N-Dimensional Binary Vector Spaces

Kenichi Arai
Tokyo University of Science
Chiba, Japan

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Summary. The binary set \{0, 1\} together with modulo-2 addition and multiplication is called a binary field, which is denoted by \(\mathbb{F}_2\). The binary field \(\mathbb{F}_2\) is defined in [1]. A vector space over \(\mathbb{F}_2\) is called a binary vector space. The set of all binary vectors of length \(n\) forms an \(n\)-dimensional vector space \(V_n\) over \(\mathbb{F}_2\). Binary fields and \(n\)-dimensional binary vector spaces play an important role in practical computer science, for example, coding theory [15] and cryptology. In cryptology, binary fields and \(n\)-dimensional binary vector spaces are very important in proving the security of cryptographic systems [13]. In this article we define the \(n\)-dimensional binary vector space \(V_n\). Moreover, we formalize some facts about the \(n\)-dimensional binary vector space \(V_n\).

MSC: 15A03 03B35

Keywords: formalization of binary vector space

MML identifier: NBVECTSP version: 8.1.01 5.13.1174

The notation and terminology used in this paper have been introduced in the following articles: [6], [1], [2], [16], [5], [7], [11], [17], [8], [9], [13], [24], [14], [4], [25], [26], [19], [23], [12], [20], [21], [22], [27], and [10].

In this paper \(m, n, s\) denote non zero elements of \(\mathbb{N}\).

Now we state the proposition:

(1) Let us consider elements \(u_1, v_1, w_1\) of Boolean\(^n\). Then \(\text{Op-XOR}((\text{Op-XOR}(u_1, v_1)), w_1) = \text{Op-XOR}(u_1, (\text{Op-XOR}(v_1, w_1)))\).

Let \(n\) be a non zero element of \(\mathbb{N}\). The functor \(\text{XOR}_B(n)\) yielding a binary operation on Boolean\(^n\) is defined by

(Def. 1) Let us consider elements \(x, y\) of Boolean\(^n\). Then \(it(x, y) = \text{Op-XOR}(x, y)\).

The functor \(\text{Zero}_B(n)\) yielding an element of Boolean\(^n\) is defined by the term

(Def. 2) \(n \mapsto 0\).

\(^1\)This research was presented during the 2013 International Conference on Foundations of Computer Science FCS’13 in Las Vegas, USA.
The functor $n$-binary additive group yielding a strict additive loop structure
is defined by the term
\[(\text{Def. 3}) \langle \text{Boolean}^n, \text{XOR}_B(n), \text{Zero}_B(n) \rangle.\]

Let us consider an element $u_1$ of $\text{Boolean}^n$. Now we state the propositions:
(2) $\text{Op-XOR}(u_1, \text{Zero}_B(n)) = u_1$.
(3) $\text{Op-XOR}(u_1, u_1) = \text{Zero}_B(n)$.

Let $n$ be a non zero element of $\mathbb{N}$. Note that $n$-binary additive group is add-
associative right zeroed right complementable Abelian and non empty and every
element of $\mathbb{Z}_2$ is Boolean.

Let $u, v$ be elements of $\mathbb{Z}_2$. We identify $u \oplus v$ with $u + v$. We identify $u \land v$
with $u \cdot v$. Let $n$ be a non zero element of $\mathbb{N}$. The functor $\text{MLT}_B(n)$ yielding a
function from (the carrier of $\mathbb{Z}_2$) into $\text{Boolean}^n$ is defined by
\[(\text{Def. 4}) \langle \text{Boolean}^n, \text{XOR}_B(n), \text{Zero}_B(n), \text{MLT}_B(n) \rangle.
\]

The functor $n$-binary vector space yielding a vector space over $\mathbb{Z}_2$ is defined
by the term
\[(\text{Def. 5}) \langle \text{Boolean}^n, \text{XOR}_B(n), \text{Zero}_B(n), \text{MLT}_B(n) \rangle.
\]

Let us note that $n$-binary vector space is finite.
Let us note that every subspace of $n$-binary vector space is finite.

Now we state the propositions:
(4) Let us consider a natural number $n$. Then $\sum n \mapsto 0_{\mathbb{Z}_2} = 0_{\mathbb{Z}_2}$.
(5) Let us consider a finite sequence $x$ of elements of $\mathbb{Z}_2$, an element $v$ of $\mathbb{Z}_2$,
and a natural number $j$. Suppose
(i) $\text{len } x = m$, and
(ii) $j \in \text{Seg } m$, and
(iii) for every natural number $i$ such that $i \in \text{Seg } m$ holds if $i = j$, then $x(i) = v$ and if $i \neq j$, then $x(i) = 0_{\mathbb{Z}_2}$.

Then $\sum x = v$. The theorem is a consequence of (4). 
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every non zero element $m$ of $\mathbb{N}$ for every finite
sequence $x$ of elements of $\mathbb{Z}_2$ for every element $v$ of $\mathbb{Z}_2$ for every natural
number $j$ such that $x_1 = m$ and $\text{len } x = m$ and $j \in \text{Seg } m$ and for every
natural number $i$ such that $i \in \text{Seg } m$ holds if $i = j$, then $x(i) = v$ and if $i \neq j$, then $x(i) = 0_{\mathbb{Z}_2}$ holds $\sum x = v$. For every natural number $k$ such that $\mathcal{P}[k]$ holds $\mathcal{P}[k + 1]$ by $[\text{[3]} (11)], \text{[5]} (59), (5), (1)]$. For every natural
number $k$, $\mathcal{P}[k]$ from $[\text{[3]} \text{ Sch. } 2]$. \hfill \Box

(6) Let us consider a (the carrier of $n$-binary vector space)-valued finite se-
quence $L$ and a natural number $j$. Suppose
(i) $\text{len } L = m$, and
(ii) $m \leq n$, and
(iii) \( j \in \text{Seg} n \).

Then there exists a finite sequence \( x \) of elements of \( \mathbb{Z}_2 \) such that

(iv) \( \text{len } x = m \), and

(v) for every natural number \( i \) such that \( i \in \text{Seg} m \) there exists an element \( K \) of \( \text{Boolean}^n \) such that \( K = L(i) \) and \( x(i) = K(j) \).

**Proof:** Define \( Q[\text{natural number, set}] \equiv \) there exists an element \( K \) of \( \text{Boolean}^n \) such that \( K = L(\$1) \) and \( \$2 = K(j) \). For every natural number \( i \) such that \( i \in \text{Seg} m \) there exists an element \( y \) of \( \text{Boolean} \) such that \( Q[i, y] \). Consider \( x \) being a finite sequence of elements of \( \text{Boolean} \) such that \( \text{dom } x = \text{Seg } m \) and for every natural number \( i \) such that \( i \in \text{Seg} m \) holds \( Q[i, x(i)] \) from [5] Sch. 5. \( \square \)

(7) Let us consider a (the carrier of \( n \)-binary vector space)-valued finite sequence \( L \), an element \( S \) of \( \text{Boolean}^n \), and a natural number \( j \). Suppose

(i) \( \text{len } L = m \), and

(ii) \( m \leq n \), and

(iii) \( S = \sum L \), and

(iv) \( j \in \text{Seg } n \).

Then there exists a finite sequence \( x \) of elements of \( \mathbb{Z}_2 \) such that

(v) \( \text{len } x = m \), and

(vi) \( S(j) = \sum x \), and

(vii) for every natural number \( i \) such that \( i \in \text{Seg} m \) there exists an element \( K \) of \( \text{Boolean}^n \) such that \( K = L(i) \) and \( x(i) = K(j) \).

The theorem is a consequence of (6). **Proof:** Consider \( x \) being a finite sequence of elements of \( \mathbb{Z}_2 \) such that \( \text{len } x = m \) and for every natural number \( i \) such that \( i \in \text{Seg} m \) there exists an element \( K \) of \( \text{Boolean}^n \) such that \( K = L(i) \) and \( x(i) = K(j) \). Consider \( f \) being a function from \( \mathbb{N} \) into \( n \)-binary vector space such that \( \sum L = f(\text{len } L) \) and \( f(0) = 0_{\text{n-binary vector space}} \) and for every natural number \( j \) and for every element \( v \) of \( n \)-binary vector space such that \( j < \text{len } L \) and \( v = L(j + 1) \) holds \( f(j + 1) = f(j) + v \). Define \( Q[\text{natural number, set}] \equiv \) there exists an element \( K \) of \( \text{Boolean}^n \) such that \( K = f(\$1) \) and \( \$2 = K(j) \). For every element \( i \) of \( \mathbb{N} \), there exists an element \( y \) of the carrier of \( \mathbb{Z}_2 \) such that \( Q[i, y] \) by [1] (3)]. Consider \( g \) being a function from \( \mathbb{N} \) into \( \mathbb{Z}_2 \) such that for every element \( i \) of \( \mathbb{N} \), \( Q[i, g(i)] \) from [3] Sch. 3]. Set \( S_j = S(j) \). \( S_j = g(\text{len } x) \cdot g(0) = 0_{\mathbb{Z}_2} \) by [1] (5)]. For every natural number \( k \) and for every element \( v_2 \) of \( \mathbb{Z}_2 \) such that \( k < \text{len } x \) and \( v_2 = x(k + 1) \) holds \( g(k + 1) = g(k) + v_2 \) by [3] (11), (13)]. \( \square \)

(8) Suppose \( m \leq n \). Then there exists a finite sequence \( A \) of elements of \( \text{Boolean}^n \) such that
(i) \( \text{len } A = m \), and
(ii) \( A \) is one-to-one, and
(iii) \( \text{rng } A = m \), and
(iv) for every natural numbers \( i, j \) such that \( i \in \text{Seg } m \) and \( j \in \text{Seg } n \) holds if \( i = j \), then \( A(i)(j) = \text{true} \) and if \( i \neq j \), then \( A(i)(j) = \text{false} \).

**Proof:** Define \( P[\text{natural number, function}] \equiv \) for every natural number \( j \) such that \( j \in \text{Seg } n \) holds if \( 1 = j \), then \( 2(j) = \text{true} \) and if \( 1 \neq j \), then \( 2(j) = \text{false} \). For every natural number \( k \) such that \( k \in \text{Seg } m \) there exists an element \( x \) of \( \text{Boolean } n \) such that \( P[k, x] \). Consider \( A \) being a finite sequence of elements of \( \text{Boolean } n \) such that \( \text{dom } A = \text{Seg } m \) and for every natural number \( k \) such that \( k \in \text{Seg } m \) holds \( P[k, A(k)] \) from [5, Sch. 5]. For every elements \( x, y \) such that \( x, y \in \text{dom } A \) and \( A(x) = A(y) \) holds \( x = y \) by [5] (5). \( \square \)

(9) Let us consider a finite sequence \( A \) of elements of \( \text{Boolean } n \), a finite subset \( B \) of \( n \)-binary vector space, a linear combination \( l \) of \( B \), and an element \( S \) of \( \text{Boolean } n \). Suppose

(i) \( \text{rng } A = B \), and
(ii) \( m \leq n \), and
(iii) \( \text{len } A = m \), and
(iv) \( S = \sum l \), and
(v) \( A \) is one-to-one, and
(vi) for every natural numbers \( i, j \) such that \( i \in \text{Seg } n \) and \( j \in \text{Seg } m \) holds if \( i = j \), then \( A(i)(j) = \text{true} \) and if \( i \neq j \), then \( A(i)(j) = \text{false} \).

Let us consider a natural number \( j \). If \( j \in \text{Seg } m \), then \( S(j) = l(A(j)) \). The theorem is a consequence of (7) and (5). **Proof:** Set \( V = n \)-binary vector space. Reconsider \( F_1 = A \) as a finite sequence of elements of \( V \). Consider \( x \) being a finite sequence of elements of \( \mathbb{Z}_2 \) such that \( \text{len } x = m \) and \( S(j) = \sum x \) and for every natural number \( i \) such that \( i \in \text{Seg } m \) there exists an element \( K \) of \( \text{Boolean } n \) such that \( K = (l \cdot F_1)(i) \) and \( x(i) = K(j) \). For every natural number \( i \) such that \( i \in \text{Seg } m \) holds if \( i = j \), then \( x(i) = l(A(j)) \) and if \( i \neq j \), then \( x(i) = 0_{\mathbb{Z}_2} \) by [5] (5), [1] (3), (5). \( \square \)

(10) Let us consider a finite sequence \( A \) of elements of \( \text{Boolean } n \) and a finite subset \( B \) of \( n \)-binary vector space. Suppose

(i) \( \text{rng } A = B \), and
(ii) \( m \leq n \), and
(iii) \( \text{len } A = m \), and
(iv) \( A \) is one-to-one, and
(v) for every natural numbers $i$, $j$ such that $i \in \text{Seg } n$ and $j \in \text{Seg } m$
holds if $i = j$, then $A(i)(j) = true$ and if $i \neq j$, then $A(i)(j) = false$.
Then $B$ is linearly independent. The theorem is a consequence of (9).
PROOF: Set $V = n$-binary vector space. For every linear combination $l$ of
$B$ such that $\sum l = 0_V$ holds the support of $l = \emptyset$ by [11] (5). □

(11) Let us consider a finite sequence $A$ of elements of $\text{Boolean}^n$, a finite subset
$B$ of $n$-binary vector space, and an element $v$ of $\text{Boolean}^n$. Suppose
(i) $\text{rng } A = B$, and
(ii) $\text{len } A = n$, and
(iii) $A$ is one-to-one.

Then there exists a linear combination $l$ of $B$ such that for every
natural number $j$ such that $j \in \text{Seg } n$ holds $v(j) = l(A(j))$. PROOF: Set
$V = n$-binary vector space. Define $Q[\text{element}, \text{element}] \equiv \text{there exists a natural number } j
\text{ such that } j \in \text{Seg } n$ and $S_1 = A(j)$ and $S_2 = v(j)$. For every element $x$ such that $x \in B$ there exists an element $y$ such that
$y \in$ the carrier of $\mathbb{Z}_2$ and $\mathcal{Q}[x, y]$ by [1] (3)]. Consider $l_1$ being a function
from $B$ into the carrier of $\mathbb{Z}_2$ such that for every element $x$ such that
$x \in B$ holds $\mathcal{Q}[x, l_1(x)]$ from [9] Sch. 1]. For every natural number $j$ such that
$j \in \text{Seg } n$ holds $l_1(A(j)) = v(j)$ by [8] (3)]. Set $f = (\text{the carrier of } V) \mapsto 0_{\mathbb{Z}_2}$. Set $l = f + l_1$. For every element $v$ of $V$ such that $v \notin B$ holds
$l(v) = 0_{\mathbb{Z}_2}$ by [17] (7)]. For every element $x$ such that $x \in$ the support
of $l$ holds $x \in B$. For every natural number $j$ such that $j \in \text{Seg } n$ holds
$v(j) = l(A(j))$ by [8] (3)]. □

(12) Let us consider a finite sequence $A$ of elements of $\text{Boolean}^n$ and a finite
subset $B$ of $n$-binary vector space. Suppose
(i) $\text{rng } A = B$, and
(ii) $\text{len } A = n$, and
(iii) $A$ is one-to-one, and
(iv) for every natural numbers $i$, $j$ such that $i, j \in \text{Seg } n$ holds if $i = j$,
then $A(i)(j) = true$ and if $i \neq j$, then $A(i)(j) = false$.

Then $\text{Lin}(B) = \langle \text{the carrier of } n$-binary vector space, the addition of $n$-bi-
mary vector space, the zero of $n$-binary vector space, the left multiplication
of $n$-binary vector space $\rangle$. The theorem is a consequence of (11) and (9).
PROOF: Set $V = n$-binary vector space. For every element $x, x \in$ the carrier
of $\text{Lin}(B)$ iff $x \in$ the carrier of $V$ by [5] (13)], [22] (7)]. □

(13) There exists a finite subset $B$ of $n$-binary vector space such that
(i) $B$ is a basis of $n$-binary vector space, and
(ii) $\overline{B} = n$, and
(iii) there exists a finite sequence $A$ of elements of $\text{Boolean}^n$ such that $\text{len} \ A = n$ and $A$ is one-to-one and $\text{rng} \ A = n$ and $\text{rng} \ A = B$ and for every natural numbers $i, j$ such that $i, j \in \text{Seg} \ n$ holds if $i = j$, then $A(i)(j) = \text{true}$ and if $i \neq j$, then $A(i)(j) = \text{false}$.

The theorem is a consequence of (8), (10), and (12).

(14) (i) $n$-binary vector space is finite dimensional, and
(ii) $\dim(\text{n-binary vector space}) = n$.

The theorem is a consequence of (13).

Let $n$ be a non zero element of $\mathbb{N}$. One can verify that $n$-binary vector space is finite dimensional.

Now we state the proposition:

(15) Let us consider a finite sequence $A$ of elements of $\text{Boolean}^n$ and a subset $C$ of $n$-binary vector space. Suppose
(i) $\text{len} \ A = n$, and
(ii) $A$ is one-to-one, and
(iii) $\text{rng} \ A = n$, and
(iv) for every natural numbers $i, j$ such that $i, j \in \text{Seg} \ n$ holds if $i = j$, then $A(i)(j) = \text{true}$ and if $i \neq j$, then $A(i)(j) = \text{false}$, and
(v) $C \subseteq \text{rng} \ A$.

Then
(vi) $\text{Lin}(C)$ is a subspace of $n$-binary vector space, and
(vii) $C$ is a basis of $\text{Lin}(C)$, and
(viii) $\dim(\text{Lin}(C)) = \text{card} \ C$.

The theorem is a consequence of (10).

REFERENCES

N-dimensional binary vector spaces


Received April 17, 2013