# Appendix A
# The Vector Space $B^n$

Lets to explore some properties of the set $B^n$ which was defined in **Chapter 3**. The following propositions (**Lemmas A.1** to **A.4**), which are related to Boolean operators XOR and AND, can be easily verified by considering the truth table of each operator. We list them in order to support the fact that set $B^n$ is in fact a Vector Space under the given definitions of vector addition and scalar multiplication.

**Lemma A.1:** *The set* G={0,1} *under the* AND ($\wedge$) *operand forms a monoid.* ◪

**Lemma A.2:** *The set* G={0,1} *under the* XOR ($\otimes$) *operand forms an Abelian group.* ◪

**Lemma A.3:** (G, XOR, AND) *form a ring.* ◪

**Lemma A.4:** *The ring* (G, XOR, AND) *is a field.* ◪

**Definition A.1:** *Let* **x**=$(x_1,\ldots,x_{2^n})$ *and* **y**=$(y_1,\ldots,y_{2^n})$ *be vectors in* $B^n$. *The vector addition in* $B^n$ *is defined as:*

$$\begin{array}{rccl} +: & B^n \times B^n & \rightarrow & B^n \\ & (\mathbf{x}, \mathbf{y}) & \mapsto & \mathbf{x}+\mathbf{y} \end{array}$$

*Where* $\mathbf{x} + \mathbf{y} = (x_1 \otimes y_1, \ldots, x_{2^n} \otimes y_{2^n})$

**Definition A.2:** *Let* $\mathbf{x} = (x_1,\ldots,x_{2^n})$ *a vector in* $B^n$ *and let* a $\in$ G. *The scalar multiplication in* $B^n$ *is defined as:*

$$\begin{array}{rccl} \cdot: & B^n & \rightarrow & B^n \\ & (a, \mathbf{x}) & \mapsto & a \cdot \mathbf{x} \end{array}$$

*Where* $a \cdot \mathbf{x} = a\cdot(x_1,\ldots,x_{2^n}) = (a \wedge x_1, \ldots, a \wedge x_{2^n})$

**Theorem 3.1:** *The set* $B^n$ *is a vector space over the field* (G, XOR, AND).

Proof:

Let **x**=$(x_1,\ldots,x_{2^n})$, **y**=$(y_1,\ldots,y_{2^n})$ and **z**=$(z_1,\ldots,z_{2^n})$ be vectors in $B^n$ and let a, b $\in$ G. The following properties are satisfied:

1) Closure of vector addition:

By Definition A.1, $\mathbf{x} + \mathbf{y} = (x_1 \otimes y_1, \ldots, x_{2^n} \otimes y_{2^n})$. Because $x_i, y_i \in G$, i = 1,…, $2^n \Rightarrow x_i \otimes y_i \in G$

$\therefore (\forall \mathbf{x}, \mathbf{y} \in B^n)(\mathbf{x} + \mathbf{y} \in B^n)$

2) Associativity of vector addition:

$\mathbf{x} + (\mathbf{y} + \mathbf{z}) = (x_1,\ldots,x_{2^n}) + (y_1 \otimes z_1, \ldots, y_{2^n} \otimes z_{2^n}) = (x_1 \otimes (y_1 \otimes z_1), \ldots, x_{2^n} \otimes (y_{2^n} \otimes z_{2^n}))$

$= ((x_1 \otimes y_1) \otimes z_1, \ldots, (x_{2^n} \otimes y_{2^n}) \otimes z_{2^n}) = (\mathbf{x} + \mathbf{y}) + \mathbf{z}$

$\therefore (\forall \mathbf{x}, \mathbf{y}, \mathbf{z} \in B^n)(\mathbf{x} + (\mathbf{y} + \mathbf{z}) = (\mathbf{x} + \mathbf{y}) + \mathbf{z})$

3) Existence of zero vector in vector addition:

Let $0 = (\underbrace{0,\ldots 0}_{2^n}) \in B^n \Rightarrow$

$\mathbf{x} + 0 = (x_1 \otimes 0, \ldots, x_{2^n} \otimes 0) = (x_1,\ldots,x_{2^n}) = \mathbf{x}$ and $0 + \mathbf{x} = (0 \otimes x_1, \ldots, 0 \otimes x_{2^n}) = (x_1,\ldots,x_{2^n}) = \mathbf{x}$

$\therefore (\exists 0 \in B^n)(\mathbf{x} + 0 = 0 + \mathbf{x} = \mathbf{x}, \forall \mathbf{x} \in B^n)$

4) Existence of an inverse element for each element in $B^n$ in vector addition:

Let $(-\mathbf{x}) = \mathbf{x} \Rightarrow \mathbf{x} + (-\mathbf{x}) = (x_1 \otimes x_1, \ldots, x_{2^n} \otimes x_{2^n}) = (-\mathbf{x}) + \mathbf{x} = (\underbrace{0,\ldots 0}_{2^n})$

$\therefore (\forall \mathbf{x} \in B^n)(\exists (-\mathbf{x}) \in B^n)(\mathbf{x} + (-\mathbf{x}) = (-\mathbf{x}) + \mathbf{x} = 0)$

5) Commutativity of vector addition:
$\mathbf{x} + \mathbf{y} = (x_1 \otimes y_1, ..., x_{2^n} \otimes y_{2^n}) = (y_1 \otimes x_1, ..., y_{2^n} \otimes x_{2^n}) = \mathbf{y} + \mathbf{x}$
$\therefore (\forall \mathbf{x}, \mathbf{y} \in B^n)(\mathbf{x} + \mathbf{y} = \mathbf{y} + \mathbf{x})$
6) Closure of scalar multiplication:
By Definition A.2, $a \cdot \mathbf{x} = (a \wedge x_1, ..., a \wedge x_{2^n})$ Because $x_i$, $a \in G$, $i = 1,\dots, 2^n \Rightarrow a \wedge x_i \in G$
$\therefore (\forall a \in G)(\forall \mathbf{x} \in B^n)(a \cdot \mathbf{x} \in B^n)$
7) Associativity of scalar multiplication:
$(a \wedge b) \cdot \mathbf{x} = ((a \wedge b) \wedge x_1,..., (a \wedge b) \wedge x_{2^n}) = (a\wedge(b\wedge x_1),...,a\wedge(b\wedge x_{2^n})) = a \cdot (b\wedge x_1,...,b\wedge x_{2^n})$
$= a \cdot (b \cdot (x_1,..., x_{2^n})) = a \cdot (b \cdot \mathbf{x})$
$\therefore (\forall a, b \in G)(\forall \mathbf{x} \in B^n)((a \wedge b) \cdot \mathbf{x} = a \cdot (b \cdot \mathbf{x}))$
8) Distributivity of vector sums:
$a \cdot (\mathbf{x} + \mathbf{y}) = a \cdot (x_1 \otimes y_1, ..., x_{2^n} \otimes y_{2^n}) = (a\wedge(x_1 \otimes y_1),...,a\wedge(x_{2^n} \otimes y_{2^n}))$
$= (a\wedge x_1 \otimes a\wedge y_1,...,a\wedge x_{2^n} \otimes a\wedge y_{2^n}) = a \cdot \mathbf{x} + a \cdot \mathbf{y}$
$\therefore (\forall a \in G)(\forall \mathbf{x},\mathbf{y} \in B^n)(a \cdot (\mathbf{x} + \mathbf{y}) = a \cdot \mathbf{x} + a \cdot \mathbf{y})$
9) Distributivity of scalar sums:
$(a \otimes b) \cdot \mathbf{x} = ((a \otimes b) \wedge x_1,..., (a \otimes b) \wedge x_{2^n}) = (a\wedge x_1 \otimes b\wedge x_1,...,a\wedge x_{2^n} \otimes b\wedge x_{2^n})$
$= (a\wedge x_1,...,a\wedge x_{2^n})+(b\wedge x_1,...,b\wedge x_{2^n}) = a \cdot \mathbf{x} + b \cdot \mathbf{x}$
$\therefore (\forall a,b \in G)(\forall \mathbf{x} \in B^n)((a \otimes b) \cdot \mathbf{x} = a \cdot \mathbf{x} + b \cdot \mathbf{x})$
10) Existence of the multiplicative identity element:
Let $1 \in G \Rightarrow 1 \cdot \mathbf{x} = (1\wedge x_1,..., 1\wedge x_{2^n}) = (x_1, ..., x_{2^n}) = \mathbf{x}$
$\therefore (1 \in G)(1 \cdot \mathbf{x} = \mathbf{x}, \forall \mathbf{x} \in B^n)$

$\therefore$ $B^n$ is vector space over the field $(G, \otimes, \wedge)$. ◪

**Definition A.3:** *Let* $\underline{A}^n \subset B^n$ *be the set of vectors that contains the* $2^n$ *permutations of* $(\underbrace{1,0,...0}_{2^n})$.

**Theorem 3.2:** *The set of vectors* $A^n$ *is linearly independent*.
Proof:
Let $a_i \in G$, $i = 1, ..., 2^n$. Let vector $0 \in B^n$ be described as a linear combination of the vectors in the set $A^n$:
$$a_1 \cdot (\underbrace{1,0,...0}_{2^n}) + ... + a_{2^n} \cdot (\underbrace{0,...0,1}_{2^n}) = 0 \Rightarrow (\underbrace{a_1 \wedge 1,0,...,0}_{2^n}) + ... + (\underbrace{0,...,0,a_1 \wedge 1}_{2^n}) = 0$$
$$\Rightarrow (a_1 \wedge 1,...,a_{2^n} \wedge 1) = 0 \Rightarrow \begin{cases} a_1 \wedge 1 = 0 \\ \vdots \\ a_{2^n} \wedge 1 = 0 \end{cases} \Rightarrow a_i = 0,\ i = 1, ..., 2^n.$$
$\therefore$ The set $A^n$ is linearly independent. ◪

**Theorem 3.3:** *The set* $A^n \subset B^n$ *forms a basis for* $B^n$.
Proof:
1) By Theorem 2.2 the set $A^n$ is linearly independent.
2) Let $\langle A^n \rangle = \{a_1 \cdot (\underbrace{1,0,...0}_{2^n}) + ... + a_{2^n} \cdot (\underbrace{0,...0,1}_{2^n}) : a_i \in G, i = 1, ..., 2^n\}$

If $(x_1, ..., x_{2^n}) \in \langle A^n \rangle \Rightarrow (x_1, ..., x_{2^n}) = a_1 \cdot (\underbrace{1,0,...0}_{2^n}) + ... + a_{2^n} \cdot (\underbrace{0,...0,1}_{2^n})$

$$\Rightarrow \begin{cases} x_1 = a_1 \wedge 1 = a_1 \in G \\ \vdots \\ x_{2^n} = a_{2^n} \wedge 1 = a_{2^n} \in G \end{cases} \Rightarrow \langle A^n \rangle = \{(a_1, ..., a_{2^n}) : a_i \in G, i = 1, ..., 2^n\} \Rightarrow \langle A^n \rangle = B^n$$

$\therefore$ $A^n$ forms a basis for $B^n$. ◪

For example, consider vector space $B^2$:

- $B^2 = \{(x_1, x_2, x_3, x_4): x_i \in \{0,1\}, i = 1, 2, 3, 4\} =$
  $\{(0,0,0,0), (1,0,0,0), (0,1,0,0), (1,1,0,0), (0,0,1,0), (1,0,1,0), (0,1,1,0), (1,1,1,0), (0,0,0,1), (1,0,0,1), (0,1,0,1), (1,1,0,1), (0,0,1,1), (1,0,1,1), (0,1,1,1), (1,1,1,1)\}$
- With basis $A^2 = \{(1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1)\} \subset B^2$.
- $\text{Dim}(B^2) = \text{Card}(A^2) = 4$.