FORMALIZED MATHEMATICS
Vol. 21, No. 2, Pages 75–81, 2013
DOI: 10.2478/forma-2013-0008

VERSITA
degruyter.com/view/j/forma

N-Dimensional Binary Vector Spaces

Kenichi Arai[1]
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], [18], [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 $\text{XOR}_\text{B}(n)$ 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 $\text{Zero}_\text{B}(n)$ 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.

ISSN 1426–2630(Print), 1898-9934(Online)

The functor n-binary additive group yielding a strict additive loop structure is defined by the term

(Def. 3) $\langle \mathit{Boolean}^n, \mathrm{XOR}_{\mathrm{B}}(n), \mathrm{Zero}_{\mathrm{B}}(n)\rangle$.

Let us consider an element u_1 of $\mathit{Boolean}^n$. Now we state the propositions:

(2) $\text{Op-XOR}(u_1, \mathrm{Zero}_{\mathrm{B}}(n)) = u_1$.

(3) $\text{Op-XOR}(u_1, u_1) = \mathrm{Zero}_{\mathrm{B}}(n)$.

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 $\mathbf{Z}_2$ is Boolean.

Let u, v be elements of $\mathbf{Z}_2$. We identify $u \oplus v$ with $u + v$. We identify $u \wedge v$ with $u \cdot v$. Let n be a non zero element of $\mathbb{N}$. The functor $\mathrm{MLT}_{\mathrm{B}}(n)$ yielding a function from (the carrier of $\mathbf{Z}_2$) $\times$ $\mathit{Boolean}^n$ into $\mathit{Boolean}^n$ is defined by

(Def. 4) Let us consider an element a of $\mathit{Boolean}$, an element x of $\mathit{Boolean}^n$, and a set i. If $i \in \operatorname{Seg} n$, then $\mathit{it}(a, x)(i) = a \wedge x(i)$.

The functor n-binary vector space yielding a vector space over $\mathbf{Z}_2$ is defined by the term

(Def. 5) $\langle \mathit{Boolean}^n, \mathrm{XOR}_{\mathrm{B}}(n), \mathrm{Zero}_{\mathrm{B}}(n), \mathrm{MLT}_{\mathrm{B}}(n)\rangle$.

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 $\sum n \mapsto 0_{\mathbf{Z}_2} = 0_{\mathbf{Z}_2}$.

(5) Let us consider a finite sequence x of elements of $\mathbf{Z}_2$, an element v of $\mathbf{Z}_2$, and a natural number j. Suppose

(i) $\operatorname{len} x = m$, and

(ii) $j \in \operatorname{Seg} m$, and

(iii) for every natural number i such that $i \in \operatorname{Seg} m$ holds if $i = j$, then $x(i) = v$ and if $i \neq j$, then $x(i) = 0_{\mathbf{Z}_2}$.

Then $\sum x = v$. The theorem is a consequence of (4). PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every non zero element m of $\mathbb{N}$ for every finite sequence x of elements of $\mathbf{Z}_2$ for every element v of $\mathbf{Z}_2$ for every natural number j such that $\$_1 = m$ and $\operatorname{len} x = m$ and $j \in \operatorname{Seg} m$ and for every natural number i such that $i \in \operatorname{Seg} m$ holds if $i = j$, then $x(i) = v$ and if $i \neq j$, then $x(i) = 0_{\mathbf{Z}_2}$ holds $\sum x = v$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [3, (11)], [5, (59), (5), (1)]. For every natural number k, $\mathcal{P}[k]$ from [3, Sch. 2]. $\square$

(6) Let us consider a (the carrier of n-binary vector space)-valued finite sequence L and a natural number j. Suppose

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

(ii) $m \leqslant n$, and

(iii) $j \in \operatorname{Seg} n$.

Then there exists a finite sequence x of elements of $\mathbf{Z}_2$ such that

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

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

PROOF: Define $\mathcal{Q}[\text{natural number}, \text{set}] \equiv$ there exists an element K of $Boolean^n$ such that $K = L(\$_1)$ and $\$_2 = K(j)$. For every natural number i such that $i \in \operatorname{Seg} m$ there exists an element y of $Boolean$ such that $\mathcal{Q}[i, y]$. Consider x being a finite sequence of elements of $Boolean$ such that $\operatorname{dom} x = \operatorname{Seg} m$ and for every natural number i such that $i \in \operatorname{Seg} m$ holds $\mathcal{Q}[i, x(i)]$ from [5, Sch. 5]. □

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

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

(ii) $m \leqslant n$, and

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

(iv) $j \in \operatorname{Seg} n$.

Then there exists a finite sequence x of elements of $\mathbf{Z}_2$ such that

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

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

(vii) for every natural number i such that $i \in \operatorname{Seg} m$ there exists an element K of $Boolean^n$ 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 $\mathbf{Z}_2$ such that $\operatorname{len} x = m$ and for every natural number i such that $i \in \operatorname{Seg} m$ there exists an element K of $Boolean^n$ 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 $\sum L = f(\operatorname{len} L)$ and $f(0) = 0_{n\text{-binary vector space}}$ and for every natural number j and for every element v of n-binary vector space such that $j < \operatorname{len} L$ and $v = L(j+1)$ holds $f(j+1) = f(j) + v$. Define $\mathcal{Q}[\text{natural number}, \text{set}] \equiv$ there exists an element K of $Boolean^n$ 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 $\mathbf{Z}_2$ such that $\mathcal{Q}[i, y]$ by [1, (3)]. Consider g being a function from $\mathbb{N}$ into $\mathbf{Z}_2$ such that for every element i of $\mathbb{N}$, $\mathcal{Q}[i, g(i)]$ from [9, Sch. 3]. Set $S_j = S(j)$. $S_j = g(\operatorname{len} x)$. $g(0) = 0_{\mathbf{Z}_2}$ by [1, (5)]. For every natural number k and for every element v_2 of $\mathbf{Z}_2$ such that $k < \operatorname{len} x$ and $v_2 = x(k+1)$ holds $g(k+1) = g(k) + v_2$ by [3, (11), (13)]. □

(8) Suppose $m \leqslant n$. Then there exists a finite sequence A of elements of $Boolean^n$ such that

(i) $\operatorname{len} A = m$, and

(ii) A is one-to-one, and

(iii) $\overline{\overline{\operatorname{rng} A}} = m$, and

(iv) for every natural numbers i, j such that $i \in \operatorname{Seg} m$ and $j \in \operatorname{Seg} n$ holds if $i = j$, then $A(i)(j) = \mathit{true}$ and if $i \neq j$, then $A(i)(j) = \mathit{false}$.

PROOF: Define $\mathcal{P}[\text{natural number}, \text{function}] \equiv$ for every natural number j such that $j \in \operatorname{Seg} n$ holds if $\$_1 = j$, then $\$_2(j) = \mathit{true}$ and if $\$_1 \neq j$, then $\$_2(j) = \mathit{false}$. For every natural number k such that $k \in \operatorname{Seg} m$ there exists an element x of $\mathit{Boolean}^n$ such that $\mathcal{P}[k, x]$. Consider A being a finite sequence of elements of $\mathit{Boolean}^n$ such that $\operatorname{dom} A = \operatorname{Seg} m$ and for every natural number k such that $k \in \operatorname{Seg} m$ holds $\mathcal{P}[k, A(k)]$ from [5, Sch. 5]. For every elements x, y such that $x, y \in \operatorname{dom} A$ and $A(x) = A(y)$ holds $x = y$ by [5, (5)]. $\square$

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

(i) $\operatorname{rng} A = B$, and

(ii) $m \leqslant n$, and

(iii) $\operatorname{len} A = m$, and

(iv) $S = \sum l$, and

(v) A is one-to-one, and

(vi) for every natural numbers i, j such that $i \in \operatorname{Seg} n$ and $j \in \operatorname{Seg} m$ holds if $i = j$, then $A(i)(j) = \mathit{true}$ and if $i \neq j$, then $A(i)(j) = \mathit{false}$.

Let us consider a natural number j. If $j \in \operatorname{Seg} m$, 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 $\mathbf{Z}_2$ such that $\operatorname{len} x = m$ and $S(j) = \sum x$ and for every natural number i such that $i \in \operatorname{Seg} m$ there exists an element K of $\mathit{Boolean}^n$ such that $K = (l \cdot F_1)(i)$ and $x(i) = K(j)$. For every natural number i such that $i \in \operatorname{Seg} m$ holds if $i = j$, then $x(i) = l(A(j))$ and if $i \neq j$, then $x(i) = 0_{\mathbf{Z}_2}$ by [5, (5)], [1, (3), (5)]. $\square$

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

(i) $\operatorname{rng} A = B$, and

(ii) $m \leqslant n$, and

(iii) $\operatorname{len} A = m$, and

(iv) A is one-to-one, and

(v) for every natural numbers i, j such that $i \in \mathrm{Seg}\, n$ and $j \in \mathrm{Seg}\, m$ holds if $i = j$, then $A(i)(j) = \mathit{true}$ and if $i \neq j$, then $A(i)(j) = \mathit{false}$.

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 [1, (5)]. □

(11) Let us consider a finite sequence A of elements of $\mathit{Boolean}^n$, a finite subset B of n-binary vector space, and an element v of $\mathit{Boolean}^n$. Suppose

(i) $\mathrm{rng}\, A = B$, and

(ii) $\mathrm{len}\, A = n$, 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 $j \in \mathrm{Seg}\, n$ holds $v(j) = l(A(j))$. PROOF: Set $V = n$-binary vector space. Define $\mathcal{Q}[\text{element}, \text{element}] \equiv$ there exists a natural number j such that $j \in \mathrm{Seg}\, n$ and $\$_1 = A(j)$ and $\$_2 = v(j)$. For every element x such that $x \in B$ there exists an element y such that $y \in$ the carrier of $\mathbf{Z}_2$ and $\mathcal{Q}[x, y]$ by [1, (3)]. Consider l_1 being a function from B into the carrier of $\mathbf{Z}_2$ 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 $j \in \mathrm{Seg}\, n$ holds $l_1(A(j)) = v(j)$ by [8, (3)]. Set $f =$ (the carrier of $V) \longmapsto 0_{\mathbf{Z}_2}$. Set $l = f {+\cdot} l_1$. For every element v of V such that $v \notin B$ holds $l(v) = 0_{\mathbf{Z}_2}$ 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 $j \in \mathrm{Seg}\, n$ holds $v(j) = l(A(j))$ by [8, (3)]. □

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

(i) $\mathrm{rng}\, A = B$, and

(ii) $\mathrm{len}\, A = n$, and

(iii) A is one-to-one, and

(iv) for every natural numbers i, j such that i, $j \in \mathrm{Seg}\, n$ holds if $i = j$, then $A(i)(j) = \mathit{true}$ and if $i \neq j$, then $A(i)(j) = \mathit{false}$.

Then $\mathrm{Lin}(B) = \langle$the carrier of n-binary vector space, the addition of n-bi-nary 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 $\mathrm{Lin}(B)$ 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) $\overline{\overline{B}} = n$, and

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

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

(14) (i) n-binary vector space is finite dimensional, and

(ii) $\dim(n\text{-binary vector space}) = n$.

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 $Boolean^n$ and a subset C of n-binary vector space. Suppose

(i) $\operatorname{len} A = n$, and

(ii) A is one-to-one, and

(iii) $\overline{\overline{\operatorname{rng} A}} = n$, and

(iv) for every natural numbers i, j such that $i, j \in \operatorname{Seg} n$ holds if $i = j$, then $A(i)(j) = true$ and if $i \neq j$, then $A(i)(j) = false$, and

(v) $C \subseteq \operatorname{rng} A$.

Then

(vi) $\operatorname{Lin}(C)$ is a subspace of n-binary vector space, and

(vii) C is a basis of $\operatorname{Lin}(C)$, and

(viii) $\dim(\operatorname{Lin}(C)) = \overline{\overline{C}}$.

The theorem is a consequence of (10).

References

[1] Jesse Alama. The vector space of subsets of a set based on symmetric difference. *Formalized Mathematics*, 16(**1**):1–5, 2008. doi:10.2478/v10037-008-0001-7.

[2] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.

[3] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[4] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[5] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[6] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.

[7] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

[8] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.

[9] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[10] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[11] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

[12] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.

[13] X. Lai. Higher order derivatives and differential cryptoanalysis. *Communications and Cryptography*, pages 227–233, 1994.

[14] Robert Milewski. Associated matrix of linear map. *Formalized Mathematics*, 5(**3**):339–345, 1996.

[15] J.C. Moreira and P.G. Farrell. *Essentials of Error-Control Coding.* John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, 2006.

[16] Hiroyuki Okazaki and Yasunari Shidama. Formalization of the data encryption standard. *Formalized Mathematics*, 20(**2**):125–146, 2012. doi:10.2478/v10037-012-0016-y.

[17] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1 (**2**):329–334, 1990.

[18] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.

[19] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.

[20] Wojciech A. Trybulec. Subspaces and cosets of subspaces in vector space. *Formalized Mathematics*, 1(**5**):865–870, 1990.

[21] Wojciech A. Trybulec. Linear combinations in vector space. *Formalized Mathematics*, 1 (**5**):877–882, 1990.

[22] Wojciech A. Trybulec. Basis of vector space. *Formalized Mathematics*, 1(**5**):883–885, 1990.

[23] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[24] Edmund Woronowicz. Many argument relations. *Formalized Mathematics*, 1(**4**):733–737, 1990.

[25] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.

[26] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

[27] Mariusz Żynel. The Steinitz theorem and the dimension of a vector space. *Formalized Mathematics*, 5(**3**):423–428, 1996.

Received April 17, 2013