FORMALIZED MATHEMATICS
Vol. 22, No. 3, Pages 269–275, 2014
DOI: 10.2478/forma-2014-0027

DE GRUYTER OPEN
degruyter.com/view/j/forma

Difference of Function on Vector Space over $\mathbb{F}$[1]

Kenichi Arai
Tokyo University of Science
Chiba, Japan

Ken Wakabayashi
Shinshu University
Nagano, Japan

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Summary. In [11], the definitions of forward difference, backward difference, and central difference as difference operations for functions on $\mathbb{R}$ were formalized. However, the definitions of forward difference, backward difference, and central difference for functions on vector spaces over $\mathbb{F}$ have not been formalized. In cryptology, these definitions are very important in evaluating the security of cryptographic systems [3], [10]. Differential cryptanalysis [4] that undertakes a general purpose attack against block ciphers [13] can be formalized using these definitions. In this article, we formalize the definitions of forward difference, backward difference, and central difference for functions on vector spaces over $\mathbb{F}$. Moreover, we formalize some facts about these definitions.

MSC: 39A70 15A03 03B35

Keywords: Mizar formalization; difference of function on vector space over $\mathbb{F}$

MML identifier: `VSDIFF_1`, version: `8.1.03 5.25.1220`

The notation and terminology used in this paper have been introduced in the following articles: [12], [15], [5], [6], [16], [1], [2], [7], [19], [20], [17], [14], [18], [9], [21], and [8].

From now on C denotes a non empty set, G_1 denotes a field, V denotes a vector space over G_1, v, u denote elements of V, W denotes a subset of V, and f, f_1, f_2, f_3 denote partial functions from C to V.

[1]This work was supported by JSPS KAKENHI Grant Number 26730067.

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

Let us consider C, G_1, and V. Let f be a partial function from C to V and r be an element of G_1. The functor $r \cdot f$ yielding a partial function from C to V is defined by

(Def. 1) $\operatorname{dom} it = \operatorname{dom} f$ and for every element c of C such that $c \in \operatorname{dom} it$ holds $it_c = r \cdot f_c$.

Let f be a function from C into V. One can check that $r \cdot f$ is total.

Let us consider v and W. The functor $v \oplus W$ yielding a subset of V is defined by the term

(Def. 2) $\{v + u : u \in W\}$.

Let F, G be fields, V be a vector space over F, W be a vector space over G, f be a partial function from V to W, and h be an element of V. The functor $\operatorname{Shift}(f, h)$ yielding a partial function from V to W is defined by

(Def. 3) $\operatorname{dom} it = -h \oplus \operatorname{dom} f$ and for every element x of V such that $x \in -h \oplus \operatorname{dom} f$ holds $it(x) = f(x + h)$.

Now we state the proposition:

(1) Let us consider an element x of V and a subset A of V. If $A =$ the carrier of V, then $x \oplus A = A$.

PROOF: For every object y, $y \in x \oplus A$ iff $y \in A$ by [17, (29), (15), (13)]. $\square$

Let F, G be fields, V be a vector space over F, W be a vector space over G, f be a function from V into W, and h be an element of V. One can verify that the functor $\operatorname{Shift}(f, h)$ yields a function from V into W and is defined by

(Def. 4) for every element x of V, $it(x) = f(x + h)$.

Let f be a partial function from V to W. The functor $\Delta_h[f]$ yielding a partial function from V to W is defined by the term

(Def. 5) $\operatorname{Shift}(f, h) - f$.

Let f be a function from V into W. Observe that $\Delta_h[f]$ is quasi total.

Let f be a partial function from V to W. The functor $\nabla_h[f]$ yielding a partial function from V to W is defined by the term

(Def. 6) $f - \operatorname{Shift}(f, -h)$.

Let f be a function from V into W. Let us note that $\nabla_h[f]$ is quasi total.

Let f be a partial function from V to W. The functor $\delta_h[f]$ yielding a partial function from V to W is defined by the term

(Def. 7) $\operatorname{Shift}(f, (2 \cdot 1_F)^{-1} \cdot h) - \operatorname{Shift}(f, -(2 \cdot 1_F)^{-1} \cdot h)$.

Let f be a function from V into W. One can check that $\delta_h[f]$ is quasi total.

The forward difference of f and h yielding a sequence of partial functions from the carrier of V into the carrier of W is defined by

(Def. 8) $it(0) = f$ and for every natural number n, $it(n + 1) = \Delta_h[it(n)]$.

We introduce $\vec{\Delta}_h[f]$ as a synonym of the forward difference of f and h.

From now on F, G denote fields, V denotes a vector space over F, W denotes a vector space over G, f, f_1, f_2 denote functions from V into W, x, h denote elements of V, and r, r_1, r_2 denote elements of G.

Now we state the propositions:

(2) Let us consider a partial function f from V to W. If x, $x+h \in \operatorname{dom} f$, then $(\Delta_h[f])_x = f_{x+h} - f_x$.

(3) Let us consider a natural number n. Then $(\vec{\Delta}_h[f])(n)$ is a function from V into W.

Proof: Define $\mathcal{X}$[natural number] $\equiv$ $(\vec{\Delta}_h[f])(\$_1)$ is a function from V into W. For every natural number k such that $\mathcal{X}[k]$ holds $\mathcal{X}[k+1]$. For every natural number n, $\mathcal{X}[n]$ from [1, Sch. 2]. □

(4) $(\Delta_h[f])_x = f_{x+h} - f_x$. The theorem is a consequence of (2).

(5) $(\nabla_h[f])_x = f_x - f_{x-h}$.

(6) $(\delta_h[f])_x = f_{x+(2\cdot 1_F)^{-1}\cdot h} - f_{x-(2\cdot 1_F)^{-1}\cdot h}$.

From now on n, m, k denote natural numbers.

Now we state the propositions:

(7) If f is constant, then for every x, $(\vec{\Delta}_h[f])(n+1)_x = 0_W$.

Proof: For every x, $f_{x+h} - f_x = 0_W$ by [17, (15)]. For every x, $(\vec{\Delta}_h[f])(n+1)_x = 0_W$ by (3), (4), [17, (15)]. □

(8) $(\vec{\Delta}_h[r \cdot f])(n+1)_x = r \cdot (\vec{\Delta}_h[f])(n+1)_x$.

Proof: Define $\mathcal{X}$[natural number] $\equiv$ for every x, $(\vec{\Delta}_h[r \cdot f])(\$_1+1)_x = r \cdot (\vec{\Delta}_h[f])(\$_1+1)_x$. For every k such that $\mathcal{X}[k]$ holds $\mathcal{X}[k+1]$ by (3), (4), [9, (23)]. $\mathcal{X}[0]$ by (4), [9, (23)]. For every n, $\mathcal{X}[n]$ from [1, Sch. 2]. □

(9) $(\vec{\Delta}_h[f_1 + f_2])(n+1)_x = (\vec{\Delta}_h[f_1])(n+1)_x + (\vec{\Delta}_h[f_2])(n+1)_x$.

Proof: Define $\mathcal{X}$[natural number] $\equiv$ for every x, $(\vec{\Delta}_h[f_1 + f_2])(\$_1+1)_x = (\vec{\Delta}_h[f_1])(\$_1+1)_x + (\vec{\Delta}_h[f_2])(\$_1+1)_x$. For every k such that $\mathcal{X}[k]$ holds $\mathcal{X}[k+1]$ by (3), (4), [17, (27), (28)]. $\mathcal{X}[0]$ by (4), [17, (27), (28)]. For every n, $\mathcal{X}[n]$ from [1, Sch. 2]. □

(10) $(\vec{\Delta}_h[f_1 - f_2])(n+1)_x = (\vec{\Delta}_h[f_1])(n+1)_x - (\vec{\Delta}_h[f_2])(n+1)_x$.

Proof: Define $\mathcal{X}$[natural number] $\equiv$ for every x, $(\vec{\Delta}_h[f_1 - f_2])(\$_1+1)_x = (\vec{\Delta}_h[f_1])(\$_1+1)_x - (\vec{\Delta}_h[f_2])(\$_1+1)_x$. $\mathcal{X}[0]$ by (4), [17, (29), (27)]. For every k such that $\mathcal{X}[k]$ holds $\mathcal{X}[k+1]$ by (3), (4), [17, (29)]. For every n, $\mathcal{X}[n]$ from [1, Sch. 2]. □

(11) $(\vec{\Delta}_h[r_1 \cdot f_1 + r_2 \cdot f_2])(n+1)_x = r_1 \cdot (\vec{\Delta}_h[f_1])(n+1)_x + r_2 \cdot (\vec{\Delta}_h[f_2])(n+1)_x$. The theorem is a consequence of (3), (9), and (8).

(12) $(\vec{\Delta}_h[f])(1)_x = (\mathrm{Shift}(f, h))_x - f_x$. The theorem is a consequence of (4).

Let F, G be fields, V be a vector space over F, h be an element of V, W be a vector space over G, and f be a function from V into W. The backward difference of f and h yielding a sequence of partial functions from the carrier of V into the carrier of W is defined by

(Def. 9) $it(0) = f$ and for every natural number n, $it(n+1) = \nabla_h[it(n)]$.

The backward difference of f and h yielding a sequence of partial functions from the carrier of V into the carrier of W is defined by

(Def. 10) $it(0) = f$ and for every natural number n, $it(n+1) = \nabla_h[it(n)]$.

We introduce $\vec{\nabla}_h[f]$ as a synonym of the backward difference of f and h.

Now we state the propositions:

(13) Let us consider a natural number n. Then $(\vec{\nabla}_h[f])(n)$ is a function from V into W.

PROOF: Define $\mathcal{X}[\text{natural number}] \equiv (\vec{\nabla}_h[f])(\$_1)$ is a function from V into W. For every natural number k such that $\mathcal{X}[k]$ holds $\mathcal{X}[k+1]$. For every natural number n, $\mathcal{X}[n]$ from [1, Sch. 2]. □

(14) If f is constant, then for every x, $(\vec{\nabla}_h[f])(n+1)_x = 0_W$.

PROOF: For every x, $f_x - f_{x-h} = 0_W$ by [17, (15)]. For every x, $(\vec{\nabla}_h[f])(n+1)_x = 0_W$ by (13), (5), [17, (15)]. □

(15) $(\vec{\nabla}_h[r \cdot f])(n+1)_x = r \cdot (\vec{\nabla}_h[f])(n+1)_x$.

PROOF: Define $\mathcal{X}[\text{natural number}] \equiv$ for every x, $(\vec{\nabla}_h[r \cdot f])(\$_1+1)_x = r \cdot (\vec{\nabla}_h[f])(\$_1+1)_x$. For every k such that $\mathcal{X}[k]$ holds $\mathcal{X}[k+1]$ by (13), (5), [9, (23)]. $\mathcal{X}[0]$ by (5), [9, (23)]. For every n, $\mathcal{X}[n]$ from [1, Sch. 2]. □

(16) $(\vec{\nabla}_h[f_1+f_2])(n+1)_x = (\vec{\nabla}_h[f_1])(n+1)_x + (\vec{\nabla}_h[f_2])(n+1)_x$.

PROOF: Define $\mathcal{X}[\text{natural number}] \equiv$ for every x, $(\vec{\nabla}_h[f_1+f_2])(\$_1+1)_x = (\vec{\nabla}_h[f_1])(\$_1+1)_x + (\vec{\nabla}_h[f_2])(\$_1+1)_x$. For every k such that $\mathcal{X}[k]$ holds $\mathcal{X}[k+1]$ by (13), (5), [17, (27), (28)]. $\mathcal{X}[0]$ by (5), [17, (27), (28)]. For every n, $\mathcal{X}[n]$ from [1, Sch. 2]. □

(17) $(\vec{\nabla}_h[f_1-f_2])(n+1)_x = (\vec{\nabla}_h[f_1])(n+1)_x - (\vec{\nabla}_h[f_2])(n+1)_x$.

PROOF: Define $\mathcal{X}[\text{natural number}] \equiv$ for every x, $(\vec{\nabla}_h[f_1-f_2])(\$_1+1)_x = (\vec{\nabla}_h[f_1])(\$_1+1)_x - (\vec{\nabla}_h[f_2])(\$_1+1)_x$. $\mathcal{X}[0]$ by (5), [17, (29), (27)]. For every k such that $\mathcal{X}[k]$ holds $\mathcal{X}[k+1]$ by (13), (5), [17, (29), (27)]. For every n, $\mathcal{X}[n]$ from [1, Sch. 2]. □

(18) $(\vec{\nabla}_h[r_1 \cdot f_1 + r_2 \cdot f_2])(n+1)_x = r_1 \cdot (\vec{\nabla}_h[f_1])(n+1)_x + r_2 \cdot (\vec{\nabla}_h[f_2])(n+1)_x$. The theorem is a consequence of (16) and (15).

(19) $(\vec{\nabla}_h[f])(1)_x = f_x - (\mathrm{Shift}(f, -h))_x$. The theorem is a consequence of (5).

Let F, G be fields, V be a vector space over F, h be an element of V, W be a vector space over G, and f be a partial function from V to W. The central difference of f and h yielding a sequence of partial functions from the carrier of V into the carrier of W is defined by

(Def. 11) $it(0) = f$ and for every natural number n, $it(n+1) = \delta_h[it(n)]$.

We introduce $\vec{\delta}_h[f]$ as a synonym of the central difference of f and h.

Now we state the propositions:

(20) Let us consider a natural number n. Then $(\vec{\delta}_h[f])(n)$ is a function from V into W.
PROOF: Define $\mathcal{X}$[natural number] $\equiv (\vec{\delta}_h[f])(\$_1)$ is a function from V into W. For every natural number k such that $\mathcal{X}[k]$ holds $\mathcal{X}[k+1]$. For every natural number n, $\mathcal{X}[n]$ from [1, Sch. 2]. □

(21) If f is constant, then for every x, $(\vec{\delta}_h[f])(n+1)_x = 0_W$.
PROOF: Define $\mathcal{X}$[natural number] $\equiv$ for every x, $(\vec{\delta}_h[f])(\$_1+1)_x = 0_W$. For every x, $f_{x+(2\cdot 1_F)^{-1}\cdot h} - f_{x-(2\cdot 1_F)^{-1}\cdot h} = 0_W$ by [17, (15)]. $\mathcal{X}[0]$. For every k such that $\mathcal{X}[k]$ holds $\mathcal{X}[k+1]$ by (20), (6), [17, (13)]. For every n, $\mathcal{X}[n]$ from [1, Sch. 2]. □

(22) $(\vec{\delta}_h[r\cdot f])(n+1)_x = r\cdot(\vec{\delta}_h[f])(n+1)_x$.
PROOF: Define $\mathcal{X}$[natural number] $\equiv$ for every x, $(\vec{\delta}_h[r\cdot f])(\$_1+1)_x = r\cdot(\vec{\delta}_h[f])(\$_1+1)_x$. For every k such that $\mathcal{X}[k]$ holds $\mathcal{X}[k+1]$ by (20), (6), [9, (23)]. $\mathcal{X}[0]$ by (6), [9, (23)]. For every n, $\mathcal{X}[n]$ from [1, Sch. 2]. □

(23) $(\vec{\delta}_h[f_1+f_2])(n+1)_x = (\vec{\delta}_h[f_1])(n+1)_x + (\vec{\delta}_h[f_2])(n+1)_x$.
PROOF: Define $\mathcal{X}$[natural number] $\equiv$ for every x, $(\vec{\delta}_h[f_1+f_2])(\$_1+1)_x = (\vec{\delta}_h[f_1])(\$_1+1)_x+(\vec{\delta}_h[f_2])(\$_1+1)_x$. For every k such that $\mathcal{X}[k]$ holds $\mathcal{X}[k+1]$ by (20), (6), [17, (27), (28)]. $\mathcal{X}[0]$ by (6), [17, (27), (28)]. For every n, $\mathcal{X}[n]$ from [1, Sch. 2]. □

(24) $(\vec{\delta}_h[f_1-f_2])(n+1)_x = (\vec{\delta}_h[f_1])(n+1)_x - (\vec{\delta}_h[f_2])(n+1)_x$.
PROOF: Define $\mathcal{X}$[natural number] $\equiv$ for every x, $(\vec{\delta}_h[f_1-f_2])(\$_1+1)_x = (\vec{\delta}_h[f_1])(\$_1+1)_x - (\vec{\delta}_h[f_2])(\$_1+1)_x$. $\mathcal{X}[0]$ by (6), [17, (29), (27), (28)]. For every k such that $\mathcal{X}[k]$ holds $\mathcal{X}[k+1]$ by (20), (6), [17, (29), (27), (28)]. For every n, $\mathcal{X}[n]$ from [1, Sch. 2]. □

(25) $(\vec{\delta}_h[r_1\cdot f_1+r_2\cdot f_2])(n+1)_x = r_1\cdot(\vec{\delta}_h[f_1])(n+1)_x + r_2\cdot(\vec{\delta}_h[f_2])(n+1)_x$. The theorem is a consequence of (23) and (22).

(26) $(\vec{\delta}_h[f])(1)_x = (\mathrm{Shift}(f,(2\cdot 1_F)^{-1}\cdot h))_x - (\mathrm{Shift}(f,-(2\cdot 1_F)^{-1}\cdot h))_x$. The theorem is a consequence of (6).

(27) $(\vec{\Delta}_h[f])(n)_x = (\vec{\nabla}_h[f])(n)_{x+n\cdot h}$.
PROOF: Define $\mathcal{X}$[natural number] $\equiv$ for every x, $(\vec{\Delta}_h[f])(\$_1)_x = (\vec{\nabla}_h[f])(\$_1)_{x+\$_1\cdot h}$. For every k such that $\mathcal{X}[k]$ holds $\mathcal{X}[k+1]$ by (3), [15, (13), (15)], [17, (4), (15), (28)]. $\mathcal{X}[0]$ by [17, (4)], [15, (12)]. For every n, $\mathcal{X}[n]$ from [1, Sch. 2]. □

Let us assume that $1_F \neq -1_F$. Now we state the propositions:

(28) $(\vec{\Delta}_h[f])(2 \cdot n)_x = (\vec{\delta}_h[f])(2 \cdot n)_{x+n \cdot h}$.

PROOF: Define $\mathcal{X}$[natural number] $\equiv$ for every x, $(\vec{\Delta}_h[f])(2 \cdot \$_1)_x = (\vec{\delta}_h[f])(2 \cdot \$_1)_{x+\$_1 \cdot h}$. For every k such that $\mathcal{X}[k]$ holds $\mathcal{X}[k+1]$ by [15, (13), (15)], [17, (27), (28), (15)]. $\mathcal{X}[0]$ by [17, (4)], [15, (12)]. For every n, $\mathcal{X}[n]$ from [1, Sch. 2]. □

(29) $(\vec{\Delta}_h[f])(2 \cdot n+1)_x = (\vec{\delta}_h[f])(2 \cdot n+1)_{x+n \cdot h+(2 \cdot 1_F)^{-1} \cdot h}$.

PROOF: $2 \cdot 1_F \neq 0_F$ by [15, (13), (15)]. $(\vec{\delta}_h[f])(2 \cdot n)$ is a function from V into W. $(\vec{\Delta}_h[f])(2 \cdot n)$ is a function from V into W. □

ACKNOWLEDGEMENT: We sincerely thank Professor Yasunari Shidama for his helpful advices.

REFERENCES

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

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

[3] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Lecture Notes in Computer Science*, 537:2–21, 1991.

[4] E. Biham and A. Shamir. Differential cryptanalysis of the full 16-round DES. *Lecture Notes in Computer Science*, 740:487–496, 1993.

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

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

[11] Bo Li, Yan Zhang, and Xiquan Liang. Difference and difference quotient. *Formalized Mathematics*, 14(**3**):115–119, 2006. doi:10.2478/v10037-006-0014-z.

[12] Michał Muzalewski and Wojciech Skaba. From loops to Abelian multiplicative groups with zero. *Formalized Mathematics*, 1(**5**):833–840, 1990.

[13] 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.

[14] Beata Perkowska. Functional sequence from a domain to a domain. *Formalized Mathematics*, 3(**1**):17–21, 1992.

[15] Christoph Schwarzweller. The binomial theorem for algebraic structures. *Formalized Mathematics*, 9(**3**):559–564, 2001.

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

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

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

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

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

[21] Hiroshi Yamazaki and Yasunari Shidama. Algebra of vector functions. *Formalized Mathematics*, 3(**2**):171–175, 1992.

Received September 26, 2014