form over $\mathbf{Z}/2$ in order to allow nonalternating bilinear forms to be associated to a quadratic form. The price paid is that the quadratic form now takes values in $\mathbf{Z}/4$. To be more precise, we follow Brown [3].

The vector space V and bilinear form B are now defined over $\mathbf{Z}/2$. Let $j\colon \mathbf{Z}/2 \to \mathbf{Z}/4$ be the unique nontrivial group homomorphism $(j(1) = 2)$. A $\mathbf{Z}/4$-*valued quadratic form* Q on V associated to B is a function $Q\colon V \to \mathbf{Z}/4$ such that

$$Q(u+v) = Q(u) + Q(v) + jB(u, v),$$

for all $u, v \in V$. Q is said to be *nonsingular* if B is nonsingular. Note that $Q(0) = 0$ and that setting $u = v$ implies that $2Q(u) = jB(u, u)$, for all $u \in V$.

If $Q_i\colon V_i \to \mathbf{Z}/4$ are two such quadratic forms $(i = 1, 2)$, Q_1 is *isomorphic* to Q_2 if there is a linear isomorphism $T\colon V_1 \to V_2$ such that $Q_1 = Q_2 T$. $(Q_1 + Q_2)\colon V_1 \oplus V_2 \to \mathbf{Z}/4$ is defined by $(Q_1 + Q_2)(u, v) = Q_1(u) + Q_2(v)$. $(-Q_1)(u) = -Q_1(u)$. $Q_1 Q_2\colon V_1 \otimes V_2 \to \mathbf{Z}/4$ is the unique quadratic form such that $Q_1 Q_2(u \otimes v) = Q_1(u) Q_2(v)$.

Because Q has values in $\mathbf{Z}/4$, one expects that the sum $\sum_{u \in V} i^{Q(u)}$, where $i = \sqrt{-1}$, will be an invariant associated to Q. The following theorem, due to Brown [3, Theorem 1.20], summarizes the situation.

Theorem (Brown). *There is a unique function σ from nonsingular quadratic forms to $\mathbf{Z}/8$ satisfying*:

(1) *If Q_1 is isomorphic to Q_2, then $\sigma(Q_1) = \sigma(Q_2)$.*
(2) $\sigma(Q_1 + Q_2) = \sigma(Q_1) + \sigma(Q_2)$.
(3) $\sigma(-Q_1) = -\sigma(Q_1)$.
(4) $\sigma(\gamma) = 1$, *where* $\gamma\colon \mathbf{Z}/2 \to \mathbf{Z}/4$ *is* $\gamma(0) = 0$, $\gamma(1) = 1$.

Furthermore, σ satisfies:

(5) $\sigma(Q_1 Q_2) = \sigma(Q_1)\sigma(Q_2)$.
(6) *If* $Q\colon V \to \mathbf{Z}/4$, *then* $\sigma(Q) = \dim V \bmod 2$.
(7) *If* $Q = jQ'$, *where* Q' *is an ordinary* ($\mathbf{Z}/2$-*valued*) *quadratic form on* V, *then* $\sigma(Q) = l(\operatorname{Arf} Q')$, *where* $l\colon \mathbf{Z}/2 \to \mathbf{Z}/8$ *is the homomorphism sending* 1 *to* 4.
(8) *If* U *is a finitely generated free abelian group,* $\theta\colon U \otimes U \to \mathbf{Z}$ *is a symmetric, unimodular form,* $\psi(u) = \theta(u, u)$, *and* $Q\colon U/2U \to \mathbf{Z}/4$ *is defined by* $Q(u) = \psi(u) \bmod 4$, *then* Q *is a quadratic form and*

$$\sigma(Q) = (\text{signature } \psi) \bmod 8.$$

(9) *Suppose* $B\colon V \otimes V \to \mathbf{Z}/2$ *is the bilinear form associated to* $Q\colon V \to \mathbf{Z}/4$, $V_1 \xrightarrow{\nu} V \xrightarrow{\delta} V_2$ *is an exact sequence of* $\mathbf{Z}/2$ *vector spaces, and* $B'\colon V_1 \otimes V_2 \to \mathbf{Z}/2$ *is a nonsingular bilinear form such that* $B'(u, \delta v) = B(\nu u, v)$. *If* $Q\nu = 0$, *then* $\sigma(Q) = 0$.

(10) *If* $Q_1, Q_2: V \to \mathbf{Z}/4$ *have the same bilinear form* B, *then* $Q_2(u) = Q_1(u) + jB(u, x)$ *for some* x *and*

$$\sigma(Q_1) - \sigma(Q_2) = m(Q_1(x)),$$

where $m: \mathbf{Z}/4 \to \mathbf{Z}/8$ *sends* 1 *to* 2.

(11) $\sigma(Q)$ *is related to* Q *by the formula*

$$\sum_{u \in V} i^{Q(u)} = \sqrt{2}^{\dim V} e^{\frac{\pi i \sigma(Q)}{4}},$$

where $i = \sqrt{-1}$.

3. Classification

Recall from §2 that Dickson's normal form implies that ordinary nonsingular quadratic forms over $\mathbf{Z}/2$ are classified by their Arf invariants. The major theorem of this section generalizes this result to Brown's $\mathbf{Z}/4$-valued quadratic forms.

Theorem. *A nonsingular* $\mathbf{Z}/4$*-valued quadratic form* Q *is determined up to isomorphism by* $\sigma(Q)$ *and whether its associated bilinear form* B *is alternating or not.*

Proof. By hypothesis, the bilinear form B is nonsingular. Because Q satisfies $2Q(u) = jB(u, u)$, for all $u \in V$, Q is of the form $Q = jQ'$, with Q' an ordinary quadratic form, if and only if B is alternating. In this case, property (7) of σ in Brown's theorem says that $\sigma(Q)$ is just $\operatorname{Arf} Q'$, suitably interpreted. Since $\operatorname{Arf} Q'$ classifies nonsingular ordinary quadratic forms, $\sigma(Q)$ classifies nonsingular $\mathbf{Z}/4$-valued quadratic forms with B alternating.

The remaining case of interest is when B is nonalternating (and nonsingular, still). By a procedure going back to Veblen and Franklin [19, §17], V admits a B-orthogonal basis $e_1, e_2, \ldots, e_n$, where $n = \dim V$. (This theorem was generalized to all K by Albert [1, p. 392]; also see [10, p. 23].) Because B has values in $\mathbf{Z}/2$, $B(e_i, e_i) = 1$, for all i. Making use of the relation

$$Q(u + v) = Q(u) + Q(v) + jB(u, v),$$

we see that Q is completely determined by its values on the orthogonal basis elements. Since $2Q(e_i) = jB(e_i, e_i) = 2$, $Q(e_i) = \pm 1$. We will say that Q has type (p, q) if $Q(e_i) = 1$ for p of the basis elements and $Q(e_i) = -1$ for q of the them. Of course, $p + q = \dim V$. It follows immediately from property (8) of Brown's theorem that if Q has type $(p, q) = (p, \dim V - p)$, then $\sigma(Q) = (2p - \dim V) \bmod 8$.

It is important to realize that the type $(p, \dim V - p)$ of Q depends upon the choice of orthogonal basis for V. In fact, p is only well defined mod 4. To see this, suppose that $\dim V \geq 4$, $p \geq 4$, and that e_1, e_2, e_3, e_4 all have Q-value $+1$. Define new vectors $f_1 = e_2 + e_3 + e_4$, $f_2 = e_1 + e_3 + e_4$, $f_3 = e_1 + e_2 + e_4$, $f_4 = e_1 + e_2 + e_3$, $f_5 = e_5, \ldots, f_n = e_n$. Then $f_1, f_2, \ldots, f_n$ is another B-orthogonal basis for V, and each of f_1, f_2, f_3, f_4 now has Q-value -1. In terms of the f-basis, Q has type $(p - 4, \dim V - p + 4)$.

The value of $\sigma(Q)$ mod 8 uniquely determines the value of p mod 4 by the formula $\sigma(Q) = (2p - \dim V) \bmod 8$. Thus $\sigma(Q)$ also classifies nonsingular $\mathbf{Z}/4$-valued quadratic forms with B nonalternating. □

4. An extension theorem

In this section, we let K be an arbitrary field of characteristic two and V be a finite-dimensional vector space over K. Suppose W is a linear subspace of V. If B is a bilinear form on V, an injective homomorphism $f: W \to V$ is called a *B-isometry* if $B(f(x), f(y)) = B(x, y)$, for all $x, y \in W$.

Similarly, suppose Q is a quadratic form on V with associated bilinear form B. (Here, Q can be an ordinary quadratic form with values in K, or a $\mathbf{Z}/4$-valued quadratic form if $K = \mathbf{Z}/2$.) An injective homomorphism $f: W \to V$ is a *Q-isometry* if $Q(f(x)) = Q(x)$, for all $x \in W$. It follows easily that any Q-isometry is also a B-isometry.

A natural question is: given an isometry (for B or Q) $f: W \to V$, can f be extended to a global isometry $\tilde{f}: V \to V$? The first such theorem was proved by Witt [21] in 1937, and most extension theorems of this type are referred to as *Witt's theorem.*

Historical survey. Witt [21] proved in 1937 that every B-isometry $f: W \to V$ can be extended to an isometry $\tilde{f}: V \to V$, when B is a nonsingular symmetric bilinear form over a field of characteristic not two. Arf [2] proved the (ordinary) Q-isometry version of Witt's theorem in 1941, and Pall [13] generalized Witt's B-isometry theorem to arbitrary division rings of characteristic not two in 1945. Dieudonné proved Witt's theorem for nonsingular alternating forms B over any field K in the first edition (1948) of his monograph [6, §2]. Kaplansky [9] extended Witt's theorem to the infinite-dimensional setting in 1950.

It was recognized that the B-extension problem could not always be solved in characteristic two. Dieudonné [6, §27] had identified obstructions, and a simple counterexample appears in Jacobson's text [8, p. 171]. The difficulties can only occur when B is nonalternating, as Dieudonné showed. If V admits an ordinary quadratic form Q, the associated bilinear form B is alternating: this is compatible with Arf's proof of the extension theorem for ordinary Q's.

The monographs of Chevalley [4, §1.4] and Dieudonné [7, §§I.11 and I.16] prove generalizations of Witt's theorem for hermitian forms B of trace type in any characteristic, and give new proofs of Arf's theorem for Q-isometries. In characteristic two, a symmetric bilinear form of trace type is alternating, so this generalization does not remedy the obstruction difficulties in characteristic two.

In the early 1960s, the extension problem for nonalternating B in characteristic two was solved by work of Wall [20], Pless [14, 15], and Prange [17]. The obstruction to solving the extension problem was identified as the subspace $I(V)^{\perp}$, where $I(V)$ is the subspace of B-null vectors. (More generally for hermitian forms, the obstruction is the space orthogonal to the subspace of vectors u whose value $B(u, u)$ is a trace in K.) Dieudonné [6, §27] had already identified $I(V) \cap I(V)^{\perp}$ as an obstruction. The subspace $I(V)^{\perp}$ is fixed pointwise by every B-isometry. As long as $f: W \to V$ is compatible with $I(V)^{\perp}$ being fixed pointwise, f can be extended.

Obstructions to extending B-isometries. In treating the case of $\mathbf{Z}/4$-valued quadratic forms, we shall need to understand the obstructed extension problem for nonalternating B's.

We assume that B is a nonsingular symmetric bilinear form on V over K

of characteristic two. Let

$$I(V) = \{u \in V \mid B(u, u) = 0\};$$

$I(V)$ is a subspace of V (characteristic two is essential, here). If $W \subset V$ is a subspace of V, then, by definition, $W^{\perp} = \{u \in V \mid B(u, w) = 0, \text{ for all } w \in W\}$. The following lemma, due to Wall [20, Corollary to Lemma 1.2.2], shows that $I(V)^{\perp}$ is an obstruction to extending B-isometries.

Lemma (Wall). *A point $u \in V$ is fixed by every isometry $f: V \to V$ if and only if $u \in I(V)^{\perp}$.*

Those B-isometries which are compatible with Wall's lemma can indeed be extended, as this next version of Witt's theorem describes.

Theorem. *Suppose that B is a nonsingular symmetric bilinear form on the vector space V. Let W_1 and W_2 be subspaces of V, and suppose that $f: W_1 \to V$ is an isometry, with image $W_2 = f(W_1)$. Then f can be extended to an isometry $\tilde{f}: V \to V$ if and only if $W_1 \cap I(V)^{\perp} = W_2 \cap I(V)^{\perp}$ and f restricted to $W_1 \cap I(V)^{\perp}$ is the identity.*

Remark. This formulation of the extension theorem, due to Prange [17], is intermediate in generality between the two versions of Witt's theorem due to Pless in [14, 15]. Pless's statement in [14] is already enough for our purposes. An exposition of Prange's proof of this theorem is provided in the Appendix.

Z/4-valued case. We turn now to the case where Q is a $\mathbf{Z}/4$-valued quadratic form on a finite-dimensional vector space V over $\mathbf{Z}/2$. Let B denote the bilinear form associated to Q. Define

$$I(V) = \{u \in V \mid B(u, u) = 0\}.$$

Any notions of orthogonality (e.g., $I(V)^{\perp}$) are with respect to B. The conditions present in the versions of Witt's theorem due to Pless and Prange are precisely those needed here.

Theorem. *Suppose that Q is a nonsingular $\mathbf{Z}/4$-valued quadratic form on the $\mathbf{Z}/2$-vector space V. Let W_1 and W_2 be subspaces of V, and suppose that $f: W_1 \to V$ is a Q-isometry with image $W_2 = f(W_1)$. Then f can be extended to a Q-isometry $\tilde{f}: V \to V$ if and only if $W_1 \cap I(V)^{\perp} = W_2 \cap I(V)^{\perp}$ and f restricted to $W_1 \cap I(V)^{\perp}$ is the identity.*

Proof. Because any Q-isometry is also a B-isometry, the conditions stated are necessary (see Wall's lemma of the previous subsection). For the converse, we modify the proof for ordinary quadratic forms due to Chevalley [4, §1.4] (also see [7, §§I.11 and I.16]). Before launching into the proof, let us remember the classification of $\mathbf{Z}/4$-valued quadratic forms from §3. If the bilinear form B is alternating (and nonsingular), then Q is just an ordinary quadratic form and Chevalley's proof applies. Notice that if B is alternating, then $I(V) = V$, so that $I(V)^{\perp} = V^{\perp} = 0$, and there is no obstruction.

The theorem only needs to be proved, now, for the case when B is not alternating. V then admits an orthonormal basis $e_1, e_2, \ldots, e_n$, where $\dim V = n$. Denote by $\mathbf{1}$ the "all-one" vector $e_1 + e_2 + \cdots + e_n$. Since V is a vector space over $\mathbf{Z}/2$, $B(u, u) = B(u, \mathbf{1})$, for all $u \in V$. Consequently, $I(V) = (\mathbf{1})^{\perp}$, and $I(V)^{\perp}$ is the one-dimensional subspace spanned by $\mathbf{1}$.

If one wishes to extend f as a Q-isometry to the subspace $W_1 + (x)$ by setting $f(x) = y$, one needs $x \notin W_1$, $y \notin W_2$, $Q(x) = Q(y)$, and $B(x, w) = B(y, f(w))$, for all $w \in W_1$. One can easily extend f (via the identity) to those elements of $I(V)^\perp$ which are not in W_1. Let $x \in I(V)^\perp$, $x \notin W_1$. By hypothesis, $x \notin W_2$. $Q(x) = Q(x)$, of course. $B(x, w) + B(x, f(w)) = B(x, w + f(w)) = 0$, since $w + f(w) \in I(V)$. So, without loss of generality, we may assume that $I(V)^\perp \subset W_1 \cap W_2$ and that f restricted to $I(V)^\perp$ is the identity.

We can thus rephrase the statement of the theorem to: if $f: W_1 \to V$ is a Q-isometry with image $f(W_1) = W_2$, such that $I(V)^\perp \subset W_1 \cap W_2$ and f restricted to $I(V)^\perp$ is the identity, then f extends to a Q-isometry $\tilde{f}: V \to V$. We proceed to prove this statement of the theorem by induction on the dimension of W_1. The initial case where $I(V)^\perp = W_1 = W_2$ is obvious; just extend by $\tilde{f}$ equal to the identity.

For the induction step, let U be any codimension one subspace of W_1 which contains $I(V)^\perp$. By induction, the restriction of f to U admits an isometric extension $g: V \to V$. Let $h = g^{-1} \circ f: W_1 \to V$. Then h is a Q-isometry which fixes every element of the subspace U. If $\tilde{h}$ extends h, then $g \circ \tilde{h}$ extends f. So, without loss of generality, we may assume that f fixes every element of U.

Next, we wish to extend f "maximally by the identity." Let $\mathscr{A}$ be the set of subspaces A of V having the following property: f can be extended to a Q-isometry defined on $W_1 + A$ such that the elements of A are all fixed. Let A' be a maximal element of $\mathscr{A}$, and let f' be the Q-isometry defined on $W_1' = W_1 + A'$ which extends f and which fixes every element of A'. Set $W_2' = f'(W_1')$ and $U' = U + A'$. Note that f' fixes every element of the subspace U' of W_1'. If $U' = W_1'$, then f' is the identity, and the result is obvious. If not, then U' has codimension one in W_1', and there exists $a \in W_1'$, $a \notin U'$, so that $W_1' = U' + (a)$. Setting $b = f'(a)$, we have $W_2' = U' + (b)$, $Q(a) = Q(b)$, and $b \neq a$, by the maximality of A'.

We still must show that $f': W_1' \to V$ can be extended to all of V. To extend f' by setting $f'(z) = \bar{z}$, we require that $z \notin W_1'$, $\bar{z} \notin W_2'$, $Q(z) = Q(\bar{z})$, and $B(z, w) = B(\bar{z}, f'(w))$, for all $w \in W_1'$. This last condition is equivalent to two requirements: $B(z, a) = B(\bar{z}, b)$ and $B(z, u) = B(\bar{z}, u)$, for all $u \in U'$, i.e., $z + \bar{z}$ is orthogonal to U'.

By the maximality of A', $\bar{z}$ cannot equal z in a possible extension of f'. This means that if $\bar{z} = z$ satisfies the extension requirement $B(z, a) = B(z, b)$, then $z \in W_1' \cup W_2'$. This implies that the hyperplane $H = (a + b)^\perp$ (remember, $a \neq b$) is contained in $W_1' \cup W_2'$. The only way this can happen is for H to be contained in one of W_1' or W_2'. In particular, the subspaces W_1' and W_2' are either both equal to V (in which case the theorem is obvious) or both of codimension one (in which case, H equals one of W_1' or W_2'). In fact, in the latter case, we claim that $W_1' = W_2' = H$. If $H = W_1'$, then $B(a + b, a) = 0$. But $f'(a) = b$, so $Q(b) = Q(a)$. But then $jB(b, b) = 2Q(b) = 2Q(a) = jB(a, a)$, and $B(a, a) = B(b, b) = B(a, b)$, since $B(a+b, a) = 0$. Thus $B(b, a+b) = 0$, too, and $b \in H = (a+b)^\perp = W_1'$. This forces $W_2' = W_1'$. A similar argument works when $H = W_2'$. Note at this point that $Q(a + b) = Q(a) + Q(b) + jB(a, b) = 2Q(a) + jB(a, a) = Q(2a) = 0$, so that $a + b$ is Q-isotropic.

Let us review where we are. There are subspaces $U' \subset W_1' \subset V$. If we let n denote $\dim V$, then $\dim W_1' = n-1$ and $\dim U' = n-2$. The Q-isometry f' maps W_1' to itself, fixing every element of the subspace U', and sending the element $a \in W_1'$, $a \notin U'$, to $b \in W_1'$, $b \notin U'$, with $a \neq b$, $W_1' = (a+b)^\perp$, $B(a+b, b) = 0$, and $Q(a+b) = 0$. Because $W_1' = U' + (a) = U' + (b)$ and because we are working over $\mathbf{Z}/2$, it follows that $a+b \in U'$.

The orthogonal space $U'^\perp$ has dimension two. Since $U' \subset W_1'$, we have $W_1'^\perp = (a+b) \subset U'^\perp$. Thus $a+b \in U'^\perp$, too. Write

$$U'^\perp = \{0, a+b, c, c+a+b\},$$

for some $c \neq a+b$. Remember that the all-one vector $\mathbf{1} \in I(V)^\perp \subset U'$. Thus $0 = B(c, \mathbf{1}) = B(c, c)$, and $Q(c)$ equals 0 or 2.

We now seek to extend f' to V by finding $z \neq \bar{z}$ satisfying: $z, \bar{z} \notin W_1'$, $z + \bar{z}$ orthogonal to U', $B(z, a) = B(\bar{z}, b)$, and $Q(z) = Q(\bar{z})$. Fix any $z \in V$, $z \notin W_1'$. Because W_1' has codimension one in V over $\mathbf{Z}/2$, we can write $\bar{z} = z + e$, for some as yet undetermined $e \in W_1'$. We need to see if $e \in W_1'$ can be chosen in such a way as to guarantee that the extension conditions above will be satisfied. In particular, we need $e \neq 0$.

In order that $z + \bar{z} = e$ be orthogonal to U', we need $e \in U'^\perp$. We write

$$e = \xi(a+b) + \eta c.$$

We next compute $B(\bar{z}, b) + B(z, a) = B(z + \xi(a+b) + \eta c, b) + B(z, a) = B(z, a+b) + \xi B(a+b, b) + \eta B(c, b)$. Remember that $B(a+b, b) = 0$, and observe that $B(z, a+b) = 1$, since $z \notin W_1' = (a+b)^\perp$. Consequently, $B(\bar{z}, b) = B(z, a)$ if and only if $\eta B(c, b) = 1$.

Note at this point that if $B(c, b) = 0$, then, together with $B(a+b, b) = 0$, we would have that $B(U'^\perp, b) = 0$ and $b \in U'$, a contradiction. Thus $B(c, b) = 1$, and a similar argument shows that $B(c, a) = 1$, also. Naturally, we take $\eta = 1$, so that, so far, $\bar{z} = z + \xi(a+b) + c$.

Finally, we compute

$$\begin{aligned} Q(\bar{z}) - Q(z) &= Q(z + \xi(a+b) + c) - Q(z) \\ &= \xi Q(a+b) + Q(c) + j\xi B(z, a+b) \\ &\quad + jB(z, c) + j\xi B(a+b, c). \end{aligned}$$

Remember that $a+b \in U'$ and $c \in U'^\perp$, so that $B(a+b, c) = 0$. Also recall that $Q(a+b) = 0$ and $B(z, a+b) = 1$. This simplifies the formula to $Q(\bar{z}) - Q(z) = Q(c) + j\{B(z, c) + \xi\}$. Since $Q(c)$ is even, one can solve for ξ in order to make $Q(\bar{z}) - Q(z) = 0$. The prescribed choice of z and $\bar{z}$ allows us to extend f'. □

5. Applications and examples

In this final section, we discuss some aspects of isotropic subspaces for $\mathbf{Z}/4$-valued quadratic forms and their relationships to coding theory. In particular, we determine the maximal dimension of a Q-isotropic subspace, where Brown's σ-invariant will play an important role. One corollary will be a generalization of the coding theory result that doubly-even self-dual binary codes occur only in dimensions divisible by 8.

Throughout this section, Q will denote a nonsingular $\mathbf{Z}/4$-valued quadratic form on the $\mathbf{Z}/2$-vector space V of dimension $\dim V = n$. Denote by B the bilinear form associated to Q.

Isotropic subspaces. A subspace $W \subset V$ is a *B-isotropic* (or *B-totally isotropic*) subspace if $B(w_1, w_2) = 0$, for all $w_1, w_2 \in W$. Another way of saying this is $W \subset W^{\perp}$. A *Q-isotropic* subspace W satisfies $Q(w) = 0$, for all $w \in W$.

Proposition. *If a subspace $W \subset V$ is Q-isotropic, then W is also B-isotropic.*

Proof. Let $w_1, w_2 \in W$. Since W is a subspace, $w_1 + w_2 \in W$. The result follows from the formula

$$Q(w_1 + w_2) = Q(w_1) + Q(w_2) + jB(w_1, w_2). \quad \square$$

A Q-isotropic (resp., B-isotropic) subspace $W \subset V$ is said to be a *maximal* Q-isotropic (resp., B-isotropic) subspace if W is not a proper subspace of another Q-isotropic (resp., B-isotropic) subspace, i.e., if $W \subset Z$, where Z is also Q-isotropic (resp., B-isotropic), then $W = Z$. An important corollary of Witt's theorem is that maximal isotropic subspaces have the same dimension.

Theorem. *Let W_1, W_2 be two maximal Q-isotropic (resp., B-isotropic) subspaces of V. Then* $\dim W_1 = \dim W_2$.

Proof. Without loss of generality, suppose that $\dim W_1 \leq \dim W_2$. Let $f: W_1 \to W_2$ be any injective linear transformation. Because the subspaces are isotropic, f is an isometry for Q (resp., for B). By Witt's theorem, f extends to an isometry $\tilde{f}: V \to V$. Then $\tilde{f}^{-1}(W_2)$ is an isotropic subspace which contains W_1. Because W_1 is maximal, $W_1 = \tilde{f}^{-1}(W_2)$, and $\dim W_1 = \dim W_2$, as desired. $\square$

For a fixed vector space V, denote by $i(Q)$ (resp., $i(B)$) the dimension of a maximal Q-isotropic (resp., B-isotropic) subspace of V. We shall refer to $i(Q)$ (resp., $i(B)$) as the *Witt index* of Q (resp., B). Of course, the theorem above says that the Witt index is well defined. The Witt indices $i(Q)$ and $i(B)$ will be computed below.

Coding theory. We review quickly some relevant material from coding theory. A useful reference is [12], especially Chapters 1 and 19. We still denote by V a $\mathbf{Z}/2$-vector space of dimension $\dim V = n$.

Any linear subspace W of V is called a *binary linear code.* Now suppose that B is a nonsingular, nonalternating bilinear form, with $e_1, e_2, \ldots, e_n$ a fixed orthonormal basis for V. In terms of this basis, B is just the standard $\mathbf{Z}/2$-valued dot product. A B-isotropic subspace W (i.e., $W \subset W^{\perp}$) is called a *self-orthogonal* code. If, in fact, $W = W^{\perp}$, then W is called a *self-dual* code (in which case the dimension n of V is necessarily even, and $\dim V = 2 \dim W$).

If an element $u \in V$ is expressed in terms of the orthonormal basis as $u = \sum_{i=1}^{n} u_i e_i$, then the *weight* $\mathrm{wt}(u)$ equals the number of nonzero coefficients u_i. Note that $\mathrm{wt}(u) = B(u, u) \bmod 2$, so that every element of a self-orthogonal code has even weight. A self-orthogonal code W is called *doubly-even* if every element $w \in W$ satisfies $\mathrm{wt}(w) = 0 \bmod 4$. Self-orthogonal codes have been studied extensively, with [12, 16, 23] being useful references for our purposes.

There are two ways to interpret doubly-even self-orthogonal codes as isotropic subspaces for quadratic forms: in terms of ordinary quadratic forms and in terms of $\mathbf{Z}/4$-valued quadratic forms. For the first interpretation, let

$$I(V) = \{u \in V \mid B(u, u) = 0\}.$$

Every self-orthogonal code is contained in $I(V)$. Because $I(V)$ consists of those elements of V having even weight, we define Q on $I(V)$ by

$$Q(u) = \tfrac{1}{2}\operatorname{wt}(u) \bmod 2, \qquad u \in I(V).$$

One can verify that Q is an ordinary quadratic form on $I(V)$ with B its associated bilinear form. Quillen [18] described the Arf invariants for these Q's, and we shall provide an alternate calculation below.

The second interpretation avoids the contrivance of having an ordinary Q being defined on $I(V)$ by using $\mathbf{Z}/4$-valued quadratic forms directly on V. Simply let

$$Q(u) = \operatorname{wt}(u) \bmod 4, \qquad u \in V.$$

By property (8) of Brown's theorem, Q is a $\mathbf{Z}/4$-valued quadratic form with $\sigma(Q) = \dim V \bmod 8$. A Q-isotropic subspace, being B-isotropic, is a self-orthogonal code; that it is also doubly-even is clear.

Calculation of the Witt index. We now wish to calculate the Witt indices $i(Q)$ and $i(B)$ over a fixed $\mathbf{Z}/2$-vector space V of dimension $\dim V = n$. Each proof consists of displaying a maximal isotropic subspace and determining its dimension.

Theorem. *Suppose B is a nonsingular symmetric bilinear form on the $\mathbf{Z}/2$-vector space V of dimension $\dim V = n$. Then the Witt index $i(B)$ equals $[n/2]$, the integer part of $n/2$.*

Proof. If B is alternating, V is necessarily of even dimension $n = 2k$ and admits a "symplectic basis" $e_1, e_2, \ldots, e_{2k}$ such that $B(e_i, e_{k+i}) = B(e_{k+i}, e_i) = 1$ $(i = 1, 2, \ldots, k)$, with all other pairings of basis elements vanishing [7, §I.8]. One then verifies easily that W equaling the span of $\{e_1, e_2, \ldots, e_k\}$ is a maximal B-isotropic subspace. Thus $i(B) = k = [n/2]$.

When B is not alternating, we use the normal form for B discussed in §3: V admits an orthonormal basis $e_1, e_2, \ldots, e_n$. Let $k = [n/2]$. Define W to be the span of $\{e_1 + e_2, e_3 + e_4, \ldots, e_{2k-1} + e_{2k}\}$. W is a B-isotropic subspace which is easily verified to be maximal. Again, $i(B) = k = [n/2]$. □

For $\mathbf{Z}/4$-valued quadratic forms Q, both the dimension of V and the invariant $\sigma(Q)$ enter into the description of $i(Q)$.

Theorem. *Suppose Q is a nonsingular $\mathbf{Z}/4$-valued quadratic form on V, with $\dim V = n$. Then*

$$i(Q) = \begin{cases} [n/2] & \text{if } \sigma(Q) = 0, 1, 7 \bmod 8, \\ [n/2] - 1 & \text{if } \sigma(Q) = 2, 3, 4, 5, 6 \bmod 8. \end{cases}$$

Proof. Let B denote the nonsingular bilinear form associated to Q. If B is alternating, then $\dim V = n = 2k$ is necessarily even, Q is just an ordinary quadratic form, and $\sigma(Q)$ is just the Arf invariant, as in property (7) of Brown's theorem. We use Dickson's normal forms from §2.

If $\mathrm{Arf}(Q) = 0$, i.e., $\sigma(Q) = 0$, then there exists a basis $e_1, e_2, \ldots, e_{2k}$ of V such that

$$Q(u) = \sum_{i=1}^{k} u_{2i-1}u_{2i}, \qquad u = \sum_{i=1}^{2k} u_i e_i.$$

It then follows that

$$B(u, v) = \sum_{i=1}^{k} (u_{2i-1}v_{2i} + v_{2i-1}u_{2i}), \qquad u = \sum_{i=1}^{2k} u_i e_i, \ v = \sum_{i=1}^{2k} v_i e_i.$$

By setting W equal to the span of $\{e_2, e_4, \ldots, e_{2k}\}$, one can verify that W is a maximal Q-isotropic subspace of dimension $k = [n/2]$. Indeed, the basis $e_2, e_4, \ldots, e_{2k}$ of W satisfies $Q(e_{2i}) = 0$, $B(e_{2i}, e_{2j}) = 0$, for all $i, j = 1, 2, \ldots, k$. From the property $Q(u+v) = Q(u)+Q(v)+B(u, v)$ for ordinary quadratic forms, it follows that W is Q-isotropic, hence B-isotropic. Since $i(B) = k$ already, W is maximal as a B-isotropic subspace. Consequently, W is also maximal as a Q-isotropic subspace.

If $\mathrm{Arf}(Q) = 1$, i.e., $\sigma(Q) = 4$, then there is a basis $e_1, e_2, \ldots, e_{2k}$ of V with

$$Q(u) = \sum_{i=1}^{k-1} u_{2i-1}u_{2i} + u_{2k-1}^2 + u_{2k-1}u_{2k} + u_{2k}^2, \qquad u = \sum_{i=1}^{2k} u_i e_i.$$

Again,

$$B(u, v) = \sum_{i=1}^{k} (u_{2i-1}v_{2i} + v_{2i-1}u_{2i}), \qquad u = \sum_{i=1}^{2k} u_i e_i, \ v = \sum_{i=1}^{2k} v_i e_i.$$

This time set W equal to the span of $\{e_2, e_4, \ldots, e_{2k-2}\}$. As above, it is easy to check that W is a Q-isotropic subspace of dimension $k-1 = [n/2]-1$. To show that W is maximal, suppose $z = \sum_{i=1}^{2k} z_i e_i \in V$ is chosen so that $W+(z)$ is Q-isotropic. Then for all $w \in W$, $0 = Q(z+w) = Q(z)+Q(w)+B(z, w) = B(z, w)$, since $Q(z) = 0$. By setting $w = e_{2i}$, $i = 1, 2, \ldots, k-1$, we see that $0 = B(z, e_{2i}) = z_{2i-1}$. Then $0 = Q(z) = z_{2k-1}^2 + z_{2k-1}z_{2k} + z_{2k}^2$ implies that $z_{2k-1} = z_{2k} = 0$, so that $z \in W$. Thus W is maximal Q-isotropic, and $i(Q) = k - 1 = [n/2] - 1$.

Now suppose that B is not alternating. We proceed as in §3. There exists an orthonormal basis $e_1, e_2, \ldots, e_n$ for V, with $Q(e_i) = +1$ for $i = 1, 2, \ldots, p$, and $Q(e_i) = -1$ for $i = p+1, p+2, \ldots, n$. Then $\sigma(Q) = 2p-n \bmod 8$. By interchanging signs, we may assume that $p \leq n-p$. Begin by setting W equal to the span of $\{e_1+e_{p+1}, e_2+e_{p+2}, \ldots, e_p+e_{2p}\}$. W is Q-isotropic of dimension p. We next wish to enlarge W to a maximal Q-isotropic subspace W' of the form $W' = W \oplus A$. First notice that if $w \in W$ and $a \in A$, then $0 = Q(w + a) = Q(w) + Q(a) + jB(w, a)$, so that $B(w, a) = 0$. Thus it is necessary that $A \subset W^{\perp}$.

Let us examine when an element $u = \sum_{i=1}^{n} u_i e_i$ of V is in $W^{\perp}$. Since $B(e_j + e_{p+j}, u)$ must vanish for all $j = 1, 2, \ldots, p$, we see that $u \in W^{\perp}$ if and only if $u_j + u_{p+j} = 0$, for all $j = 1, 2, \ldots, p$. Simply put, this says that $W^{\perp} = W \oplus W_1$, where W_1 is the span of $\{e_{2p+1}, e_{2p+2}, \ldots, e_n\}$.

Our problem of finding a maximal Q-isotropic extension W' of W of the form $W' = W \oplus A$ now reduces to finding a subspace A which is maximal

among all subspaces with the following property: A is Q-isotropic and $A \subset W_1$. If we denote by Q_1 the restriction of Q to W_1, then the maximal A we seek is just a maximal Q_1-isotropic subspace of W_1. On W_1, Q_1 has type $(0, n-2p)$, so that A is just an ordinary doubly-even self-orthogonal code in an ambient space of dimension $n-2p$. By the known theory of such codes [23, Remark 3.23], such a maximal A has dimension

$$\dim A = \begin{cases} [(n-2p)/2] & \text{if } n-2p = 0, 1, 7 \bmod 8, \\ [(n-2p)/2]-1 & \text{if } n-2p = 2, 3, 4, 5, 6 \bmod 8. \end{cases}$$

The result is now apparent. □

The following corollary generalizes the coding theory result that a doubly-even self-dual code can occur only in a space V whose dimension is a multiple of 8.

Corollary. *Suppose Q is a nonsingular $\mathbf{Z}/4$-valued quadratic form on a $\mathbf{Z}/2$-vector space V, with associated bilinear form B. Then there exists a Q-isotropic subspace W of V which is self-dual (i.e., $W = W^{\perp}$) if and only if $\sigma(Q) = 0 \bmod 8$.*

Proof. Self-duality implies that $\dim V = n$ is even and equal to $2 \dim W$. Among the admissible dimensions for maximal Q-isotropic subspaces from the theorem, we clearly need $\dim W = n/2$, in which case $\sigma(Q) = 0, 1, 7 \bmod 8$. From property (6) of Brown's theorem, we are reminded that $\sigma(Q) = \dim V \bmod 2$. Since $\dim V$ is even, $\sigma(Q) = 0 \bmod 8$ is forced.

Conversely, if $\sigma(Q) = 0 \bmod 8$, then $\dim V$ is even and $i(Q) = [n/2] = n/2$. Thus any maximal Q-isotropic subspace is self-dual. □

Some calculations of Arf invariants. We mentioned above, in connection with doubly-even self-orthogonal codes, that these codes can be interpreted both as Q-isotropic subspaces for the $\mathbf{Z}/4$-valued quadratic form $Q(u) = \mathrm{wt}(u) \bmod 4$ on V, as well as Q-isotropic subspaces for the ordinary quadratic form $Q(u) = \frac{1}{2}\mathrm{wt}(u) \bmod 2$ on $I(V)$. Quillen described the Arf invariants of the ordinary quadratic forms in [18, §2], and here we provide an alternate calculation, using the σ-invariant.

Property (11) of Brown's theorem says that $\sigma(Q)$ is related to Q by

$$\sum_{u \in V} i^{Q(u)} = \sqrt{2}^{\dim V} e^{\frac{\pi i \sigma(Q)}{4}},$$

where $i = \sqrt{-1}$. If $\dim V = n$ and $Q(u) = \mathrm{wt}(u) \bmod 4$ with respect to an orthonormal basis $e_1, e_2, \ldots, e_n$ of V, then there are $\binom{n}{k}$ elements of V having weight k. If we let $S(Q)$ denote the sum $\sum_{u \in V} i^{Q(u)}$, then

$$\begin{aligned} S(Q) = \sum_{u \in V} i^{Q(u)} &= \sum_{k=0}^{n} \binom{n}{k} i^k = (1+i)^n \\ &= \sqrt{2}^n \left(\frac{1+i}{\sqrt{2}}\right)^n = \sqrt{2}^n e^{\frac{i\pi n}{4}} \end{aligned}$$

and $\sigma(Q) = n \bmod 8$. Of course, this also follows from property (8) of Brown's theorem.

Next we restrict Q to

$$I(V) = \{u \in V \mid B(u, u) = 0\} = \{u \in V \mid u \text{ has even weight}\}.$$

If we denote this restricted quadratic form by Q_1, then we can describe $S(Q_1)$.

Proposition. $S(Q_1) = \sqrt{2}^n \cos(\pi n/4) = \chi(n)2^{[n/2]}$, *where*

$$\chi(n) = \begin{cases} 1, & n = 0, 1, 7 \bmod 8, \\ 0, & n = 2, 6 \bmod 8, \\ -1, & n = 3, 4, 5 \bmod 8. \end{cases}$$

Proof. $S(Q_1) = \sum_{u \in I(V)} i^{Q(u)}$. But $I(V)$ consists of those $u \in V$ having even weight, i.e., those $u \in V$ with $Q(u)$ even. This means that $S(Q_1)$ is just the real part of $S(Q) = \sqrt{2}^n e^{i\pi n/4}$, and the result follows. □

In order to calculate $\sigma(Q_1)$, we must remember that Brown's theorem on $\sigma(Q)$ applies only to nonsingular Q's. If $n = \dim V$ is even, then $\dim I(V) = n - 1$ is odd, and it is impossible for B (necessarily alternating on $I(V)$) to be nonsingular on $I(V)$. We can be more precise: $I(V) = (\mathbf{1})^{\perp}$, where $\mathbf{1}$ is the "all-one" vector $\mathbf{1} = e_1 + e_2 + \cdots + e_n$. B is nonsingular on $I(V)$ if and only if $\mathbf{1} \notin I(V)$, i.e., if and only if n is odd.

If n is odd, then $[n/2] = (n-1)/2$, and $S(Q_1) = \chi(n)\sqrt{2}^{\dim I(V)}$. Thus $\sigma(Q_1) = 0 \bmod 8$ if $\chi(n) = 1$ ($n = 1, 7 \bmod 8$), and $\sigma(Q_1) = 4 \bmod 8$ if $\chi(n) = -1$ ($n = 3, 5 \bmod 8$). For ordinary quadratic forms, these cases correspond to Arf invariants 0 and 1, respectively, by property (7) of Brown's theorem.

If n is even, $\mathbf{1} \in I(V)$ and B is singular on $I(V)$. We must next distinguish two cases which depend on the value of $Q(\mathbf{1})$. $Q(\mathbf{1}) = n \bmod 4$, so $Q(\mathbf{1}) = 0$ if $n = 0 \bmod 4$, and $Q(\mathbf{1}) = 2$ if $n = 2 \bmod 4$. When $Q(\mathbf{1}) \neq 0$ ($n = 2 \bmod 4$), Q is said to be a *defective* quadratic form [7, §I.16]; this case lies outside the scope of our theory.

When $Q(\mathbf{1}) = 0$ ($n = 0 \bmod 4$), then we can reduce to the nonsingular case by working with the induced quadratic form Q' on the quotient space $N = I(V)/(\mathbf{1})$. Modulo $(\mathbf{1})$, every element of $I(V)$ of weight $> n/2$ is equivalent to one of weight $< n/2$ (just add $\mathbf{1}$). In addition, every element u of weight precisely $n/2$ such that $B(u, e_n) = 1$ is equivalent to the element $u + \mathbf{1}$ of weight $n/2$ but with $B(u+\mathbf{1}, e_n) = 0$. So, to calculate $S(Q')$, we sum only over elements of $I(V)$ with weight $< n/2$ or with weight $= n/2$ and $B(u, e_n) = 0$. But this yields exactly half of $S(Q_1)$! Thus $S(Q') = \frac{1}{2}S(Q_1) = \frac{1}{2}\chi(n)2^{n/2} = \chi(n)\sqrt{2}^{\dim N}$, and $\sigma(Q') = 0$ if $n = 0 \bmod 8$, $\sigma(Q') = 4$ if $n = 4 \bmod 8$. These correspond to Arf invariants 0 and 1, respectively.

We summarize these results in the following proposition.

Proposition. *Let V have dimension n, and let Q be the ordinary quadratic form on $I(V)$ defined by*

$$Q(u) = \tfrac{1}{2}\operatorname{wt}(u) \bmod 2.$$

(1) *If n is odd, then Q is nonsingular, and* $\operatorname{Arf}(Q) = 0$ *if* $n = 1, 7 \bmod 8$, $\operatorname{Arf}(Q) = 1$ *if* $n = 3, 5 \bmod 8$.

(2) *If* $n = 0 \bmod 4$, Q *is singular, but* Q' *on* $I(V)/(\mathbf{1})$ *is nonsingular with* $\operatorname{Arf}(Q') = 0$ *when* $n = 0 \bmod 8$, *and* $\operatorname{Arf}(Q') = 1$ *when* $n = 4 \bmod 8$.

(3) *If* $n = 2 \bmod 4$, Q *is defective.*

Final example. It was proved in the classification results of §3 that if B was not alternating, then Q had a certain type $(p, n-p)$, where p was uniquely determined mod 4. We wish to exploit the mod 4 ambiguity of p to give a final example.

If V has dimension $\dim V = n$ and B is not alternating, then V admits an orthonormal basis $e_1, e_2, \ldots, e_n$. If a $\mathbf{Z}/4$-valued quadratic form Q has B as its associated bilinear form and Q has type $(p, n-p)$, then we can assume that $Q(e_i) = 1$, for $i = 1, 2, \ldots, p$, and that $Q(e_i) = -1$, for $i = p+1, p+2, \ldots, n$. It follows that $\sigma(Q) = 2p - n \bmod 8$.

Suppose now that $n = 0 \bmod 8$, say $n = 8k$, and that we consider the $\mathbf{Z}/4$-valued quadratic form Q of type $(4k, 4k)$. There is an obvious maximal Q-isotropic subspace W given by the span of $\{e_1 + e_{4k+1}, e_2 + e_{4k+2}, \ldots, e_{4k} + e_{8k}\}$, such that $\dim W = 4k$.

Because the type of Q depends upon the choice of orthonormal basis, it is possible to find a new orthonormal basis of V which makes Q of type $(8k, 0)$. Expressed in terms of this new basis, W becomes a doubly-even self-dual code. For example, if one makes the following change of basis:

$$
\begin{aligned}
f_i &= e_i, \qquad i = 1, 2, \ldots, 4k, \\
f_{4j+1} &= e_{4j+2} + e_{4j+3} + e_{4j+4}, \\
f_{4j+2} &= e_{4j+1} + e_{4j+3} + e_{4j+4}, \\
f_{4j+3} &= e_{4j+1} + e_{4j+2} + e_{4j+4}, \\
f_{4j+4} &= e_{4j+1} + e_{4j+2} + e_{4j+3}, \qquad j = k, k+1, \ldots, 2k-1,
\end{aligned}
$$

then Q has type $(8k, 0)$, and W becomes a product of k copies of the extended Hamming code E_8 (see [16] or [23, 3.14]).

We invite the reader to experiment with other changes of basis in order to produce other doubly-even self-dual codes.

Appendix. Prange's proof of Witt's extension theorem

In this appendix we include an exposition of a proof of Witt's extension theorem for ordinary quadratic forms in characteristic two due to E. Prange [17]. There are many interesting ideas in Prange's proof; among them are: considering the graph of the isometry, showing that the graph is totally isotropic, and phrasing the extension conditions for the isometry in terms of orthogonality properties of the graph. These ideas deserve a larger audience. Since Prange never published his proof, the author hopes that the following exposition of Prange's work will fill a gap in the literature and be useful to other mathematicians.

Notation is as in §4. Recall the statement of the theorem.

Theorem. *Suppose that* B *is a nonsingular symmetric bilinear form on the vector space* V. *Let* W_1 *and* W_2 *be subspaces of* V, *and suppose that* $f\colon W_1 \to V$ *is an isometry, with image* $W_2 = f(W_1)$. *Then* f *can be extended to an isometry* $\tilde{f}\colon V \to V$ *if and only if* $W_1 \cap I(V)^{\perp} = W_2 \cap I(V)^{\perp}$ *and* f *restricted to* $W_1 \cap I(V)^{\perp}$ *is the identity.*

Proof. Wall's lemma of §4 implies that the conditions listed are necessary. For the converse, assume that the conditions listed are satisfied. The key idea is that the graph of an isometry is a totally isotropic subspace of the product space $V \times V$.

We shall often use the product space $V \times V$, equipped with the bilinear form $\overline{B}$,

$$\overline{B}((u_1, v_1), (u_2, v_2)) = B(u_1, u_2) + B(v_1, v_2).$$

Note that $\overline{B}((u, v), (u, v)) = B(u, u) + B(v, v) = B(u + v, u + v)$. Thus $(u, v) \in I(V \times V)$ if and only if $u + v \in I(V)$.

Let G be the graph of the isometry $f: W_1 \to W_2$, i.e.,

$$G = \{(u, f(u)) \mid u \in W_1\} \subset W_1 \times W_2 \subset V \times V.$$

Because f is an isometry, it follows that $G \subset G^\perp$ and hence that $G \subset I(V \times V)$. Another way to write this is $u + f(u) \in I(V)$, for all $u \in W_1$.

In order to extend f to a subspace $W_1 + (x)$ by setting $f(x) = y$, the following conditions must hold: $x \notin W_1$, $y \notin W_2$, $(x, y) \in I(V \times V)$ (the fancy way of saying that $B(x, x) = B(y, y)$), and $(x, y) \in G^\perp$. The last two conditions say that the extended map is an isometry.

The first step is to extend f (via the identity) to those points of $I(V)^\perp$ which are not in W_1. Let $x \in I(V)^\perp$, $x \notin W_1$. By hypothesis, $x \notin W_2$. Clearly, $(x, x) \in I(V \times V)$. Finally, $(x, x) \in G^\perp$, because $\overline{B}((x, x), (u, f(u))) = B(x, u) + B(x, f(u)) = B(x, u + f(u)) = 0$, and $u + f(u) \in I(V)$. Thus setting $f(x) = x$ extends f to all of $I(V)^\perp$. From here on, we may assume that $I(V)^\perp \subset W_1 \cap W_2$.

Once $I(V)^\perp \subset W_1 \cap W_2$, the conditions for extending f by setting $f(x) = y$ can be simplified. We claim that $G^\perp \subset I(V \times V)$. Let $(u_1, u_2) \in G^\perp$ and $v \in I(V)^\perp$ (so $(v, v) \in G$). Then $0 = \overline{B}((u_1, u_2), (v, v)) = B(u_1, v) + B(u_2, v) = B(u_1 + u_2, v)$, so that $u_1 + u_2 \in I(V)$. This implies that $(u_1, u_2) \in I(V \times V)$. The conditions needed to extend f by setting $f(x) = y$ are now: $x \notin W_1$, $y \notin W_2$, and $(x, y) \in G^\perp$.

Denote by N the subspace $W_1^\perp \times W_2^\perp$, which is contained in $G^\perp$. Because $G \subset G^\perp$, $G + N \subset G^\perp$. We claim that

$$\{(x, y) \in G^\perp \mid x \in W_1 \text{ or } y \in W_2\} \subset G + N.$$

Indeed, if $(x, y) \in G^\perp$ and $x \in W_1$, then it suffices to show that $(x, y) + (x, f(x)) = (0, y + f(x)) \in G^\perp$ is actually in N. Since $0 \in W_1^\perp$, all that remains is to show that $y + f(x) \in W_2^\perp$. To this end, let $v \in W_2 = f(W_1)$, so there exists $u \in W_1$ with $f(u) = v$. Then $B(y + f(x), v) = B(0, u) + B(y + f(x), v) = \overline{B}((0, y + f(x)), (u, v)) = 0$, since $(0, y + f(x)) \in G^\perp$ and $(u, v) \in G$. A similar argument applies when one assumes that $y \in W_2$.

The final step of the proof begins by observing that $W_1^\perp \subset W_1$ if and only if $W_2^\perp \subset W_2$. To see this, note that the isometry $f: W_1 \to W_2$ induces an isometry between $W_1^\perp \cap W_1$ and $W_2^\perp \cap W_2$. The result follows by counting dimensions.

To finish the proof, we wish to show that if W_1 is a proper subspace of V, then we can extend f by setting $f(x) = y$, for some $x \notin W_1$, $y \notin W_2$, $(x, y) \in G^\perp$. We examine two cases, depending upon whether $W_1^\perp \subset W_1$ or not.

If $W_1^\perp \not\subset W_1$, then, as above, $W_2^\perp \not\subset W_2$. Now choose any $x \in W_1^\perp \setminus W_1$, $y \in W_2^\perp \setminus W_2$. Clearly, $(x, y) \in G^\perp$, and we can extend f.

If $W_1^\perp \subset W_1$, then any point of $G^\perp$ which is not in $G + N$ will define an extension for f, because $G + N$ contains the subset $\{(x, y) \in G^\perp \mid x \in W_1 \text{ or } y \in W_2\}$. It remains to show that such points exist whenever W_1 is a proper subset of V. We do this by a dimension count. Let $n = \dim V$ and $t = \dim W_1 = \dim W_2 = \dim G$. Then $\dim N = 2(n - t)$, and

$$\dim(G \cap N) = \dim(W_1 \cap W_1^\perp) = \dim W_1^\perp = n - t.$$

(This uses $W_1^\perp \subset W_1$, and so $W_2^\perp \subset W_2$.) Thus $\dim(G + N) = n$. But $\dim G^\perp = 2n - t$ is greater than $n = \dim(G+N)$ whenever $t < n$, i.e., whenever W_1 is a proper subspace of V. Thus, extensions always exist whenever W_1 is a proper subspace of V. □

Acknowledgments

The author thanks William Browder for suggesting Brown's paper and Edward F. Assmus, Jr. for teaching him about the work of Prange, for suggesting that an exposition of Prange's work be included here, and for other helpful advice and encouragement.

This paper was written while the author was on sabbatical leave from Bowdoin College and visiting Lehigh University. The author thanks both institutions for their hospitality and financial support.

References

1. A. A. Albert, *Symmetric and alternate matrices in an arbitrary field*, Trans. Amer. Math. Soc. **43** (1938), 386–436.
2. Č. Arf, *Untersuchungen über quadratische Formen in Körpern der Charakteristik* 2. I, J. Reine Angew. Math. **183** (1941), 148–167.
3. E. H. Brown, Jr., *Generalizations of the Kervaire invariant*, Ann. of Math. (2) **95** (1972), 368–383.
4. C. Chevalley, *The algebraic theory of spinors*, Columbia Univ. Press, New York, 1954.
5. L. E. Dickson, *Linear groups*, Dover, New York, 1958; first published in 1901 by B. G. Teubner, Leipzig.
6. J. Dieudonné, *Sur les groupes classiques*, 3rd ed., Actualités Sci. Indust., no. 1040, Hermann, Paris, 1973; first edition was published in 1948.
7. ———, *La géométrie des groupes classiques*, Ergeb. Math. Grenzgeb., vol. 5, Springer-Verlag, Berlin, Göttingen, and Heidelberg, 1955.
8. N. Jacobson, *Lectures in abstract algebra*, Vol. 2, Linear Algebra, Van Nostrand, Toronto, New York, and London, 1953.
9. I. Kaplansky, *Forms in infinite dimensional spaces*, An. Acad. Brasil. Ciênc. **22** (1950), 1–17.
10. ———, *Linear algebra and geometry: A second course*, Allyn and Bacon, Boston, Mass., 1969.
11. W. Klingenberg and E. Witt, *Über die Arfische Invariante quadratischer Formen* mod 2, J. Reine Angew. Math. **193** (1954), 121–122.
12. F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland Math. Library, vol. 16, North-Holland, Amsterdam, New York, and Oxford, 1978.
13. G. Pall, *Hermitian quadratic forms in a quasi-field*, Bull. Amer. Math. Soc. **51** (1945), 889–893.

14. V. Pless, *On Witt's theorem for nonalternating symmetric bilinear forms over a field of characteristic* 2, Proc. Amer. Math. Soc. **15** (1964), 979–983.
15. ———, *On the invariants of a vector subspace of a vector space over a field of characteristic two*, Proc. Amer. Math. Soc. **16** (1965), 1062–1067.
16. ———, *A classification of self-orthogonal codes over* $GF(2)$, Discrete Math. **3** (1972), 209–246.
17. E. Prange, *Witt's theorem for characteristic two*, unpublished manuscript dated July 5, 1963.
18. D. Quillen, *The* mod 2 *cohomology rings of extra-special* 2*-groups and the spinor groups*, Math. Ann. **194** (1971), 197–212.
19. O. Veblen and P. Franklin, *On matrices whose elements are integers*, Ann. of Math. (2) **23** (1921), 1–15.
20. G. E. Wall, *On the conjugacy classes in the unitary, symplectic and orthogonal groups*, J. Austral. Math. Soc. **3** (1963), 1–62.
21. E. Witt, *Theorie der quadratischen Formen in beliebigen Körpern*, J. Reine Angew. Math. **176** (1937), 31–44.
22. ———, *Über eine Invariante quadratischer Formen* mod 2, J. Reine Angew. Math. **193** (1954), 119–120.
23. J. A. Wood, *Spinor groups and algebraic coding theory*, J. Combin. Theory Ser. A **51** (1989), 277–313.

Department of Mathematics, Computer Science, and Statistics, Purdue University Calumet, Hammond, Indiana 46323–2094
E-mail address: woodja@pucal.bitnet