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 $V$.

\footnote{1This work was supported by JSPS KAKENHI 26730067.}
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) \[ \text{dom } it = \text{dom } f \text{ and for every element } c \text{ of } C \text{ such that } c \in \text{dom } it \text{ holds } it_c = r \cdot f_c. \]

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) \[ \text{dom } it = -h \oplus \text{dom } f \text{ and for every element } x \text{ of } V \text{ such that } x \in -h \oplus \text{dom } f \text{ holds } it(x) = f(x + h). \]

Now we state the proposition:

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

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

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 $\Delta_h[f]$ 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 $x, x+h \in \text{dom } f$, then $(\Delta_h[f])_x = f_{x+h} - f_x$.

(3) Let us consider a natural number $n$. Then $(\Delta_h[f])(n)$ is a function from $V$ into $W$.

\textbf{Proof:} Define $X[\text{natural number}] \equiv (\Delta_h[f])_{(1)}$ is a function from $V$ into $W$. For every natural number $k$ such that $X[k]$ holds $X[k+1]$ for every natural number $n$, $X[n]$ 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) $(\delta_h[f])_x = f_{x+(2.1f)^{-1}h} - f_{x-(2.1f)^{-1}h}$.

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

Now we state the propositions:

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

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

(8) $(\Delta_h[r \cdot f])(n+1)_x = r \cdot (\Delta_h[f])(n+1)_x$.

\textbf{Proof:} Define $X[\text{natural number}] \equiv$ for every $x$, $(\Delta_h[r \cdot f])_{(1)} = r \cdot (\Delta_h[f])_{(1)}$. For every $k$ such that $X[k]$ holds $X[k+1]$ by (3), (4), [9] (23). $X[0]$ by (4), [9] (23). For every $n, X[n]$ from [11 Sch. 2]. □

(9) $(\Delta_h[f_1 + f_2])(n+1)_x = (\Delta_h[f_1])(n+1)_x + (\Delta_h[f_2])(n+1)_x$.

\textbf{Proof:} Define $X[\text{natural number}] \equiv$ for every $x$, $(\Delta_h[f_1 + f_2])_{(1)} = (\Delta_h[f_1])_{(1)} + (\Delta_h[f_2])_{(1)}$. For every $k$ such that $X[k]$ holds $X[k+1]$ by (3), (4), [17] (27), (28). $X[0]$ by (4), [17] (27), (28). For every $n, X[n]$ from [11 Sch. 2]. □

(10) $(\Delta_h[f_1 - f_2])(n+1)_x = (\Delta_h[f_1])(n+1)_x - (\Delta_h[f_2])(n+1)_x$.

\textbf{Proof:} Define $X[\text{natural number}] \equiv$ for every $x$, $(\Delta_h[f_1 - f_2])_{(1)} = (\Delta_h[f_1])_{(1)} - (\Delta_h[f_2])_{(1)}$. $X[0]$ by (4), [17] (29), (27). For every $k$ such that $X[k]$ holds $X[k+1]$ by (3), (4), [17] (29). For every $n, X[n]$ from [11 Sch. 2]. □

(11) $(\Delta_h[r_1 \cdot f_1 + r_2 \cdot f_2])(n+1)_x = r_1 \cdot (\Delta_h[f_1])(n+1)_x + r_2 \cdot (\Delta_h[f_2])(n+1)_x$.

The theorem is a consequence of (3), (9), and (8).

(12) $(\Delta_h[f])(1)_x = (\text{Shift}(f,h))_x - f_x$. 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) \[ i_t(0) = f \text{ and for every natural number } n, \ i_t(n + 1) = \nabla_h[i_t(n)]. \]

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) \[ i_t(0) = f \text{ and for every natural number } n, \ i_t(n + 1) = \nabla_h[i_t(n)]. \]

We introduce $\nabla_h[f]$ 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 $(\nabla_h[f])(n)$ is a function from $V$ into $W$.

**Proof:** Define $x'[\text{natural number}] \equiv (\nabla_h[f])(n)$ is a function from $V$ into $W$. For every natural number $n$, $x'[n]$ holds $x'[n + 1]$. For every natural number $n$, $x'[n]$ from [1] Sch. 2.

(14) If $f$ is constant, then for every $x$, $(\nabla_h[f])(n + 1)_x = 0_w$.

**Proof:** For every $x$, $f_x - f_{x-h} = 0_w$ by [17] (15). For every $x$, $(\nabla_h[f])(n + 1)_x = 0_w$ by (13), (5), [17] (15).

(15) $(\nabla_h[r \cdot f])(n + 1)_x = r \cdot (\nabla_h[f])(n + 1)_x$.

**Proof:** Define $x'[\text{natural number}] \equiv$ for every $x$, $(\nabla_h[r \cdot f])(n + 1)_x = r \cdot (\nabla_h[f])(n + 1)_x$. For every $k$ such that $x'[k]$ holds $x'[k + 1]$ by (13), (5), [9] (23). $x'[0]$ by (5), [9] (23). For every $n$, $x'[n]$ from [1] Sch. 2.

(16) $(\nabla_h[f_1 + f_2])(n + 1)_x = (\nabla_h[f_1])(n + 1)_x + (\nabla_h[f_2])(n + 1)_x$.

**Proof:** Define $x'[\text{natural number}] \equiv$ for every $x$, $(\nabla_h[f_1 + f_2])(n + 1)_x = (\nabla_h[f_1])(n + 1)_x + (\nabla_h[f_2])(n + 1)_x$. For every $k$ such that $x'[k]$ holds $x'[k + 1]$ by (13), (5), [17] (27), (28). $x'[0]$ by (5), [17] (27), (28). For every $n$, $x'[n]$ from [1] Sch. 2.

(17) $(\nabla_h[f_1 - f_2])(n + 1)_x = (\nabla_h[f_1])(n + 1)_x - (\nabla_h[f_2])(n + 1)_x$.

**Proof:** Define $x'[\text{natural number}] \equiv$ for every $x$, $(\nabla_h[f_1 - f_2])(n + 1)_x = (\nabla_h[f_1])(n + 1)_x - (\nabla_h[f_2])(n + 1)_x$. $x'[0]$ by (5), [17] (29), (27). For every $k$ such that $x'[k]$ holds $x'[k + 1]$ by (13), (5), [17] (29), (27). For every $n$, $x'[n]$ from [1] Sch. 2.

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

(19) $(\nabla_h[f])(n + 1)_x = f_x - (\text{Shift}(f, -h))_x$. 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) \[ i_t(0) = f \text{ and for every natural number } n, \ i_t(n + 1) = \delta_h[i_t(n)]. \]
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 $X[$natural number$] \equiv (\vec{\delta}_h[f])(\$1)$ is a function from $V$ into $W$. For every natural number $k$ such that $X[k]$ holds $X[k+1]$. For every natural number $n$, $X[n]$ from \[1\] Sch. 2. □

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

Proof: Define $X[$natural number$] \equiv$ for every $x$, $(\vec{\delta}_h[f])(\$1+1)x = 0_W$. For every $x$, $f_{x+(2\cdot1_F)^{-1}h} - f_{x-(2\cdot1_F)^{-1}h} = 0_W$ by \[17\] (15). $X[0]$. For every $k$ such that $X[k]$ holds $X[k+1]$ by (20), (6), \[17\] (13). For every $n$, $X[n]$ 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 $X[$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 $X[k]$ holds $X[k+1]$ by (20), (6), \[9\] (23). $X[0]$ by (6), \[9\] (23). For every $n$, $X[n]$ 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 $X[$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 $X[k]$ holds $X[k+1]$ by (20), (6), \[17\] (27), (28), $X[0]$ by (6), \[17\] (27), (28). For every $n$, $X[n]$ 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 $X[$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 $X[k]$ holds $X[k+1]$ by (20), (6), \[17\] (29), (27), (28). For every $n$, $X[n]$ 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) $(\vec{\delta}_h[f])(1)x = (\text{Shift}(f, (2 \cdot 1_F)^{-1} \cdot h))x - (\text{Shift}(f, -(2 \cdot 1_F)^{-1} \cdot h))x$. 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 $X[$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 $X[k]$ holds $X[k+1]$ by (3), \[15\] (13), (15), \[17\] (4), (15), (28), $X[0]$ by \[17\] (4), \[15\] (12). For every $n$, $X[n]$ 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 $X[$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 $X[k]$ holds $X[k+1]$ by \[15\] (13), (15),
For every $n$, $X[n]$ from [17, (27), (28), (15)]. For every $n$, $X[n]$ from [17, (4), (12)]. For every $n$, $X[n]$ from [1, Sch. 2]. □

\[(\Delta_h[f])(2 \cdot n + 1) = (\delta_h[f])(2 \cdot n + 1)_{x + n \cdot h + (2 \cdot 1_F)^{-1} \cdot h}.
\]

**Proof:** $2 \cdot 1_F \neq 0_F$ by [15, (13), (15)]. $(\delta_h[f])(2 \cdot n)$ is a function from $V$ into $W$. $(\Delta_h[f])(2 \cdot n)$ is a function from $V$ into $W$. □

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

**References**


Received September 26, 2014
DIFFERENCE OF FUNCTION ...