International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 10 | Oct 2020 www.irjet.net p-ISSN: 2395-0072

Quadratic Boolean Modules

Dawit Cherinet Kifetew

Department of Mathematics, Arba Minch University, Arba Minch, Ethiopia,

---

Abstract - *This is a brief account of a study of quadratic Boolean modules over Boolean like rigs. This study can be understood as a kind of synthesis of Subrahmanyam's[5] papers on Boolean vector spaces and Gopala Rao's paper[3] on Vector spaces over a regular ring. As to terminology, I differ from both authors. The reasons are as follows. The notions "vector space" and "modules over a ring" have a very precise and widely accepted meaning in algebra and I don't want to divert from common use. On the other hand, the algebraic structures of this study have much in common with modules over a ring. To highlight their specific features. I have decided to introduce the concept of a quadratic Boolean modules. Why this was chosen will be made clear in the course of this text. It turns out that much of the results known for Boolean rings and regular rings extend with minor adaptations.*

Key Words: Boolean Like Rings (BLRs), Quadratic Boolean Modules

1. On the Structure of Boolean like Rings (BLR for short):

A commutative ring R with 1 is called a Boolean Like Ring ([2]) (BLR) if it satisfies the following conditions:

1. *R has characteristic two*
2. $a(1-a)b(1-b) = 0 \; for \; all \; a, b \in R$

It turns out that

$$B := \{a^2 : a \in R\}$$

is a subring, denoted by B or B(R), which consists of all idempotent elements of R. It is a Boolean ring, named as the Boolean subring of R. Let N or N(R) denote the ideal of all nilpotents elements of R. We have

1. $n.m = 0$ *for all nilpotent elements* $n, m \in N$
2. $N = \{a \in R : a^2 = 0\}$
3. $N = B + N, B \cap N = \{0\}$
4. $R/N \cong B$

Note that N is a B-module (in the normal sense of module theory). Alternatively, a BLR can be characterized as a zero-extension $B \oplus N$ of a Boolean ring by an arbitrary B-module N. The addition is clear. Concerning multiplication, we have:

$$(e+n)(f+m) = ef + (em + fn)$$

where $e, f \in B; \; n, m \in N$*:*

Throughout this paper we keep the notation: R for the BLR, B its subring of idempotent elements, N its ideal of nilpotent elements, elements of R are written as $a, b, c, \ldots$ *, those of B as* $e, f, g, \ldots$*, and those of N as* $n, m, u, \ldots$*. The group of units of R will be denoted by E or* $E(R)$*, and elements of units will be represented by* $\mu, \eta, \ldots$*. It is known that*

$$E = \{1 + n | \; n \in N\} = \{a \in R | = 1\}$$

The multiplicative group E and the additive group N are isomorphic via the isomorphism $log : E \longrightarrow N, \mu \mapsto \mu - 1$ *with inverse* $exp : N \longrightarrow E, n \mapsto 1 + n$

1.1. Special elements in BLRs.

For any given $a \in R$ *the element a2 is idempotent. Hence,* $a^{2n} = a^2, a^{2n+1} = a^3 \; for \; n \geq 1$ *and a; a2; a3 is the list of all powers of a which actually occur. It may happen that not all of them are distinct. An element* $a \in R$ *is* ***idempotent***

If $a = a^2$*, it is called* ***weakly idempotent*** *if* $a = a^3$ *, and it is called* ***weakly nilpotent*** *if* $a^2 = a^3$*. Note that a is weakly idempotent and weakly nilpotent if and only of a is idempotent. Idempotents and units are samples of weakly idempotent elements, and idempotents and nilpotents are samples of weakly nilpotent elements. The weakly idempotent elements play a big role in the study of quadratic Boolean modules. In fact, one is dealing with finite sequences* $a_1, a_2, \ldots, a_n \in R$ *subject to the conditions*

$$\sum_{i=1}^{n} a_i^2 = 1, a_i . a_j = 0 \; if \; i \neq j$$

Necessarily, each a_i *is weakly idempotent.*

As stated in the last section every $a \in R$ *has a unique decomposition of the type*

$a = e + n$ *where e is idempotent, n is nilpotent*

Using this fact, one proves

Proposition 1.1: ***L****et* $a = e + n$ *where e is idempotent, n is nilpotent. Then*

1. *a is weakly idempotent iff* $e.n = n$*„*
2. *a is weakly nilpotent iff* $e.n = 0$*,*
3. *a is weakly idempotent iff* $a = e.\epsilon$ *for some idempotent e, unit* ϵ *. It is* $e = a^2$ *in this decomposition.*

Furthermore, it turns out that a is weakly nilpotent if and only if $1-a$ is weakly idempotent. The set of weakly idempotent elements (resp. weakly nilpotent elements) is closed under the two operations

$$(a,b) \rightarrowtail ab;\ (a,b) \rightarrowtail a + b + ab$$

Given an idempotent e, then $e = e^2$, what implies that the nilpotent part N of R decomposes into the two eigenspaces N_0, N_1. We get

$$N_0 = \{n | e.n = 0\}, N_1 = \{n | e.n = n\}, N = N_0 \oplus N_1$$

Then $e + N_0$ is a set of weakly nilpotent and $e + N_1$ a set of weakly idempotent elements. If $N \neq N_0, N_1$ then we get elements a such that all powers a, a^2, a^3 are distinct.

The next statement is fundamental for quadratic Boolean modules over BLR's.

***Proposition 1.2**. ([4]) Given $a \in R$, there is a unique decomposition of the type $a = b + n$ where b is weakly idempotent, n is nilpotent and $b.n = 0$. In this decomposition we have $b = a^3, n = a - a^3$.*

1.2 Primary Ideals

A BLR has Krull dimension zero, so every prime ideal is maximal. The maximal ideals of R, denoted by M, lie over the maximal ideals of B, denoted by m. Regarding the intersection of all maximal (=prime) ideals we obtain,

$$\cap M = N, \cap m = \{0\}$$

A commutative ring R is called primary if every zero divisor is nilpotent, an ideal I of R is called primary if the residue ring R/I is a primary ring. A primary ideal Q of the BLR R restricts, by intersecting with B, to a maximal ideal m of B. So, $Q \supseteq mR$. The ideal $I = mR$ is a primary ideal of R since

$$R/I \cong F_2 \oplus N$$

and the latter ring is primary due to the following statement.

***Proposition 1.3**. The following statements are equivalent for a BLR R:*

1. *R is a local ring,*
2. *$|B| = 2, i.e\ R = F_2 \oplus N$*
3. *R is a primary ring.*

Proof. The proof of $(1) \Rightarrow (2)$ uses the identity $e(1-e) = 0$ for every idempotent e. To deduce (3) from (2) one uses the fact $R = E \cup N$ under the given hypothesis. Finally, the remaining implication is shown by arguing that the radical $\sqrt{0}$ is a prime, hence a maximal ideal.

Moreover, one gets that an ideal I of R is primary iff it contains an ideal of the type mR. Hence the ideals mR, where m ranges over the maximal ideals of B are exactly the minimal primary ideals of R. Additionally, the minimal primary ideals of R are pairwise coprime.

Theorem 1.4.

***1.** $\{\mathbf{0}\} = \cap$ **Q, Q** ranging over all primary ideals of R,*

2. R is a subdirect product of BLRs of the type $F_2 \oplus N$, i.e. of primary BLRs,

3. if R has only finitely many idempotents, then R is a finite product of primary BLRs.

Proof. The proof makes use of the fact that R/mR is a primary BLR for each maximal ideal m of B. Once the first statement is proven the other two follows at once. To prove the first result, one has to show that $\cap mR = 0$. Consider an element $a \in R$ in the intersection and pick a maximal ideal m of B. Then there is a presentation

$$a = \sum_i e_i a_i \text{ , with idempotents } a_i \text{ and elements } a_i$$

Now, using the identity

$$ea + fb = (e + f + ef)(ea + fb)$$

one derives that $a = eb$ for some $e \in m;\ b \in R$. This implies that for each maximal ideal m we find e_m such that $(1 - e_m)a = 0$. We next consider the annihilator ideal

$$I = \{f \in B | f.a = 0\}. \text{ If } I = B \text{ then } a = 1.a = 0. \text{ Assume}$$

*$I \neq B$. Then I must be contained in some maximal ideal **m** of **B**. This implies $(1 - e_m)a = 0, e_m a = 0$, so again $a = 0$ follows.*

2. Quadratic Boolean Modules

2.1 Axioms and Examples.

Let R be a BLR, V an abelian group, and a mapping

$R \times V \longrightarrow V, (a,x) \mapsto ax$ be given. Elements of V are denoted by $x, y, \ldots$. This setting is called a Quadratic Boolean Module over R ([1]) if the following axioms are satisfied:

1. *$a^2(x + y) = ax + ay$*
2. *$a(bx) = (ab)x$ if either a is idempotent or both a, b are units*
3. *$1x = x$*
4. *$(a + b)x = ax + bx$ if $ab = 0$*

Because of the first axiom (1), I have chosen the term "Quadratic". The last axiom is a typical Boolean condition; hence the term "Boolean" is introduced. For short, quadratic

Boolean modules over a BLR are referred to as Boolean modules.

This set of axioms is consistent as shown by the subsequent examples.

1. ***The case of Boolean rings:*** *If R is a Boolean ring then any R-module in the normal sense of module theory, referred to as module hereafter, satisfies the axioms. As Foster has shown, a quadratic Boolean module over a Boolean ring is a module Iff the group V satisfies* $x + x = 0$ *for all* $x \in V$ *.*
2. ***The case of R-algebras:*** *There are other samples of Boolean modules over an arbitrary BLR R. Let S be any R - algebra, not necessarily commutative, with unit 1, i.e. S is a ring with unit and a R - module satisfying*

$$a(st) = (as)t = s(at) for\ all\ a \in R;\ s,t \in S.$$

In this situation, the set $R1$ *is a subring of S contained in the center of S. Let's assume that* $a1 = 0 \Longrightarrow a = 0$*. Then,* $R \cong R1$*, and, alternatively, we are dealing with a BLR R which is contained in the center of an extension ring S with unit where* $1_R = 1_S$*. Yet, the original setting of R-algebras is more flexible in view of the following important examples:*

$S = R[G]$*, the group ring of a group G over R, or* $S = Mn(R)$*, the ring of* $n \times n$ *matrices over R. So far, it is known that the group ring is fundamental for the so-called group extensions of a group by a BLR. The case of the ring of matrices is yet to be explored.*

It is notable that, via those R-algebras, one can produce examples of Boolean modules without requiring the group V to be abelian. So, it seems feasible to extend the present study to the case of non-abelian Boolean modules. However, for the sake of simplicity, this study focuses on the abelian case apart from presenting a few samples in a more general setting.

In the setting above, we take $(V, +) = (S^*, .)$*,* S^* *the group of units of S. The scalar multiplication* $R \times S^* \longrightarrow S^*$ *is denoted by the symbol* $*$ *to avoid confusion with the multiplication in S. We denote* $(a, x) \mapsto a * x$ *as follows:*

$$a * x = 1 - a^2 + a^3 x$$

The proof that $a * x$ *is in fact a unit in S makes uses of the condition that* $R1$ *lies in the center of S, and* $(1 - a^2)a^3 = 0$ *what leads to the following statement:*

$$if\ xy = 1\ then\ (1 - a^2 + a^3 x).(1 - a^2 + a^3 y) = 1$$

By direct calculations one verifies that $R, V = S^*, (a, x) \mapsto a * x$*, constitute a model for the axioms for a Boolean module. Boolean modules of this type share special features:*

$$ax = a^3 x, \{a0 = 0\} \Leftrightarrow a^2 = a^3$$

provided $r1 = 0 \Rightarrow r = 0$*. These two properties will be encountered in the next section again, in a quite natural manner.*

3. ***The case of E and N:*** *We take* $R = S$ *and obtain that E is a Boolean R-module under the scalar multiplication* $a * x = 1 - a^2 + a^3 x$*. In particular,* $\epsilon * n = \epsilon n$*. This shows that in this case, expressed in the additive notation,* $V = R0_V = R^*0_V$*. This is the first instance of a so called free Boolean module.*

As stated earlier, the group of units E is isomorphic to the additive group N via the mapping $1 + n \mapsto n$*. Transferring the Boolean module structure of E one obtains that N is a Boolean R-module under the scalar multiplication*

$$a * n = -a^2 + a^3 + a^3 n.$$

3. Construction via Boolean modules over Boolean rings

Given any Boolean module V over a BLR R we can restrict the scalar multiplication from R to the subring B of idempotent elements which is a Boolean ring. The topic dealt with in this section is the reconstruction of the R-module V from the underlying B-module V . For the sake of simplicity, we restrict to abelian groups V. However, with little more care various statements can be extended to the non-abelian case.

Lemma 3.1*.*

1. $.e(x + y) = ex + ey;\ e0 = 0$ *for all* $e \in B;\ x, y \in V$ *,*
2. $a^2 0 = 0;\ 2(a0) = 0\ for\ all\ a \in R,$
3. $0x = 0\ for\ all\ x \in V$ *.*

Proposition 3.2*.* $ax = a^2 x + (1 - a^2 + a^3)0 + (a - a^3)0$ *for all* $a \in R$

Proof. The proof starts from the equation $a^2 x = ax + a0$*, uses* $a0 = -a0$ *to get* $ax = a^2 x + a0$*. The next input is the decomposition of a into a weakly idempotent and a nilpotent part:*

$$a = a^3 + (a - a^3)$$

Using axiom (4) one derives $a0 = a^3 0 + (a - a^3)0$*. Apply axiom (4) and lemma* $1, (1)$ *to* $1 - a^2, a^3$ *to get* $a^3 0 = (1 - a^2 + a^3)0$*, and the proof is complete.*

The ingredients of the decomposition above of ax have distinguished meanings: The term $a^2 x$ *refers to V as a Boolean B-module, the second term is of the type* $\epsilon 0$ *since* $(1 - a^2 + a^3)^2 = 1$*, and the third one is of the type* $n0$ *since* $(a - a^3)^2 = 0$*.*

Therefore, one has to study the mappings

$\varphi : E \longrightarrow V_2;\ \epsilon \mapsto \epsilon 0$ *and* $\psi : N \longrightarrow V_2;\ n \mapsto n0$

with $V_2 = \{x \in V \mid 2x = 0\}$:

Lemma 3.3*.*

1. $\epsilon x = x + \epsilon 0;\ \epsilon x + \eta y = \epsilon\eta(x + y)$ *for all units* ϵ, η *and all* $x, y \in V$ *,*

2. $nx = n0;\ n0 + m0 = (n + m)0$ *for all nilpotent elements* n, m*.*

The first statements in (1), (2) *follow from proposition* 3.2*. The second statement in* (2) *is a consequence of axiom* (4)*. Furthermore,* $\epsilon x + \eta y = (x + \epsilon 0) + \eta y =$

$$x + (\eta y + \epsilon 0) = x + \epsilon(\eta y) = x + (\epsilon\eta)y$$
$$= x + y + (\epsilon\eta)0 = (\epsilon\eta)(x + y).$$

As consequence we get that the mappings φ, ψ *are group homorphisms. As shown above,* E *and* N *are Boolean R-modules, hence Boolean B-modules:*

$e * \epsilon = 1 - e + e\epsilon;\ e * n = en.$ *It turns out that both mappings are even B-linear, i.e*

$\varphi(e * \epsilon) = e\varphi(\epsilon);\ \psi(e * \eta) = e\,\psi(\eta).$

It is the content of the next theorem that all three ingredients can be chosen arbitrarily, subject to the conditions obtained so far. The verification is straightforward.

Theorem 3.4. *A Boolean R-module is given by a Boolean* $B -$ *module* V *and*

arbitrarily chosen B-linear group homomorphisms

$\varphi : E \longrightarrow V_2$ *and* $\psi : N \longrightarrow V_2$ *by virtue of the formula*

$$ax = a^2x + \varphi(1 - a^2 + a^3) + \psi(a - a^3)$$

3.1 Modifications of Boolean Modules.

Theorem 3.4 *allows to modify the structure of a Boolean module by changing the mappings* φ, ψ *and but preserving the B-module structure. If the mappings are changed then we get a new scalar product denoted by* $a\ o\ x$*. Keeping the*

B-module structure means $ax = a\ o\ x$ *if* a *is an idempotent. In view of results to follow in the next section it is interesting to preserve also the products* ax *if* a *is weakly idempotent, i.e.* $a = a^3$*. Looking at the formula in theorem* 3.4*, this*

means we have to preserve the Boolean B-module structure and the mapping $\varphi : E \longrightarrow V_2$*. This observation leads to the notion of a nilpotent modification of a Boolean* $R -$ *module* V *.*

Definition 3.5*. Let a Boolean R-module* V *be given, and* $\tau : E \longrightarrow V_2$ *be any B-linear group homomorphism then the nilpotent modification of Boolean* $R -$ *module* $V\_$ *is defined by the scalar multiplication*

$$a\ o\ x = ax + \tau(a - a^3)$$

The nilpotent modifications of a given Boolean R-module preserve the scalar products ax *for weakly idempotent elements. Among them we find a distinguished one where* $n0 = 0$ *for each nilpotent element* n*. This one is obtained from a given one by choosing* $\tau = \psi$*. This distinguished Boolean module deserves a special name:*

Definition 3.6. *A Boolean R-module is called regular if* $n0 = 0$ *for every* $n \in N$*.*

A Boolean R-module has a unique nilpotent modification which is regular. One concludes that a Boolean R-module is regular $ax = a^3x$ *for every* $a \in R$*. Regular Boolean modules are characterized by the formula*

$ax = a^2x + (1 - a^2 + a^3)0;\ a \in R;\ x \in V.$

If V *is regular and is weakly nilpotent then* $a0 = 0$*.*

3.2 Normed Boolean B-modules.

We consider a Boolean ring B *and a Boolean* $B -$ *module* V*. A mapping* $||: V \longrightarrow B$ *is called a Boolean norm if it satisfies the conditions*

1. $|x| = 0$ *if and only if* $x = 0$;
2. $|ex| = e|x|$ *for all* $e \in B$

In the following we will be referring to the order structure in Boolean rings and the annihilator ideal

$$ann(x) = \{e \mid ex = 0\}$$

$$e \leq f \Leftrightarrow ef = e; sup(e; f) = e + f + ef;$$

$$inf(e; f) = ef$$

That $ann(x)$ *is an ideal of* B *follows from the axioms* (2), (4)*: let* $ex = fx = 0$*, then*

$(e + f + ef)x = [e + (1 + e)f]x = ex + (1 + e)(fx) = 0$*, so* $e + f + ef \in ann(x)$*.*

Also, $eg \in ann(x)$ *for any* $g \in B$*. In particular,* $e + f = (e + f)(e + f + ef) \in ann(x)$*. We also get that the ideal* $ann(x)$ *is closed under taking the supremum*

of finitely many elements. Furthermore, in Boolean rings principal ideals have a uniquely determined generator.

Proposition 3.7*. The following statements are equivalent:*

1. *A norm exists,*
2. $for\ all\ x \in V, min\{f \mid fx = x\}\ exists,$

3. $for\ all\ x \in V, max\{f|fx = x\}\ exists$
4. $for\ all\ x \in V$, *the annihilator ideal* $ann(x)$ *is a principal ideal.*

If a norm exists, then it is unique and we have

$$ann(x) = (1 - |x|);\ 1 - |x| = max\{e|ex = 0\};$$

$$|x| = min\{f|fx = x\}$$

Proof. Here I present the proof for last statement the proposition. The reader can easily verify the rest. Assume that $ann(x) = (e_x)$. *Note that the generator*

is uniquely determined. Then set $|x| := 1 - e_x$. *One gets that* $|x| = 0\ iff\ x = 0$. *Next consider* $y = fx$. *Then* $1 - f, e_x \in ann(y) = (e_y)$ *and we derive that*

$sup(1 - f;\ e_x) = 1 - f - e_x f \in (ey)$. *This means:* $1 - f - e_x f \leq e_y$. *On the other hand* $e_y f \in ann(x)$, *hence* $e_y f e_x = e_y f$ *what yields*

$(1 - f - fe_x)e_y = e_y \Rightarrow e_y \leq 1 - f - fe_x$,

Altogether

$$ey = 1 - f - fe_x; |y| = 1 - e_y = f(1 + e_x) = f|x|.$$

Conversely, let's assume that a norm exists. Then from

$|(1 - |x|)x| = (1 - |x||x| = 0$ *one gets that* $1 - |x| \in ann(x)$. *Assume* $ex = 0$ *then* $e|x| = 0$ *which implies* $e = f(1 - |x|)$. *So, it is proven that*

$$ann(x) = (1 - |x|).$$

According to the last result, a norm exists whenever the Boolean ring has the strong property that each set which is closed under finite suprema has indeed a maximum. In particular, this applies to finite Boolean rings. In this case, I guess one should be able to interpret the norm via the decomposition of V *into the eigenspaces attached to the multiplication by the finitely many idempotents in* B. *The arguments above can be applied to the special case of a BLR* R *considered as module over its ring of idempotents* B. *It turns out that* R *as*

$a\ B - module\ admits\ a\ norm\ if\ and\ only\ if\ N\ is\ a\ normed\ B - module.$ *Note that the*

Boolean module structure on N *coincides with the usual module structure as a* $B - module$. *So, one could study normed BLRs, for instance if* B *is finite.*

REFERENCES

[1] *Dawit Cherinet and K. Venkateswarlu: On Boolean like ring extension of group, International Journal of Algebra, 8(2014),no. 3, 121-128*

[2] *Foster A.L. The theory of Boolean Like Rings, Trans. Amer.Math.Soc. Vol. 59(1946),166-187*

[3] *Gopala Rao, N.R: Vector Spaces over a regular ring, Math annalen, 167, 280-291(1966)*

[4] *Swaminathan V: On Foster's Boolean Like Rings, Math. Seminar Notes, Kobe University, Japan, Vol. 8, 1980, 347-367*

[5] *N.V. Subrahmanyam: Boolean Vector Space I, Math Zeitschr, 83 (1964).422-433.*