FORMALIZED MATHEMATICS
Vol. 16, No. 1, Pages 1–5, 2008
DOI: 10.2478/v10037-008-0001-7

The Vector Space of Subsets of a Set Based on Symmetric Difference

Jesse Alama
Department of Philosophy
Stanford University
USA

Summary. For each set X, the power set of X forms a vector space over the field $\mathbf{Z}_2$ (the two-element field $\{0, 1\}$ with addition and multiplication done modulo 2): vector addition is disjoint union, and scalar multiplication is defined by the two equations ($1 \cdot x := x$, $0 \cdot x := \emptyset$ for subsets x of X). See [10], Exercise 2.K, for more information.

MML identifier: `BSPACE`, version: `7.8.05 4.89.993`

The articles [8], [19], [20], [13], [21], [5], [14], [7], [6], [4], [1], [9], [2], [3], [16], [18], [11], [17], [15], and [12] provide the notation and terminology for this paper.

1. Preliminaries: Induction on Sequences of Elements of a 1-sorted Structure

Let S be a 1-sorted structure. The functor ε_S yielding a finite sequence of elements of S is defined as follows:

(Def. 1) $\varepsilon_S = \varepsilon_{(\Omega_S)}$.

In the sequel S denotes a 1-sorted structure, i denotes an element of $\mathbb{N}$, p denotes a finite sequence, and X denotes a set.

We now state two propositions:

(1) For every finite sequence p of elements of S such that $i \in \operatorname{dom} p$ holds $p(i) \in S$.

(2) If for every natural number i such that $i \in \operatorname{dom} p$ holds $p(i) \in S$, then p is a finite sequence of elements of S.

ISSN 1426–2630(p), 1898-9934(e)

The scheme *IndSeqS* deals with a 1-sorted structure $\mathcal{A}$ and a unary predicate $\mathcal{P}$, and states that:

For every finite sequence p of elements of $\mathcal{A}$ holds $\mathcal{P}[p]$

provided the parameters have the following properties:

- $\mathcal{P}[\varepsilon_{\mathcal{A}}]$, and
- For every finite sequence p of elements of $\mathcal{A}$ and for every element x of $\mathcal{A}$ such that $\mathcal{P}[p]$ holds $\mathcal{P}[p \frown \langle x \rangle]$.

2. The Two-element Field $\mathbf{Z}_2$

The field $\mathbf{Z}_2$ is defined by:

(Def. 2) $\mathbf{Z}_2 = \mathbb{Z}_2^{\mathrm{R}}$.

One can prove the following propositions:

(3) $\Omega_{\mathbf{Z}_2} = \{0, 1\}$.

(4) For every element a of $\mathbf{Z}_2$ holds $a = 0$ or $a = 1$.

(5) $0_{\mathbf{Z}_2} = 0$.

(6) $1_{\mathbf{Z}_2} = 1$.

(7) $1_{\mathbf{Z}_2} + 1_{\mathbf{Z}_2} = 0_{\mathbf{Z}_2}$.

(8) For every element x of $\mathbf{Z}_2$ holds $x = 0_{\mathbf{Z}_2}$ iff $x \neq 1_{\mathbf{Z}_2}$.

3. Set-theoretical Preliminaries

Let X, x be sets. The functor $X^{@}x$ yields an element of $\mathbf{Z}_2$ and is defined as follows:

(Def. 3) $X^{@}x = \begin{cases} 1_{\mathbf{Z}_2}, & \text{if } x \in X, \\ 0_{\mathbf{Z}_2}, & \text{otherwise.} \end{cases}$

Next we state several propositions:

(9) For all sets X, x holds $X^{@}x = 1_{\mathbf{Z}_2}$ iff $x \in X$.

(10) For all sets X, x holds $X^{@}x = 0_{\mathbf{Z}_2}$ iff $x \notin X$.

(11) For all sets X, x holds $X^{@}x \neq 0_{\mathbf{Z}_2}$ iff $X^{@}x = 1_{\mathbf{Z}_2}$.

(12) For all sets X, x, y holds $X^{@}x = X^{@}y$ iff $x \in X$ is equivalent to $y \in X$.

(13) For all sets X, Y, x holds $X^{@}x = Y^{@}x$ iff $x \in X$ is equivalent to $x \in Y$.

(14) For every set x holds $\emptyset^{@}x = 0_{\mathbf{Z}_2}$.

(15) For every set X and for all subsets u, v of X and for every element x of X holds $(u \div v)^{@}x = u^{@}x + v^{@}x$.

(16) For all sets X, Y holds $X = Y$ iff for every set x holds $X^{@}x = Y^{@}x$.

4. The Boolean Vector Space of Subsets of a Set

Let X be a set, let a be an element of $\mathbf{Z}_2$, and let c be a subset of X. The functor $a \cdot c$ yields a subset of X and is defined as follows:

(Def. 4)(i) $a \cdot c = c$ if $a = 1_{\mathbf{Z}_2}$,

(ii) $a \cdot c = \emptyset_X$ if $a = 0_{\mathbf{Z}_2}$.

Let X be a set. The functor Σ_X yields a binary operation on 2^X and is defined by:

(Def. 5) For all subsets c, d of X holds $\Sigma_X(c, d) = c \dot{-} d$.

We now state four propositions:

(17) For every element a of $\mathbf{Z}_2$ and for all subsets c, d of X holds $a \cdot (c \dot{-} d) = (a \cdot c) \dot{-} (a \cdot d)$.

(18) For all elements a, b of $\mathbf{Z}_2$ and for every subset c of X holds $(a + b) \cdot c = (a \cdot c) \dot{-} (b \cdot c)$.

(19) For every subset c of X holds $1_{\mathbf{Z}_2} \cdot c = c$.

(20) For all elements a, b of $\mathbf{Z}_2$ and for every subset c of X holds $a \cdot (b \cdot c) = a \cdot b \cdot c$.

Let X be a set. The functor $\cdot_X$ yielding a function from (the carrier of $\mathbf{Z}_2$) $\times$ 2^X into 2^X is defined by:

(Def. 6) For every element a of $\mathbf{Z}_2$ and for every subset c of X holds $\cdot_X(a, c) = a \cdot c$.

Let X be a set. The functor B_X yielding a non empty vector space structure over $\mathbf{Z}_2$ is defined as follows:

(Def. 7) $B_X = \langle 2^X, \Sigma_X, \emptyset_X, \cdot_X \rangle$.

The following propositions are true:

(21) B_X is Abelian.

(22) B_X is add-associative.

(23) B_X is right zeroed.

(24) B_X is right complementable.

(25) For every element a of $\mathbf{Z}_2$ and for all elements x, y of B_X holds $a \cdot (x + y) = a \cdot x + a \cdot y$.

(26) For all elements a, b of $\mathbf{Z}_2$ and for every element x of B_X holds $(a + b) \cdot x = a \cdot x + b \cdot x$.

(27) For all elements a, b of $\mathbf{Z}_2$ and for every element x of B_X holds $(a \cdot b) \cdot x = a \cdot (b \cdot x)$.

(28) For every element x of B_X holds $\mathbf{1}_{\mathbf{Z}_2} \cdot x = x$.

(29) B_X is vector space-like.

Let X be a set. One can verify that B_X is vector space-like, Abelian, right complementable, add-associative, and right zeroed.

5. The Linear Independence and Linear Span of Singleton Subsets

Let X be a set. We say that X is singleton if and only if:

(Def. 8) X is non empty and trivial.

One can check that every set which is singleton is also non empty and trivial and every set which is non empty and trivial is also singleton.

Let X be a set and let f be a subset of X. Let us observe that f is singleton if and only if:

(Def. 9) There exists a set x such that $x \in X$ and $f = \{x\}$.

Let X be a set. The functor S_X is defined as follows:

(Def. 10) $S_X = \{f \subseteq X\colon f \text{ is singleton}\}$.

Let X be a set. Then S_X is a subset of B_X.

Let X be a non empty set. One can check that S_X is non empty.

The following proposition is true

(30) For every non empty set X and for every subset f of X such that f is an element of S_X holds f is singleton.

Let F be a field, let V be a vector space over F, let l be a linear combination of V, and let x be an element of V. Then $l(x)$ is an element of F.

Let X be a non empty set, let s be a finite sequence of elements of B_X, and let x be an element of X. The functor $s^{@}x$ yielding a finite sequence of elements of $\mathbf{Z}_2$ is defined as follows:

(Def. 11) $\operatorname{len}(s^{@}x) = \operatorname{len} s$ and for every natural number j such that $1 \leq j \leq \operatorname{len} s$ holds $(s^{@}x)(j) = s(j)^{@}x$.

The following propositions are true:

(31) For every non empty set X and for every element x of X holds ${\varepsilon_{(B_X)}}^{@}x = \varepsilon_{(\mathbf{Z}_2)}$.

(32) For every set X and for all elements u, v of B_X and for every element x of X holds $(u + v)^{@}x = u^{@}x + v^{@}x$.

(33) Let X be a non empty set, s be a finite sequence of elements of B_X, f be an element of B_X, and x be an element of X. Then $(s \frown \langle f \rangle)^{@}x = (s^{@}x) \frown \langle f^{@}x \rangle$.

(34) Let X be a non empty set, s be a finite sequence of elements of B_X, and x be an element of X. Then $(\sum s)^{@}x = \sum s^{@}x$.

(35) Let X be a non empty set, l be a linear combination of B_X, and x be an element of B_X. If $x \in$ the support of l, then $l(x) = \mathbf{1}_{\mathbf{Z}_2}$.

(36) $S_\emptyset = \emptyset$.

(37) S_X is linearly independent.

(38) For every element f of B_X such that there exists a set x such that $x \in X$ and $f = \{x\}$ holds $f \in S_X$.

(39) For every finite set X and for every subset A of X there exists a linear combination l of S_X such that $\sum l = A$.

(40) For every finite set X holds $\mathrm{Lin}(S_X) = B_X$.

(41) For every finite set X holds S_X is a basis of B_X.

Let X be a finite set. Observe that S_X is finite.

Let X be a finite set. One can verify that B_X is finite dimensional.

Next we state three propositions:

(42) $\overline{\overline{S_X}} = \overline{\overline{X}}$.

(43) $\overline{\overline{\Omega_{B_X}}} = 2^{\overline{\overline{X}}}$.

(44) $\dim(B_\emptyset) = 0$.

References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[3] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(**3**):433–439, 1990.
[4] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[5] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[6] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[7] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[8] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[9] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[10] John L. Kelley. *General Topology*, volume 27 of *Graduate Texts in Mathematics*. Springer-Verlag, 1955.
[11] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[12] Christoph Schwarzweller. The ring of integers, euclidean rings and modulo integers. *Formalized Mathematics*, 8(**1**):29–34, 1999.
[13] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[14] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[15] Wojciech A. Trybulec. Basis of vector space. *Formalized Mathematics*, 1(**5**):883–885, 1990.
[16] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[17] Wojciech A. Trybulec. Linear combinations in vector space. *Formalized Mathematics*, 1(**5**):877–882, 1990.
[18] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[19] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[20] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[21] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received October 9, 2007