BULL. AUSTRAL. MATH. SOC. 13M05, 12D15, 11E81
VOL. 73 (2006) [47–64]

A CLASS OF FINITE COMMUTATIVE RINGS CONSTRUCTED FROM WITT RINGS

THOMAS CRAVEN AND MONIKA VO

Motivated by constructions of Witt rings in the algebraic theory of quadratic forms, the authors construct new classes of finite commutative rings and explore some of their properties. These rings are constructed as quotient rings of a special class of integral group rings for which the group is an elementary 2-group. The new constructions are compared to other rings in the literature.

1. INTRODUCTION

Finitely generated reduced Witt rings of a formally real field are quite well understood. It was proved in [3, Theorem 2.1] that they can all be constructed by a very concrete recursive process. This has the advantage that theorems about them can be proved by induction via that recursion. These rings, as well as more general Witt rings of equivalence classes of quadratic forms, are prominent in the algebraic theory of quadratic forms (see for example [10, 11, 13]). By beginning with finitely generated reduced Witt rings (and generalisations thereof from [8]), and considering a type of finite quotient ring (which does *not* arise naturally in quadratic form theory), we are led to a large class of previously undescribed finite commutative rings.

We begin with the general ring theoretic setting of [8, 9] and specialise in the final section to rings which occur in quadratic form theory. In [8], Knebusch, Rosenberg and Ware define a class of commutative rings which are certain quotients of integral group rings. The aim of that paper was to provide a ring-theoretic approach to the study of Witt rings of equivalence classes of anisotropic quadratic forms over a field of characteristic not 2. The purpose of this paper is to develop a special class of finite rings within the general context of [8] which do not naturally occur in quadratic form theory. These will be called QWitt rings. A special subclass of these, called SQWitt rings, will be those which occur as quotients of Witt rings of fields. In spite of this, the majority of this paper is self-contained and requires no knowledge of the theory of quadratic forms. There are other quotient constructions in the literature for somewhat different classes of rings. We shall see in Section 4 how the quotient construction by Marshall in [13] fits with ours. It is not

Received 29th August, 2005

clear how the quotient construction of [6] fits with ours. The class of rings they begin with intersects ours in essentially the finitely generated Witt rings of formally real fields. It would be interesting to see what rings are generated by their quotient construction in the cases in which it fails to give back a ring in the class they begin with; however the abstract axiomatic form they use is so different as to make the comparison to ours quite nontrivial.

DEFINITION 1.1: ([8, Definition 3.12], [9, Section 3], [7, Section 1].) Let G be a group of exponent 2. A *Witt ring for* G is a quotient ring $R = \mathbb{Z}[G]/K$ such that R has only 2-torsion.

Several equivalent conditions are given in [8, Theorem 3.9]. The Witt ring of a field F is a ring of equivalence classes of nondegenerate quadratic forms where the group G can be taken to be the square factor group $\dot{F}/\dot{F}^2$. In general, these rings naturally break into two disjoint cases [8, Propositions 3.15, 3.16]: Either the ring R is torsion or the torsion subgroup equals the nilradical $\operatorname{Nil} R$. We work only with the latter class of rings here, as in [9]. All Witt rings of formally real fields are in this class. We shall factor out the torsion and assume that our rings are all torsion free and have nilradical equal to zero (that is, the ring is *reduced*). We shall later restrict to finite groups G in order to construct finite rings, but for now we work in greater generality. These rings have a very concrete description.

For any Witt ring $R = \mathbb{Z}[G]/K$, let X_R denote the set of ring homomorphisms from R to $\mathbb{Z}$. These are in bijective correspondence with the set of minimal, nonmaximal prime ideals of R [9, Lemma 3.3]. We shall follow the terminology coming from quadratic form theory and refer to X_R as the set of *signatures* of R. (When the Witt ring comes from a formally real field, it can also be viewed as the set of orderings of the field.) Giving X_R the induced Zariski topology makes it into a Boolean topological space (compact, Hausdorff and totally disconnected). In particular, it will be discrete when it is finite, so topology will play a minimal role in our considerations. When R is torsion free, it can be viewed as a subring of $\mathcal{C}(X_R, \mathbb{Z})$, the ring of continuous functions from X_R to $\mathbb{Z}$, where $\mathbb{Z}$ is endowed with the discrete topology; indeed, the element $r \in R$ induces the function $\widehat{r}\colon X_R \to \mathbb{Z}$ via $\widehat{r}(x) = x(r)$. As a subring of $\mathcal{C}(X_R, \mathbb{Z})$, the ring R is generated by 1 and all elements of the form $2\chi_U$, where χ_U is the characteristic function of the set U, and U ranges over the subsets of X_R of the form

$$H(a) = \{\, x \in X_R \mid x(a) = 1 \}\qquad (a \in G)$$

and their complements $H(-a)$. Furthermore, the sets U above form a subbasis for the topology of X_R, usually referred to as the *Harrison subbasis* [9, Section 3]. For a given ring R, we shall denote the collection of sets of the Harrison subbasis by $\mathcal{H}_R$. Notice that the set $\mathcal{H}_R$ is closed under symmetric difference of sets: $H(-a) + H(-b) = H(-ab)$. Conversely, given any subbasis of clopen (both closed and open) sets $\mathcal{H}$ for a Boolean

space X, which is closed under symmetric difference and complementation, one obtains a Witt ring in this way, where the group G is given by $\{ 1 - 2\chi_H \mid H \in \mathcal{H} \}$ [9, Proposition 3.8]. Since $\mathcal{H}_R$ is a group of exponent 2, we shall often think of it as a vector space over the two element field $\mathbb{F}_2$.

This gives us two rather different, but equivalent, ways of viewing these rings as the following proposition shows. It will be important to us to have both ways available in this paper. We include a proof because this does not seem to have ever been made explicit in the literature.

PROPOSITION 1.2. *Let $R = \mathbb{Z}[G]/K$ be a reduced Witt ring and let X_G be the space of signatures of $\mathbb{Z}[G]$. The canonical surjection $\varphi\colon \mathbb{Z}[G] \to R$ induces an injection $\widehat{\varphi}\colon X_R \to X_G$. Considering R and $\mathbb{Z}[G]$ as rings of continuous functions, the mapping φ is the restriction of functions from X_G to X_R.*

PROOF: If we view the spaces as sets of prime ideals, the mapping $\widehat{\varphi}$ is defined in the usual way, namely by $\widehat{\varphi}(P) = \varphi^{-1}(P)$. Since φ is surjective, this mapping is injective. The final claim comes from the fact that the following diagram commutes

$$\begin{array}{ccc} \mathbb{Z}[G] & \xrightarrow{\varphi} & R \\ \downarrow & & \downarrow \\ \mathcal{C}(X_G, \mathbb{Z}) & \xrightarrow{\text{res}} & \mathcal{C}(X_R, \mathbb{Z}) \end{array}$$

where the vertical maps are the injections defined above and the bottom mapping is restriction of functions. □

It should probably be emphasised here that, even though we begin with a well-studied class of rings, the quotients we work with, as in both Proposition 1.2 and what follows, are very different than the quotients studied previously (see, for example, [7, Proposition 1.8], [9, Lemma 4.15]). The results cited come from naturally occurring homomorphisms induced by field (or ring) extensions. Only very complicated field extensions would induce a homomorphism such as that in Proposition 1.2, and in most cases such an extension would not even be possible. This is because it is difficult to eliminate a subset of orderings which does not comprise a Harrison subbasic set. This issue is addressed explicitly for rational function fields in [4, Section 5]. Our interest for this paper is in the quotient rings $\overline{R} = \mathcal{C}\Big(X_R, \bigcup_{x \in X} \mathbb{Z}/(n_x)\Big)$, where $\overline{f} \in \overline{R}$ means $\overline{f}(x) \in \mathbb{Z}/(n_x)$ for each $x \in X$. As defined in [9], we say a subring of $\mathcal{C}(X, \mathbb{Z})$ satisfying Definition 1.1 is a Witt subring of $\mathcal{C}(X, \mathbb{Z})$.

DEFINITION 1.3: A *QWitt* ring is a ring $\overline{R}$ formed by taking the quotient ring of a Witt subring R of $\mathcal{C}(X, \mathbb{Z})$ with $|X| < \infty$, defined by taking the function $f \in R$ to a function $\overline{f}\colon X \to \cup\mathbb{Z}/(n_x)$ such that $\overline{f}(x) \in \mathbb{Z}/(n_x)$ for each $x \in X$. That is, the restriction mapping to each point $x \in X$ is composed with the quotient mapping $\mathbb{Z} \to \mathbb{Z}/(n_x)$. We shall refer to the set of numbers $\{n_x\}$ as the *data associated with* $\overline{R}$.

The rings defined by Knebusch, Rosenberg and Ware are somewhat more general than Witt rings of fields. The ones which do come from fields give us a more special class of rings. The following special subclass of QWitt rings, more closely associated with quadratic form theory, will be considered in Section 5.

DEFINITION 1.4: An *SQWitt* ring is a ring $\overline{R}$ formed by taking the quotient ring of a torsion free Witt ring $W(F)$ (for some formally real field F), viewed as a subring of $\mathcal{C}(X_F, \mathbb{Z})$ with $|X_F| < \infty$, defined by taking the function $f \in W(F)$ to a function $\overline{f}\colon X_F \to \cup\mathbb{Z}/(n_x)$ such that $\overline{f}(x) \in \mathbb{Z}/(n_x)$ for each $x \in X_F$. That is, the restriction mapping to a point $x \in X_F$ becomes the signature at the ordering associated with x composed with the quotient mapping $\mathbb{Z} \to \mathbb{Z}/(n_x)$.

Studying quotient rings of the sort mentioned here gives yet another way in which a Witt ring R can be obtained from the group ring as shown below. The observation is interesting, but its proof is immediate from our definitions. We shall improve this result in Section 4.

PROPOSITION 1.5. *Let $\mathbb{Z}[G]$ be a group ring with space of signatures X_G, and let S denote the image of its injection into $\mathcal{C}(X_G, \mathbb{Z})$. Let Y be any closed subspace of X_G. The ring R obtained by restricting functions in S to the subspace Y is isomorphic to the quotient of S obtained by replacing any function $f\colon X_G \to \mathbb{Z}$ with a function which agrees with $f(x)$ if $x \in Y$ and is zero otherwise. In terms of Definition 1.3, this means taking* $n_x = \begin{cases} 0, & \text{if } x \in Y \\ 1, & \text{if } x \notin Y \end{cases}$.

EXAMPLE 1.6. We consider the quotient of $\mathbb{Z}[\mathbb{Z}_2]$, where $|X| = |\{x, y\}| = 2$ and we take $n_x = 4$, $n_y = 8$. Then we view R as a subring of $\mathbb{Z}/(4) \times \mathbb{Z}/(8)$. If we write the group $\mathbb{Z}_2 = \{e, g\}$, then the homomorphism to $\mathcal{C}(X, \mathbb{Z})$ is $\mathbb{Z}[\mathbb{Z}_2] \xrightarrow{\varphi} R$ defined by $r \cdot e + s \cdot g \mapsto ([r+s]_4, [r-s]_8)$. This makes $\varphi(g) = (1, 7)$ and

$$(1.1)\quad R = \{(0,0),(1,1),(2,2),(3,3),(0,4),(1,5),(2,6),(3,7)\} \text{ (the image of } \mathbb{Z}) \cup \{(1,7),(2,0),(3,1),(0,2),(1,3),(2,4),(3,5),(0,6)\},$$

where $2\varphi(g) = (2,6) = (-2,-2)$ is back in the image of $\mathbb{Z}$ inside $\mathbb{Z}/(4) \times \mathbb{Z}/(8)$. The first set in (1.1) is isomorphic to $\mathbb{Z}/(8)$ and the second set is obtained by adding $\varphi(g)$ to each element of the first set. Thus, since R must be a quotient of $\mathbb{Z}/(8)[\{e, g\}]$ and it has 16 elements, it must be isomorphic to $\mathbb{Z}/(8)[\{e, g\}]/(2 + 2g)$. This ring has 16 elements since the ideal $(2 + 2g) = \{0, 2 + 2g, 4 + 4g, 6 + 6g\}$ has four elements.

This example shows that we are getting rings beyond the scope of [**13**], in which an attempt is made to capture Witt rings of fields in an axiomatic way. Indeed, the small Witt rings are all known [**13**, Section 5.5]; for characteristic 8, these rings must have order an odd power of 2. Thus the example above is among the most general rings

considered in [8]. In particular, it is a Witt ring for $G = \mathbf{Z}_2$, it has a unique maximal ideal and it has no other prime ideals [8, Proposition 3.16]. By [8, Lemma 3.21], the units have 2-power order. These are precisely the elements outside the maximal ideal

$$\mathfrak{m} = \{(0,0),(2,2),(0,4),(2,6),(2,0),(0,2),(2,4),(0,6)\} = \big((2,0),\ (0,2)\big).$$

Replacing g by x, we can view this ring as a quotient of a polynomial ring, namely $\mathbb{Z}_8[x]/(x^2-1, 2+2x)$, in which the maximal ideal is generated by $\{2, \overline{x}-1\}$, where $\overline{x}$ denotes the image of x in R.

EXAMPLE 1.7. More generally, we consider the quotient of $\mathbb{Z}[\mathbb{Z}_2]$, where $|X| = |\{x,y\}| = 2$ and we take $n_x = 2^m$, $n_y = 2^n$ with $m \leqslant n$. Now we view R as a subring of $\mathbb{Z}/(2^m) \times \mathbb{Z}/(2^n)$. If we write the group $\mathbb{Z}_2 = \{e, g\}$ as above, then the homomorphism $\mathbb{Z}[\mathbb{Z}_2] \xrightarrow{\varphi} R$ is defined by $r \cdot e + s \cdot g \mapsto \big([r+s]_{2^m}, [r-s]_{2^n}\big)$. This makes

$$R \cong \mathbb{Z}/(2^n) \cup \big(\mathbb{Z}/(2^n) + \varphi(g)\big) \cup \cdots \cup \big(\mathbb{Z}/(2^n) + 2^{m-2}\varphi(g)\big),$$

where

$$2^{m-1}\varphi(g) = (2^{m-1}, -2^{m-1}) = (-2^{m-1}, -2^{m-1}) = -2^{m-1}(1,1)$$

is back in the image of $\mathbb{Z}$. Thus, since R must be a quotient of $\mathbb{Z}/(2^n)$ and it has 2^{m+n-1} elements, it must be isomorphic to $\mathbb{Z}/(2^n)\big[\{e,g\}\big]/\big(2^{m-1}(1+g)\big)$. The ideal $\big(2^{m-1}(1+g)\big)$ has 2^{n-m+1} elements.

The previous two examples are sufficiently simple that they are included in the generalisations found in both sections 3 and 4.

We conclude this section with the following generalisation of [2, Lemma 3.7]. It is a combinatorial result which will be needed at various times in the sequel to obtain independence and counting results.

PROPOSITION 1.8. *Let $\mathcal{H}$ be a subbasis of clopen subsets of a Boolean space X which is closed under symmetric difference and complement.*

(1) *Assume that the collection $\mathcal{T} = \{H_1, \ldots, H_r\}$ of sets in $\mathcal{H}$ has the property that for any $T \subseteq \mathcal{T}$, there is a point x in every set in T and in none of the sets in the complement T^c. Then the collection of all intersections of sets in $\mathcal{T}$,*

$$\mathcal{S} = \left\{ \bigcap_{k=1}^{s} H_{i_k} \;\middle|\; s = 0, \ldots, r \right\}, \qquad (H_{i_k} \text{ distinct sets in } \mathcal{T})$$

is linearly independent in the $\mathbf{F}_2$-vector space $\mathcal{H}$. (Following the usual convention, an empty intersection is the space X.)

(2) *If $H_1, \ldots, H_r, X$ are $\mathbf{F}_2$-linearly independent and come from a group ring $\mathbb{Z}[G]$, with $|G| = 2^n = |X|$, then $\left|\bigcap_{i=1}^{r} H_i\right| = 2^{n-r}$.*

https://doi.org/10.1017/S0004972700038612 Published online by Cambridge University Press

PROOF: If $r = 0$ or $r = 1$, then $\mathcal{S} = \{X\}$ or $\mathcal{S} = \{H_1, X\}$ and we clearly have linear independence. Now assume that $r > 1$ and assume there is a dependence relation; write it in the form $\bigcap_{k=1}^{m} H_{i_k} = \sum_{i=1}^{p} A_i$, where the left hand side is chosen so that m is the maximal number of sets in any intersection in the relation and each A_i, $i = 1, \ldots, p$, is some intersection of (at most m) sets from $\mathcal{T}$. Intersect this equation with the intersection of all other sets H_i not among the H_{i_k} (if any), obtaining

$$A := \bigcap_{i=1}^{r} H_i = \sum_{i=1}^{p} B_i, \tag{1.2}$$

where all intersections on the right hand side (denoted B_i) are now less than r-fold, since if the original A_i was an m-fold intersection, then some member of $\mathcal{T}$ is duplicated in the intersection. We shall show the impossibility of equation (1.2), eliminating one k at a time, where the intersections are k-fold in the right hand sum.

We first note that X does not occur in the sum, for by hypothesis (with $T = \emptyset$), there exists an element $x \in X$ not in any H_i, which would then lie in the right hand side of equation (1.2) but not the left. This is the $k = 0$ case. Next we claim that the sum of all 1-fold intersections must be empty. Otherwise, assume H_1, say, actually occurs in the sum. Choose an element $x \in H_1$ such that $x \notin H_i$, $i > 1$. Then x lies in the right hand side since it is found in precisely one term of the sum, but not the left. This argument continues. Having eliminated intersections of $k - 1$ subsets of $\mathcal{T}$, the sum of the k-fold intersections must be empty since if $\bigcap_{i=1}^{k} H_i$, say, actually occurs on the right, we know there exists an element $x \in \bigcap_{i=1}^{k} H_i$, but not in $\bigcup_{i=k+1}^{r} H_i$. Then x will lie in the right hand side but not in the left. This reduces the equation (1.2) to $A = \emptyset$, contradicting the hypothesis that A is nonempty.

The second claim is just [**2**, Lemma 3.7(b)]. □

2. THE DATA FOR QWITT RINGS

We show in this section that the only case in which interesting new rings occur is when the data are all powers of 2. It is well known that every finite commutative ring is a product of local rings [**12**]. Consequently, we are really interested only in the connected QWitt rings. Throughout this section R will denote a QWitt ring and X will be written for X_R.

THEOREM 2.1. *Let R be a QWitt ring with data n_x, $x \in X$. The ring R is local if and only if either every n_x is a power of 2 or $|X| = 1$ and n_x is a power of a prime.*

The only part that is clear, *a priori*, is that if $|X| = 1$ and $n_x = p^n$ for some prime p, then R is the local ring $\mathbb{Z}/(p^n)$. The remainder of the cases will be handled in a series of lemmas.

https://doi.org/10.1017/S0004972700038612 Published online by Cambridge University Press

LEMMA 2.2. *If some n_x is divisible by distinct primes $p \neq q$, then R is not local.*

PROOF: Viewing R as a subring of $\mathcal{C}\left(X, \bigcup_{x \in X} \mathbb{Z}_{n_x}\right)$, we construct the homomorphism $\varphi\colon R \to \mathbb{Z}_p$ as the composition $R \xrightarrow{\text{res}} \mathbb{Z}_{n_x} \to \mathbb{Z}_p$ where the first homomorphism is restriction of functions to the point x and the second is the canonical surjection. Similarly, we have a surjective homomorphism $\psi\colon R \to Z_q$. Since $\ker\varphi$ and $\ker\psi$ are distinct maximal ideals of R, the ring cannot be local. □

LEMMA 2.3. *If there exist $x, y \in X$ such that $n_x = p^r$ and $n_y = q^s$ for primes $p \neq q$ and integers $r, s \geqslant 1$, then R is not local.*

PROOF: The proof is similar to the previous lemma. We consider the homomorphisms $\varphi\colon R \xrightarrow{\text{res}} \mathbb{Z}_{n_x} \to \mathbb{Z}_p$ and $\psi\colon R \xrightarrow{\text{res}} \mathbb{Z}_{n_y} \to \mathbb{Z}_q$. Since $\ker\varphi$ and $\ker\psi$ are distinct maximal ideals of R, the ring cannot be local. □

LEMMA 2.4. *If $|X| \geqslant 2$ and each n_x is a nonzero power of an odd prime p, then R is not local.*

PROOF: In this case, we shall construct a nontrivial idempotent in R, showing that R is not connected and hence not local. By Definitions 1.1 and 1.3, there is a group G of exponent 2 such that R is a quotient of a Witt ring S for G. That is, we have vertical surjections and horizontal injections in the commutative diagram

$$\begin{array}{ccc} \mathbb{Z}[G] & & \\ \downarrow & & \\ S & \longrightarrow & \mathcal{C}(X, \mathbb{Z}) \\ \downarrow & & \downarrow \\ R & \longrightarrow & \mathcal{C}\left(X, \bigcup_{x \in X} \mathbb{Z}_{n_x}\right) \end{array} \tag{2.1}$$

Furthermore, we may assume that no element of G maps to a constant function ± 1 in $\mathcal{C}(X, \mathbb{Z})$, as we could then obtain S as a Witt ring for a quotient group of G. Since $|X| \geqslant 2$, the group G is nontrivial, so let $g \in G$, $g \neq e$; our assumption on G implies that $H(g) \neq \emptyset, X$. Let r be the maximum exponent of p for $x \in H(g)$ and consider the image $f \in R$ of the group ring element $(p^r + 1)/2e + (p^r + 1)/2g$. We obtain $f(x) = p^r + 1 \equiv 1 \pmod{n_x}$ for all $x \in H(g)$ and $f(x) = 0$ for all $x \notin H(g)$. Therefore f is a nontrivial idempotent element of R. □

LEMMA 2.5. *If each n_x is a power of 2, then R is a local ring. If we write $n_x = 2^{m_x}$, the maximal ideal of R is contained in*

$$\left\{ f\colon X \to \bigcup_{x \in X} \mathbb{Z}_{2^{m_x}} \;\middle|\; f(x) \equiv 0 \pmod 2 \quad \text{for all } x \in X \right\}. \tag{2.2}$$

https://doi.org/10.1017/S0004972700038612 Published online by Cambridge University Press

The units of R are contained in

$$\left\{ f\colon X \to \bigcup_{x\in X} \mathbb{Z}_{2^{m_x}} \;\middle|\; f(x) \equiv 1 \pmod 2 \quad \text{for all } x \in X \right\}. \tag{2.3}$$

PROOF: We again assume the situation of the commutative diagram (2.1). Since the elements of G have order at most 2, each $g \in G$ can take on only the values ± 1 at any point $x \in X$. Therefore any element of the group ring $\sum n_i g_i$ maps to an element $\sum n_i \widehat{g}_i$ of $\mathcal{C}(X, \mathbb{Z})$ with a parity condition:

$$\sum n_i \widehat{g}_i(x) \equiv \sum n_i \widehat{g}_i(y) \equiv \sum n_i \pmod 2 \qquad \text{for any } x, y \in X.$$

This parity carries over to elements of R as well since all n_x are powers of 2. From this it is clear that any element of R induces a function in one of the sets in (2.2) or (2.3). If an element of R induces a function f in the set in (2.3), then it is a unit in each $\mathbb{Z}_{2^{m_x}}$ and so some power of f is 1, making it a unit in R. On the other hand, the set of elements of R which map into the set in (2.2) is clearly an ideal, and hence must be the unique maximal ideal. □

3. Finite quotients of SAP Witt rings

The purpose of this section is to look at one of the two extreme cases of the definition; that where $S = \mathbb{Z} + \mathcal{C}(X, 2Z)$, which is a Witt ring of maximal size for the set X. These rings can be characterised in many ways, not the least of which is the *strong approximation property* (see [9, Theorem 3.20], [7, Proposition 1.23]), so we shall call them SAP rings. The importance of this case stems from the fact that every finitely generated Witt ring is a subring of one of these rings.

THEOREM 3.1. *Let X be a finite Boolean space and let R be a finite quotient of the associated SAP Witt ring with data $2^{m_x} > 1$ for $x \in X$. Then*

1. *R consists of all functions f on X with the parity condition $f(x) \equiv f(y) \pmod 2$ for all $x, y \in X$.*
2. *The function f is a unit in R if and only if its values are congruent to 1 modulo 2, and f is in the unique maximal ideal otherwise.*
3. *The cardinality of R is given by*

$$2 \prod_{x\in X} 2^{m_x - 1}. \tag{3.1}$$

PROOF: Statements (1) and (2) follow from Lemma 2.5 and the fact that R is a QWitt quotient of $\mathbb{Z} + \mathcal{C}(X, 2Z)$. For statement (3), we use that fact that each quotient ring $\mathbb{Z}/(2^m)$ has 2^{m-1} units and 2^{m-1} nonunits. Thus the group of units, which is the

https://doi.org/10.1017/S0004972700038612 Published online by Cambridge University Press

product of the units in each ring $\mathbb{Z}/(2^{m_x})$, has $\prod_{x\in X} 2^{m_x-1}$ elements and the maximal ideal, which is the product of the maximal ideals, has the same number. Together, these give $|R| = 2\prod_{x\in X} 2^{m_x-1}$. □

Since every QWitt ring is a subring of a ring described in the previous theorem by Lemma 2.5, we obtain a general description of the units and maximal ideal of a QWitt ring.

COROLLARY 3.2. *Let R be a QWitt ring with associated set X and data $2^{m_x} > 1$ for $x \in X$. Let $m = \max_{x\in X} m_x$. Then*

1. $\operatorname{char} R = 2^m$.
2. *There is a one-to-one correspondence between units of R and elements of the unique maximal ideal M given by $m \leftrightarrow 1 + m$ for any $m \in M$.*
3. $|M| = |R|/2$.

PROOF: The value of $\operatorname{char} R$ is clear. The rest follows from the fact that R/M is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. □

PRODUCTS OF QWITT RINGS. We can define products in the category of QWitt rings as follows: Give two QWitt rings, R_1 and R_2, let the maximal ideals be M_1, M_2 and the groups of units be U_1, U_2, respectively. (We know $U_i = 1 + M_i$ by the previous corollary.) Form the new ring $R = M_1 \times M_2 \cup U_1 \times U_2$. The set X_R is then just the disjoint union of X_{R_1} and X_{R_2}. It is well known that the (finitely generated) SAP Witt rings are products of copies of $\mathbb{Z}$ in the category of reduced Witt rings [3]; therefore the quotients of SAP Witt rings are products of the rings $\mathbb{Z}/(2^{m_x})$ as defined in this section. We return to products in Section 5.

4. FINITE QUOTIENTS OF INTEGRAL GROUP RINGS

The purpose of this section is to look at the other of the extreme cases of the definition; that where $\mathbb{Z}[G]$ is an integral group ring over a finite group G of exponent 2. This is the case where the size of the Harrison subbasis is as small as possible for a given cardinality of X. The importance of this case stems from the fact that every finitely generated Witt ring is a quotient ring of one of these rings. We begin by improving Proposition 1.5, seeing in the process that integral group rings are, in fact, the general case as well as one extreme.

THEOREM 4.1. *Let S be a Witt ring for a group G, with corresponding spaces of signatures $X_S \subseteq X_G$. Let R be a QWitt quotient of S. Then R is canonically isomorphic to a QWitt quotient R_0 of $\mathbb{Z}[G]$ for which $X_{R_0} = X_G$.*

PROOF: With R, we have the data n_x for $x \in X_S$. For $x \in X_G \setminus X_S$, set $n_x = 2$. The ring R_0 is defined by extending the functions in R to all of X_G as follows: Given

https://doi.org/10.1017/S0004972700038612 Published online by Cambridge University Press

$f \in R$, let $\alpha = \sum_{g \in G} n_g g$ be a preimage of f in $\mathbb{Z}[G]$. Since each g must map to ± 1 in $\mathbb{Z}$, we have a parity condition: $\alpha(x) \equiv \alpha(y) \pmod 2$ for all $x, y \in X_G$, and these values are clearly independent of how we lift f. Thus we can extend f to $x \in X_G \setminus X_S$ in only one reasonable way, defining $f(x)$ to be 0 or 1 according to the value of $\alpha(x)$ modulo 2. Therefore we obtain a QWitt quotient R_0 of $\mathbb{Z}[G]$, which is isomorphic to R since the extension of each function was uniquely determined. □

We now consider an integral group ring $\mathbb{Z}[G]$, where $|G| = 2^n$. Viewing the group G as a $\mathbb{F}_2$-vector space, it has a basis $g_1, \ldots, g_n$. We wish to explicitly compute the QWitt quotient ring R by determining the kernel of the homomorphism $\mathbb{Z}[G] \to R$. The ultimate goal is to compute the cardinality of R in terms of the data n_x which determine it. This seems to be very difficult in general. Until now, we have been able to ignore a potential ambiguity. In a general Witt ring for a group G of the form $R = \mathbb{Z}[G]/K$, the element -1 may or may not be identified with an element of the group G. This is not an issue for the integral group ring, but will be for counting elements in finite quotient rings. We now explicitly assume for the remainder of this paper that G is always the minimal choice for a group for a Witt ring R; in particular, -1 is not an element of G, so the elements of order 2 in R have the form $\pm g$ for $g \in G$. Note that for $\mathbb{Z}[G]$, if $|G| = 2^n$, then also $|X_G| = 2^n$ and each Harrison subbasic set H other than $\emptyset$ and X_G has cardinality 2^{n-1} [2, Theorem 3.8].

We shall need the concept of a *fan* from the quadratic form theory of formally real fields. For group rings, this has a particularly simple form. From [14], particularly Corollary 4.4(i), and [2, Section 3], one sees that the fans for X_G are precisely the nonempty intersections of sets in $\mathcal{H} = \{ H(\pm g) \mid g \in G \}$. We shall need the following special case of a very general theorem. For completeness, we include a proof here.

PROPOSITION 4.2. ([14, Theorem 5.5]) *A function $f \in \mathcal{C}(X_G, \mathbb{Z})$ is in the image of $\mathbb{Z}[G]$ if and only if*

$$\sum_{y \in Y} f(y) \equiv 0 \pmod{|Y|} \qquad \text{for all fans } Y \subseteq X \text{ with } |Y| \geqslant 4. \tag{4.1}$$

PROOF: For any $g \in G$, we see from Proposition 1.8 that, as a function on any fan Y, either g is constantly 1, constantly -1 or $|H(g) \cap Y| = |Y|/2$, so that g is 1 on exactly half of the elements. In any case, $\sum_{y \in Y} g(y) \equiv 0 \pmod{|Y|}$. It follows that any $f = \sum_{g \in G} n_g g \in \mathbb{Z}[G]$ satisfies this congruence as well.

Conversely, let $f \in \mathcal{C}(X, \mathbb{Z})$. We write χ_x for the characteristic function of the point $\{x\}$. An element $g \in G$, viewed as a function $X \to \mathbb{Z}$, is $1 - 2\chi_{H(-g)}$, so the element $e + x(g_i)g_i \mapsto 1 + x(g_i)(1 - 2\chi_{H(-g_i)})$ which is equal to 2 on the set $H(x(g_i)g_i)$ and 0 on

its complement. Therefore, the function induced by $\prod_{i=1}^{n}(e+x(g_i)g_i)$ is $2^n\chi_z$. We compute

$$
\begin{aligned}
f &= \frac{1}{2^n}\sum_{x\in X} f(x)\cdot 2^n\chi_x \\
&= \frac{1}{2^n}\sum_{x\in X} f(x)\prod_{i=1}^{n}(e+x(g_i)g_i) \\
&= \frac{1}{2^n}\sum_{x\in X} f(x)\sum_{S\subseteq\{1,2,\dots,n\}}\prod_{i\in S} x(g_i)g_i \qquad (4.2)\\
&= \frac{1}{2^n}\sum_{S\subseteq\{1,2,\dots,n\}}\Big(\sum_{x\in X} f(x)\,x\Big(\prod_{i\in S} g_i\Big)\Big)\Big(\prod_{i\in S} g_i\Big)
\end{aligned}
$$

We see from this that if $\sum_{x\in X} f(x)\,x(g)$ is divisible by 2^n for every $g\in G$, then f is in the image of $\mathbb{Z}[G]$. This is true by hypothesis if $g=e$. Otherwise, $H(g)$ is a fan with $|H(g)| = 2^{n-1}$, so we can write

$$
\begin{aligned}
\sum_{x\in X} f(x)\,x(g) &= \sum_{x\in H(g)} f(x) - \sum_{x\in H(-g)} f(x) \\
&= 2\sum_{x\in H(g)} f(x) - \sum_{x\in X} f(x) \equiv 0 \pmod{2^n}
\end{aligned}
$$

by hypothesis. □

LEMMA 4.3. *For any fan $Y = \bigcap_{i=1}^{m} H(\varepsilon_i a_i)$, $a_i\in G$, $\varepsilon_i\in\{\pm 1\}$, the function $2^m\chi_Y$ can be written as a $\mathbb{Z}$-linear combination of functions of the form $2^m\chi_Z$, where $Z = \bigcap_{k=1}^{r} H(g_{i_k})$, $r\leqslant m$, and where the g_{i_k} are among the basis elements for G.*

PROOF: Each a_i can be written as a product of basis elements for G. The elements of $\mathcal{H}$ can be expanded with the formula $H(-g_1g_2) = H(g_1)+H(g_2)$. Minus signs can be eliminated with $H(-g) = H(g)+X$. The characteristic function for a symmetric difference satisfies $\chi_{A+B} = \chi_A+\chi_B-2\chi_A\chi_B$. It follows that we can write $2^m\chi_Y = \prod 2\chi_{H(\varepsilon_i a_i)}$ as an m-fold product of sums (with coefficients being positive or negative powers of 2), which can then be expanded into a sum of m-fold products of the specified form, using $\chi_X = 1$. □

DEFINITION 4.4: In the context of quadratic form theory, the functions $2^m\chi_Y$ of the previous lemma are derived from Pfister forms. For this reason, we shall refer to them as *Pfister functions.* An ideal is called a *Pfister ideal* if it is generated by the Pfister functions contained in it. For any ideal I of $\mathbb{Z}[G]$, we shall refer to the ideal generated by the Pfister functions contained in I as the *Pfister subideal of I.*

https://doi.org/10.1017/S0004972700038612 Published online by Cambridge University Press

When the quotient data n_x is sufficiently large, the kernel of $\mathbb{Z}[G] \to R$ is always a Pfister ideal, but this is not true in general. The next example and theorem show the current state of our knowledge.

EXAMPLE 4.5. (This example is an easy modification of an example of Elman, Lam and Wadsworth in [5].) Let R be the image of $\mathbb{Z}[G]$ in $\mathcal{C}\Big(X, \bigcup_{x\in X} \mathbb{Z}_{n_x}\Big)$ where $|G| = |X| = 16$. To be explicit, let G have a basis $g_1, \ldots, g_4$ as a $\mathbb{F}_2$-vector space. Think of X as the dual space G^*, with dual basis $x_1, \ldots, x_4$; that is, signs are chosen so that $x_i(g_i) = +1$ and $x_i(g_j) = -1$ if $j \neq i$. This makes, for example, $H(g_1) = \{0, x_1, x_2x_3, x_2x_4, x_3x_4, x_1x_2x_3, x_1x_2x_4, x_1x_3x_4\}$. Now define the data to be

$$n_x = \begin{cases} 2, & \text{if } x \in \{x_1x_2, x_3x_4, x_1x_2x_3, x_1x_3x_4, x_1x_2x_4, x_2x_3x_4\} \\ 2^4, & \text{if } x \in \{0, x_1, x_2, x_3, x_4, x_1x_3, x_1x_4, x_2x_3, x_2x_4, x_1x_2x_3x_4\} \end{cases}$$

The effect of this, by Theorem 4.1, is basically to restrict attention to the set Y of the 10 points for which $n_x = 16$. Let $\mathfrak{p}$ be the kernel of $\mathbb{Z}[G] \to R$. One can check that $f = (e + g_1)(e + g_2) - (e + g_3)(e + g_4)$ lies in $\mathfrak{p}$. It is basically shown in [5, Proposition 6.8] that f is not in the ideal generated by the Pfister functions in $\mathfrak{p}$. The difference is that we also have in our ideal the 4-fold products associated with each of the 10 elements of Y, but the essence of the proof in [5] is that the ideal $\mathfrak{p}$ contains no 1-fold or 2-fold Pfister functions. The higher degree functions have no effect.

Next we look at the condition that the data be large enough to guarantee a Pfister ideal. In this case we obtain rings which Marshall refers to as *Pfister quotients* of $\mathbb{Z}[G]$ [13, Section 4.7]. Indeed, it is easy to see that any finite Pfister quotient of a reduced Witt ring can be obtained via our construction. These rings have particularly nice properties as they are all SQWitt rings [13, Proposition 4.24].

THEOREM 4.6. *With the notation above, let R be the image of $\mathbb{Z}[G]$ in $\mathcal{C}\Big(X, \bigcup_{x\in X} \mathbb{Z}_{n_x}\Big)$, where $n_x = 2^{m_x} > 1$ for each $x \in X = X_G$. If each $m_x \geqslant n = \log_2 |G|$, then the kernel of $\mathbb{Z}[G] \to R$ is generated by $N = \max_{x\in X} n_x$ and the Pfister functions*

$$2^{m_x - n} \prod_{i=1}^{n} (e + x(g_i)g_i) \qquad (x \in X). \tag{4.3}$$

Therefore, in this case the kernel is a Pfister ideal and we can write the quotient ring as

$$R \cong \mathbb{Z}_N[G] \Big/ \Big\langle 2^{m_x - n} \prod_{i=1}^{n} (e + x(g_i)g_i), x \in X \Big\rangle.$$

If the $m_x > 0$ are not otherwise restricted, then the Pfister subideal of the kernel is generated by the 3^n elements of the form

$$2^s \prod_{j=1}^{r} (e + \varepsilon_i g_{i_j}), \tag{4.4}$$

https://doi.org/10.1017/S0004972700038612 Published online by Cambridge University Press

where $0 \leqslant r \leqslant n$, $\varepsilon_i \in \{\pm 1\}$, *the subscripts* i_j *are distinct integers in* $1, \ldots, n$, *and* $s = (\max_{x \in Y} m_x) - r$, *where* $Y = \bigcap_{i=1}^{r} H(\varepsilon_i g_{i_j})$.

PROOF: As in the proof of Proposition 4.2, the function obtained from $\prod_{i=1}^{n}(e+x(g_i)g_i)$ is just $2^n\chi_x$. It follows that the elements of (4.3) all lie in the kernel. The fact that they generate the kernel is also clear as any element in the kernel must be an integral combination of these functions in order to be zero at each point of X.

For unrestricted m_x, we need more generators. A similar argument shows that all elements of (4.4) are also in the kernel as the value at each x is at least 2^{m_x}. Furthermore, the condition on the exponent s clearly gives the minimum value so that each of the Pfister functions is congruent to zero at all the points where it is not actually equal to zero. □

For purposes of counting the elements of the quotient ring R, we shall use a different way of expressing the kernel. We shall deal only with the constant n_x case. The following corollary does this for us.

COROLLARY 4.7. *Let* R *be as above and assume that each* $n_x = 2^m$ *for all* $x \in X$ *with* $m \geqslant n$. *Then the kernel of* $\mathbb{Z}[G] \to R$ *is generated by the elements*

$$2^{m-r} \prod_{g \in G_{rk}} (e - g), \qquad \left(0 \leqslant r \leqslant n;\ 1 \leqslant k \leqslant \binom{n}{r}\right) \tag{4.5}$$

where G_{rk} *ranges over the* r*-subsets of* $\{g_1, g_2, \ldots, g_n\}$ *as* $k = 1, \ldots, \binom{n}{r}$. *In this case, we have*

$$|R| = 2^{(2m-n)2^{n-1}} \tag{4.6}$$

PROOF: By Theorem 4.6, we have

$$R \cong \mathbb{Z}_{2^m}[G] \Big/ \left\langle 2^{m-n} \prod_{i=1}^{n} (e + x(g_i)g_i),\ x \in X \right\rangle.$$

We need to show that the ideal

$$J = \left\langle 2^{m-n} \prod_{i=1}^{n} (e + x(g_i)g_i),\ x \in X \right\rangle$$

is the same as the ideal

$$I = \left\langle 2^{m-r} \prod_{g \in G_{rk}} (e - g);\quad 0 \leqslant r \leqslant n,\ 1 \leqslant k \leqslant \binom{n}{r} \right\rangle$$

It is clear that the generators of I take values in $2^m\mathbb{Z}$, hence are contained in J. Therefore it will suffice to show that each of the generators of J lies in I.

https://doi.org/10.1017/S0004972700038612 Published online by Cambridge University Press

So consider the element $\mu = 2^{m-n}\prod_{i=1}^{n}(e+\varepsilon_i g_i)$. We prove this lies in I with an induction on n. If $n=1$, we have $2^{m-1}(e-g) \in I$ and $2^{m-1}(e+g) = -2^{m-1}(e-g)+2^m e \in I$. If all $\varepsilon_i = -1$, then μ is among the generators for I. Otherwise, we may assume that $\varepsilon_1 = 1$. Then

$$2^{m-n}(e+g_1)\prod_{i=2}^{n}(e+\varepsilon_i g_i) = -2^{m-n}(e-g_1)\prod_{i=2}^{n}(e+\varepsilon_i g_i) + 2^{m-n+1}\prod_{i=2}^{n}(e+\varepsilon_i g_i),$$

in which the last two terms are in I by the induction hypothesis since they involve a smaller group generated by $g_2, \ldots, g_n$.

In order to count the number of elements in R we shall first show that the generators in (4.5) are linearly independent over $\mathbb{Z}$. Assume there is a dependence relation

$$\sum a_{rk}\left[2^{m-r}\prod_{g\in G_{rk}}(e-g)\right] = 0.$$

Without loss of generality, we may assume that the integers a_{rk} have no common prime factor. Now view this equation as a functional equation on X, replacing each $2^{m-r}\prod_{g\in G_{rk}}(e-g)$ by $2^m\prod_{g\in G_{rk}}\chi_{H(-g)}$. Divide by 2^m and we obtain $\sum a_{rk}\prod_{g\in G_{rk}}\chi_{H(-g)} = 0$. Modulo 2, this gives a relation on the subbasic sets of the form $\sum \overline{a_{rk}}\prod_{g\in G_{rk}} H(-g)$, where $\overline{a_{rk}} \in \{0,1\}$ and sum and product are interpreted as symmetric difference and intersection, respectively. Applying Proposition 1.8, with $\mathcal{T} = \{H(-g_1), \ldots, H(-g_n)\}$, we conclude that all a_{rk} must be even, a contradiction. Removing 2^m from the generating set gives us a set of generators for $\bar{I}$, the image of I in $\mathbb{Z}_{2^m}[G]$, and these generators are linearly independent over $\mathbb{Z}_{2^m}$. We have $\left|\mathbb{Z}_{2^m}[G]\right| = 2^{m2^n}$; an arbitrary element of $\bar{I}$ is a sum of terms of the form $a_{rk}\left[2^{m-r}\prod_{g\in G_{rk}}(e-g)\right]$ where the coefficient a_{rk} can take on any one of 2^r values in $\mathbb{Z}_{2^m}$. There are $\binom{n}{r}$ such terms, and r runs from 1 through n, so we have $|\bar{I}| = \prod_{r=1}^{n}(2^r)^{\binom{n}{r}} = 2^{\sum_1^n r\binom{n}{r}} = 2^{n2^{n-1}}$. Putting this together with the value for $\left|\mathbb{Z}_{2^m}[G]\right|$ gives $|R| = 2^{(2m-n)2^{n-1}}$ as desired. □

5. SQWitt rings

This section is devoted to elucidating some of the ways in which SQWitt rings differ from QWitt rings. For one thing, one might expect some sort of recursion can be used in their construction as in the case of finitely generated reduced Witt rings (see [**13**, **3**]). It is not quite so nice because of the problem of computing the quotients, but there is a result of this sort. We conclude with a theorem and example showing how the powers of the maximal ideal behave much more nicely for SQWitt rings.

https://doi.org/10.1017/S0004972700038612 Published online by Cambridge University Press

Let R be an SQWitt ring; that is, the quotient of a torsion free Witt ring $S = W(F)$, for some pythagorean field F with space of orderings X. By [3], the ring S can be constructed recursively from the ring of integers $\mathbb{Z}$ using two operations:

1. Group extension: given a ring R_0, form the group ring $R_0[\mathbb{Z}_2]$.
2. Direct product (in the category of torsion free Witt rings): given two rings in the category $R_i = \mathbb{Z} + M_i$, $i = 1, 2$, the product is $\mathbb{Z} + M_1 \times M_2$. Here M_i denotes the unique maximal ideal of R_i and is viewed as a subset of the functions $C(X_i, 2\mathbb{Z})$. The space X for the product is the disjoint union of X_1 and X_2.

Thus any such ring is a subring of the largest possible allowed collection of functions, that of a SAP Witt ring defined in Section 3. We refer the reader to [1] for a much more general discussion of the torsion free rings and generalisations. Most expositions of [3, Theorem 2.1], such as that in [1], emphasise the effect on the sets of minimal prime ideals. For group extension, the space X is duplicated, with the nontrivial group element being $+1$ on one copy and -1 on the other. For the product, one obtains the disjoint union of X_1 and X_2.

This recursive construction is almost unique. The only non-uniqueness arises in forming the group ring $\mathbb{Z}[\mathbb{Z}_2]$, which also occurs as the product of $\mathbb{Z}$ with itself in this category. That is, there are two ways to form the ring with $|X| = 2$, whose quotients were carefully analysed in Example 1.7.

It is now somewhat clear that a recursive construction can be used to create any SQWitt ring, but there are complications. For example, we can take $n = \max_{x \in X} n_x$, begin with $\mathbb{Z}_n$ in place of $\mathbb{Z}$ and use the constructions above. Then at the end, factor out the additional amount needed at each point $x \in X$. We cannot, however, build the SQWitt ring R with all factorisations in place as we go. This is not a problem for products, as the product construction commutes with our sort of quotient ring construction. But the group ring construction does not. For example, if we work with $S = \mathbb{Z}[\mathbb{Z}_2 \times \mathbb{Z}_2]$, the set X has four elements. Forming R from a quotient of $\mathbb{Z}$, then forming a group ring will make all values n_x the same, and forming it from a quotient of $\mathbb{Z}[\mathbb{Z}_2]$ will make them equal in pairs. We can only obtain the full generality we want by making an additional quotient construction at the end. While this largely loses any uniqueness for our constructions, it does still allow most of the power of the recursive construction for proofs and for computations. There is one further complication as is evident in the special case of Example 1.7; group ring constructions do not inject into the ring of functions, but rather have elements such as $\operatorname{char} R/2(e + g)$ inducing the zero function. This is a fundamental fact of our situation since we cannot distinguish the group elements modulo 2, as they are functions taking values ± 1. More generally, one can check that the kernel consists precisely of the elements $\{a \in R \mid 2a = 0\}$. This discussion, together with the exposition of products in Section 3, now gives us the following theorem.

THEOREM 5.1. *The collection of all SQWitt rings with only 2-torsion is precisely the set $\mathcal{M}$ of rings constructed as follows:*

1. *The rings $\mathbb{Z}/2^n\mathbb{Z} \in \mathcal{M}$ for each $n = 1, 2, \ldots$.*
2. *Given any $R \in \mathcal{M}$, the quotient of the group ring $R[\{e, g\}]/\{a \in R \mid 2a = 0\} \in \mathcal{M}$.*
3. *Given $R_i = \mathbb{Z}_{n_i} + M_i \in \mathcal{M}$, the product, $\mathbb{Z}_{\max(n_1,n_2)} + M_1 \times M_2 \in \mathcal{M}$.*
4. *Given $R \in \mathcal{M}$, any further quotient as in Definitions 1.3 and 1.4 is in $\mathcal{M}$.*

The restriction to having only 2-torsion is a technicality which was mentioned in Section 2. Any SQWitt ring is a ring-theoretic product of a finite set of rings in $\mathcal{M}$ and a finite set of rings $\mathbb{Z}_n$, n odd, where either of the sets may be empty.

In order to illustrate the special nature of SQWitt rings, we end this section with a result for these rings which does not hold in general for QWitt rings. Let S be a Witt ring for a group G of exponent 2. The kernel of the augmentation mapping $\mathbb{Z}[G] \to Z$ followed by reduction modulo 2 contains the kernel of $\mathbb{Z}[G] \to S$ by [8, Theorem 3.9]. Thus we obtain an induced homomorphism $S \to \mathbb{Z}/2\mathbb{Z}$, the kernel of which will be called the *augmentation ideal* of S and denoted by I_S. If S can be realised as the Witt ring of a field, then the n-th power of this ideal, viewed as functions on X_S, consists precisely of the elements of $S \cap \mathcal{C}(X_S, 2^n\mathbb{Z})$ [3, Theorem 4.1]. Therefore we have the following proposition for SQWitt rings.

PROPOSITION 5.2. *Let S be a finitely generated torsion free Witt ring of a field with SQWitt quotient R. Then the maximal ideal I_R of R satisfies*

$$I_R^n = R \cap \mathcal{C}(X_R, \cup 2^n\mathbb{Z}_{n_x}) \qquad n = 1, 2, \ldots$$

Furthermore, if we have all $n_x = 2^m$ for some $m \geqslant 0$, then the kernel of the surjection $S \to R$ is I_S^m.

In general, this result fails for QWitt rings, though the construction of examples is somewhat complicated. We shall see that it holds for QWitt rings for $n = 1, 2$, but fails for $n = 3$.

PROPOSITION 5.3. *Let S be a Witt ring for a group G of exponent 2. Then*

$$S \cap \mathcal{C}(X_S, 2\mathbb{Z}) = I_S \quad \text{and} \tag{5.1}$$

$$S \cap \mathcal{C}(X_S, 4\mathbb{Z}) = I_S^2 \,. \tag{5.2}$$

PROOF: We know that $\mathcal{C}(X_S, 2\mathbb{Z})$ is the unique maximal ideal in $\mathcal{C}(X_S, \mathbb{Z})$ containing 2. Since the maximal ideal I_S is contained in the proper ideal $S \cap \mathcal{C}(X_S, 2\mathbb{Z})$, we have equality (5.1).

We clearly have $I_S^2 \subseteq S \cap \mathcal{C}(X_S, 4\mathbb{Z})$. On the other hand, $f \in S \cap \mathcal{C}(X_S, 4\mathbb{Z})$ implies that $f \in I_S$, so we can write $f = \sum n_A \, 2\chi_A$, where $n_A \in \mathbb{Z}$ and $A \in \mathcal{H}_S$. Since

https://doi.org/10.1017/S0004972700038612 Published online by Cambridge University Press

$4\chi_A = 2 \cdot 2\chi_A \in I_S^2$, we obtain $f \equiv \sum_{i=1}^{s} 2\chi_{A_i} \pmod{I_S^2}$. Furthermore, $\chi_A + \chi_B = \chi_{A+B} + 2\chi_A\chi_B$ implies that $2\chi_A + 2\chi_B \equiv 2\chi_{A+B} \pmod{I_S^2}$. Therefore $f \equiv 2\chi_{\sum A_i} \pmod{I_S^2}$. But $f(x) \equiv 0 \pmod 4$ for all $x \in X_S$, so we must have $\chi_{\sum A_i} = 0$, and thus $f \in I_S^2$. □

We now turn to a specific example which shows that it is not always true that $S \cap \mathcal{C}(X_S, 8\mathbb{Z}) = I_S^3$.

EXAMPLE 5.4. Let $Y = \{0,1\}^6$ and for $i = 1, \ldots, 6$, set $M_i = \{y \in Y \mid y(i) = 0\}$. Let $Z = M_1 \cap M_2 + M_3 \cap M_4 + M_5 \cap M_6 \subseteq Y$, where as usual, sum denotes symmetric difference, and set $X = Y \setminus Z$. Let $H_i = X \cap M_i$ for $i = 1, \ldots, 6$. One can check that the subbasis $\mathcal{H}$ generated by these sets under complement and symmetric difference consists of all subsets of X with 0, 16, 20 or 36 elements. Let S be the subring of $\mathcal{C}(X, \mathbb{Z})$ generated by $\mathbb{Z}$ and the functions $2\chi_H$ for $H \in \mathcal{H}$. Then S is a Witt ring for the group of exponent 2 with 64 elements. We claim that $I_S^3 \subsetneq S \cap \mathcal{C}(X, 8\mathbb{Z})$.

Indeed, note that $\bigcap_{i=1}^{4} H_i = \{(0,0,0,0,1,0), (0,0,0,0,0,1), (0,0,0,0,1,1)\}$ and consider the element

$$\begin{aligned} f &= 8\chi_{H_1}\chi_{H_2}\chi_{H_3}\chi_{H_4} = 4\chi_{H_1}\chi_{H_2} + 4\chi_{H_3}\chi_{H_4} - 4\chi_{H_1H_2+H_3H_4} \\ &= 4\chi_{H_1}\chi_{H_2} + 4\chi_{H_3}\chi_{H_4} - 4\chi_{H_5}\chi_{H_6} \in S \cap \mathcal{C}(X, 8\mathbb{Z}) \end{aligned} \tag{5.3}$$

Suppose that $f \in I_S^3$. Then f can be written in the form

$$f = \sum 8n_i\chi_{A_{i1}}\chi_{A_{i2}}\chi_{A_{i3}} \qquad (A_{ij} \in \mathcal{H},\ n_i \in \mathbb{Z})\ . \tag{5.4}$$

We set the equations (5.3) and (5.4) equal and divide by 8. Now each A_{ij} can be written as a sum of the generating sets H_i and possibly X. Using the formula $\chi_{A+B} = \chi_A + \chi_B - 2\chi_A\chi_B$, we expand the right hand side to obtain an equation of the form

$$\chi_{H_1}\chi_{H_2}\chi_{H_3}\chi_{H_4} = \sum \prod_{n=1}^{3} \chi_{H_{i_n}} + \sum \prod_{n=1}^{2} \chi_{H_{j_n}} + \sum \chi_{H_k} + \delta + 2\gamma,$$

where δ is zero or one depending on whether χ_X ends up in the sum and γ is a sum of products of characteristic functions arising from using the formula to break up characteristic functions of symmetric differences. Modulo 2, this gives us an equation in the $\mathbb{F}_2$-vector space $\mathcal{H}$

$$H_1 \cap H_2 \cap H_3 \cap H_4 = \sum \bigcap_{n=1}^{3} H_{i_n} + \sum \bigcap_{n=1}^{2} H_{j_n} + \sum H_k + \delta X\ .$$

This equation contradicts Proposition 1.8, proving our claim.

REFERENCES

[1] C. Andradas, L. Bröcker and J. Ruiz, *Constructible sets in real geometry* (Springer–Verlag, Berlin, 1966).

[2] T. Craven, 'Stability in Witt rings', *Trans. Amer. Math. Soc.* **225** (1977), 227–242.

[3] T. Craven, 'Characterizing reduced Witt rings of fields', *J. Algebra* **53** (1978), 68–77.

[4] T. Craven, 'Fields maximal with respect to a set of orderings', *J. Algebra* **115** (1988), 200–218.

[5] R. Elman, T.Y. Lam and A.R. Wadsworth, 'Pfister ideals in Witt rings', *Math. Ann.* **245** (1979), 219–245.

[6] R. Fitzgerald and J. Yucas, 'Combinatorial techniques and abstract Witt rings, II', *Rocky Mountain J. Math.* **19** (1989), 687–708.

[7] J. Kleinstein and A. Rosenberg, 'Signatures and semisignatures of abstract Witt rings and Witt rings of semilocal rings', *Canadian J. Math.* **30** (1978), 872–895.

[8] M. Knebusch, A. Rosenberg and R. Ware, 'Structure of Witt rings and quotients of abelian group rings', *American J. Math.* **94** (1972), 119–155.

[9] M. Knebusch, A. Rosenberg and R. Ware, 'Signatures on semilocal rings', *J. Algebra* **26** (1973), 208–250.

[10] T.Y. Lam, *The algebraic theory of quadratic forms*, Mathematics Lecture Note Series, (Revised second printing) (Benjamin/Cummings Publishing Co., Inc., Advanced Book Program, Reading, Mass., 1980).

[11] T.Y. Lam, *Orderings, valuations and quadratic forms*, CBMS Regional Conference Series in Mathematics **52** (Amer. Math. Soc., Providence, RI, 1983).

[12] B.R. MacDonald, *Finite rings with identity*, Pure and Applied Mathematics **28** (Marcel Dekker, New York, 1974).

[13] M. Marshall, *Abstract Witt rings*, Queen's Papers in Pure and Appl. Math. **57** (Queen's University, Kingston, Ontario, 1980).

[14] M. Marshall, 'The Witt ring of a space of orderings', *Trans. Amer. Math. Soc.* **258** (1980), 505–521.

[15] M. Vo, *New classes of finite commutative rings*, (Ph.D. thesis) (University of Hawaii, Honolulu, HI, 2003).

Department of Mathematics
University of Hawaii
Honolulu, HI 96822
United States of America
e-mail: tom@math.hawaii.edu

Department of Mathematics and Sciences
Saint Leo University
Saint Leo, FL 33574
United States of America
e-mail: monika.vo@saintleo.edu