Boolean Linear Combinations

Dawit Cherinet Kifetew

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

---

Abstract - *This article discusses the concept of Boolean linear combinations over Quadratic Boolean modules. The concept actually mimics the famous Inclusion- Exclusion Formula in set theory or combinatorics. The Boolean representation of elements of the Quadratic Boolean Module allows us to study the concept of partition matrices and study some properties which is very interesting in its own way. Finally, Boolean generators and free*

Boolean modules have been studied.

Key Words Boolean Like Rings (BLRs), Boolean Linear Combinations, Partition Matrices, Boolean Generators

1. Preliminaries

1.1 On the Structure of Boolean Like Rings (BLR for short):

A commutative ring R with 1 is called a Boolean Like Ring ([3]) (BLR) if it satisfies the following conditions:

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

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⊕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*

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

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

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* $n \geq 1$ *([4]) 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*

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

Necessarily, each a_i *is weakly idempotent. Every* $a \in R$ *has a unique decomposition of the type*

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

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.*

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.*([2]) 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.*

Theorem 1.4. ([2])

1. $\{\mathbf{0}\} = \cap\, \boldsymbol{Q}, \boldsymbol{Q}$ *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.

1.3 Quadratic Boolean Modules

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 ([2]) 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* $ab = 0$

Lemma 1.5.*([2])*

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

Lemma 1.7. *([2])*

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.

2. The Inclusion-Exclusion Formula.

Suggested by this formula one is directed to introducing the notion of sets of Boolean generators of the section (5). Boolean generators present a feature that is distinctive for Boolean modules and has no counterpart in the usual module theory. The name of this formula stems from the well-known inclusion-exclusion formula of set theory or combinatorics, paraphrased in the context of Boolean rings. Given two subsets A, B *of a set* C then

$$C = (A^c \cap B^C) \cup (A \cap B^c) \cup (A^C \cap B) \cup (A \cap B).$$

In Boolean rings this decomposition reads:

$$1 = (1 - e)(1 - f) + e(1 - f) + (1 - e)f + ef$$

Given a *Boolean module* $V(B - module)$ and elements $x\ y \in V$, we derive the following formula

Proposition 2.1. Given elements $e, f \in B$ *and* x, y in a $B - module\ V$

$$ex + fy = (1 - e)(1 - f)0 + \big(e(1 - f)\big)x + \big((1 - e)f\big)y + ef(x + y).$$

Proof. The proof uses the fact $g0 = 0$ for every idempotent g as well as axioms (1), (4). The coefficients $a_1, \ldots, a_4$ satisfy the two conditions

$$a_i a_j = 0 \text{ if } i \neq j;\ \sum_{i=1}^{4} {a_i}^2 = 1$$

where $a_1 = (1 - e)(1 - f)$, $a_2 = \big(e(1 - f)\big), a_3 = \big((1 - e)f\big), a_4 = ef$

This proposition already displays the essential features of the general inclusion-exclusion formula. This formula starts with a general sum $\sum_{i=1}^{n} a_i x_i$ with a *BLR R*, *a Boolean R − module V* , elements $a_i \in R;\ x_i \in V;\ i = 1, \ldots, n$ are given. It then presents a new representation with distinguished properties of the coefficients. To express these new coefficients, we introduce the following notation:

Let $S = \{1, \dots, n\}$, set

$$a_S := (\prod_{i \in S} a_i)(\prod_{j \notin S}(1 - a_j{}^2)), x_S := \sum_{i \in S} x_i, x_\emptyset = 0$$

Properties of the a_S are listed in the following lemma. We make use of the symmetric difference of two sets:

$$S \Delta T = (S \cap T^C) \cup (S^c \cap T).$$

Lemma 2.2.

1. $a_S a_T = (\prod_{i \in S \cup T} a_i{}^2)(\prod_{j \in S^c \cap T^c} 1 - a_j{}^2)(\prod_{k \in S \Delta T}(a_k - a_k{}^3))$
2. $Let\ S \neq T$, then
   a. $a_S a_T = 0$ if each a_i is weakly idempotent
   b. $a_S{}^2 a_T{}^2 = 0$
3. $\sum_S a_{S=} 1 + \sum_{i \in S}(a_i - a_i{}^2)$; $\sum_S a_S{}^2 = 1$

Proof. The proof of (1) is straightforward. Since for any a the element $a - a^3$ is nilpotent we get that $a_S{}^2 a_T{}^2 = 0\ if\ S \neq T$. The same conclusion holds if all a_i are weakly idempotent.

The proof of (3) starts with the identity:

$$\prod_{i \in S}(a_i + (1 - a_i{}^2)) = \sum_S a_S$$

which is obtained by distributivity. Next, use $a_i + (1 - a_i{}^2 = 1 + (a_i - a_i{}^2)$

fact that for any a the element $a - a^2$ is nilpotent and that $nm = 0$ for any two nilpotent elements n, m. As a consequence, we get the right-hand side ofthe first claim in statement (3) above. Also, this sum is a unit, hence the rest follows.

Theorem 2.3 (Inclusion-Exclusion Formula). In the situation above:

1. $\sum_{i=1}^n a_i x_i = \sum_{S \subseteq \{1,\dots,n\}} a_S\, x_S$
2. $\sum_{S \subseteq \{1,\dots,n\}} a_S{}^2 = 1$
3. if all a_i are weakly idempotent then all a_S likewise and $a_S a_T = 0\ if\ S\ \neq T$

Proof. Since $a_\emptyset x_\emptyset = 0$, the case of the empty set could be omitted. For symmetry, it is listed as well. Regarding the statements (2), (3) the lemma above.

The proof of (1) proceeds by studying the cases (1) to (4) .

1. $all\ a_i = e_i \in B,$
2. $all\ a_i = \epsilon_i \in E,$
3. all $a_i$are weakly idempotent,
4. arbitrary a_i.

Case (1): We proceed by induction on $n, n = 2$ is settled above. In the induction step, write

$$\Sigma = \sum_{i=1}^{n+1} e_i x_i = \sum_{S \subseteq \{1,\dots,n\}} e_S x_S + e_{n+1} x_{n+1}$$

Since $1 = \sum_{S \subseteq \{1,\dots,n\}} e_S x_S$, we obtain

$$\Sigma = \sum_{S \subseteq \{1,\dots,n\}}(e_S\, x_S + e_S e_{n+1} x_{n+1})$$

The inner sum equals $e_S(1 - e_{n+1})x_S + e_S e_{n+1}(x_S + x_{n+1}))$ due the case of n = 2. So, the claim is proven.

Case (2): Under this hypothesis the claim boils down to the assertion $\sum_{i=1}^n \epsilon_i x_i = (\prod_{i=1}^n \epsilon_i)(\sum_{i=1}^n x_i)$ since $\epsilon^2 = 1$ for every unit ϵ. This statement follows by in duction from lemma 1.7.

Case (3): Under this hypothesis we have

$a_i = a_i{}^2\, \epsilon_i, where\ \epsilon_i$ a unit.

Setting $y_i = \epsilon_i x_i$ and using axiom (2), we can deal with

$$\sum_{i=1}^n a_i x_i = \sum_{i=1}^n a_i{}^2 x_i$$

by invoking the results of cases (1), (2) to derive the assertion.

Case (4): We will be using the decomposition

$$a = a^3 + n(a)\ with\ n(a) = a - a^3$$

$where\ a^3 n(a) = 0\ and\ n(a) is\ nilpotent.$

Simplifying the notation, we set $n(a_i) =: n_i$. Then, invoking lemma 1.7

$$\sum_{i=1}^n a_i x_i = \sum_{i=1}^n (a_i{}^3 + n_i)x_i = (\sum_{i=1}^n a_i{}^3 x_i) + (\sum_{i=1}^n n_i)0$$

$$\sum_{S \subseteq \{1,\dots,n\}} a_S{}^3 x_S + (\sum_{i=1}^n n_i)0$$

$$= \sum_{S \subseteq \{1,\dots,n\}} a_S{}^3 x_S + (\sum_S n_S + \sum_{i=1}^n n_i)0$$

where $n_S = a_S{}^3 - a_S$

$$= \left[\prod_{i \in S}(a_i + n_j)\right][\prod_{j \in S}(1 - a_j{}^2)]$$

The product of any two nilpotent element is zero. Hence,

$$n_S = \sum_{i\in S} (\prod_{j\in S\{i\}} a_j) (\prod_{k\notin S} (1 - a_k{}^2)) n_i$$

This leads to

$$\sum_S n_S = \sum_i [\sum_{S,i\in S} (\prod_{j\in S\{i\}} a_j) (\prod_{k\notin S} (1 - a_k{}^2))] n_i$$

The term in brackets [ ] can be dealt with by lemma 2.2, applied to the set

$\{1. \dots, n\} - \{i\}$ and the elements a_j ; $j \neq i$. We obtain

$$\sum_S n_S = \sum_i \left[1 + \sum_{j\neq i} (a_j - a_j{}^2)\right] n_i = \sum_i n_i$$

since the value in [ ] is a unit, and $\epsilon . n = n$ for any unit ϵ and nilpotent element n. Finally, $\sum_S n_S + \sum_i n_i = 0$ and the proof is complete.

3. Boolean Linear Combinations.

The inclusion-exclusion formula suggests to study linear combination of the following type:

$$x = \sum_i a_i x_i \text{ where } a_i a_j = 0 \text{ for } i \neq j \text{ and } \sum_i a_i{}^2 = 1$$

Such a linear combination $\sum_i a_i x_i$ is called a Boolean linear combination, and the representation $x = \sum_i a_i x_i$ by a Boolean linear combination is called a Boolean representation of x. It is a very nice fact that the sum $x + y$ and the scalar product ax can be expressed by using Boolean representations.

Proposition 3.1. $x = \sum_i a_i x_i$ *and* $y = \sum_i b_j x_j$ be Boolean representations of $x, y \in V$ *and* $c \in R$, Then

1. $x + y = \sum_{i,j} a_i b_j (x_i + x_j)$
2. $cx = (c - c^3)0 + [(1 - c^2 + c^3 a_1)0 + \sum_{i\neq 1} (c^3 a_i) x_i]$

Remark 3.2. In (1) the right-hand side is a Boolean representation. In (2) the second term [ ] is a Boolean linear combination of the sequence $0, x_1, \dots, x_n$.

If $0 = x_i$ *for some* i, *say* $0 = x_1$ then

$$cx = (c - c^3)0 + [(1 - c^2 + c^3 a_1)0 + \sum_{i\neq 1} (c^3 a_i) x_i$$

and this term [ ] is a Boolean linear combination of the sequence $(x_i)_i$

The last proposition together with the inclusion-exclusion formula allows to describe the submodules of V which are generated by given sets X, denoted by $< X >$.

Definition 3.3.

$Bspan(X) =$ $\{all\ Boolean\ linear\ combinations\ of\ x \in V\ \}$ is called the Boolean span of X.

Theorem 3.4. Let G denote the subgroup of V generated by X. Then

$$< \mathrm{X} >= \mathrm{Bspan(G)} + \mathrm{N0}$$

Proof. It is clear that $< X >$ must contain the set on the right-hand side, *say* W. It remains to show that W is already a submodule. $Bspan(G)$ is a subgroup by the last proposition, $N0$ as well by lemma 1.7. To prove that

W is closed under scalar multiplication , First note the relation $a(x + n0) = a^2(x + n0) + a0 = (a^2 x + a0) + (a^2 n)0 = ax + (a^2 n)0$. Then apply the last proposition 3.1.

The statements in this proposition are particularly nice if we consider the Boolean span of a subgroup $G\ of\ V$. In this case we get

1. $\sum_{g\in G} a_g x_g + \sum_{g\in G} b_g x_g = \sum_{g\in G} (\sum_{(h,k):h+k=g} a_h b_k x_g)$
2. $c. \sum_{g\in G} a_g x_g = (c - c^3)0 + [(1 - c^2 + c^3 a_1)0 + \sum_{0\neq g} (c^3 a_i) x_g$

4. Partition matrices.

This section is needed in the subsequent study of Boolean modules with a Boolean basis and it deserves attention in its own right. It deals with interesting groups of the so-called partition matrices which, by the way, present new samples of Boolean modules, not necessarily commutative.

In the last section we were dealing with sequences $(a_i)_i$ subject to the conditions

$$a_i a_j = 0\ for\ i \neq j\ and \sum_j a_j{}^2 = 1$$

In this situation the element $\epsilon \coloneqq \sum_i a_i$ is a unit, and the fact

$\sum_j a_j{}^2 = 1$ can be interpreted as a partition. Each term $a_i{}^2$

gives rise to the "component" $a_i{}^2 = a_i$.

We express these facts by saying that $(a_i)_i$ is a partition of a unit. Accordingly, we call the column vector

$$\begin{pmatrix} a_1 \\ . \\ . \\ . \\ a_n \end{pmatrix}$$

a partition vector over R.

A $n \times m$ matrix over R is called a partition matrix if all columns are partition vectors over R. The set of all $n \times m$ partition matrices is denoted by $B_{n,m}$, where we set $B_n := B_{n,m}$.

The following lemma is proven by direct verification.

Lemma 4.1.

1. If A is a $n \times m$ partition matrix over R and $x \in R^n$ a partition vector, then Ax is a partition vector in R^n.
2. Let B be a $m \times r$ partition matrix then AB is a $n \times r$ partition matrix over R.

Remark 4.2. As a consequence of the last lemma we get that B_n is closed under multiplication, i.e. it is a monoid.

If the $BLR\ R$ is a primary (=local) ring then partition vectors and matrices feature a simple structure as will be remarked soon. By reducing the general case to this special one we are able to derive surprising results about invertible partition matrices. This reduction is performed by making use of the minimal primary ideals mR. The canonical residue homomorphism

$$R \mapsto \frac{R}{mR} = F_2 \oplus N, a \longmapsto a_m := a + m$$

induces, by reducing the entries of vectors and matrices mod mR, a mapping of vectors and matrices, $A \longmapsto A_m$, which preserves all usual operations with vectors and matrices:

$$(\mathrm{A}+\mathrm{B})_m = \mathrm{A}_m + \mathrm{B}_m;\ (\mathrm{A.B})_m = \mathrm{A}_m.\mathrm{B}_m, \det(\mathrm{A}_m) = (\det(\mathrm{A}))_m, (\mathrm{A}^{-1})_m = (\mathrm{A}_m)^{-1}$$

Theorem 1.40 $=\cap\, mR$ tells where m runs through all maximal ideals of B. This entails: if A, B, C are matrices over R then

$$\mathrm{A} = \mathrm{B}(\mathrm{resp}:\ \mathrm{AB} = \mathrm{C}) \Leftrightarrow \mathrm{A}_m = \mathrm{B}_m(\mathrm{resp}:\ \mathrm{A}_m\mathrm{B}_m = \mathrm{C}_m) \text{ for all m}$$

Using $(ab)_m = a_m b_m, (\sum_i {a_i}^2)_m = \sum_i [a_i]_m{}^2$, we get that

Lemma 4.3. *A is a partition matrix (resp. invertible partition matrix) if and only if A_m is a partition matrix (resp. invertible partition matrix) for all m.*

We now consider the case of a primary BLR $R = F_2 \oplus N$ and keep this convention unless we explicitly return to the general case. Such ring is local with maximal ideal N, any element outside N is a unit.

Let a sequence $(a_i)_i$ be given where $a_i.a_j = 0\ if\ i \neq j$ and $\sum_i {a_i}^2 = 1$. Then some a_i must lie outside N, so it is a unit. This implies that $a_j = 0\ if\ j \neq i$. Hence, a partition vector is of the type

$$\epsilon \times\ unit\ vector$$

Let's consider quadratic matrices in $M_n(R)$. Then, partition matrices $A \in M_n(R)$ are just the matrices of the type

$A = D{:}U$ where $D = diag(\epsilon_1, \epsilon_2, \ldots, \epsilon_n)$ a diagonal matrix of units ϵ_i and U a matrix whose columns are unit vectors.

Such a decomposition $A = D{:}U$ is unique. In particular, an invertible $n\_ \times n$ matrix is a partition matrix if it is a product of an invertible diagonal matrix $D = diag(\epsilon_1, \epsilon_2, \ldots, \epsilon_n$ and a permutation matrix composed of unit vectors $(e_{\sigma(i)})_i$ where σ is a permutation in the symmetric group S_n.

We now return to the case of a general BLR. Using lemma 4.3, we get

Theorem 4.4. 1. Let A be an invertible partition matrix over R. Then, the inverse A^{-1} and the transpose $A^t$are again partition matrices,

2. The set of invertible partition $n \times n$ matrices form a subgroup, denoted by ${B^*}_n$ of the general linear group $GL_n(R)$.

Corollary 4.5. ${B^*}_n$ is a (not necessarily commutative) R-module under the scalar product $(a, A) \longmapsto (1 - a^2)E + a^3 A$

It could be interesting to study this R-module. I found the first statement of the last theorem very surprising. In particular, it says that the row vectors of an invertible partition matrix are also partition vectors. But, partition matrices were defined by only requiring the column vectors to be partition vectors.

5. Boolean Generators and Free Boolean Modules

Let V be a Boolean module and $X \subseteq V$. If $V = Bspan(X)$ then X is called a set of Boolean generators of V . If each $x \in V$ has a unique Boolean representation

$$x = \sum_x a_x x \text{ where almost } \mathrm{a}_x = 0;\ \mathrm{a}_x a_y = 0 \text{ if } \mathrm{x} \neq \mathrm{y} \text{ and } \sum_x {a_x}^2 = 1$$

then X is called a *Boolean basis of V* .

In Boolean representations only weakly idempotent coefficients occur. This implies that we can pass to any nilpotent modification of **V** without changing the Boolean representations and losing the property that X is a set of Boolean generators. Therefore, till the end of this summary we will assume that the Boolean module, V is regular, i.e. $N.0 = 0$.

We need a calculus of Boolean spans $Bspan(X)$. First,

$$BSpan(X) = \cup\, Bspan(X_0)$$

where X_0 *ranges over all finite subsets of* X

Therefore we can confine ourselves to finite sets $X = \{x_1, x_2, \dots, x_n\}$. Let $Let\ Y = \{y_1, y_2, \dots, y_m\} \subseteq Bspan(X)$. Then we have Boolean representations

$$y_j = \sum_i a_{i,j}\, x_i, \text{and an n} \times \text{m partition matrix A} = (\mathrm{a}_{i,j})$$

Since each y_j may have distinct Boolean representations the partition matrix A is possibly not uniquely determined in terms of the $(x_i)'s, (y_j)'s$. Nevertheless, by abuse of notations, we set $A = T(X|Y)$ and call it a transformation matrix from X *to* Y .

Proposition 5.1. Given any Boolean representation $\sum_j b_j y_j$ then $\sum_j b_j y_j = \sum_i a_i x_i$ *with* $\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = T(X|Y) \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$

Proof. The proof follows from proposition 3.1.

Corollary 5.2. 1. $Bspan(Y) \subseteq Bspan(X)$;

2. if $T(X|Y)$ *is invertible then* $Bspan(Y) = Bspan(X)$.

Proposition 5.3. Let X be a Boolean basis of V and Y any set of Boolean generators of V, $|X| = n; |Y| = m$. Then $T(X|Y)T(Y|X) = E_n$, the $n \times n$ unit matrix. In particular, $n \leq m$.

Regarding the proof one uses that each x_is a Boolean linear combination of the y_j and that X is a basis. We deduce from this proposition that the cardinality of any basis is an invariant of the free Boolean module. We set

Definition 5.4. Let V be a free Boolean module, then the dimension $dim(V)$ is defined as $|X| - 1$ for any basis X *of* V

The reason why -1 was subtracted is to be seen in the behaviour of $a0$. Different from usual vector space theory these values may be non-zero, and we are forced to include 0 into basis or something alike.

Proposition 5.5. Every free Boolean module contains a basis X with $0 \in X$ and we have: $a0 = 0 \Leftrightarrow a^2 = a^3$.

In theorem 3.4, it was proven that $Bspan(G)$ is a Boolean submodule for any subgroup $G \subseteq V$. So, it is not guaranteed that for arbitrary set X the Boolean span $Bspan(X)$ is a module at all. In this regard one can prove

Proposition 5.6. $Bspan(X)$ is a Boolean submodule of V if the following three conditions are satisfied;

1. $0 \in Bspan(X)$,
2. $for\ all\ x \in X\ we\ have -x \in Bspan(X)$;
3. $for\ all\ x, y \in X, we\ have\ x + y \in Bspan(X)$.

The conditions are clearly necessary. They are sufficient in view of propositions 3.1.

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] *Dawit Cherinet, Quadratic Boolean Modules, Unpeblished*

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

[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.*