PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 141, Number 5, May 2013, Pages 1505–1517
S 0002-9939(2012)11428-5
Article electronically published on October 11, 2012

WITT RINGS AND MATROIDS

THOMAS C. CRAVEN AND ZACHARY A. KENT

(Communicated by Ken Ono)

Abstract. The study of Witt rings of formally real fields in the algebraic theory of quadratic forms has led to a particularly good understanding of the finitely generated torsion free Witt rings. In this paper, we work primarily with a somewhat more general class of rings which can be completely characterized by (binary) matroids. The different types of standard constructions and invariants coming from algebra and from combinatorics lead to previously unstudied problems for both areas; in particular, there are new invariants for Witt rings and new constructions for matroids with many open questions.

1. Introduction

We begin with a class of quotient rings of integral group rings. These rings, modulo their nilradicals, are the basic objects we wish to classify with matroids.

Definition 1.1 ([KRW1, Definition 3.12], [KRW2, §3], [KR, §1])**.** Let G be a group of exponent 2. An *abstract Witt ring* is a quotient ring $R = \mathbb{Z}[G]/K$ such that R has only 2-torsion.

These rings were originally studied as a ring-theoretic method of obtaining results concerning Witt rings of equivalence classes of quadratic forms over a field F, where the group G was the square class group $F^\times/F^{\times 2}$. We will mention some of the connections in passing, but no knowledge of this theory will be needed to understand the matroid constructions of this paper.

We now quickly summarize the most relevant parts of the literature concerning these rings. They can be expressed as rings of functions when they are torsion free, the case we shall be concerned with here, and are obtained in general by factoring out the nilradical. For any Witt ring $R = \mathbb{Z}[G]/K$, let X_R denote the set of ring homomorphisms from R to the ring of integers $\mathbb{Z}$. These are in bijective correspondence with the set of minimal, nonmaximal prime ideals of R [KRW2, 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 equivalence classes of quadratic forms over a formally real field, the set X_R 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

Received by the editors August 29, 2011.
2010 *Mathematics Subject Classification.* Primary 13M05; Secondary 12D15, 11E81.

endowed with the discrete topology; indeed, the element $r \in R$ induces the function $\hat{r}\colon X_R \to \mathbb{Z}$ via $\hat{r}(x) = x(r)$. 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* [KRW2, 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 $\{\, 1 - 2\chi_H \mid H \in \mathcal{H} \,\}$ [KRW2, 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 $\mathbb{F}_2$, and its dimension will determine the rank of an associated matroid (see Corollary 5.2).

The category of torsion free abstract Witt rings is equivalent to the category of prespaces of orderings as defined in [ABR]. With stronger conditions, one obtains spaces of orderings, an abstract way of viewing reduced Witt rings of ordered fields [Ma1], [Ma2].

Definition 1.2. Let G be a group of exponent 2 and let $\hat{G} = \mathrm{Hom}(G, \{\pm 1\})$ be the topological dual group of G for the discrete topology on G. Let $-1 \neq 1$ be a distinguished element of G and let Y be a subset of $\hat{G}$. The pair (Y, G) is called a *prespace of orderings* if the following conditions hold:

- Y is closed in $\hat{G}$.
- $\sigma(-1) = -1$ for all $\sigma \in Y$.
- The element $g = 1$ in G is the unique element of G such that $\sigma(g) = +1$ for all $\sigma \in Y$.

As above, we shall write $\mathcal{H}$ for the Harrison subbasis, i.e. the collection of sets

$$H(g) = \{\, \sigma \in Y \mid \sigma(g) = 1 \,\} \qquad (g \in G).$$

In the next section we look at the major constructions usually performed in this category of rings, or equivalently prespaces of orderings. In later sections we show how they can be viewed as matroids and explore their properties.

2. Constructions

There are three constructions known for building new finite prespaces of orderings from existing ones. Two of them, applied recursively to a one-point space, yield all finite spaces of orderings (finitely generated reduced Witt rings of fields); these are group extension and sum (direct product in the appropriate category of rings). They have been described in numerous places, such as [ABR, Chapter IV.2], [Cr2], [Ma1] and [CS2, Def. 2.2, 2.3], but since we will make extensive use of them, we give a brief description here.

Definition 2.1 ([ABR, Def. 2.1])**.** Let (Y_1, G_1), (Y_2, G_2) be two prespaces of orderings. Their *sum* is defined to be the space (Y, G), where $Y = Y_1 \cup Y_2$ is the disjoint union of Y_1 and Y_2 and $G = G_1 \times G_2$.

Example 2.2. We shall use SAP_n to denote a sum of n one-point prespaces. In this case the set X is a set of n points and the corresponding Harrison subbasis $\mathcal{H}$ is the power set of X.

Definition 2.3 ([ABR, Def. 2.7])**.** Let (Y', G'), be a prespace of orderings. The *extension* of (Y', G') by $\mathbb{Z}_2$ is defined to be the space $(Y, G) = (\hat{\mathbb{Z}}_2 \times Y', \mathbb{Z}_2 \times G')$ with distinguished element $(1, -1) \in G$ and the action $(\alpha, \sigma)(h, g) = \alpha(h)\sigma(g)$ for $(\alpha, \sigma) \in \hat{\mathbb{Z}}_2 \times Y'$ and $(h, g) \in \mathbb{Z}_2 \times G'$.

In this construction, Y consists of two identical copies of Y' and $\mathcal{H}$ is generated by a copy of Y' together with unions of identical copies of each $H' \in \mathcal{H}'$ in each copy of Y'. The group $\mathbb{Z}_2$ can be replaced by any group of exponent 2, but this is also achieved just by iterating the construction.

Work with skew fields has led to a third construction, needed for semiorderings of commutative fields as well. This yields a tensor product of rings over $\mathbb{Z}$, but is most easily understood as the following prespace construction. We note that Definition 2.3 is a special case of this where (Y_2, G_2) is taken as a two-point space.

Definition 2.4 ([CS2, Def. 2.4])**.** The *product* of two prespaces of orderings (Y_1, G_1) and (Y_2, G_2) is defined to be the prespace of orderings $(Y, G) = (Y_1 \times Y_2, G_1 \dot{+} G_2)$, where $G_1 \dot{+} G_2$ is the coproduct in the category of elementary 2-groups with distinguished subgroup $\{\pm 1\}$ preserved by all homomorphisms; equivalently,

$$\begin{array}{ccc} \{\pm 1\} & \longrightarrow & G_1 \\ \downarrow & & \downarrow \\ G_2 & \longrightarrow & G_1 \dot{+} G_2 \end{array}$$

is a pushout diagram for homomorphisms preserving the distinguished element -1. Constructively, $G_1 \dot{+} G_2$ is just $(G_1 \times G_2)/\{(1,1),(-1,-1)\}$ so that $(1,-1) = (-1,1)$ is the distinguished element in $G_1 \dot{+} G_2$ and the action is given by $(\sigma_1, \sigma_2)(g_1, g_2) = \sigma_1(g_1)\sigma_2(g_2)$, for $\sigma_i \in Y_i$ and $g_i \in G_i$, $i = 1, 2$.

It is worth noting that extension by $\mathbb{Z}_2$ is a special case of a product where $Y_2 = \mathrm{SAP}_2$. A product of group rings is again a group ring, so nothing new is gained in that instance. On the other hand, a product of SAP rings, when both spaces have more than two elements, yields a prespace not found in the classical theory for spaces of orderings. The following is another such example.

Definition 2.5. The prespace of orderings E_n is defined to be (X, G), where $|X| = 2n$ and $\mathcal{H}$ consists of all subsets of X with an even number of elements. Since symmetric difference preserves this evenness, this works. Such spaces (for $n \geq 3$) seem to have no way of building them from smaller spaces and are again a new class of prespaces of orderings. The one mention of these in the literature is E_3 in [Cr1, Example 4.6], where it was shown not to be a space of orderings.

3. Prespaces of orderings as matroids

Our matroids are in fact a subset of the class of *binary matroids* described in [O, Theorem 9.1.2], but never seem to have been studied for their own sake. We wish to show the importance of these matroids by elucidating their properties and how those properties affect the rings from which we obtain them. It is interesting

that concepts as fundamental to matroid theory as independence and basis do not readily translate into ring-theoretic properties.

There are numerous equivalent definitions of a matroid. The most natural one for us to use is

Definition 3.1. A *matroid* consists of a set X together with a family $\mathcal{C}$ of nonempty subsets of X called *circuits* satisfying

(C1) no proper subset of a circuit is a circuit;
(C2) if $x \in C_1 \cap C_2$, $C_1 \neq C_2$, then $C_1 \cup C_2 \setminus \{x\}$ contains a circuit.

Given a prespace (Y, G), we can take $X = Y$ and $\mathcal{C}$ to be the collection of minimal nonempty subsets of $\mathcal{H}$. For (C2), the set $C_1 + C_2$ is in $\mathcal{H}$, where $+$ denotes symmetric difference, and so contains one of the minimal nonempty elements. To use the definition of matroid in terms of independent sets, the set $\mathcal{I}$ consists of all subsets of X which contain no member of $\mathcal{C}$. A (matroid) *basis* is a maximal independent set.

Proposition 3.2. *For a matroid arising from a prespace, the set $\mathcal{C}$ contains an $\mathbb{F}_2$-basis of $\mathcal{H}$.*

Proof. Assume that $C \in \mathcal{H}$ is linearly independent of $\mathcal{C}$. We may assume that C is a minimal such set. By the choice of $\mathcal{C}$, there is some set $C_1 \in \mathcal{C}$ strictly contained in C. But then $C + C_1 \in \mathcal{H}$ is strictly smaller than C and is again linearly independent of $\mathcal{C}$, a contradiction. □

We can now define the fundamental objects of study for this paper.

Definition 3.3. A *prespace matroid* is a matroid generated by a (finite) nonempty set X and a point-separating collection of subsets $C_1, \ldots, C_r$ of X. That is, for any $x_1, x_2 \in X$, there exists C_i such that one of the points lies in C_i and the other lies in its complement. The set of circuits $\mathcal{C}$ then consists of the set of minimal nonempty elements among the $\mathbb{F}_2$-vector space $\mathcal{H} = \{ \sum_{i \in S} C_i, X + \sum_{i \in S} C_i \mid S \subseteq \{1, 2, \ldots, r\} \}$, where sum denotes symmetric difference.

Theorem 3.4. *The contraction of a prespace matroid on X to a subset $Y \subseteq X$ is again a prespace matroid. In fact, the corresponding ring of functions on Y is obtained by restriction of functions.*

Proof. This is [Cr1, Lemma 3.1] for rings and [O, Prop. 3.1.11] for matroids. □

We note that a prespace matroid satisfies a considerably stronger circuit axiom than an arbitrary matroid.

Proposition 3.5. *Let $(X, \mathcal{C})$ be a prespace matroid with $C_1, C_2 \in \mathcal{C}$.*

(C2)* *If $x \in C_1 \cap C_2$, $C_1 \neq C_2$, then $C_1 + C_2$ is a union of disjoint circuits (excluding x).*

Proof. We know that $C_1 + C_2 \in \mathcal{H}$. If it is not minimal, then it properly contains a circuit C_3 and its complement in $C_1 + C_2$, namely $C_1 + C_2 + C_3$. Now repeat this process: if $C_1 + C_2 + C_3$ is not minimal, it properly contains a minimal circuit C_4. After a finite number of steps, one obtains a collection of disjoint circuits $C_3, C_4, \ldots$ whose union is $C_1 + C_2$. □

Example 3.6. If $X = \{a, b, c, d, e, f\}$ and $\mathcal{H}$ is generated by $C_1 = \{a, b, c\}, C_2 = \{c, d, e\}, D_1 = \{a, d\}, D_2 = \{b, e\}, D_3 = \{c, f\}$, then $C_1 + C_2 = D_1 + D_2 = D_1 \cup D_2$, so that $C_1 + C_2$ is not minimal but breaks into two minimal sets.

Condition (C2)* is equivalent to a matroid being binary [W, Theorem 10.1.3]. Furthermore, this is equivalent to any symmetric difference of circuits being a union of disjoint circuits by the previous proof.

The difference between a prespace matroid and an arbitrary binary matroid is twofold. In general, a binary matroid does not have complements included as a prespace matroid does for $\mathcal{H}$. To find an example of a binary matroid which is not a prespace matroid, we make use of the fact that the dual of any binary matroid is binary [W, Theorem 10.1.1], while this is not true of prespace matroids.

Example 3.7. The simplest example occurs with $|X| = 1$. There is only one ring possible, namely $\mathbb{Z}$, and therefore only one prespace matroid and it has a unique circuit and empty basis. The dual matroid has no circuits, so is binary but not prespace.

For a more interesting example, consider the ring $\mathbb{Z}[\mathbb{Z}_2^2]$. The associated prespace is E_2. It yields a matroid on four points with every two-element subset being a circuit. The bases are the one-point sets, so the dual basis consists of the 3-point sets. Thus the only cocircuit is the whole set X, giving no separation of points for the associated ring of functions on X.

Adding the condition that the set X must lie in $\mathcal{H}$ makes the dual a binary affine matroid [O, Prop. 9.3.1(iv)]. The second condition needed to make a binary matroid into a prespace matroid is that the elements of the circuit space $\mathcal{H}$ must separate the points of X. The space $X = \{a, b, c, d\}$ with circuits $\{a, b\}, \{c, d\}$ yields a binary matroid which is not a prespace matroid. We have thus obtained:

Proposition 3.8. *Every prespace matroid is a binary matroid. A binary matroid on a set X is a prespace matroid if its circuits separate points and the set X can be written as a symmetric difference of a set of circuits.*

Characterization of prespace matroids by matrices. Recall that the *standard representative matrix for a binary matroid* has the form $[I_n|A]$, where n is the rank of the matroid and the matrix A can be taken to be the fundamental circuit incidence matrix of any given basis [O, Cor. 9.2.3]. That is, given a basis $\mathcal{B} = \{b_1, \ldots, b_n\}$, write $X \setminus \mathcal{B} = \{x_1, \ldots, x_m\}$; the (i, j) entry of A is 1 if and only if b_i is in the unique circuit $C(x_j)$ contained in $\mathcal{B} \cup \{x_j\}$.

Theorem 3.9. *Let $[I_n|A]$ be the standard representative matrix for a binary matroid $\mathcal{M}$. Then $\mathcal{M}$ is a prespace matroid if and only if*

(1) *The sum (modulo 2) of the columns of A is the vector of all ones;*
(2) *no row of A has exactly one 1; and*
(3) *no two rows of A are identical.*

Proof. Condition (1) is equivalent to the sum of all columns in $[I_n|A]$ being the zero vector, which is equivalent to the set X being in the circuit space. Thus we have a prespace matroid if and only if we can separate points. There are three cases.

Let $\mathcal{B}$ be the chosen basis with respect to which the matrix was formed. For two elements $y_1, y_2 \notin \mathcal{B}$, the corresponding circuit $C(y_1)$ and its complement $C(y_1) + X$ separate the points. For two elements $x_1, x_2 \in \mathcal{B}$, choose a column point y for which

the rows for x_1, x_2 differ, using condition (3). Then $C(y)$ separates the points. Conversely, if the two rows are equal, it is clear that any element of the circuit space will either contain both x_1 and x_2 or neither, so points are not separated.

For condition (2), if some row of A has exactly one 1, say, corresponding to an element x in $\mathcal{B}$ and a column $y \notin \mathcal{B}$, then x will be in every element of $\mathcal{H}$ which contains y. (Recall that any element of the circuit space $\mathcal{H}$ is a symmetric difference of the circuits corresponding to such elements y [O, Theorem 9.1.2 (viii)].) On the other hand, if there is a zero in that position, then $C(y)$ separates x and y. If there is a 1 there and in another column, say y', then $C(y)+C(y')$ separates x and y. □

Matroid versions of the prespace constructions. The sum of Definition 2.1 is just the direct sum of matroids [O, p. 130]. The product construction is much harder to define for matroids since there does not seem to be any natural way to pick out the minimal elements of $\mathcal{H}$ for the circuits or to define a matroid basis given those of the factors. For prespace matroids (or indeed, more generally, for binary matroids) $(X, \mathcal{C}_X)$ and $(Y, \mathcal{C}_Y)$, the product is $(X \times Y, \mathcal{C})$, where $\mathcal{C}$ is the set of minimal nonempty elements of $\mathcal{H}$, generated under symmetric difference by sets of the form $C \times Y,\ C \in \mathcal{C}_X$ and $X \times C,\ C \in \mathcal{C}_Y$ since cross product distributes over symmetric difference. It would be good to know more about matroid properties of the product.

For the special case of group extension, $(X, \mathcal{C}_X)[\mathbb{Z}_2]$ has among its circuits the two copies of X and $\hat{\mathbb{Z}}_2 \times C$ for any $C \in \mathcal{C}_X$. They are sufficient to generate all circuits via symmetric difference. Examples are given by the matroids $E_n[\mathbb{Z}_2]$ in which all of the four-element subsets are circuits.

When is the dual of a prespace matroid again a prespace matroid? The dual of a matroid $(X, \mathcal{C}_X)$ is defined on the same set X by replacing each basis with its complement. This is not helpful in thinking about circuits and one usually loses the separation of points that we demand. By [O, Prop. 9.3.1], the dual of any prespace matroid is a binary affine matroid. The additional condition of separation of points in the prespace matroid is most easily expressed in terms of matrices, extending the last part of [O, Prop. 9.3.1]. In order for a prespace matroid $\mathcal{M}$ to have a prespace dual simply means imposing the conditions of Theorem 3.9 on the columns of A as well as on its rows.

Self-dual prespace matroids. One example is the matroid $AG(3, 2)$ corresponding to the group ring space with 8 elements. It is identically self-dual, a condition equivalent to the matrix form $[I_r|A]$ having the property that A is square and $AA^T = I_r \pmod 2$ [O, Exercise 1, p. 314]. For $AG(3, 2)$, we have the matrix

$$A = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}.$$

Using Theorem 3.9, this generalizes to a characterization of identically self-dual prespace matroids. A matroid is identically self-dual if and only if the corresponding matrix A of the theorem is an orthogonal matrix (over the field $\mathbb{F}_2$).

The example of $AG(3,2)$ clearly generalizes to any $2n \times 2n$ matrix formed by subtracting the identity from a matrix of all ones. The corresponding matroids are the matroids $E_n[\mathbb{Z}_2]$ defined above.

An example which is self-dual but not identically so is R_{10} [O, p. 359] with

$$A = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

4. Stability

The stability index is usually defined only for Witt rings of fields where it is intimately related to the structure of the ring. Lam [L2] devotes an entire chapter to it and gives four equivalent conditions (see (S2)-(S5) below). As we shall see, these cease to be equivalent for prespaces of orderings. Condition (S1) was considered in [Cr1] and is generally stronger. However, condition (S1) seems to be the best one for matroids as it is more inherent in their structure. We use it here for our definition, but describe all of the possibilities and their relationships in Theorem 4.4. This concept of stability will be important later in describing when a prespace matroid is graphical and seems to generally be an interesting invariant.

If S is a Witt subring of $\mathcal{C}(X,\mathbb{Z})$, then $\mathcal{C}(X,\mathbb{Z})/S$ is a 2-primary torsion group [KRW2, Theorem 3.18]. For a Witt ring of a formally real field, one uses the base 2 logarithm of the exponent of $\mathcal{C}(X,\mathbb{Z})/S$, denoted $\mathrm{st}(S)$, as the *stability index* of S [L2, Chap. 13]. The ring S is said to be n-stable if $n \geq \mathrm{st}(S)$.

However, we shall use the following stronger definition for prespace matroids.

Definition 4.1. For a prespace matroid $\mathcal{M} = (X, \mathcal{C})$, where $\mathcal{H}$ is the additive subbasis generated by $\mathcal{C}$, we define the *stability index* of $\mathcal{M}$ to be

$$\mathrm{st}(\mathcal{M}) = \max_{x \in X} \min\{\, n \mid \{x\} = \bigcap_{i=1}^{n} C_i,\ C_i \in \mathcal{H}\,\}.$$

Since $\mathcal{C}$ consists of the minimal elements of $\mathcal{H}$, we may rewrite this as

$$\begin{aligned} \mathrm{st}(\mathcal{M}) &= \max_{x \in X} \min\{\, n \mid \{x\} = \bigcap_{i=1}^{n} C_i,\ C_i \in \mathcal{C}\,\} \\ &= \min_{n} (\forall x \in X)(\{x\} = \bigcap_{i=1}^{n} C_i,\ C_i \in \mathcal{C}). \end{aligned}$$

Examples 4.2. Some easy examples are:

- $\mathrm{st}(\mathcal{M}) = 1$ if and only if $\mathcal{H}$ is the power set of X. That is, $\mathcal{M} = \mathrm{SAP}_n$, where $n = |X|$.
- $\mathrm{st}(E_n) = 2$.
- The stability index of a direct sum is the maximum of the stability indices of the summands.
- With more work, one can show that $\mathrm{st}(\mathcal{M}_1 \times \mathcal{M}_2) = \mathrm{st}(\mathcal{M}_1) + \mathrm{st}(\mathcal{M}_2)$.

We prove the following lemma as motivation for condition (S5) in Theorem 4.4. When possible, we cite the literature for parts of this theorem, but not all connections with our definition have been considered before. We make use of ring theory,

so we mention again that an abstract Witt ring, as a subring of the ring of functions $\mathcal{C}(X,\mathbb{Z})$, consists of all elements of the form $n+\sum 2n_i\chi_{U_i}$, where $n, n_i \in \mathbb{Z}$ and χ_U denotes the characteristic function of a set $U \in \mathcal{H}$. The ring has a maximal ideal generated by the elements $2\chi_U$, $U \in \mathcal{H}$, known as the augmentation ideal.

Lemma 4.3. *Let S be a Witt subring of $\mathcal{C}(X,\mathbb{Z})$ with augmentation ideal $\mathfrak{m}$. For any continuous function $f \in \mathcal{C}(X,\mathbb{Z})$, there exists $n \geq 0$ such that $2^n f \in \mathfrak{m}^n$.*

Proof. Any $f \in \mathcal{C}(X,\mathbb{Z})$ partitions the set X into (clopen, in general for infinite X) subsets on which f is constant. It will suffice to deal with the characteristic function of one of these subsets and add the results together, scaled by the value of f on the subset. Each of these sets is a finite union of intersections of Harrison subbasic sets. But an intersection of subbasic sets $H = \bigcap_i^n H(g_i)$ gives us $2^n\chi_H = \prod 2\chi_{H(g_i)}$ in $\mathfrak{m}^n$. Now assume that we have ϕ_1 equal to 2^{m_1} on the set C_1 and ϕ_2 equal to 2^{m_2} on the set C_2. We may assume that $m = m_1 = m_2$ by replacing ϕ_i with $2^{m-m_i}\phi_i$. Note that the characteristic functions of the subsets $C_1, C_2 \subseteq X$, satisfy $\chi_{C_1\cup C_2} = \chi_{C_1} + \chi_{C_2} - \chi_{C_1}\chi_{C_2}$. Thus $\phi = 2^{2m}\chi_{C_1\cup C_2} = 2^m(\phi_1+\phi_2) - \phi_1\phi_2 \in \mathfrak{m}^{2m}$ works for the union. In this way we can handle any finite union as long as we increase the power of $\mathfrak{m}$. □

Theorem 4.4 (See [L2, Prop. 13.1])**.** *Assume that X is finite. Let S be a Witt subring of $\mathcal{C}(X,\mathbb{Z})$ with augmentation ideal $\mathfrak{m}$ and Harrison subbasis $\mathcal{H}$. For any integer $s \geq 0$, (S1) $\implies$ (S2) $\iff$ (S3) $\iff$ (S4) $\implies$ (S1*) and (S4) $\implies$ (S5):*

- (S1) *Each point $x \in X$ can be written as an intersection of s subbasic sets.*
- (S2) *For any units $a_i \in S$, the element $\phi = 2^{s+1}\chi_{\cap_1^{s+1}H(a_i)} \in S$ can be written as 2ψ for some $\psi \in \mathfrak{m}^s$;*
- (S3) $\mathfrak{m}^{s+1} = 2\mathfrak{m}^s$;
- (S4) $\mathfrak{m}^s = \mathcal{C}(X, 2^s\mathbb{Z})$.
- (S1*) *Each point $x \in X$ can be written as a symmetric difference of intersections of s subbasic sets.*
- (S5) *For any $f \in \mathcal{C}(X,\mathbb{Z})$, we have $2^s f \in S$.*

Proof. (S2) $\iff$ (S3). By [Cr1, Prop. 1.2], the ideal $\mathfrak{m}^{s+1}$ is generated by Pfister functions ϕ, so we obtain $\mathfrak{m}^{s+1} = 2\mathfrak{m}^s$. The converse is in [Cr1, Prop. 2.3].

(S3) $\implies$ (S4). Let $f \in \mathcal{C}(X, 2^s\mathbb{Z})$, say $f = 2^s f_0$, where $f_0 \in \mathcal{C}(X,\mathbb{Z})$. By Lemma 4.3, there exists an integer m such that $2^m f_0 \in \mathfrak{m}^m$. But $\mathfrak{m}^m = 2^{m-s}\mathfrak{m}^s$ by (S3). Therefore we have $2^m f_0 = 2^{m-s}\psi$ for some $\psi \in \mathfrak{m}^s$. Thus $f = 2^s f_0 = \psi \in \mathfrak{m}^s$.

(S4) $\implies$ (S3). Indeed, $\mathfrak{m}^{s+1} = \mathcal{C}(X, 2^{s+1}\mathbb{Z}) = 2\mathcal{C}(X, 2^s\mathbb{Z}) = 2\mathfrak{m}^s$.

(S1) $\implies$ (S3). This follows immediately from [Cr1, Theorem 2.12].

(S3) $\implies$ (S1*). This is the first statement of [Cr1, Theorem 2.10].

(S4) $\implies$ (S5). Since $\mathcal{C}(X, 2^s\mathbb{Z}) = 2^s\mathcal{C}(X,\mathbb{Z}) = \mathfrak{m}^s \subseteq S$, we obtain (S5). □

When S is a representable Witt ring (i.e. comes from the reduced Witt ring of a field), we have that condition (S5) $\implies$ (S1). Indeed, it is known that (S5) implies (S2) by an argument involving representation of elements by quadratic forms [L2, Prop. 13.1]; one can then use the recursive construction for finitely generated representable Witt rings to show that both the usual stability index and the value in (S1) have the same behavior for direct sum and group extension.

The example of [CV, Example 5.4] can be shown to satisfy (S1) for $s = 4$ by direct computation. In [CV], it is shown to fail (S4) for $s = 3$. All sums of 3-fold intersections have an even number of elements, so (S1*) fails here for $s = 3$. On the other hand, (S5) actually holds for $s = 3$. Since this gives an important example for the nonreversibility of the previous theorem, we include the details here.

Example 4.5 (See [CV, 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 only of subsets of X with 0, 16, 20 or 36 elements. Let S be the subring of $\mathcal{C}(X, \mathbb{Z})$ generated by $\mathbb{Z}$ with the functions $2\chi_H$ for $H \in \mathcal{H}$ and let $\mathfrak{m}$ be its augmentation ideal $S \cap \mathcal{C}(X, 2\mathbb{Z})$. Then S is a Witt ring for the group of exponent 2 with 64 elements. It is shown in [CV] that $\mathfrak{m}^3 \subsetneq S \cap \mathcal{C}(X, 8\mathbb{Z})$ by explicitly constructing the following element $f \in S \cap \mathcal{C}(X, 8\mathbb{Z})$ but not in $\mathfrak{m}^3$. Note that $\bigcap_{i=1}^4 H_i = \{a_1 = (0,0,0,0,0,1), a_2 = (0,0,0,0,1,0), a_3 = (0,0,0,0,1,1)\}$ and define the element

$$\begin{aligned} f &= 8\chi_{H_1}\chi_{H_2}\chi_{H_3}\chi_{H_4} = 4\chi_{H_1}\chi_{H_2} + 4\chi_{H_3}\chi_{H_4} - 4\chi_{H_1H_2+H_3H_4} \\ &= 4\chi_{H_1}\chi_{H_2} + 4\chi_{H_3}\chi_{H_4} - 4\chi_{H_5}\chi_{H_6} \in S \cap \mathcal{C}(X, 8\mathbb{Z}). \end{aligned} \tag{4.1}$$

The crucial fact we need, verified by computer computation, is that all 630 of the two-point subsets of X can be written as 3-fold intersections of elements of $\mathcal{H}$. In particular, the element $8\chi_{\{a_2,a_3\}} = (2\chi_{H_1})(2\chi_{H_2})(2\chi_{H_5^c})$ lies in $\mathfrak{m}^3$. To verify (S5), it will suffice to show that the functions $8\chi_{\{x\}}$, $x \in X$, all lie in S. Now we have $8\chi_{\{a_1\}} = f - 8\chi_{\{a_2,a_3\}} \in S$, and we can modify it to obtain $8\chi_{\{x\}} = 8\chi_{\{a_1,x\}} - 8\chi_{\{a_1\}} \in S$ for any $x \in X$.

When one deals with the generality of prespace matroids (as opposed to representable Witt rings), a stability reducing operation becomes apparent. We can replace the circuit space $\mathcal{H}$ with the space generated by the 2-fold intersections $H_1 \cap H_2$, $H_i \in \mathcal{H}$ forming a new circuit space $\mathcal{H}^{(2)}$, with minimal set of elements $\mathcal{C}^{(2)}$, yielding a new matroid $\mathcal{M}^{(2)} = (X, \mathcal{C}^{(2)})$. For a matroid coming from a representable Witt ring, this generally only gives a prespace matroid. Since stability index one or two cases become SAP, the smallest example of such is the matroid $\mathcal{M}$ of a group ring with a set X of 8 elements (which has stability index 3). Then the circuits of $\mathcal{M}^{(2)}$ consist of all subsets with two elements, and this does not arise from the Witt ring of a field [Cr2], as mentioned earlier.

Proposition 4.6.

$$\operatorname{st}(\mathcal{M}^{(2)}) = \lfloor \operatorname{st}(\mathcal{M})/2 \rfloor.$$

Proof. We easily achieve the reduction by a factor of two: choose a point x where the maximum occurs, with say m sets from $\mathcal{H}$ intersected. Intersect these in pairs so that x becomes an intersection of either $m/2$ or $(m-1)/2 + 1 = (m+1)/2$ sets from $\mathcal{H}(2)$. Conversely, if fewer than $\lfloor \operatorname{st}(\mathcal{M})/2 \rfloor$ sets from $\mathcal{H}^{(2)}$ could be intersected to obtain $\{x\}$, then it would contradict that $\operatorname{st}(\mathcal{M})$ sets are needed from $\mathcal{H}$. □

5. Rank functions for prespace matroids

The *rank* of a matroid is defined to be the cardinality of a maximal subset not containing any circuit. This is not an invariant that has been studied in the context of spaces of orderings. Translating rank back to Witt rings $W(F)$, we see that the rank is the maximum size of a set of orderings $Y \subseteq X$ for which no nonempty set $H(a)$ is contained in Y. Equivalently, if $a \in F$ is not totally negative, the set of orderings in which it is positive is not contained in Y. In terms of quadratic forms, the support (as a function) of the Pfister form $\langle\langle a \rangle\rangle$ is not contained in Y.

This suggests a generalization to n-rank, the maximum size of a set of orderings $Y \subseteq X$ for which no n-fold Pfister form $\langle\langle a_1, a_2, \ldots, a_n \rangle\rangle$ has support contained in Y. This is equivalent to asking the rank of the derived matroid $\mathcal{M}^{(n)}$. Therefore we see that, while our derived matroids take us out of the category of spaces of orderings, they do produce ways of looking at questions within that category.

We now show that there is an easy computation of rank for a prespace matroid, though *a priori* this is far from obvious.

Theorem 5.1. *Let $\mathcal{M} = (X, \mathcal{C})$ be a prespace matroid. The set of fundamental circuits with respect to any matroid basis $\mathcal{B}$ is an $\mathbb{F}_2$-vector space basis for $\mathcal{H}$.*

Proof. Choose a matroid basis $\mathcal{B} \subseteq X$. For each element $x \in X \setminus \mathcal{B}$, let H_x be the unique circuit contained in $\mathcal{B} \cup \{x\}$, i.e. the fundamental circuit of x with respect to $\mathcal{B}$. Since the added elements x are distinct, it is clear that no sum of such circuits can be empty, so the sets are linearly independent. Now suppose that $\{ H_x : x \in X \setminus \mathcal{B} \}$ does not generate $\mathcal{H}$. Then there must be some element, $H \in \mathcal{H}$, that is linearly independent of $\{ H_x : x \in X \setminus \mathcal{B} \}$. We must have $|H \cap (X \setminus \mathcal{B})| \geq 2$, for otherwise $H \subseteq \mathcal{B}$ is an independent set, or $H = H_x$ for some $x \in X \setminus \mathcal{B}$. Let $x_1, \ldots, x_k \in X \setminus \mathcal{B}$, $k \geq 2$, be the distinct elements contained in $H \cap (X \setminus \mathcal{B})$. Then, by linear independence, the sum $H + H_{x_1} + \cdots + H_{x_k} \subseteq \mathcal{B}$ must be nonempty, in which case it is an independent set contained in $\mathcal{H}$, a contradiction. Therefore $\{ H_x : x \in X \setminus \mathcal{B} \}$ is a maximal linearly independent set. □

Corollary 5.2. *The matroid rank of a prespace matroid is $|X| - h$, where $|\mathcal{H}| = 2^h$.*

Proof. By the previous theorem, the dimension of $\mathcal{H}$ is $|X \setminus \mathcal{B}| = |X| - |\mathcal{B}|$; hence $|\mathcal{B}| = |X| - h$ for any basis $\mathcal{B}$ of $\mathcal{M}$. □

The proof of the previous theorem is actually more general than stated. It does not use the fact that we want $X \in \mathcal{H}$ or that $\mathcal{H}$ separates the points of X. Thus it applies to the class of binary matroids [O, 9.2.3].

Special cases of this theorem can be proved in other ways. For example the general rank formula for a contraction [O, 3.1.7] can be used to prove the following.

Corollary 5.3. *Let $\mathcal{M}_n$ be the prespace matroid associated with the group ring $\mathbb{Z}[G]$, where $|G| = 2^n$, so $|X| = 2^n$ and $|\mathcal{H}| = 2^{n+1}$. Then the rank is $2^n - (n+1)$.*

These ranks are called Eulerian numbers and comprise the second column of Euler's triangle, but we see no combinatorial connection.

6. Prespace matroids versus graphical matroids

We can completely answer the question of which graphs give rise to prespace matroids. The converse issue seems more difficult.

Theorem 6.1. *Let $\mathcal{M}(G)$ be a prespace matroid induced by a connected graph G. Then G is a 4-edge-connected Eulerian circuit or consists of a single vertex and loop.*

Proof. Let X be the edge set of G. The set X is nonempty since prespace matroids are necessarily so. Furthermore, since $\mathcal{M}(G)$ is a prespace matroid, we have $X \in \mathcal{H}$. Therefore all edges of G form a single circuit and G is Eulerian. Thus if $|X| = 1$, we have a single loop. Assume that $|X| > 1$. Let $K \subset X$ such that the subgraph consisting of the edges $X \setminus K$ is disconnected. It suffices to prove that K contains at least 4 edges. We proceed case-by-case showing that K cannot have fewer than 4 edges. If $|K| = 0$, then G is disconnected. If $|K| = 1$, then the element of K cannot be part of any circuit and therefore G is not Eulerian. If $|K| = 2$, then the elements of K cannot be separated (i.e., are not contained in disjoint circuits). If $|K| = 3$, then G is not Eulerian. □

The next theorem confirms that Theorem 6.1 gives precisely the connected graphs which induce prespace matroids. If the graph is not connected, it can contain only isolated points added to one of these graphs since extra edges prevent the edge set from being a circuit. Thus the graphs are completely characterized.

Theorem 6.2. *Let G be a 3-edge-connected Eulerian circuit. Then the matroid $\mathcal{M}(G)$ induced by G is a prespace matroid.*

Proof. Let X be the edge set of G, and let $\mathcal{H}$ be the set of all subsets of X which represent circuits or sums of circuits of G. Because G is Eulerian, we have $X \in \mathcal{H}$. At this point, it suffices to prove that the points of X (edges of G) can be separated by circuits. Suppose that $C_1 \in \mathcal{H}$ is a circuit. Let e_1, e_2 be two distinct edges of C_1. If either e_1 or e_2 is a loop, then we are done, so assume that neither is a loop. Let $X' = X - \{e_1, e_2\}$. Then, by hypothesis, the subgraph G' consisting of the edges X' is connected. It follows that there is a path P connecting the adjacent vertices of e_1 in G'. Let C_2 be the circuit in $P \cup \{e_1\}$ containing e_1. Then $e_1 \in C_2$ and $e_2 \notin C_2$. Therefore $\mathcal{H}$ separates the points of X. □

As an example of these theorems, we see that a complete graph K_n induces a prespace matroid if and only if n is odd and at least 5. Being Eulerian requires that n be odd and being 4-edge-connected forces $n \geq 5$. We note the following in passing without defining the terms for which we shall have no further use.

Proposition 6.3. *The class of prespace matroids is not minor-closed.*

Proof. Take for instance the Fano matroid F_7 which is a prespace matroid. If x denotes any element of the basis set of F_7, then it is easy to see that $F_7 \backslash x \cong \mathcal{M}(K_4)$, the matroid of the complete graph [O, Example 1.5.6], which is not a prespace matroid as just noted. □

Now we can take up the issue of when a given prespace matroid is graphical.

Theorem 6.4. *Every graphical prespace matroid has stability index at most* 2.

Proof. By Theorem 6.1, a corresponding graph G must be 4-edge-connected. Let $e = (u, v)$ be any edge of G (i.e. point of the matroid) with endpoints u and v. If $u = v$, then e is a loop, hence a circuit. Otherwise, by Menger's Theorem, there are four edge-disjoint paths from u to v, so two of them can be combined with e to form two circuits that intersect in e. Thus the stability index of the matroid is 1 or 2. □

Define a *Witt matroid* to be a prespace matroid which comes from a representable finitely generated torsion free Witt ring. These have been characterized in [Cr2], where it is shown that they all can be constructed recursively from a one-point prespace using the operations of sum and extension from Section 2. As a consequence, we can prove the following.

Proposition 6.5. *A Witt matroid is graphical if and only if its stability index is at most two.*

Proof. We have shown one direction. We must now construct graphs to show these matroids are graphical. SAP_n comes from a graph with one vertex and n loops, which takes care of stability index one. The extension of SAP_n by $\mathbb{Z}_2$ comes from an n-cycle to which we add an extra edge between each pair of adjacent vertices. Finally, a graph for a sum of such prespaces is obtained by choosing a vertex from each individual graph and identifying them. □

Arbitrary prespace matroids are not yet fully understood in this regard. Controlling the stability index is not sufficienct to make them graphical.

Example 6.6. (1) Though Proposition 6.5 does not apply, the matroid induced by the prespace E_n is graphical for all n. Indeed, it comes from a graph with two vertices and $2n$ edges connecting those vertices.

(2) The matroid induced by the prespace $\mathrm{SAP}_3 \times \mathrm{SAP}_3$ is not graphical, even though it has stability index 2. To see this, assume to the contrary that it comes from a graph G. Then G must have 9 edges, the number of points in the prespace. Since no circuit of the matroid has size one or two, the graph can have no loops or multiple edges. By Theorem 6.1, every vertex of G has even degree at least four. Since the sum of the degrees is 18, twice the number of edges, there must be a vertex of degree six. But then there are at least seven vertices, each of degree at least four, so there must be at least 14 edges, a contradiction.

References

[ABR] C. Andradas, L. Bröcker, and J. Ruiz, *Constructible Sets in Real Geometry*, Springer Verlag, Berlin, 1996. MR1393194 (98e:14056)

[Cr1] T. Craven, *Stability in Witt rings*, Trans. Amer. Math. Soc. **225** (1977), 227–242. MR0424800 (54:12758)

[Cr2] T. Craven, *Characterizing reduced Witt rings of fields*, J. Algebra **53** (1978), 68–77. MR0480332 (58:505)

[CS2] T. Craven and T. Smith, *Abstract theory of semiorderings*, Bull. Austral. Math. Soc. **72** (2005), 225–250. MR2183405 (2006k:12004)

[CV] T. Craven and M. Vo, *A class of finite commutative rings constructed from Witt rings*, Bull. Austral. Math. Soc. **73** (2006), 47–64. MR2206562 (2007b:13046)

[KR] 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. MR500241 (80a:13028)

[KRW1] M. Knebusch, A. Rosenberg, and R. Ware, *Structure of Witt rings and quotients of abelian group rings*, Amer. J. Math. **94** (1972), 119–155. MR0296103 (45:5164)

[KRW2] M. Knebusch, A. Rosenberg, and R. Ware, *Signatures on semilocal rings*, J. Algebra **26** (1973), 208–250. MR0327761 (48:6103)

[L2] T. Y. Lam, *Orderings, Valuations and Quadratic Forms*, CBMS Regional Conference Series in Mathematics, 52, Amer. Math. Soc., Providence, RI, 1983. MR714331 (85e:11024)

[Ma1] M. Marshall, *Abstract Witt rings*, Queen's Papers in Pure and Appl. Math., Vol. 57, Queen's University, Kingston, Ontario, 1980. MR674651 (84b:10032)

[Ma2] M. Marshall, *The Witt ring of a space of orderings*, Trans. Amer. Math. Soc. **258** (1980), 505–521. MR558187 (81b:10012)

[O] J. G. Oxley, *Matroid Theory*, Oxford University Press, Oxford, 1992. MR1207587 (94d:05033)

[W] D. J. A. Welsh, *Matroid Theory*, Academic Press, New York, 1976. MR0427112 (55:148)

Department of Mathematics, University of Hawaii, Honolulu, Hawaii 96822
E-mail address: tom@math.hawaii.edu

Department of Mathematics and Computer Science, Emory University, Atlanta, Georgia 30322
E-mail address: kent@mathcs.emory.edu