

# Formalization of Integral Linear Space<sup>1</sup>

Yuichi Futa  
Shinshu University  
Nagano, Japan

Hiroyuki Okazaki  
Shinshu University  
Nagano, Japan

Yasunari Shidama  
Shinshu University  
Nagano, Japan

**Summary.** In this article, we formalize integral linear spaces, that is a linear space with integer coefficients. Integral linear spaces are necessary for lattice problems, LLL (Lenstra-Lenstra-Lovász) base reduction algorithm that outputs short lattice base and cryptographic systems with lattice [8].

MML identifier: RLVECT\_X, version: 7.11.07 4.156.1112

The notation and terminology used here have been introduced in the following papers: [1], [10], [3], [9], [11], [2], [4], [6], [16], [14], [13], [12], [5], [7], [15], and [17].

## 1. PRELIMINARIES

The following propositions are true:

- (1) Let  $X$  be a real linear space and  $R_1, R_2$  be finite sequences of elements of  $X$ . If  $\text{len } R_1 = \text{len } R_2$ , then  $\sum(R_1 + R_2) = \sum R_1 + \sum R_2$ .
- (2) Let  $X$  be a real linear space and  $R_1, R_2, R_3$  be finite sequences of elements of  $X$ . If  $\text{len } R_1 = \text{len } R_2$  and  $R_3 = R_1 - R_2$ , then  $\sum R_3 = \sum R_1 - \sum R_2$ .
- (3) Let  $X$  be a real linear space,  $R_1, R_2$  be finite sequences of elements of  $X$ , and  $a$  be an element of  $\mathbb{R}$ . If  $R_2 = a R_1$ , then  $\sum R_2 = a \cdot \sum R_1$ .

---

<sup>1</sup>This work was supported by JSPS KAKENHI 22300285.

## 2. INTEGRAL LINEAR SPACE

For simplicity, we use the following convention:  $x$  denotes a set,  $a$  denotes a real number,  $i$  denotes an integer,  $V$  denotes a real linear space,  $v, v_1, v_2, v_3, u, w, w_1, w_2, w_3$  denote vectors of  $V$ ,  $A, B$  denote subsets of  $V$ ,  $L$  denotes a linear combination of  $V$ , and  $l, l_1, l_2$  denote linear combinations of  $A$ .

Let us consider  $V, i, L$ . The functor  $i \cdot L$  yielding a linear combination of  $V$  is defined as follows:

(Def. 1) For every  $v$  holds  $(i \cdot L)(v) = i \cdot L(v)$ .

Let us consider  $V, A$ . The functor  $\text{Lin}_{\mathbb{Z}} A$  yielding a subset of  $V$  is defined by:

(Def. 2)  $\text{Lin}_{\mathbb{Z}} A = \{\sum l : \text{rng } l \subseteq \mathbb{Z}\}$ .

One can prove the following propositions:

- (4)  $(i) \cdot l = i \cdot l$ .
- (5) If  $\text{rng } l_1 \subseteq \mathbb{Z}$  and  $\text{rng } l_2 \subseteq \mathbb{Z}$ , then  $\text{rng}(l_1 + l_2) \subseteq \mathbb{Z}$ .
- (6) If  $\text{rng } l \subseteq \mathbb{Z}$ , then  $\text{rng}(i \cdot l) \subseteq \mathbb{Z}$ .
- (7)  $\text{rng}(\mathbf{0}_{\text{LC}_V}) \subseteq \mathbb{Z}$ .
- (8)  $\text{Lin}_{\mathbb{Z}} A \subseteq$  the carrier of  $\text{Lin}(A)$ .
- (9) If  $v, u \in \text{Lin}_{\mathbb{Z}} A$ , then  $v + u \in \text{Lin}_{\mathbb{Z}} A$ .
- (10) If  $v \in \text{Lin}_{\mathbb{Z}} A$ , then  $i \cdot v \in \text{Lin}_{\mathbb{Z}} A$ .
- (11)  $0_V \in \text{Lin}_{\mathbb{Z}} A$ .
- (12) If  $x \in A$ , then  $x \in \text{Lin}_{\mathbb{Z}} A$ .
- (13) If  $A \subseteq B$ , then  $\text{Lin}_{\mathbb{Z}} A \subseteq \text{Lin}_{\mathbb{Z}} B$ .
- (14)  $\text{Lin}_{\mathbb{Z}}(A \cup B) = (\text{Lin}_{\mathbb{Z}} A) + \text{Lin}_{\mathbb{Z}} B$ .
- (15)  $\text{Lin}_{\mathbb{Z}}(A \cap B) \subseteq (\text{Lin}_{\mathbb{Z}} A) \cap \text{Lin}_{\mathbb{Z}} B$ .
- (16)  $x \in \text{Lin}_{\mathbb{Z}}\{v\}$  iff there exists an integer  $a$  such that  $x = a \cdot v$ .
- (17)  $v \in \text{Lin}_{\mathbb{Z}}\{v\}$ .
- (18)  $x \in v + \text{Lin}_{\mathbb{Z}}\{w\}$  iff there exists an integer  $a$  such that  $x = v + a \cdot w$ .
- (19)  $x \in \text{Lin}_{\mathbb{Z}}\{w_1, w_2\}$  iff there exist integers  $a, b$  such that  $x = a \cdot w_1 + b \cdot w_2$ .
- (20)  $w_1 \in \text{Lin}_{\mathbb{Z}}\{w_1, w_2\}$ .
- (21)  $x \in v + \text{Lin}_{\mathbb{Z}}\{w_1, w_2\}$  iff there exist integers  $a, b$  such that  $x = v + a \cdot w_1 + b \cdot w_2$ .
- (22)  $x \in \text{Lin}_{\mathbb{Z}}\{v_1, v_2, v_3\}$  iff there exist integers  $a, b, c$  such that  $x = a \cdot v_1 + b \cdot v_2 + c \cdot v_3$ .
- (23)  $w_1, w_2, w_3 \in \text{Lin}_{\mathbb{Z}}\{w_1, w_2, w_3\}$ .
- (24)  $x \in v + \text{Lin}_{\mathbb{Z}}\{w_1, w_2, w_3\}$  iff there exist integers  $a, b, c$  such that  $x = v + a \cdot w_1 + b \cdot w_2 + c \cdot w_3$ .

- (25) Let  $x$  be a set. Then  $x \in \text{Lin}_{\mathbb{Z}} A$  if and only if there exist finite sequences  $g_1, h_1$  of elements of  $V$  and there exists an integer-valued finite sequence  $a_1$  such that  $x = \sum h_1$  and  $\text{rng } g_1 \subseteq A$  and  $\text{len } g_1 = \text{len } h_1$  and  $\text{len } g_1 = \text{len } a_1$  and for every natural number  $i$  such that  $i \in \text{Seg len } g_1$  holds  $(h_1)_i = a_1(i) \cdot (g_1)_i$ .

Let  $R_4$  be a real linear space and let  $f$  be a finite sequence of elements of  $R_4$ . The functor  $\text{Lin}_{\mathbb{Z}} f$  yielding a subset of  $R_4$  is defined by the condition (Def. 3).

- (Def. 3)  $\text{Lin}_{\mathbb{Z}} f = \{ \sum g; g \text{ ranges over len } f\text{-element finite sequences of elements of } R_4; \bigvee a: \text{ len } f\text{-element integer-valued finite sequence } \bigwedge i: \text{ natural number } (i \in \text{Seg len } f \Rightarrow g_i = a(i) \cdot f_i) \}$ .

One can prove the following propositions:

- (26) Let  $R_4$  be a real linear space,  $f$  be a finite sequence of elements of  $R_4$ , and  $x$  be a set. Then  $x \in \text{Lin}_{\mathbb{Z}} f$  if and only if there exists a len  $f$ -element finite sequence  $g$  of elements of  $R_4$  and there exists a len  $f$ -element integer-valued finite sequence  $a$  such that  $x = \sum g$  and for every natural number  $i$  such that  $i \in \text{Seg len } f$  holds  $g_i = a(i) \cdot f_i$ .
- (27) Let  $R_4$  be a real linear space,  $f$  be a finite sequence of elements of  $R_4$ ,  $x, y$  be elements of  $R_4$ , and  $a, b$  be elements of  $\mathbb{Z}$ . If  $x, y \in \text{Lin}_{\mathbb{Z}} f$ , then  $a \cdot x + b \cdot y \in \text{Lin}_{\mathbb{Z}} f$ .
- (28) For every real linear space  $R_4$  and for every finite sequence  $f$  of elements of  $R_4$  such that  $f = \text{Seg len } f \mapsto 0_{(R_4)}$  holds  $\sum f = 0_{(R_4)}$ .
- (29) Let  $R_4$  be a real linear space,  $f$  be a finite sequence of elements of  $R_4$ ,  $v$  be an element of  $R_4$ , and  $i$  be a natural number. If  $i \in \text{Seg len } f$  and  $f = (\text{Seg len } f \mapsto 0_{(R_4)}) + (\{i\} \mapsto v)$ , then  $\sum f = v$ .
- (30) Let  $R_4$  be a real linear space,  $f$  be a finite sequence of elements of  $R_4$ , and  $i$  be a natural number. If  $i \in \text{Seg len } f$ , then  $f_i \in \text{Lin}_{\mathbb{Z}} f$ .
- (31) For every real linear space  $R_4$  and for every finite sequence  $f$  of elements of  $R_4$  holds  $\text{rng } f \subseteq \text{Lin}_{\mathbb{Z}} f$ .
- (32) Let  $R_4$  be a real linear space,  $f$  be a non empty finite sequence of elements of  $R_4$ ,  $g, h$  be finite sequences of elements of  $R_4$ , and  $s$  be an integer-valued finite sequence. Suppose  $\text{rng } g \subseteq \text{Lin}_{\mathbb{Z}} f$  and  $\text{len } g = \text{len } s$  and  $\text{len } g = \text{len } h$  and for every natural number  $i$  such that  $i \in \text{Seg len } g$  holds  $h_i = s(i) \cdot g_i$ . Then  $\sum h \in \text{Lin}_{\mathbb{Z}} f$ .
- (33) For every real linear space  $R_4$  and for every non empty finite sequence  $f$  of elements of  $R_4$  holds  $\text{Lin}_{\mathbb{Z}} \text{rng } f = \text{Lin}_{\mathbb{Z}} f$ .
- (34)  $\text{Lin}(\text{Lin}_{\mathbb{Z}} A) = \text{Lin}(A)$ .
- (35) Let  $x$  be a set,  $g_1, h_1$  be finite sequences of elements of  $V$ , and  $a_1$  be an integer-valued finite sequence. Suppose  $x = \sum h_1$  and  $\text{rng } g_1 \subseteq \text{Lin}_{\mathbb{Z}} A$  and  $\text{len } g_1 = \text{len } h_1$  and  $\text{len } g_1 = \text{len } a_1$  and for every natural number  $i$  such that  $i \in \text{Seg len } g_1$  holds  $(h_1)_i = a_1(i) \cdot (g_1)_i$ . Then  $x \in \text{Lin}_{\mathbb{Z}} A$ .

- (36)  $\text{Lin}_{\mathbb{Z}} \text{Lin}_{\mathbb{Z}} A = \text{Lin}_{\mathbb{Z}} A$ .  
 (37) If  $\text{Lin}_{\mathbb{Z}} A = \text{Lin}_{\mathbb{Z}} B$ , then  $\text{Lin}(A) = \text{Lin}(B)$ .

## REFERENCES

- [1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(2):377–382, 1990.  
 [2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(1):41–46, 1990.  
 [3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(1):107–114, 1990.  
 [4] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(2):357–367, 1990.  
 [5] Noboru Endou, Takashi Mitsuishi, and Yasunari Shidama. Dimension of real unitary space. *Formalized Mathematics*, 11(1):23–28, 2003.  
 [6] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(1):35–40, 1990.  
 [7] Jarosław Kotowicz. Real sequences and basic operations on them. *Formalized Mathematics*, 1(2):269–272, 1990.  
 [8] Daniele Micciancio and Shafi Goldwasser. Complexity of lattice problems: A cryptographic perspective (the international series in engineering and computer science). 2002.  
 [9] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(2):329–334, 1990.  
 [10] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(1):115–122, 1990.  
 [11] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(3):501–505, 1990.  
 [12] Wojciech A. Trybulec. Basis of real linear space. *Formalized Mathematics*, 1(5):847–850, 1990.  
 [13] Wojciech A. Trybulec. Linear combinations in real linear space. *Formalized Mathematics*, 1(3):581–588, 1990.  
 [14] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(2):291–296, 1990.  
 [15] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(1):67–71, 1990.  
 [16] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(1):181–186, 1990.  
 [17] Hiroshi Yamazaki and Yasunari Shidama. Algebra of vector functions. *Formalized Mathematics*, 3(2):171–175, 1992.

Received August 17, 2010

---