Mathematisch Instituut
Roetersstraat 15
Amsterdam   The Netherlands

BASES FOR BOOLEAN RINGS

by

P. van Emde Boas and

H.W. Lenstra, Jr.

Report: 73-05

September 1973

Bases for Boolean rings

P. van Emde Boas and H.W. Lenstra, Jr

1. Introduction

Let B be a Boolean ring, i.e. a ring with 1 in which $x^2 = x$ for all x. It is well known that B is commutative, and that $x + x = 0$ for all $x \in B$. Hence we can consider B as a vector space over $\mathbb{F}_2$ (the field of two elements). By a basis of B we mean a basis of B over $\mathbb{F}_2$, and the dimension of B is its dimension over $\mathbb{F}_2$, notation: $\dim B$.
Let $A \subset B$ be a subset. By A^* we denote the smallest subset of B which satisfies

(1.1) $\quad A \cup \{0\} \subset A^*$

(1.2) $\quad$ if $x, y \in B$ are such that A^* contains three of the elements $\{x, y, xy, x + y + xy\}$, then also the fourth one is in A^*.

Let us call a basis U of B an S-basis if $U^* = B$. The main object of this paper is to prove the following lemma, which was left open by W. Scharlau [4, lemma 5.1.1]:

Lemma (1.3). Every Boolean ring has an S-basis.

The proof is given in section 2.

By $\mathbb{Z}[B]$ we denote the commutative ring defined by generators $[x]$ $(x \in B)$ and relations

$$[x] + [y] = [x + y] + 2.[xy]$$
$$[x].[y] = [x.y],$$

cf. [1]. If B is identified with an algebra of subsets of a set X, then $\mathbb{Z}[B]$ may be thought of as the ring of functions $f: X \to \mathbb{Z}$ which satisfy:

(1.4) $\quad f[X]$ is a finite subset of $\mathbb{Z}$,

(1.5) $\quad \forall n \in \mathbb{Z}: f^{-1}[\{n\}] \in B$.

A subset U of B is called an N-basis if $\{[u] \mid u \in U\}$ is a $\mathbb{Z}$-basis of $\mathbb{Z}[B]$. From $\mathbb{Z}[B]/2\mathbb{Z}[B] \cong B$ we see:

Proposition (1.6). Every N - basis is a basis.

The converse of this proposition is discussed in section 3. A theorem of G. Nöbeling [3] asserts that every Boolean ring has an N - basis. This theorem also follows from lemma (1.3) and proposition (1.7):

Proposition (1.7). Every S - basis is an N - basis.

This proposition is proved in section 3. Although the converse of (1.7) does not hold (cf. section 3), it turns out that the N - bases constructed by G.M. Bergman [1] are actually S - bases.

2. Existence of S - bases

Lemma (2.1). Let U be a subset of B with $0 \in U$. Then the following three properties of U are equivalent:

(2.2) if $x, y \in B$ are such that U contains three of the elements $x, y, xy, x+y+xy$ then also the fourth one is in U.

(2.3) if $x, y \in U$ are such that $xy = 0$ or $xy = x$, then $x + y \in U$.

(2.4) if $x, y, xy \in U$, then $x + y \in U$.

Proof of (2.1).

(2.2) $\Rightarrow$ (2.3). If $xy = 0$ then x, y, xy are in U, hence by (2.2) also $x+y+xy = x+y$ is in U. If $xy = x$ then for $y' = x+y$ we know that x, $xy' = 0$ and $x+y'+xy' = y$ are in U, so also $y' = x+y$ is in U.

(2.3) $\Rightarrow$ (2.4). For $x' = xy$ we know $x' \in U$, $y \in U$, $x'y = x'$. Therefore by (2.3) we have $x'+y = xy+y \in U$. By symmetry, $xy+x \in U$. Now $x'' = xy+x \in U$, $y'' = xy+y \in U$ satisfy $x''y'' = 0$, so by (2.3) we see $x+y = x''+y'' \in U$.

(2.4) $\Rightarrow$ (2.2). Let three of the elements $x, y, xy, x+y+xy$ be in U. We distinguish three cases.

(a) $x, y, xy \in U$. Then $x+y \in U$ by (2.4), and since $x' = xy$, $y' = x+y$, and $x'y' = 0$ are in U, we have $x'+y' = x+y+xy \in U$.

(b) $xy, y, x+y+xy \in U$. Applying (2.4) to $x' = xy$ and $y' = y$ we find $y+xy \in J$. Then $x'' = x+y+xy$, $y'' = y+xy$ yield $x''+y'' = x \in U$.

(c) $x, y, x+y+xy \in U$. Putting $x' = x$, $y' = x+y+xy$ we find $y + xy \in U$. Then $x'' = y + xy$ and $y'' = y$ give us $x'' + y'' = xy \in U$.

This proves (2.1).

For $A \subset B$, let A^* denote the smallest subset of B which contains $A \cup \{0\}$ and satisfies the equivalent conditions (2.2), (2.3) and (2.4):

$$A^* = \cap \{U \mid \{0\} \cup A \subset U \subset B,\ U \text{ satisfies } (2.4)\}.$$

<u>Lemma</u> (2.5). Let $f: B \to B'$ be a surjective ring homomorphism, and let A be a subset of B which contains $\ker(f)$. Then

$$A^* = f^{-1}[f[A]^*],$$

where $f[A]^*$ is formed inside B'.

<u>Proof</u> of (2.5). It is clearly sufficient to prove the following three assertions:

(2.6) $A^* \subset f^{-1}[f[A]^*]$

(2.7) $A^* + \ker f = A^*$

(2.8) $f[A]^* \subset f[A^*]$.

<u>Proof</u> of (2.6). $f[A]^*$ is a subset of B' which contains $f[A] \cup \{0\}$ and satisfies (2.4). Therefore $f^{-1}[f[A]]^*$ is a subset of B containing $A \cup \{0\}$ and satisfying (2.4). Now $A^* \subset f^{-1}[f[A]]^*$ follows by definition of A^*.

<u>Proof</u> of (2.7). If $x \in A^*$, $y \in \ker f$ then $y \in A \subset A^*$ since we assumed $\ker f \subset A$. Also $xy \in x.\ker f \subset \ker f \subset A^*$, so (2.4) gives $x + y \in A^*$.

<u>Proof</u> of (2.8). Since $f[A] \cup \{0\} \subset f[A^*]$, it suffices to show that $f[A^*]$ has property (2.4). So let $x, y \in A^*$ be such that $f(x) \in f[A^*]$, $f(y) \in f[A^*]$, $f(x)f(y) \in f[A^*]$; we have to show $f(x) + f(y) \in f[A^*]$. Choose $z \in A^*$ such that $f(x)f(y) = f(z)$. Then $xy \in z + \ker f \subset A^* + \ker f = A^*$ by (2.7). So A^* contains x, y and xy, and by (2.4) we conclude $x + y \in A^*$, $f(x) + f(y) = f(x+y) \in f[A^*]$.

This concludes the proof of (2.5).

Before proving lemma (1.3) we fix some notations. For a well ordered set I, we denote the set of finite subsets of I by $F(I)$, and we wellorder $F(I)$ by putting $E' < E$ if $E, E' \in F(I)$, $E \neq E'$, are such that the largest element of the symmetric difference $(E \cup E') \setminus (E \cap E')$ is in E; this comes down to a lexicographic ordering if in each $E \in F(I)$ the elements are arranged in decreasing order. We agree that a <u>subring</u> of B always contains the unit element 1 of B.

<u>Proof</u> of (1.3).

Let $(e_i)_{i \in I}$ be a sequence of elements of B, indexed by a well ordered set I, such that B, as a subring of itself, is generated by $\{e_i \mid i \in I\}$. For $E \in F(I)$ we put

$$d_E = \Pi_{i \in E}\, e_i \in B,$$

in particular $d_\emptyset = 1$. Lemma (1.3) clearly follows from:

<u>Lemma</u> (2.9). Define $T \subset F(I)$ by

$$T = \{E \in F(I) \mid d_E \text{ is not in the } \mathbb{F}_2\text{-linear span of } \{d_{E'} \mid E' \in F(I),\ E' < E\}\}.$$

Then $\{d_E \mid E \in T\}$ is an S-basis of B.

The <u>proof</u> of lemma (2.9) is by induction on the order type of I. If $I = \emptyset$ then $B = \{0\}$, $T = \emptyset$ or $B \cong \mathbb{F}_2$, $T = \{\emptyset\}$ and the assertion of the lemma is easily checked. If the order type of I is a limit ordinal, then B is an ascending union of subrings corresponding to beginning segments of I, and the assertion of the lemma is immediate from the induction hypothesis. We are left with the case the order type of I is $\lambda + 1$ for some ordinal λ.
Let k be the largest element of I. We put $J = I \setminus \{k\}$ and $e = e_k$. The subring of B generated by $\{e_i \mid i \in J\}$ is denoted by B_o.
Let $T_1, T_2 \subset F(J)$ be defined by:

$$T_1 = T \cap F(J)$$
$$T_2 = \{E \in F(J) \mid \{k\} \cup E \in T\}.$$

Since J has order type λ, the inductive assumption shows:

$$\{d_E \mid E \in T_1\} \text{ is an } S\text{-basis of } B_o.$$

Hence we can rewrite:

$$T_2 = \{E \in F(J) \mid ed_E \text{ is not in the } \mathbb{F}_2\text{-linear span of } B_o \cup \{ed_{E'} \mid E' \in F(J),\ E' < E\}\}. \tag{2.10}$$

As a ring, B is generated by B_o and e, so $e^2 = e$ implies $B = B_o + eB_o$. Here eB_o is a Boolean ring with unit element e, although it is not a subring of B if $e \neq 1$. Clearly, $B_o \cap eB_o$ is an ideal of eB_o. Let $B' = eB_o/(B_o \cap eB_o)$. Since the function $g: B_o \to B'$, $g(b) = (eb \bmod (B_o \cap eB_o))$, is a surjective ring homomorphism, we have a sequence $(e'_j)_{j\in J} = (g(e_j))_{j\in J}$ of ring generators for B'. Applying the induction hypothesis to B', we find that $\{g(d_E) \mid E \in T'\}$ is an S-basis of B', where

$$T' = \{E \in F(J) \mid g(d_E) \text{ is not in the } \mathbb{F}_2\text{-linear span of } \{g(d_{E'}) \mid E' \subset F(J),\ E' < E\}\}.$$

By definition of g, we have

$$T' = \{E \in F(J) \mid ed_E \text{ is not in the } \mathbb{F}_2\text{-linear span of } (B_o \cap eB_o) \cup \{ed_{E'} \mid E' \in F(J),\ E' < E\}\}.$$

Comparing with (2.10) we see $T' = T_2$. So we know

$$\{ed_E \bmod (B_o \cap eB_o) \mid E \in T_2\} \text{ is an } S\text{-basis of } B_o/(B_o \cap eB_o).$$

Since

$$\{d_E \mid E \in T\} = \{d_E \mid E \in T_1\} \cup \{ed_E \mid E \in T_2\}$$

it now suffices to prove the following lemma:

Lemma (2.11). Let U_1 be an S-basis of B_o, and let $U_2 \subset eB_o$ be a subset which under the natural map $f: eB_o \to eB_o/(B_o \cap eB_o)$ maps bijectively onto an S-basis of $eB_o/(B_o \cap eB_o)$. Then $U_1 \cup U_2$ is an S-basis of $B_o + eB_o$.

Proof of (2.11). It is clear that $U_1 \cup U_2$ is an $\mathbb{F}_2$-basis of $B_o + eB_o$. Applying lemma (2.5) to $f: eB_o \to eB_o/(B_o \cap eB_o)$ and $A = (B_o \cap eB_o) \cup U_2$ we find

$$((B_o \cap eB_o) \cup U_2)^* = eB_o,$$

and since

$$B_o \cap eB_o \subset B_o = U_1^*$$

it follows that

$$eB_o = ((B_o \cap eB_o) \cup U_2)^* \subset (U_1^* \cup U_2)^* = (U_1 \cup U_2)^*.$$

Also

$$B_o = U_1^* \subset (U_1 \cup U_2)^*$$

and application of (2.4) to $U = (U_1 \cup U_2)^*$ gives immediately

$$B_o + eB_c \subset (U_1 \cup U_2)^*$$

so $U_1 \cup U_2$ is an S-basis. This proves (2.11), (2.9) and (1.3).

3. S - bases and N - bases

We first prove that every S - basis is an N - basis (1.7).
Let U be an S - basis for B, let $H \subset \mathbb{Z}[B]$ be the subgroup generated by $\{[u] \mid u \in U\}$, and let $V = \{x \in B \mid [x] \subset H\}$. Clearly, $U \cup \{0\} \subset V$. Also, for $x, y \in B$ we have in $\mathbb{Z}[B]$

$$[x] + [y] = [x + y + xy] + [xy],$$

so if three of the elements x, y, xy, $x+y+xy$ belong to V, then so does the fourth one. Now the definition of U^* implies $U^* \subset V$.
But $U^* = B$, so $V = B$. From this it follows easily that $H = \mathbb{Z}[B]$, i.e. $\{[u] \mid u \in U\}$ generates $\mathbb{Z}[B]$ as an abelian group. It remains to show that $\{[u] \mid u \in U\}$ is linearly independent over $\mathbb{Z}$. Suppose we have a relation

$$\sum_{u \in U} n_u[u] = 0, \quad n_u \in \mathbb{Z}, \quad \begin{array}{l} n_u = 0 \text{ for almost all } u, \\ n_u \neq 0 \text{ for some } u. \end{array}$$

Since $\mathbb{Z}[B]$ is torsion-free, we may assume that at least one of the n_u is odd. Then

$$\sum_{u \in U} (n_u \bmod 2) . u = 0$$

is a nontrivial dependence relation of U over $\mathbb{F}_2$, contradicting that U is a basis. This proves proposition (1.7).

We next study the converses to (1.6) and (1.7).

Let B be a Boolean ring. If $\dim B \geq 2$, then there is an $x \in B$ with $x \neq 0$, $x \neq 1$, and for this x there is an isomorphism of rings

$$B \cong B/xB \times B/(1+x)B = B_1 \times B_2$$

where B_1, B_2 are nonzero Boolean rings. By induction on k it follows that if $\dim B \geq k$ $(k \in \mathbb{Z}, k \geq 0)$, then $B \cong \Pi_{i=1}^{k} B_i$ for certain nonzero Boolean rings B_i $(1 \leq i \leq k)$.
If $\dim B = k$ is finite then every B_i is one-dimensional, so $B \cong \mathbb{F}_2^k$. In this case $\mathbb{Z}[B] \cong \mathbb{Z}^k$. A subset

$$\{e_i = (e_{ij})_{j=1}^{k} \in \mathbb{F}_2^k \mid 1 \leq i \leq k\}$$

is a basis if and only if

$$(3.1) \qquad \det((e_{ij})_{1 \leq i, j \leq k}) = 1 \in \mathbb{F}_2$$

and it is an N - basis if and only if the matrix

$$M = (e'_{ij})_{1\leq i,j\leq k}, \quad e'_{ij} = 1 \in \mathbb{Z} \text{ if } e_{ij} = 1 \in \mathbb{F}_2, \quad e'_{ij} = 0 \in \mathbb{Z} \text{ if } e_{ij} = 0 \in \mathbb{F}_2,$$

(this matrix has coefficients in $\mathbb{Z}$) satisfies

$$\det(M) = \pm 1 .$$

Of course, (3.1) is equivalent to

$$\det(M) \text{ is odd.}$$

Proposition (3.2). Let B be a Boolean ring. Then every basis of B is an N-basis if and only if $\dim B \leq 3$.

Proof. "If": Let M be a $k\times k$-matrix with coefficients $0, 1$ in $\mathbb{Z}$. Applying the Hadamard determinant inequality to a suitably chosen $(k+1) \times (k+1)$-matrix with coefficients -1, $+1$ we find [cf. 2]

$$|\det(M)| \leq 2^{-k}.(k+1)^{\frac{1}{2}(k+1)} .$$

If $k\leq 3$, it follows that

$$|\det(M)| \leq 2 ,$$

so $\det(M)$ is odd if and only if $\det(M) = \pm 1$. This proves the "if"-part.

"Only if": If $\dim B \geq 4$, we may assume $B = \Pi_{j=1}^{4} B_j$, where the B_j are nonzero Boolean rings. Let U be a basis of B containing the four elements $e_1 = (1,0,0,0)$, $e_2 - (0,1,0,0)$, $e_3 = (0,0,1,0)$ and $e_4 = (0,0,0,1)$. Replacing e_i by $1 + e_i = (1,1,1,1) + e_i$ for $1 \leq i \leq 4$, we get a new basis U', which is not an N-basis since the subgroup of $\mathbb{Z}[B]$ generated by $\{[u'] \mid u' \in U'\}$ has index 3 in the subgroup generated by $\{[u] \mid u \in U\}$. This proves (3.2).

Proposition (3.3). Let B be a Boolean ring. Then every N-basis of B is an S-basis if and only if $\dim B \leq 5$.

Proof. "If": Let $B \cong \mathbb{F}_2^k$, $k\leq 5$, and let $U \subset B$ be an N-basis. We have to show that U is an S-basis. If $u,v \in U$ satisfy $uv = v$, $u \neq v$, then replacing u by $u+v$ obviously does not change the problem. Also, this replacement lowers the number of extries 1 in the matrix $(e_{ij})_{1\leq i,j\leq k}$, where $U = \{(e_{ij})_{j=1}^{k} \subset \mathbb{F}_2^k \mid 1 \leq i \leq k\}$. We conclude that we may assume

(3.4) if $u,v \in U$, $u \neq v$, then $uv \neq v$.

A direct search shows that for $k\leq 4$ the only N-basis U satisfying (3.4) is the trivial basis corresponding to the $k \times k$ identity matrix. For $k = 5$ there are three types of N-bases satisfying (3.4), given by the three matrices

$$\begin{pmatrix}1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{pmatrix}, \quad \begin{pmatrix}0&0&1&1&1\\0&1&0&0&1\\1&0&0&1&0\\1&0&1&0&0\\1&1&0&0&0\end{pmatrix}, \quad \begin{pmatrix}1&1&0&0&0\\1&0&1&1&0\\0&1&1&0&1\\0&1&0&1&1\\0&0&1&1&1\end{pmatrix}.$$

It is easily checked that each of these bases is an S-basis. This proves the "if"-part.

"Only if": First we treat the case $B = \mathbb{F}_2^6$. Then an N-basis U is given by the rows of the matrix

$$(3.5) \qquad \begin{pmatrix}1&1&1&0&0&0\\1&1&0&1&0&0\\0&1&1&1&0&0\\0&1&0&1&1&0\\0&0&1&1&0&1\\1&0&1&0&1&1\end{pmatrix}.$$

But U is not an S-basis, since $U^* = U \cup \{0\}$.
In the general case $\dim B \geq 6$ we may write $B \cong \Pi_{j=1}^{6} B_j$, where each B_j is nonzero. Let M_j be a maximal ideal of B_j $(1 \leq j \leq 6)$. Then $B_j = M_j \cup (1 + M_j)$, so M_j generates B_j as a subring of itself. Using lemma (2.9) one easily sees that B_j has an S-basis of the form $\{1\} \cup U_j$, where U_j is a basis of M_j.
Combination of these bases yields an S-basis of B of the form $U \cup \{e_i \mid 1 \leq i \leq 6\}$, where U is a basis of $M = \Pi_{j=1}^{6} M_j$ and $e_i = (e_{ij})_{j=1}^{6} \in \Pi_{j=1}^{6} B_j$, $e_{ij} = 1$ for $i = j$, $e_{ij} = 0$ for $i \neq j$ $(1 \leq i, j \leq 6)$.
Replacing $\{e_i \mid 1 \leq i \leq 6\}$ by the rows of matrix (3.5) we get an N-basis V of B which is not an S-basis since

$$V^* \subset (V + M) \cup M \subsetneq B.$$

This proves (3.3).

<u>Remark.</u> Using the notations of lemma (2.9), we put

$$T_o = \{E \in F(I) \mid [d_E] \text{ is not in the } \mathbb{Z}\text{-linear span of } \{[d_{E'}] \mid E' \in F(I),\ E' < E\}\}.$$

Clearly $T \subset T_o$. G.M. Bergman [1, theorem 1.1] proved that $\{d_E \mid E \in T_o\}$ is an N-basis of B. But by (2.9) $\{d_E \mid E \in T\}$ is an S-basis of B, and since different bases can have no inclusion relation, it follows that $T = T_o$. So the N-bases constructed by G.M. Bergman are actually S-bases.

References

1. G.M. Bergman, Boolean rings of projection maps, J. London Math. Soc. (2), 4 (1971), 593 - 598.

2. J.H.E. Cohn, On the value of determinants, Proc. Amer. Math. Soc., 14 (1963), 581 - 588.

3. G. Nöbeling, Verallgemeinerung eines Satzes von Herrn E. Specker, Inv. Math. 6 (1968), 41 - 55.

4. W. Scharlau, Quadratische Formen und Galois-Cohomologie, Inv. Math. 4 (1967), 238 - 264.