J. Math. Soc. Japan
Vol. 58, No. 1, 2006

Hodge cycles on abelian varieties associated to the complete binary trees

By Fumio Hazama

(Received Jul. 21, 2004)
(Revised Jan. 31, 2005)

Abstract. The structure of the ring of Hodge cycles on a certain family of abelian varieties of CM-type is investigated. This leads to an interesting combinatorial problem related to posets based on complete p-ary trees. A complete solution to the problem is given for the case $p = 2$.

1. Introduction.

In [**3**] we investigated the structure of the Hodge rings of abelian varieties of CM-type where the corresponding CM-fields are *cyclic* extensions of $\boldsymbol{Q}$ of degree $2pq$ with p, q distinct odd primes. Through our efforts to generalize the results obtained there to the cases of arbitrary abelian CM-fields of non-squarefree degree, we come across the fact that there is an essential combinatorial difficulty already for the cases of prime-power degree. More precisely, we come to realize that we should understand as fully as possible the cases of CM-fields of degree $2p^n$, $n \geq 2$, with p an arbitrary prime, such that their Galois group are isomorphic to $\boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/p^n\boldsymbol{Z}$. (The corresponding abelian varieties will be called *of p-power type* for simplicity.) We, however, have found that unexpectedly our theory on the kernels of lowering operators for ranked posets developed in [**2**] helps us greatly to understand the structure of Hodge rings of those abelian varieties. The main purpose of the present paper is to describe how the theory gives us a proper perspective for the study, and to apply it to a complete classification of degenerate CM-types for the cases of abelian varieties of 2-power type. (The more general p-power cases will be treated separately in the forthcoming paper.) Our result enables one to understand a true mechanism which lies behind mysterious phenomena observed in some examples in [**4**, (3.12)] of degenerate abelian varieties of 2-power type (see *Example* in the last section). Furthermore as an application of our classification, we show that for any $n \geq 3$, the minimum of ranks of Hodge groups among those for simple 2^n-dimensional abelian varieties of 2-power type is equal to $2^{n-1} + 2$. As is the case in [**2**], [**3**], our problem can be formulated in purely combinatorial terms, and the first four sections are devoted to the study of the *raised kernels* of lowering operators for a certain family of posets. More precisely, let p be an arbitrary prime number and let $P(p) = \coprod_{0 \leq i < \infty} P(p)^{(i)}$ denote the ranked poset based on the complete p-ary tree. Let $\boldsymbol{V}^{(i)} = \left\{ \sum_{a \in P(p)^{(i)}} n_a[a]; n_a \in \boldsymbol{Z} \right\}$ be the free $\boldsymbol{Z}$-module generated by $P(p)^{(i)}$, and for any $i > j$, let $L_{i,j} : \boldsymbol{V}^{(i)} \to \boldsymbol{V}^{(j)}$ (resp. $R_{j,i} : \boldsymbol{V}^{(j)} \to \boldsymbol{V}^{(i)}$) be the lowering (resp. raising)

2000 *Mathematics Subject Classification.* 14C30, 11G10, 06A11.
Key Words and Phrases. Hodge cycle, abelian variety, binary tree.

operator defined by $L_{i,j}([a]) = \sum_{b\in P(p)^{(j)}, b\le a}[b]$ (resp. $R_{j,i}([c]) = \sum_{b\in P(p)^{(i)}, b\ge c}[b]$). For any subset $I \subset [0,n]$, let $\boldsymbol{K}_I^{(n)} = \sum_{i\in I} R_{i,n}(\mathrm{Ker}(L_{i,i-1})) \subset \boldsymbol{V}^{(n)}$ and call it the *raised kernel*. The problems we have in mind are the following:

(a) What kinds of sign-vectors are there in $\boldsymbol{K}_I^{(n)}$?
(b) What kinds of (0,1)-vectors are there in $\boldsymbol{K}_I^{(n)}$?

(Here an element $\sum n_a[a]$ is said to be sign-vector (resp. (0,1)-vector) if $n_a \in \{\pm 1\}$ (resp. $n_a \in \{0,1\}$) for any a). We give a complete solution to these problems when $p = 2$ by providing

(A) an algorithm to construct all sign-vectors (resp. (0,1)-vectors) in $\boldsymbol{K}_I^{(n)}$,
(B) an algorithm which computes a generating function for the numbers of sign-vectors (resp. (0,1)-vectors) in $\boldsymbol{K}_I^{(n)}$.

These results translate into the ones for Hodge cycles as

(A′) an algorithm to construct all *degenerate* CM-types for the CM-fields K with $\mathrm{Gal}(K/\boldsymbol{Q}) \cong \boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/2^n\boldsymbol{Z}$,
(B′) an algorithm to enumerate all Hodge cycles on the corresponding abelian varieties.

These number-theoretical results are explained in the last section.

The plan of this paper is as follows. Section two reviews and extends a part of the theory of lowering operators for ranked posets developed in [**2**]. In Section three we introduce a ranked poset $P(p)$ for any prime number p and investigate the structure of the kernels of the lowering operators. In Section four we focus our attention to the poset $P(2)$, and investigate various subsets related to the raised kernels of lowering operators. Here we come across an interesting family of Laurent polynomials which emerge as counting functions of certain combinatorial objects. (See Examples 4.11, 4.12 for concrete examples.) In Section five, we translate the combinatorial results into those for Hodge cycles on abelian varieties of 2-power type.

The author would like to thank the referee for his/her useful comments.

2. Ranked poset and related operators.

In this section we review and extend a part of the theory developed in [**2**], and fix some notation.

Let $P = \coprod_{0\le i<\infty} P^{(i)}$ be an arbitrary ranked poset (=partially ordered set) with $P^{(i)}$ the set of elements of rank i. When convenient, we add the minimum element 0 to P, and endow it with level $-1 : P^{(-1)} = \{0\}$. We assume that each $P^{(i)}$ is a *finite* set. For any $i \ge 0$, let

$$\boldsymbol{V}^{(i)} = \bigoplus_{a\in P^{(i)}} \boldsymbol{Z}[a]$$

be the free $\boldsymbol{Z}$-module with basis $[a], a \in P^{(i)}$. For any pair i, j of nonnegative integers with $i \ge j$, let

$$L_{i,j} : \boldsymbol{V}^{(i)} \to \boldsymbol{V}^{(j)}$$

be the $\boldsymbol{Z}$-linear map defined by

$$L_{i,j}([a]) = \sum_{\substack{b \in P^{(j)} \\ b \leq a}} [b] \in \boldsymbol{V}^{(j)},$$

and let $L_{0,-1} = 0 : \boldsymbol{V}^{(0)} \to \{0\}$. We call $L_{i,i-1}$ *the lowering operator at level* i. Similarly we define

$$R_{j,i} : \boldsymbol{V}^{(j)} \to \boldsymbol{V}^{(i)}, \quad 0 \leq j \leq i$$

by

$$R_{j,i}([a]) = \sum_{\substack{b \in P^{(i)} \\ a \leq b}} [b] \in \boldsymbol{V}^{(i)},$$

and call $R_{i,i+1}$ *the raising operator at level* i. A ranked poset $P = \coprod_{0 \leq i < \infty} P^{(i)}$ is said to be *regular* if for any $a \in P^{(i)}$, both numbers $\#\{b \in P^{(i-1)}; b \leq a\}$ and $\#\{c \in P^{(i+1)}; c \geq a\}$ depend only on i. For a regular ranked poset, we set

$$\ell_i = \ell_i(P) = \#\{b \in P^{(i-1)}; b \leq a\},$$
$$r_i = r_i(P) = \#\{c \in P^{(i+1)}; c \geq a\}.$$

For any $i \geq 0$ we introduce a natural nondegenerate inner product $\langle , \rangle$ on $\boldsymbol{V}^{(i)}$ by $\big\langle \sum_{a \in P^{(i)}} n_a[a], \sum_{a \in P^{(i)}} m_a[a] \big\rangle = \sum_{a \in P^{(i)}} n_a m_a \in \boldsymbol{Z}$. For any $\boldsymbol{Z}$-submodule M of $\boldsymbol{V}^{(i)}$, we denote the orthogonal compliment of M by $M^{\perp}$. The following proposition can be easily checked.

PROPOSITION 2.1. *For a regular ranked poset, we have*

$$\big\langle L_{i+1,i} R_{i,i+1}[a], [a] \big\rangle = r_i, \text{ for any } a \in P^{(i)}, \ i \geq 0,$$
$$\big\langle R_{i-1,i} L_{i,i-1}[a], [a] \big\rangle = \ell_i, \text{ for any } a \in P^{(i)}, \ i \geq 1.$$

The lowering and raising operators are dual to each other in the following sense.

PROPOSITION 2.2. *For any* $i \geq 1$, $\boldsymbol{v} \in \boldsymbol{V}^{(i)}$, $\boldsymbol{w} \in \boldsymbol{V}^{(i-1)}$, *we have*

$$\big\langle L_{i,i-1} \boldsymbol{v}, \boldsymbol{w} \big\rangle = \big\langle \boldsymbol{v}, R_{i-1,i} \boldsymbol{w} \big\rangle.$$

PROOF OF PROPOSITION 2.2. By linearity, it suffices to show this when $\boldsymbol{v} = [a] \in \boldsymbol{V}^{(i)}$, $\boldsymbol{w} = [b] \in \boldsymbol{V}^{(i-1)}$ with $a \in P^{(i)}$, $b \in P^{(i-1)}$. The left hand side is equal to

$$\left\langle L_{i,i-1}[a],[b]\right\rangle = \left\langle \sum_{\substack{c\in P^{(i-1)}\\ c\le a}} [c],[b]\right\rangle = \begin{cases} 1, & \text{if } b\le a,\\ 0, & \text{otherwise.}\end{cases}$$

On the other hand the right hand side is equal to

$$\left\langle [a], R_{i-1,i}[b]\right\rangle = \left\langle [a], \sum_{\substack{d\in P^{(i)}\\ b\le d}} [d]\right\rangle = \begin{cases} 1, & \text{if } b\le a,\\ 0, & \text{otherwise.}\end{cases}$$

Hence they are the same and the proposition is proved. □

We introduce several objects of our main concern. For any $i \ge 0$, let

$$\mathbf{Sign}^{(i)} = \left\{ \sum_{a\in P^{(i)}} n_a[a] \in \boldsymbol{V}^{(i)}; n_a \in \{\pm 1\} \text{ for any } a\right\} \subset \boldsymbol{V}^{(i)}.$$

The elements of $\mathbf{Sign}^{(i)}$ are called *sign-vectors at level i*. Similarly let

$$\mathbf{Bit}^{(i)} = \left\{ \sum_{a\in P^{(i)}} n_a[a] \in \boldsymbol{V}^{(i)}; n_a \in \{0,1\}\right\}.$$

The elements of $\mathbf{Bit}^{(i)}$ are called (0,1)-*vectors at level i*. Let

$$\mathbf{K}^{(i)} = \mathrm{Ker}(L_{i,i-1}) \subset \boldsymbol{V}^{(i)},$$
$$\mathbf{S}^{(i)} = (\mathbf{K}^{(i)})^{\perp} \cap \mathbf{Sign}^{(i)}.$$

Furthermore for any subset $I \subset [0,n]$, let

$$\mathbf{K}_I^{(n)} = \bigoplus_{i\in I} R_{i,n}(\mathbf{K}^{(i)}) \subset \boldsymbol{V}^{(n)},$$
$$\mathbf{S}_I^{(n)} = \mathbf{Sign}^{(n)} \cap \left(\mathbf{K}_I^{(n)}\right)^{\perp} \subset \boldsymbol{V}^{(n)},$$
$$\mathbf{E}_I^{(n)} = \left\{v \in \mathbf{Bit}^{(i)} \cap \left(\mathbf{K}_I^{(n)}\right)^{\perp}; v \text{ is indecomposable}\right\}\text{-}\{\mathbf{0}\}.$$

(Here an element $v \in \mathbf{Bit}^{(i)} \cap (\mathbf{K}_I^{(n)})^{\perp}$ is said to be *indecomposable* if it cannot be written as $v = v_1 + v_2, v_1, v_2 \in \mathbf{Bit}^{(i)} \cap (\mathbf{K}_I^{(n)})^{\perp}\text{-}\{\mathbf{0}\}$.) By the definition, we have $\mathbf{S}_I^{(n)} = \bigcap_{i\in I} \mathbf{S}_{\{i\}}^{(n)}$, $\mathbf{E}_I^{(n)} = \bigcap_{i\in I} \mathbf{E}_{\{i\}}^{(n)}$. Our main objective is to determine the structures of these three subsets $\mathbf{K}_I^{(n)}, \mathbf{S}_I^{(n)}, \mathbf{E}_I^{(n)} \subset \boldsymbol{V}^{(n)}$ as explicitly as possible, when the poset P is based on the complete p-ary tree with p an arbitrary prime number.

3. Ranked poset $P(p)$ and the kernel of lowering operators.

In this section we introduce a ranked poset $P(p)$, and investigate the kernels of lowering operators.

3.A. Definition of $P(p)$.

For any prime number p, let $P(p)^{(i)} = \boldsymbol{Z}/p^i\boldsymbol{Z}, i \geq 0$, and $P(p) = \coprod_{0\leq i<\infty} P(p)^{(i)}$. A partial order on it is defined by the rule that

$$\begin{aligned} &a \geq b \text{ if and only if} \\ &a \in P(p)^{(i)},\ b \in P(p)^{(j)},\ \text{with } i \geq j \text{ and } a(\mathrm{mod}\, p^j) = b. \end{aligned}$$

Thus the poset $P(p)$ is based on the complete p-ary tree with root $P(p)^{(0)} = \{0\}$. This poset is regular since

$$\begin{aligned} \ell_i &= \ell_i(P(p)) = \#\{b \in P^{(i-1)}; b \leq a\} = 1, \quad i \geq 1, \\ r_i &= r_i(P(p)) = \#\{c \in P^{(i+1)}; c \geq a\} = p, \quad i \geq 0. \end{aligned}$$

In particular, we have an important formula

$$L_{i+1,i}R_{i,i+1} = p.\mathrm{id}_{\boldsymbol{V}^{(i)}} \text{ holds for any } i \geq 0.$$

From now on we use the symbols $\boldsymbol{V}^{(i)}, \mathbf{K}^{(i)}, \ldots$, introduced in the previous section, as those for the poset $P(p)$.

3.B. Structure of the kernel $\mathbf{K}^{(i)}$.

For any $\boldsymbol{Z}$-algebra R, we identify a R-valued function $f : \boldsymbol{Z}/p^i\boldsymbol{Z} \to R$ with the element $\sum_{a\in P(p)^{(i)}} f(a)[a] \in (\boldsymbol{V}^{(i)})_R = \boldsymbol{V}^{(i)} \otimes_{\boldsymbol{Z}} R$, and denote the latter by f too. In this sense a character $\chi \in \mathrm{Hom}(\boldsymbol{Z}/p^i\boldsymbol{Z}, \boldsymbol{C}^*)$ is regarded as an element of $(\boldsymbol{V}^{(i)})_{\boldsymbol{C}}$. The following proposition says a little more.

Proposition 3.1. *For any $i \geq 0$, every character $\chi \in \mathrm{Hom}(\boldsymbol{Z}/p^i\boldsymbol{Z}, \boldsymbol{C}^*)$ of conductor p^i belongs to $(\mathbf{K}^{(i)})_{\boldsymbol{C}}$. Moreover they constitute a $\boldsymbol{C}$-basis of $(\mathbf{K}^{(i)})_{\boldsymbol{C}}$.*

Proof of Proposition 3.1. Since both assertions are obvious when $i = 0$ (recall that the lowering operator $L_{0,-1}$ is defined to be the zero map), we assume $i > 0$. For the first assertion, it suffices to show, by the nondegeneracy of the inner product, that $\langle L_{i,i-1}\chi, [b]\rangle = 0$ holds for any $b \in P^{(i-1)}$. By Proposition 2.2 we know that $\langle L_{i,i-1}\chi, [b]\rangle = \langle \chi, R_{i-1,i}[b]\rangle$, and this is, by definition, equal to

$$\begin{aligned} \big\langle \chi, R_{i-1,i}[b]\big\rangle &= \sum_{\substack{a\in P(p)^{(i)} \\ a\geq b}} \chi(a) = \sum_{\substack{a\in P(p)^{(i)} \\ a(\mathrm{mod}\, p^{i-1})=b}} \chi(a) \\ &= (\text{const.}) \cdot \sum_{0\leq j\leq p-1} \zeta_p^j \quad (\text{since the conductor of } \chi \text{ is assumed to be } p^i) \\ &= 0. \end{aligned}$$

For the second assertion, note that $L_{i,i-1} : \boldsymbol{V}^{(i)} \to \boldsymbol{V}^{(i-1)}$, $i \geq 1$, are surjective. Hence the dimension of the $\boldsymbol{C}$-vector space $(\mathbf{K}^{(i)})_{\boldsymbol{C}}$ is equal to $\#(P_i) - \#(P_{i-1}) = p^i - p^{i-1}$, which is equal to the number the characters of conductor p^i. Hence they constitute a basis of $(\mathbf{K}^{(i)})_{\boldsymbol{C}}$. This completes the proof of Proposition 3.1. □

As a corollary, we have the following.

COROLLARY 3.1.1. *$\boldsymbol{V}^{(i)} = \bigoplus_{0\leq j\leq i} R_{j,i}(\mathbf{K}^{(j)})$, where the summands are mutually orthogonal. In particular, for any subset $I \subset [0,i]$, we have*

$$\left(K_I^{(i)}\right)^{\perp} = K_{[0,i]-I}^{(i)}.$$

If we extend the scalar to $\boldsymbol{C}$, then each summand $R_{j,i}((\mathbf{K}^{(j)})_{\boldsymbol{C}})$ has a $\boldsymbol{C}$-basis

$$\{\chi \in \mathrm{Hom}(\boldsymbol{Z}/p^i\boldsymbol{Z}, \boldsymbol{C}^*);\ \chi \text{ is of conductor } p^j\}.$$

Next we construct a $\boldsymbol{Z}$-basis of $\mathbf{K}^{(i)}$.

PROPOSITION 3.2. *For each pair (s,t) of integers with $0 \leq s \leq p^{i-1}-1$, $1 \leq t \leq p-1$, let*

$$\boldsymbol{v}_{(s,t)}^{(i)} = [s] - [s + tp^{i-1}] \in \boldsymbol{V}^{(i)}.$$

Then $\{\boldsymbol{v}_{(s,t)}^{(i)}; 0 \leq s \leq p^{i-1}-1,\ 1 \leq t \leq p-1\}$ constitute a $\boldsymbol{Z}$-basis of $\mathbf{K}^{(i)}$.

PROOF OF PROPOSITION 3.2. It follows from the very definition of the lowering operator $L_{i,i-1}$ that every $\boldsymbol{v}_{(s,t)}^{(i)}$ belongs to the kernel $\mathbf{K}^{(i)}$. Moreover, since each of elements $[a]$ with $p^{i-1} \leq a \leq p^i - 1$ appears as a summand of $\boldsymbol{v}_{(s,t)}^{(i)}; 0 \leq s \leq p^{i-1}-1$, $1 \leq t \leq p-1$ once and only once. Hence the latter elements are linearly independent. This completes the proof of Proposition 3.2. □

Combining this proposition with Corollary 3.1.1 we obtain the following.

PROPOSITION 3.3.

$$\boldsymbol{V}^{(i)} = \bigoplus_{1\leq j\leq i} \left\langle R_{ji}\left(\boldsymbol{v}_{(s,t)}^{(j)}\right); 0 \leq s \leq p^{j-1}-1, 1 \leq t \leq p-1\right\rangle_{\boldsymbol{Z}} \oplus \boldsymbol{Z}.R_{0,i}([0])$$

(*orthogonal direct sum*).

3.C. Structures of $(\mathbf{K}^{(i)})^{\perp}$ and $\mathbf{S}^{(i)}$.

The following proposition shows that there is a simple $\boldsymbol{Z}$-basis of $(\mathbf{K}^{(i)})^{\perp}$.

PROPOSITION 3.4. *Let $\boldsymbol{w}_u = R_{i-1,i}([u])$ for each $u \in P^{(i-1)}$. Then $\{\boldsymbol{w}_u; u \in P^{(i-1)}\}$ constitute a $\boldsymbol{Z}$-basis of $(\mathbf{K}^{(i)})^{\perp}$. In particular, $\boldsymbol{w} = \sum_{a\in P^{(i)}} n_a[a] \in (\mathbf{K}^{(i)})^{\perp}$ if and only if the coefficients n_a for $a \geq b \in P^{(i-1)}$ depend only on b.*

PROOF OF PROPOSITION 3.4. Let $\boldsymbol{v} \in \mathbf{K}^{(i)}$. Then by duality we have

$$\langle \boldsymbol{v}, \boldsymbol{w}_u \rangle = \langle \boldsymbol{v}, R_{i-1,i}([u]) \rangle = \langle L_{i,i-1}\boldsymbol{v}, [u] \rangle = 0.$$

Moreover the elements $\boldsymbol{w}_u$, $u \in P^{(i-1)}$ are obviously linearly independent, and the number of these is equal to $\#(P^{(i-1)}) = p^{i-1}$, which is the right rank of the complement $(\mathbf{K}^{(i)})^{\perp}$. This completes the proof of Proposition 3.4. □

Now we can investigate the sets $\mathbf{S}^{(i)} = (\mathbf{K}^{(i)})^{\perp} \cap \mathbf{Sign}^{(i)}$, $i \geq 0$. The following proposition is a direct consequence of Proposition 3.4.

PROPOSITION 3.5. *For any $b \in P^{(i-1)}$, let $\boldsymbol{e}_b = R_{i-1,i}([b]) \in \boldsymbol{V}^{(i)}$. Then*

$$\mathbf{S}^{(i)} = \left\{ \sum_{b \in P^{(i-1)}} \varepsilon_b \boldsymbol{e}_b ; \varepsilon_b \in \{\pm 1\} \right\}.$$

Every element of $\mathbf{S}^{(i)}$ is invariant under the natural action of $p^{i-1}\boldsymbol{Z}/p^i\boldsymbol{Z} \cong \boldsymbol{Z}/p\boldsymbol{Z}$ on $P^{(i)} = \boldsymbol{Z}/p^i\boldsymbol{Z}$. In particular, the number of its elements is $\#(\mathbf{S}^{(i)}) = 2^{p^{i-1}}$.

4. Orthogonal complements: The case of $P(2)$.

In this section, we focus our attention solely to the poset $P(2)$, and investigate the structure of $\mathbf{S}_I^{(n)}$ and $\mathbf{E}_I^{(n)}$ for this poset.

4.A. Structure of $\mathbf{S}_I^{(n)}$.

It follows from Proposition 3.2 for $p = 2$ that the kernel $\mathbf{K}_{\{i\}}^{(i)} = \mathbf{K}^{(i)}$ is spanned by $\boldsymbol{v}_{(s,1)}^{(i)} = [s] - [s + 2^{i-1}]$, $0 \leq s \leq 2^{i-1} - 1$. We write $\boldsymbol{v}_s^{(i)} = \boldsymbol{v}_{(s,1)}^{(i)}$ for simplicity. We introduce two operators E_{even} and E_{odd} which will play a fundamental role. Let $E_{even} : P(2) \to P(2)$ denote the map defined by $a(\mathrm{mod}\, 2^i) \mapsto 2a(\mathrm{mod}\, 2^{i+1})$ for any $a \in P(2)^{(i)}$. Similarly let $E_{odd} : P(2) \to P(2)$ be the map defined by $a(\mathrm{mod}\, 2^i) \mapsto 2a + 1(\mathrm{mod}\, 2^{i+1})$. Note that both maps are injective and order-preserving. They raise the level of every element by one. Furthermore we have a disjoint sum decomposition

$$P(2) = P(2)^{(0)} \coprod E_{even}(P(2)) \coprod E_{odd}(P(2))$$

and accordingly

$$\boldsymbol{V}^{(i)} = E_{even}(\boldsymbol{V}^{(i-1)}) \oplus E_{odd}(\boldsymbol{V}^{(i-1)}), \quad i \geq 1. \tag{4.1}$$

Note here that $\mathrm{Supp}(E_{even}(\boldsymbol{V}^{(i-1)})) \cap \mathrm{Supp}(E_{odd}(\boldsymbol{V}^{(i-1)})) = \varnothing$, where we define $\mathrm{Supp}\big(\sum_{a \in P(2)^{(i)}} n_a[a]\big) = \{a \in P(2)^{(i)}; n_a \neq 0\} \subset P(2)^{(i)}$. Hence the right hand side of (4.1) is actually an orthogonal direct sum with respect to $\langle , \rangle$. The inner products on both sides are related by the formula

$$\big\langle E_{even}(w_1) + E_{odd}(w_1'),\ E_{even}(w_2) + E_{odd}(w_2') \big\rangle_{\boldsymbol{V}^{(i)}} = \langle w_1, w_2 \rangle_{\boldsymbol{V}^{(i-1)}} + \langle w_1', w_2' \rangle_{\boldsymbol{V}^{(i-1)}}$$

for any $w_1, w_2, w_1', w_2' \in \boldsymbol{V}^{(i-1)}$. Furthermore one can check that the natural commutativity relations

$$E_{even} \circ R_{i-1,n-1} = R_{i,n} \circ E_{even}, \quad E_{odd} \circ R_{i-1,n-1} = R_{i,n} \circ E_{odd} \tag{4.2}$$

$$E_{even} \circ L_{n-1,i-1} = L_{n,i} \circ E_{even}, \quad E_{odd} \circ L_{n-1,i-1} = L_{n,i} \circ E_{odd} \tag{4.3}$$

hold. By using these formulas, one can check easily the validity of the following simple criterion for an element of $\boldsymbol{V}^{(n)}$ to belong to $\big(\mathbf{K}^{(n)}_{\{i\}}\big)^{\perp}$.

PROPOSITION 4.1. *Let $i \in [2,n]$. Then an element $v \in \boldsymbol{V}^{(n)}$ belongs to $\big(\mathbf{K}^{(n)}_{\{i\}}\big)^{\perp}$ if and only if v is expressed as*:

$$v = E_{even}(w) + E_{odd}(w'), \quad w, \quad w' \in \big(\mathbf{K}^{(n-1)}_{\{i-1\}}\big)^{\perp}. \tag{4.4}$$

Since $\mathbf{S}^{(n)}_I = \bigcap_{i\in I} \mathbf{S}^{(n)}_{\{i\}}$, Proposition 4.1 implies the following.

PROPOSITION 4.2. *Suppose that $I \subset [2,n]$. Then*

$$\mathbf{S}^{(n)}_I = E_{even}\big(\mathbf{S}^{(n-1)}_{I-1}\big) + E_{odd}\big(\mathbf{S}^{(n-1)}_{I-1}\big),$$

where $I-1 = \{i-1; i \in I\} \subset [1,n-1]$.

When $I \cap \{0,1\} \neq \varnothing$, we need a little more care. First we deal with the case $I \cap \{0,1\} = \{1\}$. For any $v = \sum_{a\in P^{(n)}} v_a[a] \in \boldsymbol{V}^{(n)}$, let

$$w(v) = \sum_{a\in P^{(n)}} v_a \in \boldsymbol{Z},$$

and call it the *weight* of v. Note that if $s \in \mathbf{Sign}^{(n)}$, then $-2^n \le w(s) \le 2^n$ and $w(s)$ is always even. For any subset $T \subset \boldsymbol{V}^{(n)}$ and an integer w, we let

$$T(w) = \{s \in T; w(s) = w\}.$$

PROPOSITION 4.3. *Suppose that $I \cap \{0,1\} = \{1\}$. Then*

$$\mathbf{S}^{(n)}_I = \coprod_{-2^{n-1}\le w\le 2^{n-1}} \Big(E_{even}\big(\mathbf{S}^{(n-1)}_{I-\{1\}-1}(w)\big) + E_{odd}\big(\mathbf{S}^{(n-1)}_{I-\{1\}-1}(w)\big)\Big).$$

In particular, when $I = \{1\}$ and $n \ge 2$, we have

$$\mathbf{S}^{(n)}_{\{1\}} = \coprod_{-2^{n-1}\le w\le 2^{n-1}} \Big(E_{even}\big(\mathbf{Sign}^{(n-1)}(w)\big) + E_{odd}\big(\mathbf{Sign}^{(n-1)}(w)\big)\Big).$$

When $I = \{1\}$ and $n = 1$,

$$\mathbf{S}^{(1)}_{\{1\}} = \{[0] + [1], -[0] - [1]\}.$$

Proof of Proposition 4.3. For any $v \in \boldsymbol{V}^{(n)}$, it follows from the definition of $\mathbf{K}^n_{\{1\}}$ that $v \in \big(\mathbf{K}^n_{\{1\}}\big)^\perp$ if and only if $v = E_{even}(u) + E_{odd}(u')$ with $w(u) = w(u')$. Hence the assertion follows from Proposition 4.2. □

The case $I \cap \{0,1\} = \{0\}$ is treated similarly, since $\mathbf{K}^{(n)}_{\{0\}}$ is generated by the all-one vector $\mathbf{1}^{(n)} = \sum_{a \in P(2)^n} [a]$.

Proposition 4.4. *Suppose that $I \cap \{0,1\} = \{0\}$. Then*

$$\mathbf{S}^{(n)}_I = \coprod_{-2^{n-1} \le w \le 2^{n-1}} \Big(E_{even}\big(\mathbf{S}^{(n-1)}_{I-\{0\}-1}(w)\big) + E_{odd}\big(\mathbf{S}^{(n-1)}_{I-\{0\}-1}(-w)\big)\Big).$$

Remark 4.5. Let $\iota^{(n)}_{1,-1} : \boldsymbol{V}^{(n)} \to \boldsymbol{V}^{(n)}$ be the automorphism defined by

$$\iota^{(n)}_{1,-1}\big(E_{even}(u) + E_{odd}(u')\big) = E_{even}(u) - E_{odd}(u').$$

The two preceding propositions show that $\iota^{(n)}_{1,-1}$ induces a bijection between $\mathbf{S}^{(n)}_{\{1,i_1,i_2,\dots,i_k\}}$ and $\mathbf{S}^{(n)}_{\{0,i_1,i_2,\dots,i_k\}}$ for any subset $\{i_1, i_2, \dots, i_k\} \subset [2, n]$.

The next proposition deals with the case $I \supset \{0,1\}$.

Proposition 4.6. *Suppose $I \supset \{0,1\}$. Then*

$$\mathbf{S}^{(n)}_I = E_{even}\big(\mathbf{S}^{(n-1)}_{I-\{0,1\}-1}(0)\big) + E_{odd}\big(\mathbf{S}^{(n-1)}_{I-\{0,1\}-1}(0)\big).$$

Equivalently we have

$$\mathbf{S}^{(n)}_I = E_{even}\big(\mathbf{S}^{(n-1)}_{I-\{0\}-1}\big) + E_{odd}\big(\mathbf{S}^{(n-1)}_{I-\{0\}-1}\big).$$

Therefore if we define $\{0, j_1, \dots, j_\ell\} - 1$ to be $\{j_1 - 1, \dots, j_\ell - 1\}$, then the same equality as in Proposition 4.2 holds.

Proof of Proposition 4.6. For any $v \in \boldsymbol{V}^{(n)}$, we have the following series of equivalences

$$\begin{aligned} v \in \big(\mathbf{K}^{(n)}_{\{0\}}\big)^\perp \cap \big(\mathbf{K}^{(n)}_{\{1\}}\big)^\perp &\iff \langle v, \mathbf{1}\rangle = \big\langle v, \iota^{(n)}_{1,-1}(\mathbf{1})\big\rangle = 0 \\ &\iff v = E_{even}(u) + E_{odd}(u') \text{ with } w(u) = w(u') = 0. \end{aligned}$$

This concludes the proof of Proposition 4.6. □

The four propositions, Proposition 4.2, 4.3, 4.4, and 4.6 provide us with an effective recursive algorithm to generate all the elements of $\mathbf{S}_I^{(n)}$ once a subset $I \subset [0,n]$ is given.

4.B. Generating algorithm for $\mathbf{S}_I^{(n)}$.

We show that there is a simple inductive algorithm which generates all elements in $\mathbf{S}_I^{(n)}$.

Let $\mathscr{P}(X)$ denote the set of all subsets of X for any set X. Let two operators $L, R : \mathscr{P}(\boldsymbol{V}^{(i)}) \to \mathscr{P}(\boldsymbol{V}^{(i+1)})$, $i \in [0, n-1]$ be defined by

$$L(T) = E_{even}(T) + E_{odd}(T),$$
$$R(T) = \coprod_w \big(E_{even}(T(w)) + E_{odd}(T(w))\big).$$

For any subset $I \subset [1,n]$, we define $\boldsymbol{b}(I) \in \{1, \underline{1}\}^n$ by

$$\boldsymbol{b}(I) = \varepsilon_1 \cdots \varepsilon_n, \quad \text{where} \quad \varepsilon_i = \begin{cases} \underline{1}, & \text{if } i \in I, \\ 1, & \text{if } i \notin I. \end{cases}$$

We call elements of $\{1, \underline{1}\}^n$ *binary vectors*, and $\boldsymbol{b}(I)$ *the binary expression of* I. Note that $\boldsymbol{b}$ defines a one-to-one correspondence between $\mathscr{P}([1,n])$ and $\{1, \underline{1}\}^n$. Furthermore to any binary vector $\boldsymbol{b}$, we attach an operator

$$\mathbf{G}_{\boldsymbol{b}} = X_1 \cdots X_n : \mathscr{P}(\boldsymbol{V}^{(0)}) \to \mathscr{P}(\boldsymbol{V}^{(n)}), \quad \text{where} \quad X_i = \begin{cases} L, & \text{if } \boldsymbol{b}_i = 1, \\ R, & \text{if } \boldsymbol{b}_i = \underline{1}. \end{cases}$$

Then the contents of Propositions 4.2 and 4.3 are translated into the following formula, which gives us a simple algorithm which generates all elements in $\mathbf{S}_I^{(n)}$.

THEOREM 4.7. *Suppose that* $I \subset [1,n]$. *Then* $\mathbf{S}_I^{(n)} = \mathbf{G}_{\boldsymbol{b}(I)}(\{[0], -[0]\})$.

4.C. Weight enumerator for $\mathbf{S}_I^{(n)}$.

Our objective here is to enumerate the elements of $\mathbf{S}_I^{(n)}$. It is convenient for us to introduce the *weight enumerator* $W_I^{(n)}(x) \in \boldsymbol{Z}[x, x^{-1}]$, defined by

$$W_I^{(n)}(x) = \sum_{-2^n \le w \le 2^n} \#\big(\mathbf{S}_I^{(n)}(w)\big) x^w.$$

In particular, we have

$$\#\big(\mathbf{S}_I^{(n)}\big) = W_I^{(n)}(1). \tag{4.5}$$

Note that when $I \supset \{0\}$, every element in $\mathbf{S}_I^{(n)}$ is of weight zero, hence the corresponding weight enumerator is actually a constant. For ease of description, we define two operators,

which correspond to L and R introduced above. For any Laurent polynomial $f(x) = \sum_{-N\le n\le N} a_n x^n$, let

$$[2](f)(x) = \sum_{-N\le n\le N} a_n^2 x^{2n}.$$

Furthermore let

$$B(f)(x) = (f(x))^2,$$

and let $B^i = \underbrace{B\circ\cdots\circ B}_{i \text{ times}}$.

PROPOSITION 4.8. *Suppose that $I \subset [1,n]$. Let $I = \{i_1,\dots,i_k\}$ with $i_1 < \cdots < i_k$. Then*

$$W_I^{(n)} = \big(B^{i_1-1}\circ[2]\circ B^{i_2-i_1-1}\circ[2]\circ B^{i_3-i_2-1}\circ[2]\circ \cdots\circ[2]\circ B^{i_k-i_{k-1}-1}\circ[2]\circ B^{n-i_k}\big)W^{(0)},$$

where $W^{(0)}(x) = x + x^{-1}$.

PROOF OF PROPOSITION 4.8. We show this when $k = 3$, because it indicates a general pattern most clearly, and it is easy to extend it to the argument applicable for the general case. Let $I = \{i_1,i_2,i_3\}$, $i_1 < i_2 < i_3$. When $i_1 \ge 2$, applying Proposition 4.2 $i_1 - 1$ times, we obtain

$$\begin{aligned} W^{(n)}_{\{i_1,i_2,i_3\}} &= \big(W^{(n-1)}_{\{i_1-1,i_2-1,i_3-1\}}\big)^2 = \cdots = \big(W^{(n-i_1+1)}_{\{1,i_2-i_1+1,i_3-i_1+1\}}\big)^{2^{i_1-1}} \\ &= B^{i_1-1}\big(W^{(n-i_1+1)}_{\{1,i_2-i_1+1,i_3-i_1+1\}}\big). \end{aligned}$$

Note that the equality obtained here is valid also for the case $i_1 = 1$ since B_0 is the identity map by definition. Then Proposition 4.3 shows that

$$W^{(n-i_1+1)}_{\{1,i_2-i_1+1,i_3-i_1+1\}} = [2]\big(W^{(n-i_1)}_{\{i_2-i_1,i_3-i_1\}}\big).$$

Applying Proposition 4.2 $i_2 - i_1 - 1$ times, we obtain

$$W^{(n-i_1)}_{\{i_2-i_1,i_3-i_1\}} = \big(W^{(n-i_2+1)}_{\{1,i_3-i_2+1\}}\big)^{2^{i_2-i_1-1}} = B^{i_2-i_1-1}\big(W^{(n-i_2+1)}_{\{1,i_3-i_2+1\}}\big).$$

Then Proposition 4.3 implies that

$$W^{(n-i_2+1)}_{\{1,i_3-i_2+1\}} = [2]\big(W^{(n-i_2)}_{\{i_3-i_2\}}\big).$$

Applying Proposition 4.2 $i_3 - i_2 - 1$ times, we obtain

$$W_{\{i_3-i_2\}}^{(n-i_2)} = B^{i_3-i_2-1} W_{\{1\}}^{(n-i_3+1)}.$$

Finally Proposition 4.3 gives us the equality

$$W_{\{1\}}^{(n-i_3+1)} = [2]\big(W^{(n-i_3)}\big).$$

Hence we complete the proof when $k = 3$, and by quite a similar reasoning, we obtain the assertion for the general case. □

Note that when $I \supset \{0\}$, the weight polynomial is a constant. Let $c(f)$ denote the constant term of a Laurent polynomial f. Then by the very definition of the weight polynomial, we have the following.

PROPOSITION 4.9. *Suppose that $I \supset \{0\}$. Then $W_I^{(n)} = c(W_{I-\{0\}}^{(n)})$.*

The content of Proposition 4.8 can be expressed again by binary expression more neatly. Let $1 \in \{1, \underline{1}\}$ (resp. $\underline{1} \in \{1, \underline{1}\}$) acts on $\boldsymbol{Z}[x, x^{-1}]$ through B (resp. $[\mathbf{2}]$). Then we have the following restatement of Proposition 4.8 using binary expressions. Let $W^{(m)} = B^m W^{(0)}$, $m \geq 1$.

THEOREM 4.10. *Suppose that $I \subset [1, n]$. Then $W_I^{(n)} = \boldsymbol{b}(I) W^{(0)}$.*

Now we examine a few examples.

EXAMPLE 4.11. *The case $n = 2$.* The weight polynomials are computed as follows.

$$\begin{aligned}
W_{\{2\}}^{(2)}(x) &= (1\,\underline{1})W^{(0)}(x) = (B^1 \circ [2])W^{(0)}(x) = \big((x + x^{-1})^{[2]}\big)^2 \\
&= (x^2 + x^{-2})^2 = x^4 + 2 + x^{-4}, \\
W_{\{1\}}^{(2)}(x) &= (\underline{1}\,1)W^{(1)}(x) = (B^0 \circ [2])W^{(1)}(x) = \big((x + x^{-1})^2\big)^{[2]} \\
&= (x^2 + 2 + x^{-2})^{[2]} = x^4 + 4 + x^{-4}, \\
W_{\{0\}}^{(2)}(x) &= c(W^{(2)}) = c\big((x + x^{-1})^4\big) = 6, \\
W_{\{1,2\}}^{(2)}(x) &= (\underline{1}\,\underline{1})W^{(0)}(x) = (B^0 \circ [2] \circ B^0 \circ [2])W^{(0)}(x) = \big((x + x^{-1})^{[2]}\big)^{[2]} \\
&= (x^2 + x^{-2})^{[2]} = x^4 + x^{-4}, \\
W_{\{0,2\}}^{(2)}(x) &= c\big(W_{\{2\}}^{(2)}\big) = 2, \\
W_{\{0,1\}}^{(2)}(x) &= c\big(W_{\{1\}}^{(2)}\big) = 4, \\
W_{\{0,1,2\}}^{(2)}(x) &= c\big(W_{\{1,2\}}^{(2)}(x)\big) = 0.
\end{aligned}$$

Hence it follows from (4.5) that

$$\#\big(\mathbf{S}^{(2)}_{\{2\}}\big) = 4, \quad \#\big(\mathbf{S}^{(2)}_{\{1\}}\big) = 6, \quad \#\big(\mathbf{S}^{(2)}_{\{0\}}\big) = 6,$$
$$\#\big(\mathbf{S}^{(2)}_{\{1,2\}}\big) = 2, \quad \#\big(\mathbf{S}^{(2)}_{\{0,2\}}\big) = 2, \quad \#\big(\mathbf{S}^{(2)}_{\{0,1\}}\big) = 4, \quad \#\big(\mathbf{S}^{(2)}_{\{0,1,2\}}\big) = 0.$$

Therefore the total of elements of $\bigcup_{I\neq\varnothing} \mathbf{S}^{(n)}_I$ is computed as follows:

$$\#\Big(\bigcup_{I\neq\varnothing} \mathbf{S}^{(n)}_I\Big) = \#\big(\mathbf{S}^{(2)}_{\{2\}}\big) + \#\big(\mathbf{S}^{(2)}_{\{1\}}\big) + \#\big(\mathbf{S}^{(2)}_{\{0\}}\big) - \#\big(\mathbf{S}^{(2)}_{\{1,2\}}\big) - \#\big(\mathbf{S}^{(2)}_{\{0,2\}}\big) - \#\big(\mathbf{S}^{(2)}_{\{0,1\}}\big) + \#\big(\mathbf{S}^{(2)}_{\{0,1,2\}}\big) = 8.$$

EXAMPLE 4.12. *The case* $n = 3$. The weight polynomials are as follows. (We state the results only, because they can be computed similarly.)

$$W^{(3)}_{\{3\}}(x) = (1\,1\,\underline{1})W^{(0)}(x) = x^8 + 4x^4 + 6 + 4x^{-4} + x^{-8},$$
$$W^{(3)}_{\{2\}}(x) = (1\,\underline{1}\,1)W^{(0)}(x) = x^8 + 8x^4 + 18 + 8x^{-4} + x^{-8},$$
$$W^{(3)}_{\{1\}}(x) = (\underline{1}\,1\,1)W^{(0)}(x) = x^8 + 16x^4 + 36 + 16x^{-4} + x^{-8},$$
$$W^{(3)}_{\{0\}}(x) = c(W^{(3)}) = c\big((x + x^{-1})^8\big) = \binom{8}{4} = 70,$$
$$W^{(3)}_{\{2,3\}}(x) = (1\,\underline{1}\,\underline{1})W^{(0)}(x) = x^8 + 2 + x^{-8},$$
$$W^{(3)}_{\{1,3\}}(x) = (\underline{1}\,1\,\underline{1})W^{(0)}(x) = x^8 + 4 + x^{-8},$$
$$W^{(3)}_{\{0,3\}}(x) = c\big(W^{(3)}_{\{3\}}\big) = 6,$$
$$W^{(3)}_{\{1,2\}}(x) = (\underline{1}\,\underline{1}\,1)W^{(0)}(x) = x^8 + 16 + x^{-8},$$
$$W^{(3)}_{\{0,2\}}(x) = c\big(W^{(3)}_{\{2\}}\big) = 18,$$
$$W^{(3)}_{\{0,1\}}(x) = c\big(W^{(3)}_{\{1\}}\big) = 36,$$
$$W^{(3)}_{\{1,2,3\}}(x) = (\underline{1}\,\underline{1}\,\underline{1})W^{(0)}(x) = x^8 + x^{-8},$$
$$W^{(3)}_{\{0,2,3\}}(x) = c\big(W^{(3)}_{\{2,3\}}\big) = 2,$$
$$W^{(3)}_{\{0,1,3\}}(x) = c\big(W^{(3)}_{\{1,3\}}\big) = 4,$$
$$W^{(3)}_{\{0,1,2\}}(x) = c\big(W^{(3)}_{\{1,2\}}\big) = 16,$$
$$W^{(3)}_{\{0,1,2,3\}}(x) = c\big(W^{(3)}_{\{1,2,3\}}\big) = 0.$$

Therefore we have

$$\#(\mathbf{S}^{(3)}_{\{3\}}) = 16, \quad \#(\mathbf{S}^{(3)}_{\{2\}}) = 36, \quad \#(\mathbf{S}^{(3)}_{\{1\}}) = 70, \quad \#(\mathbf{S}^{(3)}_{\{0\}}) = 70,$$
$$\#(\mathbf{S}^{(3)}_{\{2,3\}}) = 4, \quad \#(\mathbf{S}^{(3)}_{\{1,3\}}) = 6, \quad \#(\mathbf{S}^{(3)}_{\{0,3\}}) = 6, \quad \#(\mathbf{S}^{(3)}_{\{1,2\}}) = 18,$$
$$\#(\mathbf{S}^{(3)}_{\{0,2\}}) = 18, \quad \#(\mathbf{S}^{(3)}_{\{0,1\}}) = 36,$$
$$\#(\mathbf{S}^{(3)}_{\{1,2,3\}}) = 2, \quad \#(\mathbf{S}^{(3)}_{\{0,2,3\}}) = 2, \quad \#(\mathbf{S}^{(3)}_{\{0,1,3\}}) = 4, \quad \#(\mathbf{S}^{(3)}_{\{0,1,2\}}) = 16,$$
$$\#(\mathbf{S}^{(3)}_{\{0,1,2,3\}}) = 0.$$

Hence the total of degenerate sign-vectors is equal to

$$16 + 36 + 70 + 70 - (4 + 6 + 6 + 18 + 18 + 36) + (2 + 2 + 4 + 16) = 128.$$

The binary expression also enables one to know at once what the degrees of weight enumerators are. (Here the *degree* of a *symmetric* Laurent polynomial $a_m x^m + \cdots + a_m x^{-m}$, $m \geq 0$, is defined to be m.)

PROPOSITION 4.13. *For any subset $I \subset [1, n]$, the weight enumerators $W_I^{(n)}$ have the common degree 2^n.*

PROOF OF PROPOSITION 4.13. This is simply because both operators "1" and "$\underline{1}$" raise the degree of a given Laurent polynomial by two. □

4.D. Primitivity of sign-vectors.

An element $a \in P(2)^n = \boldsymbol{Z}/2^n\boldsymbol{Z}$ acts on $\boldsymbol{V}^{(n)}$ naturally by the rule

$$a.\Big(\sum_{b\in P(2)^n} n_b[b]\Big) = \sum_{b\in P(2)^n} n_b[a+b].$$

A sign-vector $S \in \mathbf{Sign}^{(n)}$ is said to be *nonprimitive*, if $a.S = \pm S$ for some $a \in P(2)^n - \{\mathbf{0}\}$. When it is not nonprimitive, it is called *primitive*. Since $2^{n-1}\boldsymbol{Z}/2^n\boldsymbol{Z}$ is the maximal proper subgroup of $\boldsymbol{Z}/2^n\boldsymbol{Z}$, we have the following.

PROPOSITION 4.14. *A sign-vector $S \in \mathbf{Sign}^{(n)}$ is nonprimitive if and only if $2^{n-1}.S = \pm S$.*

By the definition of the tree structure of $P(2)$, the pairs $(a, a+2^{n-1})$, $0 \leq a \leq 2^{n-1}-1$ constitute all the last branches of $P(2)^{(n)}$. Hence for any $S \in \mathbf{Sign}^{(n)}$, we have

$$2^{n-1}.S = S \text{ if and only if } S \in \mathbf{S}^{(n)}_{\{n\}},$$
$$2^{n-1}.S = -S \text{ if and only if } S \in \mathbf{S}^{(n)}_{\{0,1,\ldots,n-1\}}.$$

Therefore we have the following criterion for nonprimitivity. (Note that $\mathbf{S}^{(n)}_{\{n\}} \cap \mathbf{S}^{(n)}_{\{0,1,\dots,n-1\}} = \mathbf{S}^{(n)}_{[0,n]} = \varnothing$.)

PROPOSITION 4.15. *A sign-vector $S \in \mathbf{Sign}^{(n)}$ is nonprimitive if and only if $S \in \mathbf{S}^{(n)}_{\{n\}} \coprod \mathbf{S}^{(n)}_{\{0,1,\dots,n-1\}}$. In particular the number of nonprimitive sign-vectors in $\mathbf{Sign}^{(n)}$ is equal to $2^{2^{n-1}} + 2^{2^{n-1}} = 2^{2^{n-1}+1}$.*

4.E. The structure of $\mathbf{E}^{(n)}_I$.

Our objective here is to investigate what kind of (0,1)-vectors are in $(\mathbf{K}^{(n)}_I)^\perp$. They can be investigated in a similar way to that for $\mathbf{S}^{(n)}_I = \mathbf{Sign}^{(n)} \cap (\mathbf{K}^{(n)}_I)^\perp$. We define two operators $L_i, R_i : \mathscr{P}(\mathbf{Bit}^{(i-1)}) \to \mathscr{P}(\mathbf{Bit}^{(i)})$, $i \geq 1$, by

$$L_i(C) = \bigcup_{c \in C} \left(L^{-1}_{i,i-1}(\{c\}) \cap \mathbf{Bit}^{(i)}\right),$$
$$R_i(C) = R_{i-1,i}(C),$$

for any $C \in \mathscr{P}(\mathbf{Bit}^{(i-1)})$. When the domain is understood, we write $L = L_i$, $R = R_i$.

THEOREM 4.16. *For any $I \subset [1,n]$, rewrite the string $\boldsymbol{b}(I) = e_1 \cdots e_n \in \{1, \underline{1}\}^n$ by the rule*

$$e_i \mapsto \begin{cases} L_i, & \text{if } e_i = 1, \\ R_i, & \text{if } e_i = \underline{1}, \end{cases}$$

and denote the resulted string by $\Phi(\boldsymbol{e})$. Let $\mathbf{St}^{(n)}_I = \iota(\Phi(\boldsymbol{e}))$, where ι reverses the order of a string. Then we have

$$\mathbf{E}^{(n)}_I = \mathbf{St}^{(n)}_I(\{[0]\}).$$

PROOF OF THEOREM 4.16. We prove this by induction on n. When $n = 1$, there are two binary expressions 1 and $\underline{1}$, which correspond to the subset $I = \varnothing$ and $I = \{1\}$, respectively. The corresponding sets of (0,1)-vectors are given by

$$\mathbf{E}^{(1)}_\varnothing = \{[0], [1]\}, \quad \mathbf{E}^{(1)}_{\{1\}} = \{[0] + [1]\}.$$

On the other hand, it follows from the definition that

$$\Phi(1) = L, \quad \Phi(\underline{1}) = R,$$

and hence

$$\mathbf{St}^{(1)}_\varnothing = L, \quad \mathbf{St}^{(1)}_{\{1\}} = R.$$

Therefore

$$\mathbf{St}^{(1)}_{\varnothing}(\{[0]\}) = L(\{[0]\}) = L_{10}^{-1}(\{[0]\}) \cap \mathbf{Bit}^{(1)} = \{[0],[1]\},$$
$$\mathbf{St}^{(1)}_{\{1\}}(\{[0]\}) = R(\{[0]\}) = R_{01}(\{[0]\}) = \{[0]+[1]\}.$$

This shows that the assertion holds for $n = 1$. Now assume that $n \geq 2$ and the assertion holds true for $n-1$. First we treat the case $e_1 = 1$. Then $\Phi(\boldsymbol{e}) = L_1 X_2 \cdots X_n$, hence $\mathbf{St}^{(n)}_I = X_n \cdots X_2 L_1$, where X_i $(2 \leq i \leq n)$ stands for R or L. Since $e_1 = 1$ implies $1 \notin I$, a similar proof to that for Proposition 4.2 gives the equality

$$\mathbf{E}^{(n)}_I = E_{even}\big(\mathbf{E}^{(n-1)}_{I-1}\big) \coprod E_{odd}\big(\mathbf{E}^{(n-1)}_{I-1}\big). \tag{4.6}$$

By the induction hypothesis, we have $\mathbf{E}^{(n-1)}_{I-1} = \mathbf{St}^{(n-1)}_{I-1}(\{[0]\})$. Moreover we see that $\mathbf{St}^{(n-1)}_{I-1} = X_n \cdots X_2$ by the definition. Hence

$$\mathbf{E}^{(n-1)}_{I-1} = X_n \cdots X_2(\{[0]\}).$$

Furthermore by the commutativity relations (4.2) and (4.3), we have

$$E_{even} \circ X_n \cdots X_2 = X_n \cdots X_2 \circ E_{even},$$
$$E_{odd} \circ X_n \cdots X_2 = X_n \cdots X_2 \circ E_{odd}.$$

Hence (4.6) implies that

$$\begin{aligned}
\mathbf{E}^{(n)}_I &= \big(X_n \cdots X_2 \circ E_{even}(\{[0]\})\big) \coprod \big(X_n \cdots X_2 \circ E_{odd}(\{[0]\})\big) \\
&= \big(X_n \cdots X_2(\{[0]\})\big) \coprod \big(X_n \cdots X_2(\{[1]\})\big) \\
&= X_n \cdots X_2 L_1(\{[0]\}) \\
&= \mathbf{St}^{(n)}_I(\{[0]\}).
\end{aligned}$$

Thus we see that the assertion holds when $e_1 = 1$. Next we treat the case $e_1 = \underline{1}$. Then $\Phi(\boldsymbol{e}) = R_1 X_2 \cdots X_n$, hence $\mathbf{St}^{(n)}_I = X_n \cdots X_2 R_1$, where X_i $(2 \leq i \leq n)$ stands for R or L. Since this implies $1 \in I$, the similar proof to that for Proposition 4.3 gives the equality

$$\mathbf{E}^{(n)}_I = E_{even}\big(\mathbf{E}^{(n-1)}_{I-\{1\}-1}\big) + E_{odd}\big(\mathbf{E}^{(n-1)}_{I-\{1\}-1}\big).$$

By induction hypothesis, we have

$$\mathbf{E}^{(n-1)}_{I-\{1\}-1} = \mathbf{St}^{(n-1)}_{I-\{1\}-1}(\{[0]\}).$$

Note here that

$$\Phi(I - \{1\} - 1) = X_2 \cdots X_n,$$
$$\mathbf{St}^{(n-1)}_{I-\{1\}-1} = X_n \cdots X_2.$$

Therefore by the commutativity relations (4.2), (4.3), we have

$$\begin{aligned}\mathbf{E}^{(n)}_I &= (E_{even} \circ X_n \cdots X_2)(\{[0]\}) + (E_{odd} \circ X_n \cdots X_2)(\{[0]\}) \\ &= (X_n \cdots X_2)(\{[0] + [1]\}) \\ &= (X_n \cdots X_2 R_1)(\{[0]\}) \\ &= \mathbf{St}^{(n)}_I(\{[0]\}).\end{aligned}$$

Thus the assertion is certified for the case $e_1 = \underline{1}$ too. Thus we complete the proof of Theorem 4.16. □

4.F. The number of elements of $\mathbf{E}^{(n)}_I$.

Our objective here is to enumerate the elements of $\mathbf{E}^{(n)}_I$.

Proposition 4.17. *Let $I = \{i_1, \ldots, i_k\} \subset [1, n]$ with $i_1 < \cdots < i_k$. Then all the elements in $\mathbf{E}^{(n)}_I$ have one and the same weight 2^k. The number of elements in $\mathbf{E}^{(n)}_I$ is given by*

$$\#\big(\mathbf{E}^{(n)}_I\big) = 2^{2^k n - i_1 - 2i_2 - \cdots - 2^{k-2} i_{k-1} - 2^{k-1} i_k - (2^k - 1)}.$$

Proof of Proposition 4.17. Our proof reduces essentially to the following lemma which is a direct consequence of the definition of raising and lowering operators.

Lemma 4.17.1. *Let $T \subset \mathbf{Bit}^{(i-1)}$, $i \geq 1$ such that every element in T has one and the same weight. Let $w(T)$ denote the common weight of T. Then we have*

$$\#(R_i(T)) = \#(T), \quad w(R_i(T)) = 2w(T),$$
$$\#(L_i(T)) = 2^{w(T)} \cdot \#(T), \quad w(L_i(T)) = w(T).$$

Therefore the assertions of Proposition 4.17 follow easily from Theorem 4.16 by induction. □

Note that every $\mathbf{E}^{(m)}_{I'} \subset \{0, 1\}^{2^m}$ for $m \in [1, n]$, $I' \subset [1, m]$ satisfies the assumption of the lemma. The assertions in our proposition can be proved by a simple induction using Theorem 4.16. Details will be left to the reader.

Remark 4.18. In the above two propositions, we restrict our attention to the indecomposable (0,1)-vectors. If one is interested only in the set $\mathbf{B}^{(n)}_I = \mathbf{Bit}^{(n)} \cap$

$(\mathbf{K}_I^{(n)})^\perp$ of all the (0,1)-vectors in $(\mathbf{K}_I^{(n)})^\perp$ with $I \subset [1,n]$, the following simple device provides a precise information about the weight distribution. Let $W_{\mathbf{B},I}^{(n)}(x) = \sum_{0\le w\le 2^n} \#(\mathbf{B}_I^{(n)}(w))x^w$ be the corresponding weight enumerator. Then we see that

the weight enumerator $W_{[0,1],I}^{(n)}$ can be computed by the same inductive formula as in Theorem 4.10, if we replace $W^{(0)}$ by $W_{[0,1]}^{(0)}(x) = x+1$. (4.7)

For the proof, we are only to use the fact that $\varphi : \mathbf{Sign}^{(n)} \cap \boldsymbol{V}^{(n)} \to \mathbf{Bit}^{(n)} \cap \boldsymbol{V}^{(n)}$, defined by $\varphi(v) = (v + \mathbf{1}^{(n)})/2$, gives a bijection, since $\mathbf{1}^{(n)} \in \mathbf{K}_{\{0\}}^{(n)} \subset (\mathbf{K}_I^{(n)})^\perp$ by the assumption $I \subset [1,n]$.

We illustrate the contents of Theorem 4.16, Proposition 4.17 by an example.

EXAMPLE 4.19. 1) Let $n = 3$ and $I = \{2\}$. The binary expression of I is $1\underline{1}1$. Hence we have $\mathbf{St}_{\{2\}}^{(3)} = L_3R_2L_1$. Therefore we can compute as follows. (For simplicity, we write $abc\cdots$ for $[a]+[b]+[c]+\cdots \in \boldsymbol{V}_i^{(n)}$.)

$$\begin{aligned}\mathbf{E}_{\{2\}}^{(3)} &= L_3R_2L_1(\{[0]\}) = L_3R_2(\{0,1\}) = L_3(\{02,13\})\\ &= \{02,06,42,46,13,17,53,57\}.\end{aligned}$$

The number of elements in equal to 8, which coincides with the one given by Proposition 4.17, $\#(\mathbf{E}_{\{2\}}^{(3)}) = 2^{2^1\cdot 3-2-(2^1-1)} = 2^3$.

2) Let $n = 3$ and $I = \{3\}$. The binary expression of $\{3\}$ is $1\,1\,\underline{1}$. Hence we have $\mathbf{St}_{\{3\}}^{(3)} = R_3L_2L_1$. Therefore we can compute as follows.

$$\begin{aligned}\mathbf{E}_{\{3\}}^{(3)} &= R_3L_2L_1(\{[0]\}) = R_3L_2(\{0,1\}) = R_3(\{0,2,1,3\})\\ &= \{04,26,15,37\}.\end{aligned}$$

The number of elements in equal to 4, which coincides with the one given by Proposition 4.17, $\#(\mathbf{E}_{\{3\}}^{(3)}) = 2^{2^1\cdot 3-3-(2^1-1)} = 2^2$. Note that this example shows the relevance of the *string-reversing* map ι in Theorem 4.16.

4.G. Heights of elements and subsets of $(\mathbf{K}_I^{(n)})^\perp$.

For any $v = \sum_{a\in P^{(n)}} v_a[a] \in \boldsymbol{V}^{(n)}$, we put $h(v) = \sum_{a\in P^{(n)}} |v_a| \in \boldsymbol{Z}_{\ge 0}$ and call it the height of v. Furthermore, for any subset $T \subset \boldsymbol{V}^{(n)}$, we let $h_{\min}(T) = \min\{h(v); v \in T - \{\mathbf{0}\}\}$. When $T = \{\mathbf{0}\}$, we put $h_{\min}(\{\mathbf{0}\}) = +\infty$. First we prove a simple lemma.

LEMMA 4.20. *If $v \in \boldsymbol{V}^{(m)}$, $m \ge 1$, is expressed as $v = E_{even}(w) + E_{odd}(w')$, $w, w' \in \boldsymbol{V}^{(m-1)}$, then $h(v) = h(w) + h(w')$.*

PROOF OF LEMMA 4.20. This is because $\mathrm{Supp}(E_{even}(w)) \cap \mathrm{Supp}(E_{odd}(w)) = \varnothing$.

LEMMA 4.21. *For any subset* $\boldsymbol{T} \subset \boldsymbol{V}^{(i)}$, $i \geq 0$, *let* $T_{\neq 0} = \coprod_{w \neq 0} T(w)$. *Suppose that* $\mathbf{0} \in T$. *Then we have*

(i) $h_{\min}\big(E_{even}(T) + E_{odd}(T)\big) = h_{\min}(T)$.

(ii) $$h_{\min}\Big(\coprod_{w}\big(E_{even}(T)(w) + E_{odd}(T)(w)\big)\Big) = \begin{cases} 2h_{\min}(T_{\neq 0}), & \text{if } h_{\min}(T(0)) > 2h_{\min}(T_{\neq 0}), \\ h_{\min}(T(0)), & \text{if } h_{\min}(T(0)) \leq 2h_{\min}(T_{\neq 0}). \end{cases}$$

PROOF OF LEMMA 4.21. The assertion (i) is a direct consequence of Lemma 4.20, since $\mathbf{0} \in T$. As for (ii), we note that the assumption $\mathbf{0} \in T$ implies that

$$E_{even}(T)(0) + \{\mathbf{0}\} \subset \big(E_{even}(T)(0) + E_{odd}(T)(0)\big),$$

and

$$h_{\min}\big(E_{even}(T)(0) + \{\mathbf{0}\}\big) = h_{\min}(T(0)).$$

Therefore (ii) also follows from Lemma 4.20. □

THEOREM 4.22. *For any* $n \geq 1$ *and* $I \subset [1, n]$, *the minimum* $h_I^{(n)}$ *of the heights of the elements in* $(\mathbf{K}_I^{(n)})^{\perp}$ *is given as follows*;

(i) *if* $I = \varnothing$, *then* $h_I^{(n)} = 1$,
(ii) *if there exists an* $m \in [1, n]$ *such that* $I = [m, n]$, *then* $h_I^{(n)} = 2^{n-m+1}$.
(iii) *when there exists no* $m \in [1, n]$ *such that* $I = [m, n]$, *we have* $h_I^{(n)} = 2^{n-r(I)+2}$, *where* $r(I) = \min\{i \in [1, n]; [i, n] \subset I\}$.

PROOF OF THEOREM 4.22. (i) If $I = \varnothing$, then $(\mathbf{K}_I^{(n)})^{\perp} = \boldsymbol{V}^{(n)}$. Hence any standard basis elements $[a], a \in \boldsymbol{Z}/2^n\boldsymbol{Z}$, belong to it, and we have $h_I^{(n)} = 1$.

(ii) When $I = [m, n]$, its binary expression is $1 \cdots 1 \underbrace{1 1 \cdots 1}_{n-m+1 \text{ times}}$. Therefore the corresponding operator is $L \cdots L \underbrace{R \cdots R}_{n-m+1 \text{ times}}$. Hence Theorem 4.7 shows that

$$\big(\mathbf{K}_I^{(n)}\big)^{\perp} = L \cdots L \underbrace{R \cdots R}_{n-m+1 \text{ times}} (\boldsymbol{Z}.[0]) = L \cdots L(\boldsymbol{Z}.\mathbf{1}^{(n-m+1)}).$$

Since the operator L does not increase the minimal height at each stage by Lemma 4.21 (i), we see that $h_I^{(n)} = h(\mathbf{1}^{(n-m+1)}) = 2^{n-m+1}$.

(iii) In this case the binary expression of I is of the form

$$\boldsymbol{e}\overset{i}{\breve{1}}\underbrace{1 \cdots 1}_{s \text{ times}} \underbrace{1 1 \cdots 1}_{n-r(I)+1 \text{ times}}$$

for some i, $s \geq 1$ and a string $\boldsymbol{e}$ of 1 and $\underline{1}$. Therefore the corresponding operator is given by

$$\mathbf{X}\overset{i}{\breve{R}}\underbrace{L\cdots L}_{s\ times}\ \underbrace{RR\cdots R}_{n-r(I)+1\ times},$$

where X is a string of L and R. Hence we have

$$\begin{aligned}\big(\mathbf{K}_I^{(n)}\big)^{\perp} &= \mathbf{X}\overset{i}{\breve{R}}\underbrace{L\cdots L}_{s\ times}\ \underbrace{RR\cdots R}_{n-r(I)+1\ times}\quad(\boldsymbol{Z}.[0])\\ &= \mathbf{X}\overset{i}{\breve{R}}\underbrace{L\cdots L}_{s\ times}(\boldsymbol{Z}.\mathbf{1}^{(n-r(I)+1)})\\ &= \mathbf{X}\overset{i}{\breve{R}}\big(L^s(\boldsymbol{Z}.\mathbf{1}^{(n-r(I)+1)})\big).\end{aligned}$$

Note here that the $\boldsymbol{Z}$-module $L^s(\boldsymbol{Z}.\mathbf{1}^{(n-r(I)+1)})$ is of rank 2^s and generated by the 2^s elements $R_{s,s+n-r(I)+1}([a]), a \in P^{(s)}$, all of which have height $2^{n-r(I)+1}$. Hence

$$h_{\min}\big(L^s(\boldsymbol{Z}.\mathbf{1}^{(n-r(I)+1)})(0)\big) = 2\cdot 2^{n-r(I)+1},$$

and it follows from Lemma 4.21 (ii) that

$$h_{\min}\Big(R\big(L^s(\boldsymbol{Z}.\mathbf{1}^{(n-r(I)+1)})\big)\Big) = 2^{n-r(I)+2}$$

and

$$h_{\min}\Big(R\big(L^s(\boldsymbol{Z}.\mathbf{1}^{(n-r(I)+1)})\big)(0)\Big) = 2^{n-r(I)+2}.$$

Therefore it also follows from Lemma 4.21 that

$$h_{\min}\Big(X\overset{i}{\breve{R}}\big(L^s(\boldsymbol{Z}.\mathbf{1}^{(n-r(I)+1)})\big)\Big) = 2^{n-r(I)+2}.$$

Thus we complete the proof of Theorem 4.22. □

Next we investigate the $\boldsymbol{Z}$-basis of $(\mathbf{K}_I^{(n)})^{\perp}$ whose height is minimum in some sense. More precisely, we introduce a height $h_{\max}(M)$ for any $\boldsymbol{Z}$-submodule M of $\boldsymbol{V}^{(n)}$ by the formula

$$h_{\max}(M) = \min_{B:\boldsymbol{Z}-basis\ of\ M}\max\{h(b); b\in B\}.$$

Our problem is to find a formula for $h_{\max}((\mathbf{K}_I^{(n)})^{\perp})$. As a preliminary we determine the $\boldsymbol{Z}$-rank $rank_{\boldsymbol{Z}}(\mathbf{K}_I^{(n)})^{\perp}$ of $(\mathbf{K}_I^{(n)})^{\perp}$.

THEOREM 4.23. *For any $I \subset [0,n]$, the rank of $(\mathbf{K}_I^{(n)})^{\perp}$ is given by*

$$rank_{\boldsymbol{Z}}\big(\mathbf{K}_I^{(n)}\big)^{\perp} = 2^n - \sum_{i \in I - \{0\}} 2^{i-1} - \#(I \cap \{0\}). \tag{4.8}$$

PROOF OF THEOREM 4.23. First we note the following.

LEMMA 4.23.1. *For any $\boldsymbol{Z}$-submodule M of $\boldsymbol{V}^{(n)}$, $i \geq 0$, we have*

(i) $rank_{\boldsymbol{Z}}(L(M)) = 2rank_{\boldsymbol{Z}}(M)$,
(ii) $rank_{\boldsymbol{Z}}(R(M)) = 2rank_{\boldsymbol{Z}}(M) - 1$.

PROOF OF LEMMA 4.23.1. By the definition of the operator L, we have $L(M) = E_{even}(M) \oplus E_{odd}(M)$. Hence the assertion (i) follows. On the other hand, the definition of the operator R implies that

$$R(M) = \big\{E_{even}(m) \oplus E_{odd}(m'); m,\ m' \in M \text{ and } w(m) - w(m') = 0\big\}.$$

Since the weight function w is $\boldsymbol{Z}$-linear, the assertion (ii) follows. This completes the proof of Lemma 4.23.1.

When $0 \notin I$, one can check easily the validity of Theorem 4.23 by induction on the number of elements of I, by using Lemma 4.23.1. When $0 \in I$, noting that the equality $(\mathbf{K}_I^{(n)})^{\perp} = \{v \in (\mathbf{K}_{I-\{0\}}^{(n)})^{\perp}; w(v) = 0\}$ holds, we see that the assertion (4.8) follows from the case $0 \notin I$. This completes the proof of Theorem 4.23. □

After these preliminaries, we prove the following.

THEOREM 4.24. *For any $n \geq 1$ and $I \subset [1,n]$, we have*

$$h_{\max}\Big(\big(\mathbf{K}_I^{(n)}\big)^{\perp}\Big) = 2^{\#(I)}.$$

When $0 \in I$, we have

$$h_{\max}\Big(\big(\mathbf{K}_I^{(n)}\big)^{\perp}\Big) = 2^{\#(I)-m}.$$

where $m = \max\{i; [0,i] \subset I\}$.

PROOF OF THEOREM 4.24. For any $\boldsymbol{Z}$-submodule M of $\boldsymbol{V}^{(n)}$, let

$$M_{(w,h)=(w_0,h_0)} = \{v \in M; w(v) = w_0,\ h(v) = h_0\} \subset M,$$

the subset of M consisting of elements with weight w_0 and height h_0. The crucial point is the following.

LEMMA 4.24.1. *Suppose* $I \subset [1,n]$. *Then* $(\mathbf{K}_I^{(n)})^\perp$ *is spanned by* $(\mathbf{E}_I^{(n)})_{(w,h)=(2^{\#(I)},2^{\#(I)})}$.

PROOF OF LEMMA 4.24.1. We prove this by induction on n. When $n=1$,

$$\big(\mathbf{K}_I^{(1)}\big)^\perp = \begin{cases} \langle [0],[1]\rangle_{\boldsymbol{Z}}, & \text{if } I=\varnothing, \\ \langle [0]+[1]\rangle_{\boldsymbol{Z}}, & \text{if } I=\{1\}, \end{cases}$$

hence the lemma holds. Assume that $n \geq 2$ and the lemma holds for k smaller than n. When $1 \notin I$, it follows from Proposition 4.1 that

$$\big(\mathbf{K}_I^{(n)}\big)^\perp = E_{even}\Big(\big(\mathbf{K}_{I-1}^{(n-1)}\big)^\perp\Big) \oplus E_{odd}\Big(\big(\mathbf{K}_{I-1}^{(n-1)}\big)^\perp\Big).$$

By the induction hypothesis $(\mathbf{K}_{I-1}^{(n-1)})^\perp$ is spanned by $(\mathbf{E}_{I-1}^{(n-1)})_{(w,h)=(2^{\#(I-1)},2^{\#(I-1)})}$. Noting that $\#(I-1)=\#(I)$, we see the assertion holds for n. Assume, on the other hand, that $1 \in I$. Then it follows from the proof of Proposition 4.3 that

$$\big(\mathbf{K}_I^{(n)}\big)^\perp = \coprod_w \Big(E_{even}\Big(\big(\mathbf{K}_{I-\{1\}-1}^{(n-1)}\big)^\perp(w)\Big) \oplus E_{odd}\Big(\big(\mathbf{K}_{I-\{1\}-1}^{(n-1)}\big)^\perp(w)\Big)\Big).$$

By the induction hypothesis, $(\mathbf{K}_{I-\{1\}-1}^{(n-1)})^\perp$ is spanned by $(\mathbf{E}_{I-\{1\}-1}^{(n-1)})_{(w,h)=(2^{\#(I-\{1\}-1)},2^{\#(I-\{1\}-1)})}$. Noting that $\#(I-\{1\}-1) = \#(I)-1$, we see that the assertion holds for $(\mathbf{K}_I^{(n)})^\perp$ too. This completes the proof of Lemma 4.24.1. □

Since the elements in $(\mathbf{E}_I^{(n)})_{(w,h)=(2^{\#(I)},2^{\#(I)})}$ is indecomposable by definition, the assertion of Theorem 4.24 for the case $I \subset [1,n]$ follows from Lemma 4.24.1. Furthermore when $I \cap \{0,1\} = \{0\}$, we have a height-preserving isomorphism $\iota_{1,-1}^{(n)} : (\mathbf{K}_I^{(n)})^\perp \to (\mathbf{K}_{I-\{0\}\cup\{1\}}^{(n)})^\perp$ (see Remark 4.5). Hence Theorem 4.24 holds true for this case too. For the remaining case when $\{0,1\} \subset I$, let $m = \max\{i; [0,i] \subset I\}$. For any $\boldsymbol{e} = e_1 \cdots e_m \in \{0,1\}^m$, let $E_{\boldsymbol{e}} : \boldsymbol{V}^{(i)} \to \boldsymbol{V}^{(i+m)}$ denote a map defined by

$$E_0 = E_{even}, \quad E_1 = E_{odd},$$
$$E_{\boldsymbol{e}} = E_{e_1} \circ \cdots \circ E_{e_m}.$$

Note that each $E_{\boldsymbol{e}}$ is a $\boldsymbol{Z}$-linear isomorphism onto its image. Furthermore, for any $b \in [0, 2^m-1]$, let $\boldsymbol{e}(b) \in \{0,1\}^m$ be the binary expansion of b, and let $E_b = E_{\boldsymbol{e}(b)}$. It follows from the definition that

$$\boldsymbol{V}^{(i+m)} = \bigoplus_{0 \leq b \leq 2^m-1} \big(E_b(\boldsymbol{V}^{(i)})\big), \tag{4.9}$$

the summands of which is orthogonal to each other.

LEMMA 4.24.2. *Suppose* $0 \in I$ *and let* $m = \max\{i; [0,i] \subset I\}$. *Then*

$$(\mathbf{K}_I^{(n)})^{\perp} = \bigoplus_{0 \le b \le 2^m - 1} \Big(E_b\Big((\mathbf{K}^{(n-m)}_{(I-[0,m-1])-m})^{\perp} \Big) \Big).$$

PROOF OF LEMMA 4.24.2. Note that for each $b \in [0, 2^m - 1]$, the associated map $E_b : \boldsymbol{V}^{(n-m)} \to \boldsymbol{V}^{(n)}$ induces a $\boldsymbol{Z}$-linear isomorphism

$$E_b : \big(\mathbf{K}^{(n-m)}_{(I-[0,m-1])-m}\big)^{\perp} \to \big(\mathbf{K}_I^{(n)}\big)^{\perp} \cap \big\langle [a]; L_{n,m}([a]) = [b] \big\rangle_{\boldsymbol{Z}}.$$

Therefore the decomposition (4.9) implies Lemma 4.24.2. □

Since $((I-[0,m-1])-m) \cap \{0,1\} = \{0\}$ by the definition of m, and the proposition is assured for such cases, Lemma 4.24.2 implies that $h_{\max}\big((\mathbf{K}_I^{(n)})^{\perp}\big) = 2^{\#(I)-m}$. Thus we finish the proof of Theorem 4.24. □

For $v = \sum_{a \in P^{(n)}} v_a[a] \in \boldsymbol{V}^{(n)}$, let $d(v) = \max\{|v_a|; a \in P^{(n)}\}$. Furthermore for any $\boldsymbol{Z}$-submodule M of $\boldsymbol{V}^{(n)}$, let $d_{\max}(M) = \min_{B:\boldsymbol{Z}-basis\ of\ M} \max\{d(b); b \in B\}$. An element $v = \sum_{a \in P^{(n)}} v_a[a] \in \boldsymbol{V}^{(n)}$ is said to be $\{0, \pm 1\}$-*vector* if $v_a \in \{0, \pm 1\}$, $a \in P^{(n)}$. The proof above gives the following.

COROLLARY 4.25. *For any* $I \subset [0,n]$, $(\mathbf{K}_I^{(n)})^{\perp}$ *is spanned by* $\{0, \pm 1\}$*-vectors. Therefore* $d_{\max}\big((\mathbf{K}_I^{(n)})^{\perp}\big) = 1$.

4.H. Pure sign-vectors and the minimum of ranks of $(\mathbf{K}_I^{(n)})^{\perp}$.

For any subset $I \subset [0,n]$, let $\mathbf{PureS}_I^{(n)} = \mathbf{S}_I^{(n)} - \bigcup_{J \supsetneq I} \mathbf{S}_J^{(n)}$ and call its elements *pure sign-vectors of type I.*

THEOREM 4.26. *For any* $n \ge 3$, *the minimum of ranks of* $(\mathbf{K}_I^{(n)})^{\perp}$ *such that* $\mathbf{S}_I^{(n)}$ *contains a primitive sign-vector is equal to* $2^{n-1}+2$, *and is attained by those sign-vectors in* $\mathbf{PureS}^{(n)}_{\{2,3,\ldots,n-1\}} \cup \mathbf{PureS}^{(n)}_{\{0,1,3,4,\ldots,n-1\}}$.

PROOF OF THEOREM 4.26. By Theorem 4.23 we have

$$rank\big(\mathbf{K}_I^{(n)}\big)^{\perp} = 2^n - \sum_{i \in I - \{0\}} 2^{i-1} - \#(I \cap \{0\}).$$

Furthermore it follows from Proposition 4.15 a sign-vector $S \in (\mathbf{K}_I^{(n)})^{\perp}$ is nonprimitive if

$$n \in I \ \text{ or } \ \{0, 1, \ldots, n-1\} \subset I. \tag{4.10}$$

Hence if we take aside those I satisfying (4.10), then the minimum of $rank_{\boldsymbol{Z}}(\mathbf{K}_I^{(n)})^{\perp}$ is attained when

$$I = [0, n-1] - \{0\} \ \text{ or } \ I = [0, n-1] - \{1\},$$

and the second minimum is attained when

$$I = [0, n-1] - \{0, 1\} \quad \text{or} \quad I = [0, n-1] - \{2\}.$$

When $I = [0, n-1] - \{0\}$, the number of elements $\#(\mathbf{S}^{(n)}_{[0,n-1]-\{0\}})$ is computed by Theorem 4.10 as follows.

$$\underline{1}\,\underline{1}\cdots\underline{1}\,1(x+x^{-1})\big|_{x=1} = (x^{2^n} + 2^{2^{n-1}} + x^{-2^n})\big|_{x=1} = 2^{2^{n-1}} + 2.$$

On the other hand, we have

$$\begin{aligned}\#\big(\mathbf{S}^{(n)}_{[0,n-1]}\big) &= 2^{2^{n-1}},\\ \#\big(\mathbf{S}^{(n)}_{[1,n]}\big) &= \underline{1}\,\underline{1}\cdots\underline{1}(x+x^{-1})\big|_{x=1} = (x^{2^n} + x^{-2^n})\big|_{x=1} = 2,\end{aligned}$$

hence it follows that

$$\#\big(\mathbf{PureS}^{(n)}_{[0,n-1]-\{0\}}\big) = \#\big(\mathbf{S}^{(n)}_{[0,n-1]-\{0\}}\big) - \#\big(\mathbf{S}^{(n)}_{[0,n-1]}\big) - \#\big(\mathbf{S}^{(n)}_{[1,n]}\big) = 0.$$

This means that $\mathbf{S}^{(n)}_{[0,n-1]-\{0\}} \subset \mathbf{S}^{(n)}_{[0,n-1]} \cup \mathbf{S}^{(n)}_{[1,n]}$. Thus it follows from Proposition 4.15 that no elements in $\mathbf{S}^{(n)}_{[0,n-1]-\{0\}}$ are primitive. As for $\mathbf{S}^{(n)}_{[0,n-1]-\{1\}}$, recall that the elements in $\mathbf{S}^{(n)}_{[0,n-1]-\{1\}}$ are obtained from those in $\mathbf{S}^{(n)}_{[0,n-1]-\{0\}}$ through the isomorphism $\iota^{(n)}_{1,-1}$, which is equivariant under the action of $2^{n-1} \in \boldsymbol{Z}/2^n\boldsymbol{Z}$. Thus it follows from Proposition 4.14 and the result for $\mathbf{S}^{(n)}_{[0,n-1]-\{0\}}$ that no elements in $\mathbf{S}^{(n)}_{[0,n-1]-\{1\}}$ are primitive. Hence we are reduced to showing that there exists a primitive sign-vector in $\mathbf{S}^{(n)}_{[0,n-1]-\{0,1\}} = \mathbf{S}^{(n)}_{[2,3,\ldots,n-1]}$. It follows from Theorem 4.10 that

$$\begin{aligned}\#\big(\mathbf{S}^{(n)}_{[2,3,\ldots,n-1]}\big) &= 1\,\underline{1}\,\underline{1}\cdots\underline{1}\,1(x+x^{-1})\big|_{x=1}\\ &= 1\,\underline{1}\,\underline{1}\cdots\underline{1}(x^2+2+x^{-2})\big|_{x=1}\\ &= 1(x^{2^{n-1}} + 2^{2^{n-2}} + x^{-2^{n-1}})\big|_{x=1}\\ &= (x^{2^{n-1}} + 2^{2^{n-2}} + x^{-2^{n-1}})^2\big|_{x=1}\\ &= (2^{2^{n-2}} + 2)^2\\ &= 2^{2^{n-1}} + 2^{2^{n-2}+2} + 2^2.\end{aligned}$$

Among the sign-vectors in $\mathbf{S}^{(n)}_{[2,3,\ldots,n-1]}$, the nonprimitive ones belong to either $\mathbf{S}^{(n)}_{[0,1,2,3,\ldots,n-1]}$, exclusively or $\mathbf{S}^{(n)}_{[2,3,\ldots,n-1,n]}$. The number of elements of the last two sets are given by

$$\#\big(\mathbf{S}^{(n)}_{[0,1,2,3,\dots,n-1]}\big) = 2^{2^{n-1}},$$

$$\#\big(\mathbf{S}^{(n)}_{[2,3,\dots,n-1,n]}\big) = 1\,\underline{1}\,\underline{1}\cdots\underline{1}(x+x^{-1})\big|_{x=1} = (x^{2^{n-1}}+x^{-2^{n-1}})^2\big|_{x=1} = 2^2,$$

hence there remains $2^{2^{n-2}+2}$ (>0) sign-vectors in $\mathbf{S}^{(n)}_{[2,3,\dots,n-1]}$. This completes the proof of Theorem 4.26. □

REMARK 4.27. As a typical element in $\mathbf{S}^{(n)}_{[2,3,\dots,n-1]}$, we can take

$$S = R_{1,n}([0]) + E_{odd}\Big(\sum_{0\le s\le 2^{n-2}-1}[s]-[s+2^{n-2}]\Big),$$

since $R_{1,n}([0]) \in \mathbf{K}^{(n)}_{\{0,1\}}$ and $E_{odd}\big(\sum_{0\le s\le 2^{n-2}-1}[s]-[s+2^{n-2}]\Big) \in \mathbf{K}^{(n)}_{\{n\}}$. More precisely the set $\mathbf{S}^{(n)}_{[2,3,\dots,n-1]}$ consists of the $2^{2^{n-2}+2}$ sign-vectors

$$R_{1,n}(\pm[0]) + E_{odd}\Big(\sum_{0\le s\le 2^{n-2}-1}\pm[s]-[s+2^{n-2}]\Big),$$

$$E_{even}\Big(\sum_{0\le s\le 2^{n-2}-1}\pm([s]-[s+2^{n-2}])\Big) + R_{1,n}(\pm[1]).$$

5. Hodge cycles on abelian varieties of 2-power type.

In this section, we describe how our combinatorial results that are obtained in the previous sections are translated into the ones about the structure of Hodge cycles on certain abelian varieties.

For an arbitrary positive integer n, let $G_n = \boldsymbol{Z}/2\boldsymbol{Z}\times\boldsymbol{Z}/2^n\boldsymbol{Z}$. Let K_n be a CM-field with $\mathrm{Gal}(K_n/\boldsymbol{Q}) \cong G_n$ such that the complex conjugation ρ corresponds to $(1,0)\in G_n$. Let $T\subset G_n$ be a CM-type and A_T the corresponding abelian variety with complex multiplication by K_n. Such an abelian variety is said to be *of 2-power type*. For any abelian variety A, let $Hg(A)$ denote its Hodge group. Then by [**4**] we know that

$$rank\,Hg(A_T) = \dim A_T - \#\{\chi\in\mathrm{Hom}(G_n,\boldsymbol{C}^*);\chi(\rho)=-1 \text{ and } \chi(\mathrm{T})=0\}. \tag{5.1}$$

For any CM-type $T\subset G_n$, let $S_T\in\mathbf{Sign}^{(n)}$ be the sign vector defined by

$$S_T = \sum_{a\in P(2)^{(n)}}\varepsilon_a[a], \text{ where } \varepsilon_a = \begin{cases} 1, & \text{if } (0,a)\in T,\\ -1, & \text{if } (1,a)\in T.\end{cases} \tag{5.2}$$

Conversely, for any $S=\sum_{a\in\boldsymbol{Z}/2^n\boldsymbol{Z}}s_a[a]\in\mathbf{Sign}^{(n)}$, let

$$T_S = \{(0,a)\in G_n; s_a=1\}\cup\{(1,a)\in G_n; s_a=-1\}\subset G_n.$$

Then T_S defines a CM-type for G_n. One can check that these correspondences are inverse to each other and hence define a bijection between $\mathbf{Sign}^{(n)}$ and the set of CM-types for G_n. Therefore for any $S \in \mathbf{Sign}^{(n)}$, we may write A_S for A_{T_S}. Note that for an odd character χ of G_n,

$$\chi(T) = 0 \text{ if and only if } \big(\chi\big|_{\boldsymbol{Z}/2^n\boldsymbol{Z}}\big)(S_T) = 0$$

where $\chi\big|_{\boldsymbol{Z}/2^n\boldsymbol{Z}}$ denotes the restriction of χ to the second factor of G_n. For any $S \in \mathbf{Sign}^{(n)}$, let $I_S \subset [0,n]$ denote the largest subset $I \subset [0,n]$ such that $S \in (\mathbf{K}_I^{(n)})^{\perp}$. Then it follows from (5.1) that

$$rankHg(A_S) = \dim A_S - rank_{\boldsymbol{Z}}\big(\mathbf{K}_{I_S}^{(n)}\big) = rank_{\boldsymbol{Z}}\big(\mathbf{K}_{I_S}^{(n)}\big)^{\perp}.$$

Furthermore we can determine the numbers h and N such that an abelian varieties of 2-power type is *h-degenerate* and *N-dominated*. We refer the reader for a precise definition of these notions to [**1**], [**2**]. Here we mention briefly on the role played by them for the study of the Hodge conjecture. If A is N-dominated, then the Hodge conjecture for all the self-products $A^k, k \geq 1$, is implied by the truth of the conjecture up to codimension N. On the other hand, if A is h-degenerate, then the Hodge conjecture for all the self-products $A^k, k \geq 1$, is implied by the truth of the conjecture for $A^k, k \leq h$. Now we have the following dictionary which translates various notions in the previous sections into the ones for abelian varieties of 2-power type (see [**2**], [**3**] for the relevance of this correspondence):

$$S \in \mathbf{Sign}^{(n)} \text{ is primitive} \tag{5.3}$$
$$\iff A_S \text{ is primitive.}$$

$$\text{There exists a nonempty subset } I \subset [0,n] \text{ such that } S \in \big(\mathbf{K}_I^{(n)}\big)^{\perp} \tag{5.4}$$
$$\iff A_S \text{ is degenerate.}$$

$$rankHg(A_S) = rank_{\boldsymbol{Z}}\big(\mathbf{K}_{I_S}^{(n)}\big)^{\perp}. \tag{5.5}$$

$$A_S \text{ is } d_{\max}\big(\mathbf{K}_{I_S}^{(n)}\big)\text{-degenerate.} \tag{5.6}$$

$$A_S \text{ is } h_{\max}\big(\mathbf{K}_{I_S}^{(n)}\big)/2\text{-dominated.} \tag{5.7}$$

Thus our results are paraphrased as follows.

THEOREM 5.1.

(i) *If A_S is degenerate, then A_S is always 1-degenerate.* (*See Corollary* 4.25.)
(ii) $rankHg(A_S) = 2^n - \displaystyle\sum_{i \in I_S - \{0\}} 2^{i-1} - \#(I_S \cap \{0\})$. (*See Theorem* 4.23.)
(iii) *When $0 \in I_S$, A_S is $2^{n-\#(I_S)}$-dominated.* (*See Theorem* 4.24.)
(iv) *When $0 \notin I_S$, A_S is $2^{n-\#(I_S)+m(I_S)}$-dominated, where $m(I_S) = \max\{i; [0,i] \subset [0,n] - I_S\}$.* (*See Theorem* 4.24.)

(v) *For any $n \geq 3$, the minimum of ranks of Hodge groups among those for primitive 2^n-dimensional abelian varieties of 2-power type is equal to $2^{n-1}+2$, and is attained by those sign vectors in* $\mathbf{PureS}^{(n)}_{\{2,3,\ldots,n-1\}}$. (*See Theorem* 4.26.)

REMARK 5.2. A theorem due to Lenstra says that every degenerate abelian variety with complex multiplication by an abelian CM-field has always a nondivisorial Hodge cycle [**5**, Theorem 3]. On the other hand, if the CM-field is not assumed to be abelian, this is not necessarily the case (see [**5**, Theorem 1]). Theorem 5.1 (i) strengthen Lenstra's theorem in the case of abelian varieties A of 2-power type by showing that every Hodge cycle on any of its selfproducts $A^n, n \geq 1$, is constructed essentially from those on A itself. In particular the validity of the Hodge conjecture for A implies that for all $A^n, n \geq 1$.

REMARK 5.3. Generally, for an arbitrary primitive N-dimensional abelian variety of CM-type, a lower bound for the rank of its Hodge group is given by $\log_2 N + 1$ (see [**4**, (3.5)]). Thus our minimum rank $2^{n-1}+2$ for primitive 2^n-dimensional abelian varieties of 2-power type is rather large, compared with general case.

EXAMPLE. Let $\zeta = \zeta_{32}$ be a primitive 32-nd root of unity and let $K = \boldsymbol{Q}(\zeta)$. Its Galois group $\mathrm{Gal}(K/\boldsymbol{Q})$ is isomorphic to $(\boldsymbol{Z}/32\boldsymbol{Z})^*$, and is generated by the classes of -1 and 5. Hence $\mathrm{Gal}(K/\boldsymbol{Q}) \cong \boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/8\boldsymbol{Z}$. The CM-type

$$\begin{aligned} T &= \{1,7,13,15,21,23,27,29\} \\ &= \{5^0,-5^2,5^7,-5^4,5^5,-5^6,-5^1,5^3\}, \end{aligned}$$

given in [**4**, (3.12)] as an example giving a simple degenerate abelian variety, is analyzed from our viewpoint as follows. The sign vector S_T which corresponds to T by (5.2) becomes

$$S_T = [0]-[4]-[2]-[6]-[1]+[5]+[3]+[7] \in \boldsymbol{V}^{(3)},$$

hence the maximal subset $I \subset [0,3]$ such that $S_T \in (\mathbf{K}^{(n)}_I)^{\perp}$ is easily found to be $I = \{0\}$. Hence for the corresponding abelian variety A_T, we have

(i) $\dim A_T = 8$,
(ii) $rankHg(A_T) = 7$,
(iii) A_T is 1-degenerate,
(iv) A_T is 4-dominated.

Another CM-type

$$\begin{aligned} T' &= \{1,7,9,11,13,15,27,29\} \\ &= \{5^0,-5^2,5^6,-5^5,5^7,-5^4,-5^1,5^3\} \end{aligned}$$

given in [**4**, (3.12)] is analyzed as follows. The corresponding sign vector $S_{T'}$ is equal to

$$S_{T'} = [0]-[4]-[2]+[6]-[1]-[5]+[3]+[7].$$

Hence the maximal subset $I' \subset [0,3]$ such that $S_{T'} \in (\mathbf{K}_{I'}^{(n)})^{\perp}$ is easily found to be $I' = \{0,1\}$. Hence for the corresponding abelian variety $A_{T'}$, we have

(i) $\dim A_{T'} = 8$,
(ii) $rank Hg(A_{T'}) = 6$,
(iii) $A_{T'}$ is 1-degenerate,
(iv) $A_{T'}$ is 2-dominated.

References

[1] F. Hazama, Hodge cycles on abelian varieties of S_n-type, J. Algebraic Geom., **9** (2000), 711–753.
[2] F. Hazama, On the kernels of the lowering operators for ranked posets, Far East J. Math. Sci., **3** (2001), 513–541.
[3] F. Hazama, Hodge cycles on abelian varieties with complex multiplication by cyclic CM-fields, J. Math. Sci. Univ. Tokyo, **10** (2003), 581–598.
[4] K. A. Ribet, Division fields of abelian varieties with complex multiplication, Mém. Soc. Math. Fr. (N.S.), **2** (1980), 75–94.
[5] S. P. White, Sporadic cycles on CM abelian varieties, Compositio Math., **88** (1993), 123–142.

Fumio Hazama
Department of Natural Sciences
College of Science and Engineering
Tokyo Denki University
Hatoyama, Saitama, 350-0394
Japan