Witt’s theorems for Galois Ring valued quadratic forms

M.C. López-Díaz*, I.F. Rúa

Departamento de Matemáticas, Universidad de Oviedo, Spain

ARTICLE INFO

Article history:
Received 5 September 2007
Received in revised form 25 January 2008
Available online 2 May 2008
Communicated by R. Parimala

MSC:
Primary: 11E12
secondary: 15A66
13M99

ABSTRACT

We prove Witt’s cancelation and extension theorems for Galois Ring valued quadratic forms. The proof is based on the properties of the invariant $I$, previously defined by the authors, that classifies, together with the type of the corresponding bilinear form (alternating or not), nonsingular Galois Ring valued quadratic forms. Our results extend the Witt’s theorem for mod four valued quadratic forms. On the other hand, the known relation between the invariant $I$ and the Arf invariant of an ordinary quadratic form (if the associated nonsingular bilinear form is alternating) is extended to the nonalternating case by explaining the invariant $I$ in terms of Clifford algebras.

© 2008 Elsevier B.V. All rights reserved.

1. Introduction

Galois Ring valued quadratic forms were introduced in [10] as an extension of the $\mathbb{Z}_4$-valued quadratic forms defined by Brown [2]. These forms have been used to construct different families of not necessarily equivalent Generalized Kerdock codes over a finite field of characteristic 2 [3,6]. This is an example of the increasing number of applications of finite rings (specifically Galois Rings) to Coding Theory and Cryptography (see, for instance, [12,7,9,13,4,17]).

In [10] an invariant $I$ that classifies non-singular Galois Ring valued quadratic forms, together with the type of the corresponding bilinear form (alternating or not), was introduced. It takes values in a Galois Ring of characteristic 8 and extends the corresponding invariant for $\mathbb{Z}_4$-valued quadratic forms introduced by E.H. Brown and studied by Wood in [18]. In this work the author also proved Witt’s extension theorem for $\mathbb{Z}_4$-valued quadratic forms.

The aim of this paper is two-fold. First, we prove Witt’s cancelation and extension theorems [14] for nonsingular Galois Ring valued quadratic forms. Our proof is based on relevant properties of the invariant $I$. On the other hand, we provide an explanation of this invariant in terms of Clifford algebras. These algebras explain the classic Arf invariant for nonsingular quadratic forms over a finite field of characteristic 2, and so they also explain the invariant $I$ in the case when the associated nonsingular form is alternating. Our results extend this explanation to the nonalternating case.

The structure of the paper is as follows. In Section 2, the main properties of Galois Rings are recalled, particularly in the characteristic 4 case. Also, basic notions and the needed results from the Clifford Theory are introduced. In Section 3, we consider the singular properties of the subspace $I(V)^-$, since this subspace plays a remarkable role in the study of nonsingular Galois Ring valued quadratic forms. Next, in Section 4, we prove Witt’s cancelation and extension theorems for these forms. Finally, in Section 5, we provide the explanation of the invariant $I$ in terms of Clifford algebras.

* Corresponding address: Departamento de matematicas, Facultad de Ciencias, Universidad de Oviedo, c/ Calvo Sotelo, s/n, E-33007 Oviedo, Spain. Tel.: +34 985 10 33 31; fax: +34 985 10 33 54.
E-mail addresses: cld@uniovi.es (M.C. López-Díaz), rua@uniovi.es (I.F. Rúa).

0022-4049/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.jpaa.2008.03.028
2. Preliminaries

2.1. Galois Rings of characteristic 4

In this section we briefly collect the definition and the main properties of Galois Rings of characteristic 4. See [1,12] or [11], for instance, for the general setting and details.

Throughout this paper $R = \text{GR}(4, l)$ will be the Galois Ring of $q^2$ elements ($q = 2^l$) and characteristic $2^l$. It is an associative commutative local chain ring with maximal ideal $2R$ and quotient field $\overline{R} = R/2R = GF(q)$. This ring is uniquely determined by its cardinality and characteristic and it can be constructed as the quotient ring $\mathbb{Z}_4[x]/\langle p(x) \rangle$, where $p(x) \in \mathbb{Z}_4[x]$ is any monic polynomial of degree $l$ such that $p(x) \in \mathbb{Z}_4[x]/\mathbb{Z}_2[x]$ is irreducible, i.e., a Galois polynomial. The set of units of $R$ is the multiplicative abelian group $\Gamma_R = \mathbb{Z} \setminus 2R$ and the lattice of ideals of $R$ is the strictly decreasing chain $\mathbb{Z} \supset R \supset 2R \supset 0$.

The subset $\Gamma_R = \{b \in R | b^2 = b\}$ is called the Teichmüller coordinate set (TCS) of $R$. It is a set of $q$ elements closed under the product and such that any element $b \in R$ can be presented uniquely in the form $b = b_0 + 2b_1$, where $b_i = \gamma_i(b) \in \Gamma_R$, $i = 0, 1$. This set is not closed under the addition, though.

If we consider the map $\oplus : \Gamma(R) \times \Gamma(R) \to \Gamma(R)$ given by $a \oplus b = \gamma_0(a + b)$, then $\Gamma(R)$, $\oplus$, is the finite field $K = GF(q)$. Moreover, for any $a, b \in \Gamma(R)$ the following equality holds: $\gamma_1(a + b) = (ab)^{2^{l-1}}$. Notice that in the field $\Gamma(R)$ the map $x \mapsto x^2$ is an automorphism of order $l$ and so is linear. In particular, we can write $a^{2^r}$ as $\sqrt[2^r]{a}$, since for any element $a \in \Gamma(R)$ the equality $a^2 = a$ holds. The map $x \mapsto \sqrt{x}$ is also linear.

2.2. Galois Ring valued quadratic forms

Next we recall the definition of a Galois Ring valued quadratic form and its main properties (for a complete account see [10]).

Let $V$ be a vector space of dimension $m \in \mathbb{N}$ over the finite field $K = \Gamma_R$, where $R = \text{GR}(4, l)$ ($q = 2^l$). The map $Q : V \to R$ is an $R$-valued quadratic form provided that $Q(\lambda a) = \lambda^2 Q(a)$, for all $\lambda \in K$, and for all $a \in V$, and the map $(\cdot, \cdot)_Q : V \times V \to R$ given by $(a, b)_Q = Q(a \oplus b) - Q(a) - Q(b)$, for all $a, b \in V$, is a bilinear form. Taking $R = \mathbb{Z}_4 = \text{GR}(4, 1)$ we get the $\mathbb{Z}_4$-valued quadratic forms of Brown [2].

Since $2(a, b)_Q = (a\oplus b, a \oplus b)_Q = 0$, for any $a, b \in V$, we can consider the ordinary bilinear symmetric form $B_Q(\cdot, \cdot) : V \times V \to K$ given by $2B_Q(a, b) = (a, b)_Q$ for all $a, b \in V$, i.e., $B_Q(a, b) = \gamma_1((a, b)_Q)$. In particular, for any element $a \in V$, we have $2Q(a) = 2B_Q(a, a)$, and so $Q(a) = \gamma_0(Q(a)) = B_Q(a, a)$.

In this paper the bilinear form $B_Q$ is required to be nonsingular, i.e., such that for any nonzero $a \in V$ there exists $b \in V$ with $B_Q(a, b) \neq 0$. The pair $(V, Q)$ will be called a nonsingular metric vector space. If $B_Q$ is nonalternating, i.e., there exists a $V$ such that $B_Q(a, a) \neq 0$, then the pair $(V, B_Q)$ is an orthogonal geometry [14], and there exists an orthonormal basis $\{e_1, \ldots, e_m\}$ of $V$, that is, $B_Q(e_i, e_j) = \delta_{ij}$ so that, for all $1 \leq i \leq m$, we have $Q(e_i) = 1 + 2\lambda_i$, for some $\lambda_i \in K$. We shall denote this form by $(\lambda_1, \ldots, \lambda_m).

On the other hand, if $B_Q$ is alternating, then $m$ is necessarily even, the pair $(V, B_Q)$ is a symplectic geometry [14], and there exists a symplectic basis $\{e_1, \ldots, e_m\}$ of $V$, i.e, $B_Q(e_j, e_{j-1}) = B_Q(e_{j-1}, e_j) = 1$ for all $1 \leq i \leq m/2$, and $B_Q(e_i, e_i) = 0$ in the remaining cases. Therefore, for all $1 \leq i \leq m$, we have $Q(e_i) = 2\lambda_i$, for some $\lambda_i \in K$. We shall denote this form by $(\lambda_1, \ldots, \lambda_m)$. Notice that $B_Q$ is alternating if, and only if, $Q(a) \in 2R$ for all $a \in V$. Indeed $Q = Q’, \text{ where } Q’ : V \to K$ is an ordinary quadratic form over the field $K$. We shall write $A\!r(f, \lambda_1, \ldots, \lambda_m)$ or $A\!r(Q)$, to denote the Arf invariant of the quadratic form $Q’$ [8]. This invariant is defined in the additive quotient group $K/K^*$, where $K^*$ is the additive subgroup of $K$ generated by the elements of the form $x^2 \oplus x$.

Two $R$-valued quadratic forms $Q_1, Q_2 : V \to R$ are said to be equivalent, and denoted $Q_1 \cong Q_2$, if there exists a linear transformation $L : V \to V$ such that $Q_1(L(a)) = Q_2(a)$, for all $a \in V$. The sum of $Q_1 : V_1 \to R$ and $Q_2 : V_2 \to R$ is the quadratic form $Q_1 + Q_2 : V_1 \times V_2 \to R$, given by $Q_1 + Q_2((a_1, a_2)) = Q_1(a_1) + Q_2(a_2)$, for all $a_i \in V_i$, $i = 1, 2$.

The map $\rho : (K^*, \oplus) \to (GR(8, l), +)$, given by $x \mapsto 2^x$, is a monomorphism of additive groups that allows us to identify the group $(K^*, \oplus)$ with the additive subgroup $(2^G R(8, l), +)$. By abuse of notation, we will write this subgroup as $2^{K^*}$. The invariant $I(Q)$ of $Q : V \to R$ is defined in $GR(8, l)$ (mod $2^{K^*}$), by the following way. If $B_Q$ is not alternating and $Q$ is of type $(\lambda_1, \ldots, \lambda_m)$, then $I(Q) = \sum_{i=1}^{m}(1 + 2\lambda_i + 2^2\lambda_i) \in GR(8, l)$ (mod $2^{K^*}$). If $B_Q$ is alternating and $Q$ is of type $(\lambda_1, \ldots, \lambda_m)$, then $I(Q) = 2^1\!r(Q) \in GR(8, l)$ (mod $2^{K^*}$). Notice that $I(Q)$ can be decomposed into a unique form $I(Q)_0 + 2I(Q)_1 + 2^2I(Q)_2$, where $I(Q)_i \in GR(8,i)$, $i = 0, 1, 2$. In particular, $I(Q)_0 = m$ (mod 2) depends only on the dimension of the vector space $V$. By [10, Proposition 3, Theorem 3] we have that $I(Q)$ does not depend on the basis and that a nonsingular $R$-valued quadratic form $Q$ is determined up to equivalence by $I(Q)$ together with the type of the associated bilinear form.

2.3. Clifford algebras

We conclude this section by collecting the results from the Clifford theory needed in our paper, specifically Clifford algebras for ordinary quadratic forms over a field of characteristic 2 (see [15]).

If $Q : V \to K$ is an ordinary quadratic form, then the Clifford algebra of the metric vector space $(V, Q)$ is the $K$-algebra $C((V, Q)) = T(V)/J$, where $T(V)$ is the tensor algebra of $V$, i.e., $T(V) = \bigoplus_{n \geq 0} V \otimes \cdots \otimes V$, and $J$ is the ideal of $T(V)$ generated
by all elements \( a \otimes a \oplus Q(a) \), for \( a \in V \). Since \( V \) has dimension \( m \) over \( K \), \( C(V, Q) \) is a \( 2^m \)-dimensional \( K \)-algebra. If \( m = 1 \), then \( C(V, Q) \) is isomorphic to an algebra \( K[x]/(x^2 \oplus Q(x)) \).

The Clifford algebra \( C = C((V, Q)) \) is a \( \mathbb{Z}_2 \)-graded algebra, i.e., it has a direct sum decomposition \( C = C_0 \oplus C_1 \), as \( K \)-vector space, such that \( C_i \subseteq C_{i+j} \mod 2 \). The even part \( C_0 \) is generated by the even products of elements of \( V \) and the odd part \( C_1 \) by the odd products. \( C_0 \) is a subalgebra of \( C \) and \( C_1 \) is a \( C_0 \)-module.

If \( Q_i : V_i \to K, i = 1, 2 \), are two ordinary quadratic forms, then the Clifford algebra of the sum \( Q_1 + Q_2 : V_1 \times V_2 \to K \) is the graded tensor product \( C((V_1, Q_1)) \otimes C((V_2, Q_2)) \) of the two Clifford algebras \( C((V_1, Q_1)) \) and \( C((V_2, Q_2)) \).

If \( Q : V \to K \) is an ordinary nonsingular quadratic form, then the center \( Z(C_0) \) of the even part \( C_0 \) is isomorphic to an algebra \( K[x]/(x^2 \oplus x + \Delta) \), where \( \Delta \in K \). This element \( \Delta \) is uniquely determined in the quotient group \( K/K^+ \), and it is exactly the Arf invariant of the quadratic form \( Q \).

3. The singular properties of the subspace \( I(V)^- \)

In the study of nonsingular bilinear forms over a field of characteristic 2 (and so also in the study of ordinary and Galois Ring valued quadratic forms) there is a certain subspace that plays a remarkable role (see [18, Section 4] for an historical background). This section is devoted to the main properties of this subspace in the context of Galois Ring valued quadratic forms.

3.1. \( I(V)^- \) and nonsingular bilinear forms

**Definition 1.** Let \( V \) be a vector space over \( K \), and let \( B : V \times V \to K \) be a nonsingular symmetric bilinear form on \( V \). We define:

\[
I(V) = \{ v \in V \mid B(v, v) = 0 \}.
\]

We denote by \( I(V)^- \) the set of orthogonal elements to \( I(V) \) with respect to the bilinear form \( B \), that is,

\[
I(V)^- = \{ w \in V \mid B(w, v) = 0, \forall v \in I(V) \}.
\]

We next collect some known properties of the sets \( I(V) \) and \( I(V)^- \).

**Proposition 1.** If \( B \) is a nonsingular symmetric bilinear form on a vector space \( V \) over \( K \), then:

1. \( I(V) \) and \( I(V)^- \) are \( K \)-subspaces of \( V \).
2. If \( B \) is alternating, then \( I(V) = V \), and \( I(V)^- = \{ 0 \} \).
3. If \( B \) is nonalternating and \( V \) is of finite dimension \( m \) over \( K \), then \( I(V)^- = \{ 1 \} \), where \( 1 = \bigoplus_{i=1}^{m} e_i \), and \( \{ e_1, \ldots, e_m \} \) is any orthonormal basis of \( V \). Moreover, \( I(V) \) is a \( K \)-subspace of dimension \( m - 1 \), and \( I(V)^- \subseteq I(V) \) if and only if \( m \) is even.

**Proof.**
1. The proof follows immediately from the fact that the characteristic of \( K \) is two.
2. The proof is trivial.
3. Clearly \( \{ 1 \} \subseteq I(V)^- \), since for all \( v \in V \) we have \( B(v, v) = B(1, 1)^2 \). On the other hand, if \( v \in I(V)^- \), then \( v \in e_i \oplus e_j \) for all \( 1 \leq i < j \leq m \). Hence, \( 0 = B(v, e_i \oplus e_j) = B(v, e_i) \oplus B(v, e_j) \), i.e., \( B(v, e_i) = B(v, e_j) \), and since \( v = \bigoplus_{i=1}^{m} B(v, e_i) e_i \), we get that \( v \in \{ 1 \} \). The equality \( \dim_K I(V) = m - 1 \) follows from [14, Theorem 11.8]. Finally, \( B(1, 1) = m (\mod 2) \), so that \( I(V)^- \subseteq I(V) \) if and only if \( m \) is even.

As we have just seen, the subspace \( I(V)^- \) is generated by the element \( 1 = \bigoplus_{i=1}^{m} e_i \), which depends on a chosen orthonormal basis \( \{ e_1, \ldots, e_m \} \). We shall see that this element can be actually defined independently of a choice of basis.

**Remark 1.** The vector \( 1 \) can be defined as an element in \( V \) such that \( B(v, v) = B(1, 1)^2 \), for all \( v \in V \). This element is uniquely defined since any other element \( w \) with the same property must be contained in \( I(V)^- = \{ 1 \} \), so that \( w = \lambda 1 \), where \( \lambda \in K \). Now, \( B(1, 1) = B(1, w)^2 = B(1, 1)^2 = \lambda^2 B(1, 1)^2 = \lambda^2 B(1, 1) \), so, if \( 1 \) is not isotropic, then \( \lambda = 1 \). Otherwise, consider a vector \( z \) such that \( B(z, 1) = 1 \). Hence, \( 1 = B(z, 1)^2 = B(z, z) = B(1, 1)^2 = \lambda^2 B(1, 1)^2 = \lambda^2 \), so that \( \lambda = 1 \). From now on we will consider \( 1 \) as the unique element defined in this way.

Our next task is to study the behavior of the subspace \( I(V)^- \) when isometries of the metric space are considered.

**Definition 2.** Let \( V_1 \) and \( V_2 \) be two vector spaces over \( K \), \( V_1 \) and \( V_2 \) of dimension \( m \), and let \( B_i : V_i \to K \) \( (i = 1, 2) \) be two nonsingular symmetric bilinear forms. Then a linear map \( f : V_1 \to V_2 \) is said to be a \((B_1, B_2)\)-isometry if \( B_1(v, w) = B_2(f(v), f(w)) \), for all \( v, w \in V_1 \).

Now, Wall's Lemma [16, Corollary to Lemma 1.2.2] is stated and a direct proof is given.

**Lemma 1.** Let \( V \) be a vector space over \( K \) and let \( B : V \to K \) be a nonsingular symmetric bilinear form. Then, \( v \in I(V)^- \) if and only if \( v \) is fixed by any \((B, B)\)-isometry of \( V \).
Proof. ⇒: If $B$ is alternating, $I(V)^\perp = \{0\}$ and it is obvious.

If $B$ is nonalternating, it is clear that the subspace $I(V)^\perp$ is invariant under any $(B, B)$-isometry. To see that it is elementwise fixed by any $(B, B)$-isometry $f : V \to V$ it is enough to show that $f(1) = 1$. But this is clear from Remark 1, since for all $v \in V$,

$$B(v, f(1))^2 = B(f(f^{-1}(v)), f(1))^2 = B(f^{-1}(v), 1)^2 = B(f^{-1}(v), f^{-1}(v)) = B(v, v).$$

$\Leftarrow$: Let us assume that $v \notin I(V)^\perp$, so we can find $z \in I(V)$ such that $B(v, z) \neq 0$. If $v$ is isotropic, then $(v, z)$ is a linearly independent set and the restriction $B|_{v, z}$ is nonsingular. Therefore $V$ decomposes as the orthogonal sum $(v, z) \oplus (v, z)^\perp$. The map $f : V \to V$ given by $\lambda v + \mu z + x \mapsto \mu v + \lambda z + x$ is a $(B, B)$-isometry of $V$ not fixing $v$, which is not possible. If $v$ is not isotropic, then let $y = v + z$. Then $(v, y)$ is a linearly independent set, $B(y, y) = B(v, v)$, and the restriction $B|_{v, y}$ is nonsingular. Therefore $V$ decomposes as the orthogonal sum $(v, y) \oplus (v, y)^\perp$. The map $f : V \to V$ given by $\lambda v + \mu y + x \mapsto \mu v + \lambda y + x$ is a $(B, B)$-isometry of $V$ not fixing $v$, which is also not possible. $\Box$

**Corollary 1.** Let $V_1$ and $V_2$ be two vector spaces over $K$, and let $B_i : V_i \to K (i = 1, 2)$ be nonsingular symmetric bilinear forms. If $\psi : V_1 \to V_2$ is a $(B_1, B_2)$-isometry then $v \in I(V_1)^\perp$ if and only if $f(v) = \psi(v)$, for any other $(B_1, B_2)$-isometry $f : V_1 \to V_2$.

Proof. If $f : V_1 \to V_2$ is a $(B_1, B_2)$-isometry, then $f^{-1} : V_2 \to V_1$ is a $(B_1, B_1)$-isometry. It is clear that any $(B_1, B_1)$-isometry can be presented in this way. From the former lemma we have that $v \in I(V_1)^\perp$ if and only if $f^{-1}(v) = v$, i.e., $f(v) = \psi(v)$. $\Box$

### 3.2. $I(V)^\perp$ and Galois Ring valued quadratic forms

Next we shall study properties of the subspace $I(V)^\perp$ when a nonsingular Galois Ring valued quadratic form $Q$ is considered ($B_0$ is nonalternating). In particular, we shall show the relation between the invariant $I(Q)$ and the valuation of $Q$ in the vector 1.

**Proposition 2.** If $Q$ is a nonsingular $R$-valued quadratic form of type $(\lambda_1, \ldots, \lambda_m)$, then

$$Q(1) = \begin{cases} 2(\lambda_1 \oplus \cdots \oplus \lambda_m), & \text{if } m \equiv 0(\text{mod } 4) \\ 1 + 2(\lambda_1 \oplus \cdots \oplus \lambda_m), & \text{if } m \equiv 1(\text{mod } 4) \\ 2(\lambda_1 \oplus \cdots \oplus \lambda_m \oplus 1), & \text{if } m \equiv 2(\text{mod } 4) \\ 1 + 2(\lambda_1 \oplus \cdots \oplus \lambda_m \oplus 1), & \text{if } m \equiv 3(\text{mod } 4). \end{cases}$$

That is, $Q(1) = I(Q)(\text{mod } 4)$.

Proof. It is a straightforward checking. Namely, let $\{e_1, \ldots, e_m\}$ be an orthonormal basis of $(V, B_0)$. If $m = m_0 + 2m_1 + 2^2m_2$, where $m_0, m_1 \in \{0, 1\}$, then,

$$Q(1) = Q \left( \bigoplus_{i=1}^m e_i \right) = \sum_{i=1}^m (1 + 2\lambda_i) = m + 2 \sum_{i=1}^m \lambda_i = m_0 + 2 \left( \bigoplus_{i=1}^m \lambda_i \oplus m_1 \right).$$

On the other hand,

$$I(Q)(\text{mod } 4) = \sum_{i=1}^m (1 + 2\lambda_i + 2^2\lambda_i)(\text{mod } 4) = \sum_{i=1}^m (1 + 2\lambda_i)(\text{mod } 4) = Q(1). \Box$$

As we have just seen, the vector 1 contains relevant information about the Galois Ring valued quadratic form $Q$. This fact is even more clearly noticed when we consider isometries of metric spaces.

**Definition 3.** Let $(V_1, Q_1)$ and $(V_2, Q_2)$ be two nonsingular metric vector spaces, $V_1$ and $V_2$ of dimension $m$ over $K$. Then, a linear map $f : V_1 \to V_2$ is said to be a $(Q_1, Q_2)$-isometry, if $Q_1(v) = Q_2(f(v))$, for all $v \in V_1$.

**Remark 2.** Any $(Q_1, Q_2)$-isometry $f : V_1 \to V_2$ is also a $(B_{Q_1}, B_{Q_2})$-isometry.

**Remark 3.** Two nonsingular $R$-valued quadratic forms $Q_1, Q_2$ defined over the same vector space $V$ are equivalent if and only if the nonsingular metric vector spaces $(V, Q_1)$ and $(V, Q_2)$ are $(Q_1, Q_2)$-isometric.

As a consequence of Remarks 1 and 2 we have the following result.

**Corollary 2.** Let $(V_1, Q_1)$ and $(V_2, Q_2)$ be two nonsingular metric vector spaces. If $f : V_1 \to V_2$ is a $(Q_1, Q_2)$-isometry, then:

1. $f(1_{V_1}) = 1_{V_2}$.
2. If $S_1$ is a subspace of $V_1$ and $S_2 = f(S_1)$, then $f|_{S_1 \to S_2} : S_1 \to S_2$ is a $(Q_1|_{S_1}, Q_2|_{S_2})$-isometry and $f(S_1 \cap I(V_1)^\perp) = S_2 \cap I(V_2)^\perp$. 


4. Witt’s cancelation and extension theorems

In this section we will prove Witt’s cancelation and extension theorems for nonsingular Galois Ring valued quadratic forms. Our approach follows the one given in [14] for ordinary nonsingular bilinear forms. So, first we shall obtain the cancelation theorem and, as a consequence, the extension theorem. Our proof of the cancelation theorem is based on properties of the invariant $I$. As we shall see, the subspace $I(V)^\perp$ and its singular properties play an important role in the context of these theorems.

**Theorem 1.** Let $(V_1, Q_1)$ and $(V_2, Q_2)$ be two nonsingular $(Q_1, Q_2)$-isometric spaces, with isometry $\varphi : V_1 \to V_2$. Let $(S_1, Q_{1|S_1})$ and $(S_2, Q_{2|S_2})$ be two nonsingular $(Q_{1|S_1}, Q_{2|S_2})$-isometric subspaces of $V_1$ and $V_2$ with isometry $f : S_1 \to S_2$, such that the following orthogonal decompositions hold: $V_1 = S_1 \oplus S_1^\perp$ and $V_2 = S_2 \oplus S_2^\perp$. Then, $(S_1^\perp, Q_{1|S_1}^\perp)$ and $(S_2^\perp, Q_{2|S_2}^\perp)$ are $(Q_{1|S_1}^\perp, Q_{2|S_2}^\perp)$-isometric if and only if $f(S_1 \cap I(V_1)^\perp) = S_2 \cap I(V_2)^\perp$.

**Proof.** Let us suppose that $(S_1^\perp, Q_{1|S_1}^\perp)$ and $(S_2^\perp, Q_{2|S_2}^\perp)$ are $(Q_{1|S_1}^\perp, Q_{2|S_2}^\perp)$-isometric, with isometry $f' : S_1^\perp \to S_2^\perp$ given by $(f')^*(s + s') = f(s) + f(s')$, for all $s \in S_1^\perp$, $s' \in S_1^\perp$, is a $(Q_2, Q_2)$-isometry of $V_1$ and $V_2$ such that $(f + f')(S_1 \cap I(V_1)^\perp) = f(S_2 \cap I(V_2)^\perp)$. So, from Corollary 2 the condition is necessary.

Conversely, if the condition holds, since $(V_1, Q_1)$ and $(V_2, Q_2)$ are $(Q_1, Q_2)$-isometric, their invariants must be the same, i.e., $I(Q_1) = I(Q_2)$. Moreover, in view of the orthogonal decompositions of the spaces $(V_1, Q_1)$ and $(V_2, Q_2)$, and the second property of [10, Theorem 3] we have that $Q_{1|S_1}^\perp, Q_{1|S_1}^\perp, Q_{2|S_2}^\perp, Q_{2|S_2}^\perp$ are nonsingular $R$-valued quadratic forms and that $Q_{1|S_1}^\perp + Q_{1|S_1}^\perp = I(Q_1) = I(Q_2) = I(Q_{1|S_1}) + I(Q_{2|S_2})$. The $(Q_{1|S_1}^\perp, Q_{2|S_2}^\perp)$-isometry of $(S_1, Q_{1|S_1})$ and $(S_2, Q_{2|S_2})$ provides $I(Q_{1|S_1}) = I(Q_{2|S_2})$, and so $I(Q_{1|S_1}^\perp) = I(Q_{2|S_2}^\perp)$. To conclude our result we need only to show that $B_{Q_{1|S_1}^\perp}$ and $B_{Q_{2|S_2}^\perp}$ are both alternating at the same time or not. If $B_{Q_{1|S_1}^\perp}$ (and so $B_{Q_{2|S_2}^\perp}$) is alternating, then both $B_{Q_{1|S_1}^\perp}$ and $B_{Q_{2|S_2}^\perp}$ are clearly alternating and we are done. If, on the other hand, $B_{Q_{1|S_1}^\perp}$ (and so $B_{Q_{2|S_2}^\perp}$) is not alternating, then we have two cases.

The first one is when $B_{Q_{1|S_1}^\perp}$ (and so $B_{Q_{2|S_2}^\perp}$) is alternating, so that $B_{Q_{1|S_1}^\perp}$ must be necessarily not alternating, and the same argument applies to conclude that $B_{Q_{2|S_2}^\perp}$ is not alternating.

The second case is when $B_{Q_{1|S_1}^\perp}$ (and so $B_{Q_{2|S_2}^\perp}$) is not alternating. Then we have that $B_{Q_{1|S_1}^\perp}$ is alternating iff $S_1^\perp \subseteq I(V_1)$ iff $I(V_1)^\perp \subseteq S_1$ iff $S_1 \cap I(V_1)^\perp = (V_1)^\perp$. From our hypothesis $f(S_1 \cap I(V_1)^\perp) = S_2 \cap I(V_2)^\perp$ we get that $B_{Q_{1|S_1}^\perp}$ is alternating iff $f(I(V_1)^\perp) = f(S_1 \cap I(V_1)^\perp) = S_2 \cap I(V_2)^\perp \subseteq I(V_2)^\perp$, i.e., $f(I(V_1)^\perp) = S_2 \cap I(V_2)^\perp = I(V_2)^\perp$ (the dimension of both $f(I(V_1)^\perp)$ and $I(V_2)^\perp$ is one), which is equivalent to $B_{Q_{2|S_2}^\perp}$ alternating. The theorem is proved.

With the cancelation theorem in hand we can now give the following version of Witt’s extension theorem. In the particular case of the Galois Ring $R = \mathbb{Z}_4$, we get [18, Theorem in Section 4].

**Theorem 2.** Let $(V_1, Q_1)$ and $(V_2, Q_2)$ be two nonsingular $(Q_1, Q_2)$-isometric spaces, with isometry $\varphi : V_1 \to V_2$. Let $S_1$ be a subspace of $V_1$, and $f : S_1 \to V_2$ be a linear map such that $Q_2(f(v)) = Q_1(v)$, for all $v \in S_1$. Then, $f$ can be extended to a $(Q_1, Q_2)$-isometry of $(V_1, Q_1)$ and $(V_2, Q_2)$, if and only if

1. $f(S_1 \cap I(V_1)^\perp) = f(S_1) \cap I(V_2)^\perp$.
2. $f|_{S_1 \cap I(V_1)^\perp}$ is the map $\varphi|_{S_1 \cap I(V_1)^\perp}$.

**Proof.** If $f$ can be extended to a $(Q_1, Q_2)$-isometry of $(V_1, Q_1)$ and $(V_2, Q_2)$, then from Corollaries 1 and 2 the conditions are necessary.

As for the sufficiency we distinguish the cases $B_{Q_1}$ (and so $B_{Q_2}$) alternating and not alternating. In the alternating case $Q_2 = 2Q'_i$, $i = 1, 2$, where $Q'_i : V \to K$ is an ordinary quadratic form. Notice that, in this case, $I(V_1)^\perp = (0)$ and $I(V_2)^\perp = (0)$, so that the conditions of the theorem give no information. The proof given in [5, Section 1.4] for ordinary quadratic forms applies here to conclude the result.

If $B_{Q_2}$ (and so $B_{Q_2}$) is not alternating, then we can suppose that $I(V_1)^\perp = (1) \subseteq S_1$, since if $1 \not\subseteq S_1$, then the extension of $f$ to $(1)$ by setting $f(\lambda 1) = \lambda \varphi(1)$, for all $\lambda \in K$, provides the desired inclusion. Namely, $Q_1(1) = Q_2(\varphi(1)) = Q_2(f(1))$ and, for all $v \in S_1$, $B_{Q_2}(v, 1) = B_{Q_2}(v, \varphi(1)) = B_{Q_2}(f(v), \varphi(1)) = B_{Q_2}(f(v), 1)$.

Now, if $m$ is odd, then $B_{Q_1}(1, 1) = 1$, i.e., $B_{Q_1|I(V_1)^\perp}$ is nonsingular, which provides the orthogonal decomposition $V_1 = I(V_1)^\perp \oplus I(V_1)$ [14, Theorem 11.9]. Now $S_1 = I(V_1)^\perp \oplus (S_1 \cap I(V_1))$, and the map $f|_{S_1 \cap (I(V_1)^\perp \oplus I(V_2))) : S_1 \cap I(V_1) \to I(V_2)$ can be extended to a $(Q_{1|S_1}^\perp, Q_{2|S_2}^\perp)$-isometry $f' : I(V_1) \to I(V_2)$ (notice that $I(V_1), Q_{1|S_1}^\perp$, and $I(V_2), Q_{2|S_2}^\perp$ are $(Q_{1|S_1}^\perp, Q_{2|S_2}^\perp)$-isometric subspaces with $B_{Q_1|I(V_1)}$ and $B_{Q_2|I(V_2)}$ nonsingular alternating, so that the alternating case applies). The map $f|_{I(V_1)^\perp \oplus I(V_2)} : V_1 \to V_2$ is the desired extension of $f$.

On the other hand, if $m$ is even, then $1 \in I(V_1)$. If $1 \not\subseteq I(V_1)$, then take $z \in I(V_1) \setminus I(V_2)$ with $B_{Q_1}(z, z) = 1$, so that $B_{Q_1}(z, 1) = 1$. Then, $(z, 1)$ is a linearly independent set and $B_{Q_1|z, 1}$ is nonsingular. So, $V_1$ decomposes as the orthogonal sum $(z, 1) \oplus (z, 1)^\perp$. 

2497
where \( \langle z, 1 \rangle^\perp \subseteq I(V_1) \). Now, \( S_1 = \{ z, 1 \} \oplus (S_1 \cap \langle z, 1 \rangle^\perp) \), and the map \( f|_{S_1 \cap \langle z, 1 \rangle^\perp} : S_1 \cap \langle z, 1 \rangle^\perp \to \langle f(z), f(1) \rangle^\perp \) can be extended to a \((Q_1|_{\langle z, 1 \rangle^\perp}, Q_2|_{\langle f(z), f(1) \rangle^\perp})\)-isometry \( f' : \langle z, 1 \rangle^\perp \to \langle f(z), f(1) \rangle^\perp \). Notice that \( B_{Q_1|_{\langle z, 1 \rangle^\perp}} \) is nonsingular alternating, that \( \langle z, 1 \rangle^\perp \) and \( \langle f(z), f(1) \rangle^\perp \) are \((Q_1|_{\langle z, 1 \rangle^\perp}, Q_2|_{\langle f(z), f(1) \rangle^\perp})\)-isometric because of the cancelation theorem, and so we can apply the alternating case of the Extension Theorem. The map \( f|_{\langle z, 1 \rangle^\perp} : V_1 \to V_2 \) is the desired extension of \( f \).

Finally, if \( S_1 \subseteq I(V_1) \), then we shall show that we can extend \( f \) to a subspace \( S_1 + \langle z \rangle \), where \( z \notin I(V_1) \), so that the former case applies. Consider a basis \( \{ v_1, v_2, \ldots, v_s \} \) of \( S_1 \), and extend it to get a basis \( \{ v_1, v_2, \ldots, v_s, v_{s+1}, \ldots, v_{m-1} \} \) of \( I(V_1) \). Notice that \( B_{Q_2(v_s, v_{s+1})} \) is nonsingular, since any vector \( v \in \langle v_2, \ldots, v_{m-1} \rangle \subseteq I(V_1) \) such that \( B_{Q_2}(v, v_i) = 0 \), for all \( i = 2, \ldots, m - 1 \), is contained in \( I(V_1) \perp \) (because \( B_{Q_2}(v, 1) = 0 \)), and so \( v = 0 \). Therefore, we can substitute the basis \( \{ v_2, \ldots, v_{m-1} \} \) of \( \langle v_2, \ldots, v_{m-1} \rangle \) by a symplectic one \( \{ v_2, w_3, \ldots, w_{n-2}, w_{n-1} \} \), i.e., \( B_{Q_2}(w_2, w_3) = 1 \), for all \( i = 1, \ldots, (m - 2)/2 \) and 0 in the remaining cases. Take \( z \notin I(V_1) \) such that \( B_{Q_2}(z, z') = 1 \), and define:

\[
z = z' + \sum_{i=1}^{m-1} (B_{Q_2}(z', w_{2i-2})w_{2i-1} + B_{Q_2}(z', w_{2i})w_{2i}).
\]

Then \( B_{Q_2}(z, z) = 1 \) and \( B_{Q_2}(z, w_j) = 0 \), for all \( j = 2, \ldots, m - 1 \). Finally, extend the map \( f \) to \( S_1 + \langle z \rangle \), by setting \( f(z) = \varphi(z) \). This can be done since \( Q_2(z) = Q_2(\varphi(z)) = Q_2(f(z)) \), \( B_{Q_2}(z, 1) = B_{Q_2}(\varphi(1), \varphi(z)) = B_{Q_2}(f(1), f(z)) \), and \( B_{Q_2}(z, v_i) = 0 \), for all \( i = 2, \ldots, s \). The theorem is proved. \( \square \)

5. Clifford algebras and the invariant \( I \)

In this section, we will give an explanation to the invariant \( I \) in terms of Clifford algebras. These objects provide the necessary tools to classify ordinary quadratic forms over a finite field of characteristic 2. In particular, the Arf invariant classifies completely these forms, as seen in Section 2.3. This classification is naturally extended to Galois Ring valued quadratic forms when the associated nonsingular bilinear form is alternating. Our aim is to explain also the nonalternating case. So let us begin by collecting the known results in the alternating case.

**Remark 4.** If \( Q : V \to R \) is an \( R \)-valued quadratic form such that \( B_Q \) is nonsingular alternating, then:

1. \( Q = 2Q' \), where \( Q' : V \to K \) is an ordinary nonsingular bilinear form.
2. The center of the even part of the Clifford algebra \( C((Q', V)) \) is isomorphic to an algebra \( K[x]/(x^2 \oplus x \oplus \Delta) \), where \( \Delta \in K \).
3. The element \( \Delta \) is uniquely determined in the additive group \( K/K^+ \), and it can be constructed from any \( B_Q \)-symplectic basis \( \{ e_1, \ldots, e_n \} \) of \( V \) by the following way:

\[
\Delta = \bigoplus_{i=1}^{\frac{n}{2}} Q'(e_{2i-1})Q'(e_{2i}).
\]
4. The equality \( I(Q) = 4\Delta \) holds.

As we can see, the invariant \( I(Q) \) can be explained in terms of the ordinary quadratic form \( Q' \). In the nonalternating case we shall see that a similar ordinary quadratic form can be also used to explain the invariant \( I \).

**Definition 4.** Let \( Q : V \to R \) be a nonsingular \( R \)-valued quadratic form. We define \( Q' : V \to K \) by the following way:

\( Q'(v) = Q(v)_1, \) for all \( v \in V \).

**Remark 5.** If \( B_Q \) is alternating, then the definition of \( Q' \) agrees with the ordinary quadratic form \( Q' \) of Remark 4.

In the following result we show relevant properties of the form \( Q' \).

**Proposition 3.** Let \( Q : V \to R \) be a nonsingular \( R \)-valued quadratic form where \( V \) is a vector space of dimension \( m \) over \( K \). Then \( Q' : V \to K \) is an ordinary quadratic form with associated bilinear form:

\[
(\cdot, \cdot)_{Q'} : V \times V \to K,
\]

\[
(a, b) \mapsto B_Q(a, b) \oplus \sqrt{Q(a)Q(b)}.
\]

Moreover, \( (\cdot, \cdot)_Q \) is nonsingular iff \( m \) is even. If \( m \) is odd, then the rank of \( (\cdot, \cdot)_Q \) is \( m - 1 \).

**Proof.** Let us first see that \( Q' \) is a quadratic form. If \( \lambda \in K \) and \( a, b \in V \) then, since \( Q(\lambda a) = \lambda^2 Q(a) = \lambda^2 (Q(a)_0 + 2Q(a)_1) = \lambda^2 Q(a)_0 + 2\lambda^2 Q(a)_1 \), we have

\[
Q'(\lambda a) = Q(\lambda a)_1 = \lambda^2 Q(a)_1 = \lambda^2 Q(a).
\]
On the other hand, since $Q(a \oplus b) = Q(a) + Q(b) + 2B_Q(a, b) = (Q(a)_0 \oplus Q(b)_0) + 2(Q(a)_1 \oplus Q(b)_1) \oplus B_Q(a, b) \oplus \sqrt{Q(a)_0Q(b)_0}$, we get

$$Q'(a \oplus b) = Q(a \oplus b)_1 = Q(a)_1 \oplus Q(b)_1 \oplus B_Q(a, b) \oplus \sqrt{Q(a)_0Q(b)_0} = Q'(a) \oplus Q'(b) \oplus (a, b)_{Q'}.$$ Clearly $(\cdot, \cdot)_{Q'}$ is a symmetric map and it is also bilinear:

$$(\lambda a \oplus \mu b, c)_{Q'} = B_Q(\lambda a \oplus \mu b, c) \oplus \sqrt{Q(Q(a) + \mu Q(b) + 2B_Q(\lambda a, \mu b))_0Q(c)_0}$$

for all $\lambda, \mu \in K$, and for all $a, b, c \in V$. So, $Q'$ is an ordinary quadratic form.

Let us now study the rank of the bilinear form $(\cdot, \cdot)_{Q'}$. If $B_Q$ is alternating, then $(\cdot, \cdot)_{Q'} = B_Q$, and so $(\cdot, \cdot)_{Q'}$ is nonsingular. On the contrary, if $B_Q$ is not alternating, then we fix a $B_Q$-orthonormal basis $\{e_1, \ldots, e_m\}$ of $V$. For this basis we have $(e_i, e_j)_{Q'} = B_Q(e_i, e_j) \oplus \sqrt{Q(e_i)_0Q(e_j)_0} = \delta_{ij} \oplus 1$, for all $1 \leq i, j \leq m$. If $m$ is even, let us consider the set $\{e_1, e_2; e_1 \oplus e_2 \oplus e_3, e_3 \oplus e_4; \ldots; e_{m-2} \oplus \cdots \oplus e_m \}$. It is straightforward to check that this is a $(\cdot, \cdot)_{Q'}$-symplectic basis of $V$, so that $(\cdot, \cdot)_{Q'}$ is nonsingular alternating.

If $m$ is odd, the first $m - 1$ elements of the $B_Q$-orthonormal basis $\{e_1, \ldots, e_m\}$ can be used to construct a $(\cdot, \cdot)_{Q'}$-symplectic basis of the subspace $S$ that they expand. Namely, $\{e_1, e_2, e_1 \oplus e_2 \oplus e_3, e_3 \oplus e_4; \ldots; e_{m-2} \oplus \cdots \oplus e_m \}$. If we add to this basis the element $1$, then we get a basis of $V$. It is straightforward to check that $1$ is $(\cdot, \cdot)_{Q'}$-isotropic and orthogonal to $S$. Hence, the rank of $(\cdot, \cdot)_{Q'}$ is $m - 1$. □

Next we show how the invariant $I$ of the form $Q$ is related to the form $Q'$, even in the nonalternating case. We shall first consider the case of even dimension.

**Theorem 3.** Let $Q : V \rightarrow R$ be a nonsingular $R$-valued quadratic form, with $V$ of even dimension and $B_Q$ nonalternating. Then:

$$I(Q) = 2Q'(1) + 2^2 \text{Arf}(Q').$$

**Proof.** From Proposition 2, $m$ being even, $Q(1)_0 = 0$ and $Q(1) = I(Q)(\text{mod } 4)$. Then, $I(Q)_0 = 0$ and $I(Q)_1 = Q(1) = Q'(1)$.

Let us check $I(Q)_2 = \text{Arf}(Q')$.

Notice that, since $m$ is even, we can write $m = 2m_1 + 2^2m_2 + 2^3m'$, with $m_1, m_2 \in \{0, 1\}$.

Let $\{e_1, \ldots, e_m\}$ be a $B_Q$-orthonormal basis of $V$ and $1 = \oplus_{i=1}^m e_i$. Let us assume that $Q$ is of type $(\lambda_1, \ldots, \lambda_m)$ with respect to the basis $\{e_1, \ldots, e_m\}$. From the proof of Proposition 3 we know that $\{e_1, e_2; e_1 \oplus e_2 \oplus e_3, e_3 \oplus e_4; \ldots; e_{m-2} \oplus \cdots \oplus e_m \}$ is a $(\cdot, \cdot)_{Q'}$-symplectic basis of $V$. Let us compute the Arf invariant of the form $Q'$ from this basis.

First, $Q(e_i) = 1 + 2\lambda_i$ for $1 \leq j \leq m$, and for all $1 \leq i \leq \frac{m}{2} - 1$, if we write $i = i_0 + 2i'$, with $i_0 \in \{0, 1\}$, then

$$Q(e_1 \oplus \cdots \oplus e_{2i+1}) = \sum_{j=1}^{2i+1} Q(e_j) = \sum_{j=1}^{2i+1} (1 + 2\lambda_j) = 1 + 2 \left( \sum_{j=1}^{2i+1} \lambda_j \oplus i_0 \right).$$

On the other hand, for all $1 \leq i \leq \frac{m}{2} - 1$, we have

$$Q(e_{2i+1} \oplus e_{2i+2}) = Q(e_{2i+1}) + Q(e_{2i+2}) = 1 + 2\lambda_1 + 1 + 2\lambda_2 = 2(\lambda_{2i+1} \oplus \lambda_{2i+2} \oplus 1),$$

so that

$$\text{Arf}(Q') = Q'(e_1)Q'(e_2) \oplus \bigoplus_{i=1}^{\frac{m}{2} - 1} Q'(e_1 \oplus \cdots \oplus e_{2i+1})Q'(e_{2i+1} \oplus e_{2i+2})$$

$$= \lambda_1 \lambda_2 \oplus \bigoplus_{i=1}^{\frac{m}{2} - 1} (\lambda_1 \oplus \cdots \oplus \lambda_{2i+1} \oplus i \text{ (mod } 2)) (\lambda_{2i+1} \oplus \lambda_{2i+2} \oplus 1)$$

$$= \lambda_1 \lambda_2 \oplus \bigoplus_{i=1}^{\frac{m}{2} - 1} ((\lambda_1 \oplus \cdots \oplus \lambda_{2i}) (\lambda_{2i+1} \oplus \lambda_{2i+2}) \oplus (\lambda_1 \oplus \cdots \oplus \lambda_{2i})$$

$$\oplus \lambda_{2i+1} (\lambda_{2i+1} \oplus \lambda_{2i+2} \oplus 1) \oplus i \text{ (mod } 2)) (\lambda_{2i+1} \oplus \lambda_{2i+2} \oplus 1).$$
We have that It is clear that Since both Then, for all \( \mu \): \( q \rightarrow q(\mu) \). \( \mu \) is singular, since its rank is \( 2 \). Let us check We also have so that \( J(Q)_2 = \text{Arf}(Q) \), and \( J(Q) = 2Q(1) + 2^2 \text{Arf}(Q) \), as desired. In the case of odd dimension things are more complicated. From Proposition 3 we know that the ordinary quadratic form \( Q \) is singular, since its rank is \( m - 1 \). So we cannot consider directly this form to explain the invariant \( J(Q) \) as we did in the case of even dimension. We need first to extend \( Q \) to an \( R \)-valued quadratic form \( \overline{Q} \) over a space of even dimension, so that its associated ordinary quadratic form \( \overline{Q} \) provides the desired explanation. As we shall see below the extension \( \overline{Q} \) of \( Q \) introduces no extra information in the quadratic form \( Q \), since it is constructed from the valuation of \( Q \) in the vector 1.

Definition 5. Let \( Q : V \rightarrow R \) be a nonsingular \( R \)-valued quadratic form such that \( B_Q \) is nonalternating. Then, we define

Let \( Q : V \rightarrow K \) be an \( R \)-valued quadratic form over \( V \) of dimension \( m \) with \( B_Q \) nonalternating. Then \( \overline{Q} : V \times K \rightarrow R \) is an \( R \)-valued quadratic form with associated bilinear form \( B_{\overline{Q}} \) such that for all \( (v, \mu), (w, \lambda) \) in \( V \times K \):

Moreover, if \( V \) is a vector space of odd dimension \( m \), then \( \overline{Q} \) is a nonsingular \( R \)-valued quadratic form with \( B_{\overline{Q}} \) nonalternating bilinear form.

Proof. It is clear that \( \overline{Q} \) is the sum of the quadratic forms \( Q \) and \( Q_{0(1),0(1)} \) [10, Section 3.1], so \( \overline{Q} \) is an \( R \)-valued quadratic form.

Let us check \( B_{\overline{Q}} \). For all \( (v, \mu), (w, \lambda) \) in \( V \times K \),

Then, for all \( (v, \mu), (w, \lambda) \) in \( V \times K \),

Now, if \( m \) is odd, we have that \( \overline{Q} \) is the sum of the quadratic forms \( Q \) and \( Q_{0(1),0(1)} \) (see Proposition 2). Since both \( Q \) and \( Q_{0(1),0(1)} \) are nonsingular, we get that \( \overline{Q} \) is also nonsingular. Note that for all \( (v, \mu), (w, \lambda) \) in \( V \times K \), \( B_{\overline{Q}}((v, \mu), (w, \lambda)) = B_Q((v, w) + \lambda \cdot Q(1)) \). \( B_{\overline{Q}} \) is nonalternating.

If \( m \) is even, \( Q(1)_0 = 0 \) (see Proposition 2) and for all \( (v, \mu), (w, \lambda) \) in \( V \times K \), \( B_{\overline{Q}}((v, \mu), (w, \lambda)) = B_Q((v, w)) \). Let us consider \( B_{\overline{Q}} \)-orthonormal basis \( (e_1, \ldots, e_m) \) of \( V \) and \( (1, 0, \ldots, 0) \) a basis of \( V \times K \). Clearly, \( \text{rank}(B_{\overline{Q}}) = m \).

Proposition 5. If \( Q : V \rightarrow R \) is a nonsingular \( R \)-valued quadratic form over \( V \) of odd dimension \( m \) such that \( B_Q \) is nonalternating, then

Proof. We have that \( \overline{Q} \) is the sum of the quadratic forms \( Q \) and \( Q_{0(1),0(1)} \). Now, \( J(Q_{0(1),0(1)}) = 1 + 2Q(1) + 2^2Q(1) \), and \( J(Q) = Q(1) + 2^2J(Q)_2 = 1 + 2Q(1) + 2^2J(Q)_2 \) (see Proposition 2). From [10, Theorem 3], we obtain

\[ J(\overline{Q}) = J(Q) + J(Q_{0(1),0(1)}) \]

\[ = (1 + 2Q(1) + 2^2J(Q)_2) + (1 + 2Q(1) + 2^2Q(1)) = 2 + 2^2J(Q)_2 \]
Corollary 3. Let $Q : V \to R$ be a nonsingular $R$-valued quadratic form, with $V$ of odd dimension and $B_0$ not alternating. Then:

$$I(Q) = 1 + 2Q(1) + 2^2 \text{Arf}(Q).$$

As we have just seen the invariant $I$ for Galois Ring valued quadratic forms can be completely explained by valuations on the vector 1 and Arf invariants. These results can be translated into the language of Clifford algebras. Namely, the following result holds.

Theorem 4. Let $Q : V \to R$ be a nonsingular $R$-valued quadratic form over a vector space $V$ of dimension $m$, then:

1. If $B_0$ is alternating, $Z(C(C((V, Q'))_0) \cong K[x]/(x^2 \oplus x \oplus I(Q, 2))$.
2. If $B_0$ is nonalternating,
   (a) in the case where $m$ is odd,
   $$Z(C(C((V \times K, Q'))_0) \cong K[x]/(x^2 \oplus x \oplus I(Q, 2))$$
   and
   $$C((V, Q')) \cong C((V', Q'_1)) \otimes K[x]/(x^2 \oplus I(Q, 1)),$$
   where $V = V \oplus (1)$, and $Q'_1$ is a nonsingular $R$-valued quadratic form with $B_{Q'_1}$ alternating bilinear form,
   (b) in the case where $m$ is even,
   $$Z(C(C((V, Q'))_0) \cong K[x]/(x^2 \oplus x \oplus I(Q, 2))$$
   and
   $$C((V \times K, Q')) \cong C((V, Q'_1)) \otimes K[x]/(x^2 \oplus I(Q, 1)).$$

Proof. Let $Q : V \to R$ be a nonsingular $R$-valued quadratic form over a vector space $V$ of dimension $m$.

If $B_0$ is alternating, $Q = 2Q$ and $m$ is even. From Proposition 3, $Q'$ is a nonsingular ordinary quadratic form. Then,

$$Z(C(C((V, Q'))_0) \cong K[x]/(x^2 \oplus x \oplus \text{Arf}(Q')).$$

Now, by definition of $I(Q)$ in the case where $B_0$ is alternating, $I(Q, 2) = \text{Arf}(Q')$.

If $B_0$ is nonalternating, we have to study two different cases, $m$ is even or odd.

If $m$ is odd, $\mathcal{T}$ is a nonsingular $R$-valued quadratic form with $B_{\mathcal{T}}$ nonalternating bilinear form (see Proposition 4). Now, $m + 1$ is even and from Proposition 3, $\mathcal{T}'$ is a nonsingular ordinary quadratic form. Then,

$$Z(C(C((V \times K, \mathcal{T}'))_0) \cong K[x]/(x^2 \oplus x \oplus \text{Arf}(\mathcal{T}')).$$

Now, by Corollary 3, $I(\mathcal{T}, 2) = \text{Arf}(\mathcal{T})$.

On the other hand, if we consider the $R$-valued quadratic form $Q'$, as we have seen in the proof of Proposition 3, the first $m - 1$ elements of the $B_0$-orthonormal basis $\{e_1, \ldots, e_m\}$ can be used to construct a $(\cdot, \cdot)_Q$-symplectic basis of the subspace $V'$ that expand. Namely, $\{e_1, e_2, e_1 \oplus e_2 \oplus e_3, \ldots, e_1 \oplus e_2 \oplus \cdots \oplus e_{m-2}, e_{m-2} \oplus e_{m-1}\}$. If we add to this basis the element 1, then we get a basis of $V$. It is straightforward to check that 1 is $(\cdot, \cdot)_Q$-isotropic and orthogonal to $V'$. Hence,

$$C((V, Q')) \cong C((V', Q'_1)) \otimes C((1, Q'_1)) \cong C((V', Q'_1)) \otimes K[x]/(x^2 \oplus Q'(1)).$$

Note that $C((1, Q'_1))$ is a two-dimensional Clifford algebra isomorphic to $K[x]/(x^2 \oplus Q'(1))$. Now, by Corollary 3, $I(1, 1) = Q'(1)$.

If $m$ is even, from Proposition 3, $\mathcal{T}'$ is a nonsingular ordinary quadratic form. Then, $Z(C(C((V, Q'))_0) \cong K[x]/(x^2 \oplus x \oplus \text{Arf}(Q'))$.

Now, by Theorem 3, $I(\mathcal{T}, 2) = \text{Arf}(\mathcal{T})$.

Let us consider $\mathcal{T}$ and $\mathcal{T}'$ in the case where $m$ is even. From Propositions 2–4, for all $(\nu, \mu)$, $(\nu, \lambda)$ in $V \times K$,

$$B_{\mathcal{T}}((\nu, \mu), (\nu, \lambda)) = B_0((\nu, w), (\nu, w)) \quad \text{and} \quad B_{\mathcal{T}'}((\nu, \mu), (\nu, \lambda)) = B_{\mathcal{T}}((\nu, \mu), (\nu, \lambda)) \otimes \sqrt{Q((\nu, \mu))_0 Q((\nu, \lambda))_0} = B_0((\nu, w) \oplus \sqrt{Q((\nu, w)_0 Q((\nu, w))_0} = B_0((\nu, 0), (0, 1)) \text{ a basis of } V \times K.$$

Clearly, $B_0$ is $\mathcal{T}$-isotropic and orthogonal to $(e_0, 0)$ for all $i \in [1, \ldots, m]$, and rank($B_{\mathcal{T}'}$) = $m$. Then,

$$C((V, \mathcal{T})) \cong C((V, \mathcal{T}'_1)) \otimes C((K, \mathcal{T}'_1)) \cong C((V, \mathcal{T}'_1)) \otimes K[x]/(x^2 \oplus \mathcal{T}'((0, 1)))),$$

where $\mathcal{T}'((0, 1)) = \mathcal{T}((0, 1)) = (\mathcal{T}'(1)).$ Note that $C((K, \mathcal{T}'_1))$ is a two-dimensional Clifford algebra isomorphic to $K[x]/(x^2 \oplus \mathcal{T}'((0, 1))))$. Now, by Theorem 3, $I(\mathcal{T}) = Q'(1)$. 

6. Concluding remarks

We have proved Witt’s cancelation and extension theorems for quadratic forms that take values in Galois Rings of characteristic 4. Our results are based on properties of a certain invariant for these forms, and they extend some previous work by J.A. Wood. On the other hand, we have also provided an explanation of that invariant in terms of Arf invariants and Clifford algebras of closely related ordinary quadratic forms. The importance of the orthogonal subspace of the isotropic elements and the valuation of the quadratic form on it is revealed in our study.
Acknowledgments

This work has been partially supported by MEC 04-MTM-2004-08115-C04-01, FICYT (IB05-186) and MEC-MTM-2007-67884-C04-01.

References