Free Cyclic Submodules and Non-Unimodular Vectors

Joanne Hall, Metod Saniga

Free Cyclic Submodules and Non-Unimodular Vectors

Joanne L. Hall[1,2] and Metod Saniga[2]
[1]School of Mathematical and Geospatial Sciences, RMIT University
GPO Box 2476, Melbourne 3001
Australia
(joanne.hall@rmit.edu.au)
and
[2]Astronomical Institute, Slovak Academy of Sciences
SK-05960 Tatranská Lomnica
Slovak Republic
(msaniga@astro.sk)

Abstract
Given a finite associative ring with unity, R, and its two-dimensional left module, ${}^2R$, the following two problems are addressed: 1) the existence of vectors of ${}^2R$ that do not belong to any free cyclic submodule (FCS) generated by a unimodular vector and 2) conditions under which such (non-unimodular) vectors generate FCSs. The main result is that for a non-unimodular vector to generate an FCS of ${}^2R$, R must have at least two maximal right ideals of which at least one is non-principal.

Keywords: Finite Unital Rings – Free Cyclic Submodules – Non-Unimodular Vectors

1 Introduction

Projective geometries over finite associative rings with unity have recently found important applications in coding theory (see, e. g.,[1]) and quantum information theory (see, e. g., [2, 3, 4]). When constructing a geometry over a ring, a majority of authors consider as points of such a geometry only free cyclic submodules (FCSs) generated by unimodular vectors [5], whilst some authors consider all submodules [6, 7]. It has recently been shown [9] that there exists rings for which some vectors of the submodule are not contained in an FCS generated by a unimodular vector. These vectors have been called outliers. Even more interesting is that some outliers themselves generate FCSs. A geometry may be constructed using all FCSs.

Analysing all finite associative rings with unity up to order 31 inclusive, only several rings are found to feature outliers. Out of these, only few non-commutative rings exhibit FCSs comprising solely non-unimodular vectors [8]; the smallest example being the ring of ternions over the Galois field of order two [9]. These examples motivated a more systematic and general treatment of the questions of the existence of outliers and FCSs generated by them. The outcomes of our explorations are not only interesting on their own, but they can also have interesting physical bearings (like, e. g., those proposed in [10]).

2 Definitions and Preliminaries

All rings considered are finite, but not necessarily associative. R^* is the group of units of a ring, R. $R \setminus R^*$ is the set of zero divisors. 1 is the unity element of a ring. It is well known that in a finite associative ring all elements are either units or zero divisors (see, for example, [11, §2.1]). The symbol $\subset$ stands for strict inclusion.

Definition 1. Let $\langle R, \cdot, + \rangle$ be a ring. A *left ideal*, I_l, is a subgroup of $\langle R, + \rangle$ such that $rx \in I_l$ for all $r \in R$ and $x \in I_l$. A *right ideal*, I_r, is a subgroup of $\langle R, + \rangle$ such that $xr \in I_r$ for all $x \in I_r$ and $r \in R$. An ideal is *principal* if it is generated by a single element of R. For $a \in R$ the *principal left ideal* generated by a is Ra, and a *principal right ideal* generated by a is aR.

For further background on rings see, for example, [12].

Definition 2. [5, Defi 2.9][13, p. 16] Let $S \subseteq R$. The left (right) *annihilator* of S, denoted ${}^{\perp}S$ ($S^{\perp}$), is defined as:

$$\begin{aligned} {}^{\perp}S &= \{x \in R : xa = 0, \forall a \in S\}, \\ S^{\perp} &= \{x \in R : ax = 0, \forall a \in S\}. \end{aligned}$$

For sets containing a single element, the notation is simplified ${}^{\perp}\{a\} := {}^{\perp}a$.

Lemma 3. *Let $P, S \subseteq R$, then ${}^{\perp}S$ is a left ideal, $S^{\perp}$ is a right ideal and*

$${}^{\perp}P \cap {}^{\perp}S = {}^{\perp}(P \cup S).$$

Definitions below are given for left modules, the mirrored definitions can be given for right modules.

Definition 4. [5] Let R be a ring with unity, and ${}^2R$ be a left module over R. $(a, b) \in {}^2R$ is unimodular if it satisfies the following equivalent conditions:

- $aR \oplus bR = R$,
- there exists $x, y \in R$ such that $ax + by = 1$.

Note that aR and bR are principal right ideals of R.

Definition 5. $R(a, b)$ is a *cyclic submodule* of ${}^2R$ generated by (a, b):

$$R(a, b) = \{(\alpha a, \alpha b) : \alpha \in R\}.$$

If $(\alpha a, \alpha b) = (0, 0)$ only when $\alpha = 0$, then $R(a, b)$ is *free*. Equivalently, if all the vectors in a cyclic submodule are distinct, then the submodule is *free*.

Reworking the definition of a free cyclic submodule using annihilators leads to the obvious lemma:

Lemma 6. *Let R be a finite associative ring with unity. $R(a, b)$ is a free cyclic submodule of ${}^2R$ if and only if*

$${}^{\perp}a \cap {}^{\perp}b = \{0\}. \tag{1}$$

Proof. Let (a, b) be the generating vector, then by definition $R(a, b)$ is free if $\alpha(a, b) = (0, 0)$ only if $\alpha = 0$. This is equivalent to equation (1). □

Lemma 7. *[5, §1] Let (a, b) be a unimodular vector in ${}^2R$, then $R(a, b)$ is a free cyclic submodule.*

Unimodular vectors have other useful properties [5], and for many rings all free cyclic submodules are generated by unimodular vectors. Corollaries 21 and 24 show two classes of rings for which the reverse of Lemma 7 is true.

Definition 8. An *outlier* is a vector which is not contained in any free cyclic submodule generated by a unimodular vector.

The aim of this research is to get some insight into which rings contain outliers, and, more specifically, which rings contain outliers that generate free cyclic submodules. This question is of interest for general ${}^nR$, but we only treat the simplified case of ${}^2R$ where R is a finite associative ring.

3 Results

3.1 Unimodular vectors

We begin by collecting some important facts about unimodular vectors.

If $a \in R^*$, then $aR = R$, hence for all $b \in R$, $aR \oplus bR = R$. Thus any vector containing an entry which is a unit, is a unimodular vector. Unimodular vectors may be divided into two types:

- Type I: vectors which contain an entry which is a unit;
- Type II: vectors where both entries are zero-divisors.

Theorem 9. *Let R be a finite associative ring with unity. If $a, b \in R \setminus R^*$, then (a, b) is a unimodular vector in ${}^2R$ if and only if there exist distinct maximal right ideals, I_1, I_2, such that $a \in I_1 \setminus I_2$ and $b \in I_2 \setminus I_1$.*

Proof. $\Rightarrow$ Since $a, b \in R \setminus R^*$, aR and bR are right ideals strictly contained in R. If there is some proper right ideal, I, that contains a and b, then $aR \oplus bR \subseteq I \subset R$. Hence, if (a, b) is unimodular, then a and b cannot belong to the same maximal ideal.

$\Leftarrow$ aR and bR are right ideals for which $aR \subset I_1$ and $bR \subset I_2$. $aR \oplus bR$ is a right ideal not contained in either I_1 or I_2. Therefore $aR \oplus bR$ must be contained in a right ideal that contains both I_1 and I_2. Since I_1 and I_2 are maximal, the only right ideal containing them both is R. Hence $aR \oplus bR = R$, and (a, b) is a unimodular vector of ${}^2R$. □

All type II unimodular vectors of ${}^2R$ conform to the conditions of Theorem 9.

Theorem 10. *Let R be a finite associative ring with unity. If (a, b) is a unimodular vector in ${}^2R$, then $(\alpha a, \alpha b)$ is also unimodular if and only if $\alpha \in R^*$.*

Proof. $\Rightarrow$ (a, b) is unimodular, thus by definition there exists some $x, y \in R$ such that $ax + by = 1$. Let $\alpha \in R^*$ then

$$\begin{aligned} ax + by &= 1, \\ \alpha(ax + by) &= \alpha, \\ \alpha(ax + by)\alpha^{-1} &= 1, \\ (\alpha a)(x\alpha^{-1}) + (\alpha b)(y\alpha^{-1}) &= 1. \end{aligned}$$

Hence $(\alpha a, \alpha b)$ is unimodular.

$\Leftarrow$ Suppose $(\alpha a, \alpha b)$ is unimodular, then for some $x, y \in R$

$$\begin{aligned} \alpha ax + \alpha by &= 1, \\ \alpha(ax + by) &= 1; \end{aligned}$$

hence, $\alpha \in R^*$. □

Theorem 11. *Let R be a finite associative ring with unity. Then $R(\alpha a, \alpha b) \subseteq R(a, b)$. If $\alpha \in R^*$, then $R(\alpha a, \alpha b) = R(a, b)$.*

Proof. R is associative, thus $\beta(\alpha a) = (\beta\alpha)a$ for all $\beta, \alpha, a \in R$. Thus $R(\alpha a, \alpha b) \subseteq R(a, b)$. Let $\alpha \in R^*$, $\beta a = \beta\alpha^{-1}\alpha a$, thus $R(a, b) \subseteq R(\alpha a, \alpha b)$.

For unimodular vectors this is a corollary of Theorem 10. □

Theorems 9 to 11 give criteria for checking for unimodular vectors of ${}^2R$. More difficult is finding outliers.

3.2 Outliers

In the light of Theorem 10 we can refine our notion of outlier.

Definition 12. Let R be a finite associative ring with unity. (a, b) is an *outlier* of ${}^2R$ if there does not exist $\alpha, c, d \in R$ such that $(a, b) = (\alpha c, \alpha d)$ and (c, d) is unimodular.

Theorem 13. *Let R be a finite associative ring with unity. (a, b) is an outlier of ${}^2R$ if and only if there exists a right ideal $I \subseteq R$, such that $a, b \in I$ and*

1. *there are no principal right ideals which contain both a and b;*
2. *or if there is a principal right ideal αR such that $a, b \in \alpha R$, then $aR \oplus bR \subset \alpha R$.*

Proof. $\Rightarrow$ Theorem 9 shows that if (a, b) is an outlier of ${}^2R$ then a and b are contained in some maximal right ideal. If there does not exist $(\alpha c, \alpha d) = (a, b)$ then either $a, b \notin \alpha R$ for some $\alpha \in R \setminus R^*$ (showing part 2) or (c, d) is not unimodular. Assume that there exists $(\alpha c, \alpha d) = (a, b)$ with (c, d) not unimodular. Let $C = \{c : \alpha c = a\}$ and $D = \{d : \alpha d = b\}$. If $\alpha x = \alpha y$ with $x \neq y$, then $\alpha(x - y) = 0$, thus $(x - y) \in \alpha^\perp$. Since,

$$C = \{c\} \oplus \alpha^\perp \qquad \text{and} \qquad D = \{d\} \oplus \alpha^\perp, \tag{2}$$

one gets

$$\begin{aligned} aR \oplus bR &= \alpha cR \oplus \alpha dR \\ &= \alpha(cR \oplus dR \oplus \alpha^\perp). \end{aligned}$$

Thus $aR \oplus bR = \alpha R$ if and only if there exists $c \in C$ and $d \in D$ such that $cR \oplus dR \oplus \alpha^\perp = R$. Since we can choose any $c \in C$ and $d \in D$, we require that

$$CR \oplus DR \oplus \alpha^\perp = R.$$

From equation (2) it follows:

$$CR \oplus DR \oplus \alpha^\perp = CR \oplus DR.$$

If $CR \oplus DR = R$, then there exists $c \in C$ and $d \in D$ and $x, y \in R$ such that $cx + dy = 1$, implying that (c, d) is a unimodular vector. This contradicts that (a, b) is an outlier, and hence we find that $aR \oplus bR \subset \alpha R$ (showing part 1).

$\Leftarrow$ 1. If all right ideals that contain a and b are non-principal, then there does not exist $\alpha \in R^*$ such that $a, b \in \alpha R$. Hence (a, b) is an outlier of ${}^2R$.

2. Let αR be a principal right ideal for which $a, b \in \alpha R$. Then there exists c, d such that $\alpha c = a$ and $\alpha d = b$. If $aR \oplus bR \subset \alpha R$, then

$$\begin{aligned} (\alpha c)R \oplus (\alpha d)R &\subset \alpha R, \\ \alpha(cR \oplus dR) &\subset \alpha R, \\ cR \oplus dR &\subset R, \end{aligned}$$

and (c, d) is not unimodular. And, hence, (a, b) is an outlier. □

If R is commutative then (a, b) is an outlier of the left module exactly when $(a, b)^T$ is an outlier of the right module. In a non-commutative ring, the set of left outliers may be different to the set of right outliers (the smallest example is the ring of ternions of order 8 [9]). The set of outliers is dependent on the structure of the ideals of the ring. If the left and right ideals of a ring have different structures, then a left outlier may be right unimodular.

From Theorems 9 and 13 we get that:

Lemma 14. *If a, b are in some right ideal which is non principal, but not in any principal right ideals, and in different maximal left ideals, then (a, b) is an outlier and $(a, b)^T$ is unimodular.*

3.3 Free cyclic submodules and outliers

We have established that the structure of the ideals of a ring determines the set of outliers and unimodular vectors. The Jacobson radical is an important ideal and of crucial importance in the study of unimodular vectors.

Definition 15. [12, §4] For a finite ring R, the *Jacobson radical*, J, may be equivalently defined as:

- the intersection of all the maximal left ideals of R;
- the largest left ideal J such that $1 + j \in R^*$ for all $j \in J$.

Note that the Jacobson radical is a left *and* right ideal.

Definition 16. [12, Defi 4.9] A one-sided or two-sided ideal, I, is *nilpotent* of *nilpotency* m if $a_1.a_2 \dots a_m = 0$ for any set of elements $a_1, a_2, \dots, a_m \in I$.

Lemma 17. *[12, Thm 4.12] Let R be a finite associative ring. Then J is nilpotent.*

Theorem 18. *If R is a finite associative ring, then no vector from ${}^nJ$ generates a free cyclic submodule.*

Proof. From Lemma 17 it readily follows that J has nilpotency m for some $m \in \mathbb{N}$. Let $(a_1, a_2, \dots, a_n) \in {}^nJ$, $x_1, x_2, \dots, x_{m-1} \in J$ and $\alpha = x_1.x_2 \dots x_{m-1}$. Then $(\alpha a_1, \alpha a_2, \dots, \alpha a_n)$ $= (0, 0, \dots, 0)$. Hence $R(a_1, a_2, \dots, a_n)$ is not a free cyclic submodule. □

Definition 19. [12, §19] A *local* ring is an associative ring that has exactly one maximal left (and also right) ideal.

As a side note we mention that geometries over local rings are called Hjelmslev geometries [5, §9], and have applications in coding theory [1].

Theorem 20. *Let R be a local ring.*

1. *No outliers of ${}^2R$ generate free cyclic submodules.*
2. *(a, b) is an outlier of ${}^2R$ if and only if $a \notin bR$ and $b \notin aR$.*

Proof. 1. R has exactly one maximal ideal, which is therefore the Jacobson radical, J. All ring elements not belonging to J are units. Hence any outlier of ${}^2R$ has both entries as elements of J. Theorem 18 shows that no vectors with both entries from J can generate a free cyclic submodule.

2. J, the unique maximal ideal of R, cannot generate R. By Theorem 9, no unimodular vector of ${}^2R$ can contain elements of the same maximal ideal. Since every element of R is either a unit or an element of J, all unimodular vectors have a unit entry; all unimodular vectors are of type I. So, the outliers of ${}^2R$ are those vectors which are not contained in a free cyclic submodule of ${}^2R$ generated by $(1, x)$ or $(x, 1)$, $x \in R$. A vector which is not an outlier is of the form

$$(a, ax) \qquad \text{or} \qquad (ax, a), \text{ for some } a, x \in R.$$

Thus outliers are those vectors which do not fit this form. If (a, b) is contained in a free cyclic submodule then there exists $x \in R$, such that $ax = b$ or $bx = a$. Hence $b \in aR$ or $a \in bR$. If $a \notin bR$ and $b \notin aR$, then (a, b) is an outlier. □

Corollary 21. *If R is a finite local ring, then $R(a, b)$ is a free cyclic submodule if and only if (a, b) is unimodular.*

This is a class of rings for which the reverse of Lemma 7 holds. In particular, this means that Hjelmslev geometries (which are geometries over a local ring) cannot have non-unimodular points.

Next we look at another property of ideals which precludes the existence of non-unimodular free cyclic submodules.

Lemma 22. *Let R be a finite associative ring with unity. Let a, b be elements of the same principal proper right ideal, αR, then $R(a, b)$ is not a free cyclic submodule of ${}^2R$.*

Proof. $a = \alpha c$ and $b = \alpha d$. Then

$$\begin{aligned} {}^{\perp}a &= \{x : xa = 0\} \\ &= \{x : x\alpha c = 0\} \\ &\supseteq \{x : x\alpha = 0\} \\ &= {}^{\perp}\alpha. \end{aligned}$$

By the same logic ${}^{\perp}b \supseteq {}^{\perp}\alpha$. Hence ${}^{\perp}a \cap {}^{\perp}b \supseteq {}^{\perp}\alpha \neq \{0\}$. □

Lemma 22 then gives the following important result.

Theorem 23. *Let R be a finite associative ring with unity. If every right ideal is a principal ideal, then there are no free cyclic submodules of ${}^2R$ generated by non-unimodular vectors.*

This shows that a necessary condition for the existence of non-unimodular free cyclic submodules of ${}^2R$ is the presence of non-principal right ideals.

Corollary 24. *Let R be a principal ideal ring, then $R(a, b)$ is a free cyclic submodule if and only if (a, b) is unimodular.*

This is another class of rings (see Corollary 21) for which the reverse of Lemma 7 holds.

When using associative rings free cyclic submodules are generated by either unimodular vectors or outliers. If the assumption of associativity is removed, then this is no longer true.

Lemma 25. *Let R be a finite ring with unity and let (a, b) be a unimodular vector in ${}^2R$. If there exists α such that $(\alpha a, \alpha b)$ is a non-unimodular vector and $R(\alpha a, \alpha b)$ is a free cyclic submodule of ${}^2R$, then R is non-associative.*

Proof. Assume that R is associative. Then, by Theorem 10, if $(\alpha a, \alpha b)$ is non-unimodular, then $\alpha \in R \setminus R^*$. If $R(\alpha a, \alpha b)$ is free, then $R(\alpha a, \alpha b) = R(a, b)$. Thus there exists $\beta \in R$ such that

$$(\beta\alpha a, \beta\alpha b) = (a, b),$$

under the assumption that R is associative, this requires that $\beta\alpha = 1$, contradicting that $\alpha \in R \setminus R^*$.

Hence if there exists α such that $(\alpha a, \alpha b)$ is a non-unimodular vector and $R(\alpha a, \alpha b)$ is a free cyclic submodule, then R is non-associative. □

Examples have been calculated of non-associative rings of order 8, where (a, b) is unimodular, $R(\alpha a, \alpha b)$ is free and $R(\alpha a, \alpha b) \not\subseteq R(a, b)$.

4 Conclusion and Further Directions

To find FCSs of ${}^2R$ that are generated by non-unimodular vectors ("non-unimodular FCSs"), R must have at least two maximal right ideals, at least one of which is non-principal. This is a necessary condition. Calculated examples [8] show that this is not sufficient; other

properties of a ring are required to guarantee the presence of FCSs generated by non-unimodular vectors.

As already mentioned in the introduction, in our worked examples [8] non-unimodular FCSs have been only found for non-commutative rings. One would be tempted to conjecture that non-commutativity is essential in this respect. Yet, this is questionable because some rings feature non-unimodular FCSs in ${}^2R$, but not in R^2 (and *vice versa*). Hence, it is highly desirable to clarify to what extent the existence of non-unimodular FCSs depends on the non-commutativity of the ring; in particular, what is the smallest commutative ring featuring non-unimodular FCSs?

Further, in all analysed examples, a non-unimodular FCS was found to share with *any other* FCS at least one vector apart from $(0, 0)$; is this true in general, or just a feature of the particular small-order rings? Finally, within our bank of examples, we found rings where all outliers generate FCSs (like the smallest ring of ternions [9]), as well as rings where only some outliers have this property. What distinguishes the two kinds of rings? These are exciting open questions we would like to focus on in the near future.

Acknowledgement

JLH gratefully acknowledges the support from the National Scholarship Programme of the Slovak Republic. This work was also partially supported by the VEGA grant agency projects 2/0092/09 and 2/0098/10.

References

[1] Honold T., and Landjev I., Linear codes over finite chain rings and projective Hjelmslev geometries, in Codes Over Rings: Series on Coding Theory and Cryptology 6, Editor P. Solé, World Scientific, Hackensack NJ, 2009, 60–123.

[2] Planat M., Saniga M., and Kibler M. R., Quantum entanglement and projective ring geometry, *Symmetry, Integrability and Geometry: Methods and Applications* **2** (2006), 066 (arXiv:quant-ph/0605239).

[3] Havlicek H., and Saniga M., Projective ring line of an arbitrary single qudit, *Journal of Physics A: Mathematical and Theoretical* **41** (2008), 015302 (arXiv:0710.0941).

[4] Saniga M., Planat M., Pracna P., Projective ring line encompassing two-qubits, *Theoretical and Mathematical Physics* **155** (2008), 463–473 (arXiv:quant-ph/0611063).

[5] Veldkamp F.D., Geometry over rings, in Handbook of Incidence Geometry, Editor F. Buekenhout, Amsterdam, Elsevier, 1995, 1033–1084.

[6] Brehm U., Greferath M., and Schmidt S. E., Projective geometry on modular lattices, in Handbook of Incidence Geometry, Editor F. Buekenhout, Amsterdam, Elsevier, 1995, 1115–1142.

[7] Faure C.-A., Morphisms of projective spaces over rings, *Advances in Geometry* **4** (2004), 19–31.

[8] Saniga M., Projective lines over finite rings, an invited Kempner colloquium given at the Department of Mathematics, University of Colorado, Boulder, Colorado (U. S. A.), on April 28, 2011; available on-line at `http://www.ta3.sk/~msaniga/pub/ftp/boulder.pdf`.

[9] Havlicek H., and Saniga M., Vectors, cyclic submodules and projective spaces linked with ternions, *Journal of Geometry* **92** (2009), 79–90 (arXiv:0806.3153).

[10] Saniga M., and Pracna P., Space versus time: unimodular versus non-unimodular projective ring geometries?, *Journal of Cosmology* **4** (2010), 719–735 (arXiv:0808.0402).

[11] Raghavendran R., Finite associative rings, *Compositio Mathematica* **21** (1969), 195–229.

[12] Lam T.-Y., A First Course in Noncommutative Rings, *Graduate Texts in Mathematics* **131**, Springer, New York, 2001.

[13] Hughes D. R., and Piper F. C., Projective Planes, Springer, New York, 1973.