BUCHSTABER INVARIANTS OF SKELETA OF A SIMPLEX

YUKIKO FUKUKAWA AND MIKIYA MASUDA

BUCHSTABER INVARIANTS OF SKELETA OF A SIMPLEX

YUKIKO FUKUKAWA AND MIKIYA MASUDA

ABSTRACT. A moment-angle complex $\mathcal{Z}_K$ is a compact topological space associated with a finite simplicial complex K. It is realized as a subspace of a polydisk $(D^2)^m$, where m is the number of vertices in K and D^2 is the unit disk of the complex numbers $\mathbb{C}$, and the natural action of a torus $(S^1)^m$ on $(D^2)^m$ leaves $\mathcal{Z}_K$ invariant. The Buchstaber invariant $s(K)$ of K is the maximum integer for which there is a subtorus of rank $s(K)$ acting on $\mathcal{Z}_K$ freely.

The story above goes over the real numbers $\mathbb{R}$ in place of $\mathbb{C}$ and a real analogue of the Buchstaber invariant, denoted $s_{\mathbb{R}}(K)$, can be defined for K and $s(K) \leqq s_{\mathbb{R}}(K)$. In this paper we will make some computations of $s_{\mathbb{R}}(K)$ when K is a skeleton of a simplex. We take two approaches to find $s_{\mathbb{R}}(K)$ and the latter one turns out to be a problem of integer linear programming and of independent interest.

1. Introduction

Davis and Januszkiewicz ([3]) initiated the study of topological analogue of toric geometry and introduced a compact topological space $\mathcal{Z}_K$ associated with a finite simplicial complex K. Then Buchstaber and Panov ([2]) intensively studied the topology of $\mathcal{Z}_K$ by realizing it in a polydisk $(D^2)^m$, where m is the number of vertices in K and D^2 is the unit disk of the complex numbers $\mathbb{C}$, and noted that $\mathcal{Z}_K$ is a deformation retract of the complement of the union of coordinate subspaces in $\mathbb{C}^m$ associated with K. They named $\mathcal{Z}_K$ a *moment-angle complex* associated with K. Although the construction of $\mathcal{Z}_K$ is simple, the topology of $\mathcal{Z}_K$ is complicated in general and the space $\mathcal{Z}_K$ is getting more attention of topologists, see [4].

Date: August 24, 2009.

2000 *Mathematics Subject Classification.* Primary 57S17; Secondary 90C10.

Key words and phrases. moment-angle complex, Buchstaber invariant, integer linear programming.

The second author was partially supported by Grant-in-Aid for Scientific Research 19204007.

The coordinatewise multiplication of a torus $(S^1)^m$ on $\mathbb{C}^m$, where S^1 is the unit circle of $\mathbb{C}$, leaves $\mathcal{Z}_K$ invariant. The action of $(S^1)^m$ on $\mathcal{Z}_K$ is not free but its restriction to a certain subtorus of $(S^1)^m$ can be free. The maximum integer $s(K)$ for which there is a subtorus of dimension $s(K)$ acting freely on $\mathcal{Z}_K$ is a combinatorial invariant and called the *Buchstaber invariant* of K. When K is of dimension $n-1$, $s(K) \leqq m-n$ and Buchstaber ([1], [2]) asked

Problem. *Find a combinatorial description of* $s(K)$.

If P is a simple convex polytope of dimension n, then its dual P^* is a simplicial polytope and the boundary ∂P^* of P^* is a simplicial complex of dimension $n-1$. The Buchstaber invariant $s(P)$ of P is then defined to be $s(\partial P^*)$. We note that $s(P) = m-n$, where m is the number of vertices of P^*, if and only if there is a quasitoric manifold over P. Although several inequalities are known among $s(P)$'s and one of them involves $s(K)$ for K a skeleton of a simplex (see [1, Theorem 6.6]), no substantial computation seems done for $s(P)$ and $s(K)$.

The story mentioned above goes over the real numbers $\mathbb{R}$ in place of $\mathbb{C}$. In this case, the moment-angle complex $\mathcal{Z}_K$ is replaced by a *real moment-angle complex* $\mathbb{R}\mathcal{Z}_K$ and the torus $(S^1)^m$ is replaced by a 2-torus $(S^0)^m$ where $S^0 = \{\pm 1\}$. Then a real analogue of the Buchstaber invariant can be defined for K, which we denote by $s_{\mathbb{R}}(K)$. Namely $s_{\mathbb{R}}(K)$ is the maximum integer for which there is a 2-subtorus of rank $s_{\mathbb{R}}(K)$ acting freely on $\mathbb{R}\mathcal{Z}_K$. The complex conjugation on $\mathbb{C}$ induces an involution on $\mathcal{Z}_K$ with $\mathbb{R}\mathcal{Z}_K$ as the fixed point set and this implies that $s(K) \leqq s_{\mathbb{R}}(K)$.

In this paper we make some computations of $s_{\mathbb{R}}(K)$ when K is a skeleton of a simplex. Let Δ_r^{m-1} be the r-skeleton of the $(m-1)$-simplex. Then it follows from the definition of $\mathbb{R}\mathcal{Z}_K$ (see [2, p.98]) that

$$\mathbb{R}\mathcal{Z}_{\Delta^{m-1}_{m-p-1}} = \bigcup (D^1)^{m-p} \times (S^0)^p \subset (D^1)^m \tag{1.1}$$

where D^1 is the interval $[-1,1]$ in $\mathbb{R}$ so that S^0 is the boundary of D^1 and the union is taken over all $m-p$ products of D^1 in $(D^1)^m$. We denote the invariant $s_{\mathbb{R}}(\Delta^{m-1}_{m-p-1})$ simply by $s_{\mathbb{R}}(m,p)$. The moment-angle complex $\mathbb{R}\mathcal{Z}_{\Delta^{m-1}_{m-p-1}}$ is sitting in the complement $U_{\mathbb{R}}(m,p)$ of the union of all coordinate subspaces of dimension $p-1$ in $\mathbb{R}^m$ and $s_{\mathbb{R}}(m,p)$ may be thought of as the maximal integer for which there is a 2-subtorus of rank $s_{\mathbb{R}}(m,p)$ acting freely on $U_{\mathbb{R}}(m,p)$.

We easily see $s_{\mathbb{R}}(m,0) = 0$ and assume $p \geqq 1$. We take two approaches to find $s_{\mathbb{R}}(m,p)$ and here is a summary of the results obtained from the first approach developed in Section 2.

Theorem. *Let $1 \leqq p \leqq m$.*

(1) *$1 \leqq s(m,p) \leqq p$ and $s_{\mathbb{R}}(m,p) = p$ if and only if $p = 1, m-1, m$.*
(2) *$s(m,p)$ increases as p increases but decreases as m increases.*
(3) *If $m-p$ is even, then $s_{\mathbb{R}}(m,p) = s_{\mathbb{R}}(m+1,p)$.*
(4) *$s_{\mathbb{R}}(m+1,m-2) = s_{\mathbb{R}}(m,m-2) = [m-\log_2(m+1)]$ for $m \geqq 3$, where $[r]$ for a real number r denotes the greatest integer less than or equal to r.*

It seems difficult to find a computable description of $s_{\mathbb{R}}(m,p)$ in terms of m and p in general. From Section 3 we take another approach to find $s_{\mathbb{R}}(m,p)$, that is, we investigate values of m and p for which $s_{\mathbb{R}}(m,p)$ is a given positive integer k. It turns out that $s_{\mathbb{R}}(m,p) = 1$ if and only if $m \geqq 3p-2$ (Theorem 3.1) and that there is a non-negative integer $m_k(b)$ associated to integers $k \geqq 2$ and $b \geqq 0$ such that

$$s_{\mathbb{R}}(m,p) = k \text{ if and only if } m_{k+1}(p-1) < m \leqq m_k(p-1).$$

Therefore, finding $s_{\mathbb{R}}(m,p)$ is equivalent to finding $m_k(p-1)$ for all k. In fact, $m_k(b)$ is the maximum integer which the linear function $\sum_{v\in(\mathbb{Z}/2)^k\backslash\{0\}} a_v$ takes on lattice points (a_v) in $\mathbb{R}^{2^k-1}$ satisfying these (2^k-1) inequalities

$$\sum_{(u,v)=0} a_v \leqq b \quad \text{for each } u \in (\mathbb{Z}/2)^k\backslash\{0\}$$

and $a_v \geqq 0$ for every v, where $\mathbb{Z}/2 = \{0,1\}$ and $(\ ,\ )$ denotes the standard scalar product on $(\mathbb{Z}/2)^k$. Finding $m_k(b)$ is a problem of integer linear programming and of independent interest. Here is one of the main results on $m_k(b)$.

Theorem (Theorem 7.6)**.** *Let $b = (2^{k-1}-1)Q + R$ with non-negative integers Q, R with $0 \leqq R \leqq 2^{k-1}-2$. We may assume that $2^{k-1} - 2^{k-1-\ell} \leqq R \leqq 2^{k-1} - 2^{k-1-(\ell+1)}$ for some $0 \leqq \ell \leqq k-2$. Then*

$$(2^k-1)Q + R + 2^{k-1} - 2^{k-1-\ell} \leqq m_k(b) \leqq (2^k-1)Q + 2R,$$

and the lower bound is attained if and only if $R - (2^{k-1} - 2^{k-1-\ell}) \leqq k-\ell-2$ and the upper bound is attained if and only if $R = 2^{k-1} - 2^{k-1-\ell}$.

More explicit values of $m_k(b)$ can be found in Sections 5 and 6. All of our computations support a conjecture that

$$m_k((2^{k-1}-1)Q + R) = (2^k-1)Q + m_k(R)$$

would hold for any Q and R. This is equivalent to $m_k(b + 2^{k-1} - 1) = m_k(b) + 2^k - 1$ for any b and we prove in Section 9 that the latter identity holds when b is large.

2. Some properties and computations of $s_{\mathbb{R}}(m,p)$

In this section we translate our problem to a problem of linear algebra, deduce some properties of $s_{\mathbb{R}}(m,p)$ and make some computations of $s_{\mathbb{R}}(m,p)$.

The real moment-angle complex $\mathbb{R}\mathcal{Z}_{\Delta^{m-1}_{m-p-1}}$ in (1.1) with $p=0$ is the disk $(D^1)^m$. Since the action of $(S^0)^m$ on $(D^1)^m$ has a fixed point, that is the origin, we have

$$s_{\mathbb{R}}(m,0)=0. \tag{2.1}$$

Another extreme case is when $p=m$. Since $\mathbb{R}\mathcal{Z}_{\Delta^{m-1}_{m-p-1}}$ in (1.1) with $p=m$ is $(S^0)^m$, we have

$$s_{\mathbb{R}}(m,m)=m. \tag{2.2}$$

In the following we assume $p\geqq 1$.

Lemma 2.1. *Let $A=(\mathbf{a}_1,\dots,\mathbf{a}_m)$ be a $k\times m$ matrix with entries in $\mathbb{Z}/2$ and let $\rho_A\colon (S^0)^k\to (S^0)^m$ be a homomorphism defined by $\rho_A(g)=(g^{\mathbf{a}_1},\dots,g^{\mathbf{a}_m})$, where $g^{\mathbf{a}}=\prod_{i=1}^k g_i^{a^i}$ for $g=(g_1,\dots,g_k)\in (S^0)^k$ and a column vector $\mathbf{a}=(a^1,\dots,a^k)^T$ in $(\mathbb{Z}/2)^k$. Then the action of $(S^0)^k$ on $\mathbb{R}\mathcal{Z}_{\Delta^{m-1}_{m-p-1}}$ in (1.1) through ρ is free if and only if any p column vectors in A span $(\mathbb{Z}/2)^k$.*

Proof. The action of $(S^0)^k$ on $\mathbb{R}\mathcal{Z}_{\Delta^{m-1}_{m-p-1}}$ through ρ_A leaves each subspace $(D^1)^{m-p}\times(S^0)^p$ in (1.1) invariant and the action on $\mathbb{R}\mathcal{Z}_{\Delta^{m-1}_{m-p-1}}$ is free if and only if it is free on each $(D^1)^{m-p}\times(S^0)^p$. The latter is equivalent to the action being free on each $\{0\}\times(S^0)^p$ and this is equivalent to ρ composed with the projection from $(S^0)^m$ onto $(S^0)^p$ being injective. This is further equivalent to a matrix formed from any p column vectors in A being of full rank (that is k), which is equivalent to the last statement in the lemma. □

Since any rank k subgroup of $(S^0)^m$ is obtained as $\rho_A((S^0)^k)$ for some A in Lemma 2.1, Lemma 2.1 implies

Corollary 2.2. *The invariant $s_{\mathbb{R}}(m,p)$ is the maximum integer k for which there exists a $k\times m$ matrix A with entries in $\mathbb{Z}/2$ such that any p column vectors in A span $(\mathbb{Z}/2)^k$.*

Here are some properties of $s_{\mathbb{R}}(m,p)$.

Proposition 2.3.
1. *$1\leqq s_{\mathbb{R}}(m,p)\leqq p$ for $p\geqq 1$. In particular, $s_{\mathbb{R}}(m,1)=1$.*
2. *$s_{\mathbb{R}}(m,p)\leqq s_{\mathbb{R}}(m,p')$ if $p\leqq p'$.*
3. *$s_{\mathbb{R}}(m,p)\geqq s_{\mathbb{R}}(m',p)$ if $m\leqq m'$.*

Proof. The inequality (1) is obvious from Corollary 2.2 and the inequality (2) follows from the fact that if $p' \geqq p$, then $\mathbb{R}\mathcal{Z}_{\Delta^{m-1}_{m-p-1}}$ in (1.1) contains $\mathbb{R}\mathcal{Z}_{\Delta^{m-1}_{m-p'-1}}$ as an invariant subspace.

Let $m' \geqq m$ and set $k = s_{\mathbb{R}}(m', p)$. Then there is a $k \times m'$ matrix A' with entries $\mathbb{Z}/2$ such that any p column vectors in A' span $(\mathbb{Z}/2)^k$. Let A be a $k \times m$ matrix formed from arbitrary m column vectors in A'. Since any p column vectors in A span $(\mathbb{Z}/2)^k$, it follows from Corollary 2.2 that $s_{\mathbb{R}}(m,p) \geqq k = s_{\mathbb{R}}(m',p)$. □

We denote by $\{\mathbf{e}_1, \dots, \mathbf{e}_k\}$ the standard basis of $(\mathbb{Z}/2)^k$.

Theorem 2.4. *$s_{\mathbb{R}}(m, m-1) = m-1$ for $m \geqq 2$.*

Proof. We have $s_{\mathbb{R}}(m, m-1) \leqq m-1$ by Proposition 2.3 (1). On the other hand, any $m-1$ column vectors in an $(m-1)\times m$ matrix $A = (\mathbf{e}_1, \dots, \mathbf{e}_{m-1}, \sum_{i=1}^{m-1}\mathbf{e}_i)$ span $(\mathbb{Z}/2)^{m-1}$, so $s_{\mathbb{R}}(m, m-1) \geqq m-1$ by Lemma 2.1. □

If A is a $k\times m$ matrix with entries in $\mathbb{Z}/2$ which realizes $s_{\mathbb{R}}(m,p) = k$, then A must be of full rank (that is k); so we may assume that the first k column vectors in A are linearly independent if necessary by permuting columns and moreover that they are $\mathbf{e}_1, \dots, \mathbf{e}_k$ by multiplying A by an invertible matrix of size k from the left.

Lemma 2.5. *$s_{\mathbb{R}}(m,p) \leqq p-1$ when $2 \leqq p \leqq m-2$.*

Proof. Since $s_{\mathbb{R}}(m,p) \leqq p$ by Proposition 2.3 (1), it suffices to prove that $s_{\mathbb{R}}(m,p) \neq p$ when $2 \leqq p \leqq m-2$. Suppose $s_{\mathbb{R}}(m,p) = p$ and let A be a $p \times m$ matrix $(\mathbf{e}_1, \dots, \mathbf{e}_p, \mathbf{a}_{p+1}, \dots, \mathbf{a}_m)$ which realizes $s_{\mathbb{R}}(m,p) = p$. Then all $\mathbf{a}_j$'s for $j = p+1, \dots, m$ must be equal to $\sum_{i=1}^{p}\mathbf{e}_i$ because any $p-1$ vectors from $\mathbf{e}_1, \dots, \mathbf{e}_p$ together with one $\mathbf{a}_j$ span $(\mathbb{Z}/2)^p$. The number of $\mathbf{a}_j$'s is more than one as $p \leqq m-2$, so p column vectors in A containing more than one $\mathbf{a}_j$ do not span $(\mathbb{Z}/2)^p$, which is a contradiction. □

Theorem 2.6. *If $m-p$ is even, then $s_{\mathbb{R}}(m,p) = s_{\mathbb{R}}(m+1,p)$.*

Proof. When $p = 0$ or 1, $s_{\mathbb{R}}(m,p) = p$ for any m by (2.1) and Proposition 2.3 (1). When $p = m$, the theorem also holds by (2.2) and Theorem 2.4. Therefore we assume that $2 \leqq p \leqq m-1$ and $m-p$ is even in the following.

Set $s_{\mathbb{R}}(m,p) = k$. Since $m-p$ is even and positive, $k \leqq p-1$ by Lemma 2.5. Let $A = (\mathbf{e}_1, \dots, \mathbf{e}_k, \mathbf{a}_{k+1}, \dots, \mathbf{a}_m)$ be a $k \times m$ matrix which realizes $s_{\mathbb{R}}(m,p) = k$. We denote the i-th row of a $k \times (m-k)$

submatrix $(\mathbf{a}_{k+1},\dots,\mathbf{a}_m)$ by $\mathbf{a}^i$ and the number of 1 in $\mathbf{a}^i$ by $\#\mathbf{a}^i$ for $i=1,\dots,k$. Then we set

$$s^i := \begin{cases} 1 & \text{if } \#\mathbf{a}^i \text{ is even,} \\ 0 & \text{if } \#\mathbf{a}^i \text{ is odd,} \end{cases} \tag{2.3}$$

and define a column vector $\mathbf{s}\in(\mathbb{Z}/2)^k$ to be the transpose of $(s^1,\dots,s^k)$.

Claim. Any p column vectors in a $k\times(m+1)$ matrix $(A,\mathbf{s})$ span $(\mathbb{Z}/2)^k$.

The Claim implies that $s_{\mathbb{R}}(m+1,p)\geqq k$ while $k=s_{\mathbb{R}}(m,p)\geqq s_{\mathbb{R}}(m+1,p)$ by Proposition 2.3 (3). Therefore it suffices to prove the Claim to establish the theorem. The rest of the proof is devoted to the proof of the Claim.

Choose any p column vectors in $(A,\mathbf{s})$. If the vector $\mathbf{s}$ is not contained in the chosen p column vectors, then the p column vectors span $(\mathbb{Z}/2)^k$ because they are column vectors in A and A realizes $s_{\mathbb{R}}(m,p)=k$. Thus we may assume that the chosen p column vectors contain $\mathbf{s}$, so the other chosen vectors are $k-q$ ones from $\mathbf{e}_1,\dots,\mathbf{e}_k$ and $p-k+q-1$ ones from $\mathbf{a}_{k+1},\dots,\mathbf{a}_m$ for some q. Without loss of generality we may assume that they are $\mathbf{e}_{q+1},\dots,\mathbf{e}_k$ and $\mathbf{a}_{k+1},\dots,\mathbf{a}_{p+q-1}$. If these $p-1$ vectors span $(\mathbb{Z}/2)^k$, we have nothing to do. So we may assume that they do not span $(\mathbb{Z}/2)^k$.

For an element $\mathbf{a}\in(\mathbb{Z}/2)^k$, we denote by $\mathbf{a}(q)$ the element of $(\mathbb{Z}/2)^q$ whose entries are the first q entries of $\mathbf{a}$. Note that $\mathbf{a}_{k+1}(q),\dots,\mathbf{a}_{p+q-1}(q)$ do not span $(\mathbb{Z}/2)^q$ because $\mathbf{e}_{q+1},\dots,\mathbf{e}_k,\mathbf{a}_{k+1},\dots,\mathbf{a}_{p+q-1}$ do not span $(\mathbb{Z}/2)^k$. However,

$$\mathbf{e}_{q+1},\dots,\mathbf{e}_k,\mathbf{a}_{k+1},\dots,\mathbf{a}_{p+q-1} \text{ and one } \mathbf{e}_i\ (1\leqq i\leqq q) \text{ span } (\mathbb{Z}/2)^k \tag{2.4}$$

because the number of those vectors is p and A realizes $s_{\mathbb{R}}(m,p)=k$. These mean that $\mathbf{a}_{k+1}(q),\dots,\mathbf{a}_{p+q-1}(q)$ span a codimension 1 subspace of $(\mathbb{Z}/2)^q$, denoted by W. So there is a (unique) normal vector $\mathbf{n}\in(\mathbb{Z}/2)^q$ to W with respect to the standard scalar product $(\ ,\ )$ on $(\mathbb{Z}/2)^q$. Since each $\mathbf{e}_i(q)$ for $i=1,\dots,q$ is not contained in W by (2.4), $(\mathbf{n},\mathbf{e}_i(q))\neq 0$, that is 1, since we are working over $\mathbb{Z}/2$. This means that all entries in $\mathbf{n}$ must be 1. It follows that $\#\mathbf{a}_j(q)$ is even for $k+1\leqq j\leqq p+q-1$ because $(\mathbf{n},\mathbf{a}_j(q))=0$.

Similarly, $\mathbf{e}_{q+1},\dots,\mathbf{e}_k,\mathbf{a}_{k+1},\dots,\mathbf{a}_{p+q-1}$ together with one $\mathbf{a}_\ell$ for $p+q\leqq\ell\leqq m$ span $(\mathbb{Z}/2)^k$, so $\mathbf{a}_{k+1}(q),\dots,\mathbf{a}_{p+q-1}(q)$ together with $\mathbf{a}_\ell(q)$ span $(\mathbb{Z}/2)^q$. This implies that $\#\mathbf{a}_\ell(q)$ must be odd because $\#\mathbf{a}_j(q)$'s for $k+1 \leqq j \leqq p+q-1$ are all even. Consequently

$$\sum_{j=k+1}^{m} \#\mathbf{a}_j(q) \equiv m-(p+q-1) \equiv q+1 \pmod 2 \tag{2.5}$$

where we used the assumption that $m-p$ is even at the second congruence.

We denote the i-th row of a submatrix $(\mathbf{a}_{k+1}(q), \dots, \mathbf{a}_{p+q-1}(q))$ by $\mathbf{b}^i$ for $i = 1, \dots, q$ and set

$$\mathbf{c}^i := (\mathbf{b}^i, s^i).$$

We note that $\mathbf{e}_{q+1}, \dots, \mathbf{e}_k, \mathbf{a}_{k+1}, \dots, \mathbf{a}_{p+q-1}, \mathbf{s}$ span $(\mathbb{Z}/2)^k$ if and only if $\mathbf{a}_{k+1}(q), \dots, \mathbf{a}_{p+q-1}(q), \mathbf{s}(q)$ span $(\mathbb{Z}/2)^q$ and the latter is equivalent to the matrix

$$(\mathbf{a}_{k+1}(q), \dots, \mathbf{a}_{p+q-1}(q), \mathbf{s}(q)) = \begin{pmatrix} \mathbf{b}^1 & s^1 \\ \mathbf{b}^2 & s^2 \\ \vdots & \vdots \\ \mathbf{b}^q & s^q \end{pmatrix} = \begin{pmatrix} \mathbf{c}^1 \\ \mathbf{c}^2 \\ \vdots \\ \mathbf{c}^q \end{pmatrix}$$

being of full rank (that is q). Therefore, it suffices to show that the q row vectors $\mathbf{c}^1, \dots, \mathbf{c}^q$ are linearly independent. It follows from (2.4) that $\mathbf{a}_{k+1}(q), \dots, \mathbf{a}_{p+q-1}(q)$ together with one $\mathbf{e}_i(q)$ span $(\mathbb{Z}/2)^k$, which means that the matrix

$$(\mathbf{a}_{k+1}(q), \dots, \mathbf{a}_{p+q-1}(q), \mathbf{e}_i(q)) = \begin{pmatrix} \mathbf{b}^1 & 0 \\ \vdots & \vdots \\ \mathbf{b}^i & 1 \\ \vdots & \vdots \\ \mathbf{b}^q & 0 \end{pmatrix}$$

is of full rank and hence $\mathbf{b}^1, \dots, \mathbf{b}^{i-1}, \mathbf{b}^{i+1}, \dots, \mathbf{b}^q$ are linearly independent. Since this holds for any $1 \leqq i \leqq q$, any $q-1$ vectors from $\mathbf{b}^1, \dots, \mathbf{b}^q$ are linearly independent. In particular, any $p-1$ vectors from $\mathbf{c}^1, \dots, \mathbf{c}^q$ are linearly independent.

In the sequel, in order to prove that $\mathbf{c}^1, \dots, \mathbf{c}^q$ are linearly independent, it suffices to prove that $\sum_{i=1}^q \mathbf{c}^i$ is non-zero. Suppose that it is zero. Then $\sum_{i=1}^q s^i = 0$ in $\mathbb{Z}/2$. Therefore the number of s^i's equal to 1 is even, say $2r$, so the number of s^i's equal to 0 is $q-2r$. It follows from (2.3) that

$$\sum_{i=1}^{q} \#\mathbf{a}^i \equiv q-2r \equiv q \pmod 2 \tag{2.6}$$

which cotradcits (2.5) because $\mathbf{a}^i$'s ($1 \leqq i \leqq q$) are the row vectors of $(\mathbf{a}_{k+1}(q), \dots, \mathbf{a}_m(q))$ and hence $\sum_{j=k+1}^m \#\mathbf{a}_j(q) = \sum_{i=1}^q \#\mathbf{a}^i$. Thus $\sum_{i=1}^q \mathbf{c}^i$ is non-zero, completing the proof of the theorem. □

If we take $p = m-2 \geqq 4$ in Lemma 2.5, we have $s_{\mathbb{R}}(m, m-2) \leqq m-3$ for $m \geqq 4$. In fact, $s_{\mathbb{R}}(m, m-2)$ is given as follows.

Theorem 2.7. $s_{\mathbb{R}}(m+1, m-2) = s_{\mathbb{R}}(m, m-2) = [m - \log_2(m+1)]$ *for* $m \geqq 3$.

Proof. The first identity follows from Theorem 2.6, so it suffices to prove the second identity.

Set $s_{\mathbb{R}}(m, m-2) = k$ and let $A = (\mathbf{e}_1, \dots, \mathbf{e}_k, \mathbf{a}_{k+1}, \dots, \mathbf{a}_m)$ be a matrix which realizes $s_{\mathbb{R}}(m, m-2) = k$. Then any $m-2$ column vectors in A span $(\mathbb{Z}/2)^k$. This means that for each $i = 1, \dots, k$ the set

$$A(i) := \{\ell \mid \text{the } i\text{-th component of } \mathbf{a}_\ell \text{ is } 1\} \subset \{k+1, \dots, m\}$$

contains at least two elements because if $A(i)$ consists of only one element, say ℓ, for some i, then the $m-2$ column vectors in A except $\mathbf{e}_i$ and $\mathbf{a}_\ell$ will not generate a vector with 1 at the i-th component. Another constraint on $A(i)$'s is that they are mutually distinct because if $A(i) = A(j)$ for some i and j in $\{1, \dots, k\}$, then $m-2$ column vectors in A except $\mathbf{e}_i$ and $\mathbf{e}_j$ will not generate $\mathbf{e}_i$ and $\mathbf{e}_j$. Conversely, if $A(i)$ contains at least two elements for each i and $A(i)$'s are mutually distinct, then any $m-2$ column vectors in A span $(\mathbb{Z}/2)^k$.

The number of subsets of $\{k+1, \dots, m\}$ which contain at least two elements is given by

$$\sum_{n=2}^{m-k} \binom{m-k}{n} = 2^{m-k} - 1 - m + k.$$

Since the number of $A(i)$'s is k, the argument above shows that k should be the maximum integer which satisfies

$$k \leqq 2^{m-k} - 1 - m + k, \quad \text{i.e.,} \quad k \leqq m - \log_2(m+1).$$

This proves the theorem. □

3. Another approach to compute $s_{\mathbb{R}}(m, p)$

We know $s_{\mathbb{R}}(m, p) = p$ when $p = 0, 1$. So we will assume $p \geqq 2$ in the following. It seems difficult to find a computable description of $s_{\mathbb{R}}(m, p)$ in terms of m and p in general. Hereafter we take a different approach to find values of $s_{\mathbb{R}}(m, p)$ for $p \geqq 2$, i.e. we find values of m and p for which $s_{\mathbb{R}}(m, p)$ is a given positive integer k. We begin with

Theorem 3.1. *$s_{\mathbb{R}}(m,p)=1$ if and only if $m \geqq 3p-2$, in other words, $s_{\mathbb{R}}(m,p)\geqq 2$ if and only if $m\leqq 3(p-1)$.*

Proof. Since $s_{\mathbb{R}}(m,p)$ decreases as m increases by Proposition 2.3 (3), it suffices to show

(1) $s_{\mathbb{R}}(3(p-1),p)\geqq 2$, and
(2) $s_{\mathbb{R}}(3p-2,p)=1$.

Proof of (1). Let A be a $2\times 3(p-1)$ matrix formed from $p-1$ copies of $(\mathbf{e}_1,\mathbf{e}_2,\mathbf{e}_1+\mathbf{e}_2)$. Then any p column vectors in A span $(\mathbb{Z}/2)^2$, which means $s_{\mathbb{R}}(3(p-1),p)\geqq 2$.

Proof of (2). Suppose that $s_{\mathbb{R}}(3p-2,p)\geqq 2$. Then there is a $2\times(3p-2)$ matrix A such that any p column vectors in A span $(\mathbb{Z}/2)^2$. Let $\mathbf{e}_i$ (resp. $\mathbf{e}_1+\mathbf{e}_2$) appear a_i (resp. a_{12}) times in A. Then

$$a_1+a_2+a_{12}=3p-2 \tag{3.1}$$

and inequalities

$$a_i\leqq p-1 \quad \text{for } i=1,2 \qquad \text{and} \qquad a_{12}\leqq p-1$$

must be satisfied for any p column vectors in A to span $(\mathbb{Z}/2)^2$. These inequalities imply that $a_1+a_2+a_{12}\leqq 3p-3$ which contradicts (3.1). □

The above argument can be developed for general values of k with $s_{\mathbb{R}}(m,p)\geqq k$. Let $(\ ,\ )$ be the standard bilinear form on $(\mathbb{Z}/2)^k$. Since it is non-degenerate, the correspondence

$$(\mathbb{Z}/2)^k \to \mathrm{Hom}((\mathbb{Z}/2)^k,\mathbb{Z}/2) \quad \text{given by } u\to(u,\ ) \tag{3.2}$$

is an isomorphism.

Lemma 3.2. *If $u\in(\mathbb{Z}/2)^k$ is non-zero, then the kernel of $(u,\ )$ is a codimension 1 subspace of $(\mathbb{Z}/2)^k$. On the other hand, any codimension 1 subspace V of $(\mathbb{Z}/2)^k$ is obtained as the kernel of $(u,\ )$ for some non-zero $u\in(\mathbb{Z}/2)^k$ and u is uniquely determined by V.*

Proof. The former statement in the lemma follows from the fact that the bilinear form $(\ ,\ )$ is non-degenerate. Let V be a codimension 1 subspace of $(\mathbb{Z}/2)^k$. Then the quotient vector space of $(\mathbb{Z}/2)^k$ by V is one-dimensional, so it is isomorphic to $\mathbb{Z}/2$ and hence defines an element of $\mathrm{Hom}((\mathbb{Z}/2)^k,\mathbb{Z}/2)$ whose kernel is V. This together with (3.2) implies the latter statement in the lemma. □

Lemma 3.3. *Suppose $k\geqq 2$. Then $s_{\mathbb{R}}(m,p)\geqq k$ if and only if there is a set of non-negative integers $\{a_v \mid v\in(\mathbb{Z}/2)^k\backslash\{0\}\}$ with $\sum a_v=m$,* *which satisfy the following* (2^k-1) *inequalities*

$$\sum_{(u,v)=0} a_v \leqq p-1 \quad \textit{for each } u \in (\mathbb{Z}/2)^k \backslash \{0\}.$$

Proof. Any codimension 1 subspace of $(\mathbb{Z}/2)^k$ is the kernel of a homomorphism $(u,\ )\colon (\mathbb{Z}/2)^k \to \mathbb{Z}/2$ for some non-zero $u \in (\mathbb{Z}/2)^k$ by Lemma 3.2. Therefore any p column vectors in a $k \times m$ matrix with a_v numbers of column vector v for each v span $(\mathbb{Z}/2)^k$ if and only if the a_v's satisfy the inequalities in the lemma. This proves the lemma. □

The lemma above shows that our problem is a problem of *integer* linear programming. If we consider the problem over real numbers, then it is easy to find the solution of the problem as shown by the following lemma.

Lemma 3.4. *Suppose that* $k \geqq 2$ *and let* b *be a real number. If we allow* a_v*'s to be real numbers and* a_v*'s satisfy the following* (2^k-1) *inequalities*

$$\sum_{(u,v)=0} a_v \leqq b \quad \textit{for each } u \in (\mathbb{Z}/2)^k \backslash \{0\}, \tag{3.3}$$

then the linear function $\sum a_v$ *on* $\mathbb{R}^{2^k-1}$ *takes the maximum value*

$$(2^k-1)b/(2^{k-1}-1)$$

at a unique point $x=(a_v) \in \mathbb{R}^{2^k-1}$ *with* $a_v = b/(2^{k-1}-1)$ *for every* v.

Proof. Each a_v appears in exactly $(2^{k-1}-1)$ times in the inequalities (3.3) because there are exactly $(2^{k-1}-1)$ numbers of $u \in (\mathbb{Z}/2)^k\backslash\{0\}$ such that $(u,v)=0$. Therefore, taking sum of the (2^k-1) inequalities (3.3) over $u \in (\mathbb{Z}/2)^k\backslash\{0\}$, we obtain

$$(2^{k-1}-1)\sum a_v \leqq (2^k-1)b$$

and the equality is attained at the point x in the lemma; so the maximum value of $\sum a_v$ satisfying (3.3) is $(2^k-1)b/(2^{k-1}-1)$.

We shall observe that the maximum value $(2^k-1)b/(2^{k-1}-1)$ is attained only at the point x. Suppose that $\sum a_v$ takes the maximum value on a_v's satisfying (3.3). Then the argument above shows that all the inequalities in (3.3) must be equalities, i.e.

$$\sum_{(u,v)=0} a_v = b \quad \text{for each } u \in (\mathbb{Z}/2)^k \backslash \{0\}. \tag{3.4}$$

We choose one v arbitrarily and take sum of (3.4) over all non-zero u's with $(u,v)=0$. The number of such u is $2^{k-1}-1$, so a_v appears

$2^{k-1}-1$ times in the sum. But $a_{v'}$ with $v' \neq v$ appears $2^{k-2}-1$ times in the sum because the number of non-zero u with $(u,v)=(u,v')=0$ is $2^{k-2}-1$. Therefore we obtain

$$(2^{k-1}-1)a_v + (2^{k-2}-1)\sum_{v'\neq v} a_{v'} = (2^{k-1}-1)b. \tag{3.5}$$

Here

$$\sum_{v'\neq v} a_{v'} = (2^k-1)b/(2^{k-1}-1) - a_v \tag{3.6}$$

since $\sum_v a_v$ is assumed to take the maximum value $(2^k-1)b/(2^{k-1}-1)$. Plugging (3.6) in (3.5), we obtain

$$2^{k-2}a_v + (2^{k-2}-1)\frac{(2^k-1)b}{(2^{k-1}-1)} = (2^{k-1}-1)b$$

and a simple computation shows $a_v = b/(2^{k-1}-1)$. □

Lemma 3.4 tells us that the point x is a unique vertex of the polyhedron $P(b)$ defined by the inequalities (3.3) and (2^k-1) hyperplanes $\sum_{(u,v)=0} a_v = b$ in $\mathbb{R}^{2^k-1}$ $(u \in (\mathbb{Z}/2)^k \backslash \{0\})$ are in general position. Motivated by Lemma 3.3 we make the following definition.

Definition. For a positive integer $k \geqq 2$ and a non-negative integer b, we define $m_k(b)$ to be the maximum integer which the linear function $\sum a_v$ takes on lattice points satisfying (3.3) and $a_v \geqq 0$ for every v.

One easily sees that $m_k(0) = 0$ and $m_k(b) \geqq b$ for any b. The importance of finding values of $m_k(b)$ lies in the following lemma.

Lemma 3.5. *$s_{\mathbb{R}}(m,p) = k$ for $k \geqq 2$ if and only if $m_{k+1}(p-1) < m \leqq m_k(p-1)$.*

Proof. Since $s_{\mathbb{R}}(m,p)$ decreases as m increases by Proposition 2.3 (3), the lemma follows from Lemma 3.3. □

Remark. Since $s_{\mathbb{R}}(m,p) \leqq p$ by Proposition 2.3 (1), the equality $s_{\mathbb{R}}(m,p) = k$ makes sense only when $k \leqq p$. In other words, $m_k(b)$ has the matrix interpretation discussed for $s_{\mathbb{R}}(m,p)$ in Section 2 only when $k \leqq b+1$.

The following is essentially a restatement of Theorem 2.6.

Theorem 3.6. *$m_k(b) \equiv b \pmod 2$.*

Proof. It is not difficult to see that $m_k(b) = b$ when $b \leqq k-2$ (see Theorem 5.1), so the the theorem holds in this case. Suppose $b \geqq k-1$ and set $b = p-1$. Then $s_{\mathbb{R}}(m_k(p-1), p) = k$ by Lemma 3.5. If

$m_k(p-1)-p$ is even, then $s_{\mathbb{R}}(m_k(p-1)+1,p)=k$ by Theorem 2.6. But this contradicts the maximality of $m_k(p-1)$. Therefore $m_k(p-1)-p$ is odd, i.e., $m_k(b)-b$ is even. □

The following corollary follows from Lemma 3.4 and the last statement in the corollary also follows from Theorem 3.1.

Corollary 3.7. *For any non-negative integer b we have*

$$m_k(b) \leqq \left[\frac{(2^k-1)b}{2^{k-1}-1}\right] = 2b + \left[\frac{b}{2^{k-1}-1}\right] \tag{3.7}$$

and the equality is attained when b is divisible by $2^{k-1}-1$, i.e.

$$m_k((2^{k-1}-1)Q) = (2^k-1)Q \tag{3.8}$$

for any non-negative integer Q. In particular

$$m_2(b) = 3b \text{ for any } b. \tag{3.9}$$

One can find some values of $s_{\mathbb{R}}(m,p)$ using (3.8).

Example 3.8. Take $p=(2^{k-1}-1)(2^k-1)q+1$ where q is any positive integer. Then

$$m_k(p-1) = (2^k-1)^2 q, \quad m_{k+1}(p-1) = (2^{k+1}-1)(2^{k-1}-1)q$$

by (3.8). Therefore it follows from Lemma 3.5 that $s_R(m,p)=k$ for m with $(2^{k+1}-1)(2^{k-1}-1)q < m \leqq (2^k-1)^2 q$.

4. Some more properties of $m_k(b)$

In this section, we study some more properties of $m_k(b)$.

Lemma 4.1. *For any non-negative integers b, b' we have*

$$m_k(b) + m_k(b') \leqq m_k(b+b'). \tag{4.1}$$

In particular,

(1) $m_k(b) + b' \leqq m_k(b+b')$,
(2) $m_k(b) + (2^k-1)Q \leqq m_k(b+(2^{k-1}-1)Q)$ *for any non-negative integer Q.*

Proof. Let $\{a_v\}$ (resp. $\{a'_v\}$) be a set of non-negative integers which satisfy (3.3) and $\sum a_v = m_k(b)$ (resp. (3.3) with b replaced by b' and $\sum a'_v = m_k(b')$). Then $\{a_v + a'_v\}$ is a set of non-negative integers which satisfy (3.3) with b replaced by $b+b'$ and $\sum(a_v+a'_v) = m_k(b)+m_k(b')$. Therefore (4.1) follows.

The inequality (1) follows from (4.1) and the fact that $m_k(b') \geqq b'$. The inequality (2) follows by taking $b' = (2^{k-1}-1)Q$ in (4.1) and using (3.8). □

We will see in later sections that the equality in Lemma 4.1 (1) holds for special values of b and b' but does not hold in general. However, (3.8) and results obtained in later sections imply that the equality in Lemma 4.1 (2) would hold for arbitrary values of b and Q. We shall formulate it as the following conjecture.

Conjecture. $m_k((2^{k-1}-1)Q+R) = (2^k-1)Q + m_k(R)$ for any non-negative integers Q and R, where we may assume $0 \leqq R \leqq 2^{k-1}-2$ without loss of generality.

The following lemma enables us to find an upper bound for $m_k(b)$ by induction on k and we will see that the former inequality in (4.2) is not always but often an equality.

Lemma 4.2. *If b is not divisible by $2^{k-1}-1$ and $Q = [b/(2^{k-1}-1)]$, then*

$$m_k(b) \leqq m_{k-1}(b-q-1)+q+1$$

for any integer $0 \leqq q \leqq Q$ and $m_{k-1}(b-q-1)+q+1$ increases as q decreases; so in particular

$$m_k(b) \leqq m_{k-1}(b-Q-1)+Q+1 \leqq m_{k-1}(b-1)+1. \tag{4.2}$$

Proof. Let $\{a_v\}$ be a set of non-negative integers which satisfy (3.3) and $\sum a_v = m_k(b)$. Then

$$\sum_{(u,v)=0} a_v = b \text{ for some } u \in (\mathbb{Z}/2)^k \backslash \{0\} \tag{4.3}$$

because otherwise we can add 1 to some a_v so that the resulting set of non-negative integers still satisfy (3.3) but their sum is $m_k(b)+1$, which contradicts the definition of $m_k(b)$. Therefore $a_v \geqq Q+1$ for some a_v in (4.3) because if $a_v \leqq Q$ for any v, then $\sum_{(u,v)=0} a_v \leqq (2^{k-1}-1)Q$ and $(2^{k-1}-1)Q$ is strictly smaller than b since b is not divisible by $2^{k-1}-1$ by assumption.

Through a linear transformation of $(\mathbb{Z}/2)^k$, we may assume that the v with $a_v \geqq Q+1$ is $\mathbf{e}_k = (0,\dots,0,1)^T$, so

$$a_{\mathbf{e}_k} \geqq Q+1. \tag{4.4}$$

The kernel $\mathbf{e}_k^\perp$ of the homomorphism $(\mathbf{e}_k,\ ) : (\mathbb{Z}/2)^k \to \mathbb{Z}/2$ can naturally be identified with $(\mathbb{Z}/2)^{k-1}$. For $u \in \mathbf{e}_k^\perp$, (3.3) reduces to

$$a_{\mathbf{e}_k} + \sum_{(u,v)=0, v\neq \mathbf{e}_k} a_v \leqq b. \tag{4.5}$$

Let $\pi\colon (\mathbb{Z}/2)^k \to (\mathbb{Z}/2)^{k-1}$ be the natural projection. For $u \in \mathbf{e}_k^\perp$, we have $(u,v)=0$ if and only if $(\pi(u),\pi(v))=0$. Therefore (4.5) reduces to

$$\sum_{(\pi(u),\bar{v})=0} a_{\bar{v}} \leqq b - a_{\mathbf{e}_k}$$

where $\bar{v}$ runs over all non-zero elements of $(\mathbb{Z}/2)^{k-1}$ and $a_{\bar{v}} = \sum_{\pi(v)=\bar{v}} a_v$. It follows that $\sum a_{\bar{v}} \leqq m_{k-1}(b - a_{\mathbf{e}_k})$ and hence

$$m_k(b) = \sum a_v = a_{\mathbf{e}_k} + \sum a_{\bar{v}} \leqq a_{\mathbf{e}_k} + m_{k-1}(b - a_{\mathbf{e}_k}). \tag{4.6}$$

Here $q + m_{k-1}(b-q)$ increases as q decreases because it follows from Lemma 4.1 that

$$q + m_{k-1}(b-q) \leqq q - 1 + m_{k-1}(b - q + 1).$$

Therefore, the inequalities in the lemma follow from (4.6) and (4.4). □

Corollary 4.3. *$m_k(b) \leqq m_{k-1}(b)$ for any b and $k \geqq 3$.*

Proof. Since $m_{k-1}(b-q-1) + q + 1 \leqq m_{k-1}(b)$ by Lemma 4.1 (1), the corollary follows from Lemma 4.2. □

We shall give another application of Lemma 4.2. Our conjecture stated in this section can be thought of as a periodicity of $m_k(b)$ for a fixed k. The following proposition implies another periodicity of $m_k(b)$, where k varies. It in particular says that once we know values of $m_k(b)$ for all b, we can find values of $m_{k+1}(b)$ for "half" of all b.

Proposition 4.4. *Suppose that*

$$m_k((2^{k-1}-1)Q + R) = (2^k - 1)Q + m_k(R)$$

for some k, R and any Q where $0 \leqq R \leqq 2^{k-1} - 2$. Then

$$m_{k+1}((2^k - 1)Q + 2^{k-1} + R) = (2^{k+1} - 1)Q + 2^k + m_k(R), \tag{4.7}$$

more generally,

$$m_{k+\ell}((2^{k+\ell-1}-1)Q+2^{k+\ell-1}-2^{k-1}+R) = (2^{k+\ell}-1)Q+2^{k+\ell}-2^k+m_k(R) \tag{4.8}$$

for any non-negative integer ℓ.

Proof. The latter identity (4.8) easily follows if we use the former statement repeatedly, so we prove only (4.7). When $R = 0$, (4.7) follows from (3.8); so we may assume $R \neq 0$. It follows from Lemma 4.2 and the assumption in the lemma that

$$
\begin{aligned}
&m_{k+1}((2^k-1)Q+2^{k-1}+R)\\
\leqq &m_k((2^k-1)Q+2^{k-1}+R-Q-1)+Q+1\\
= &m_k((2^{k-1}-1)(2Q+1)+R)+Q+1\\
= &(2^k-1)(2Q+1)+m_k(R)+Q+1\\
= &(2^{k+1}-1)Q+2^k+m_k(R).
\end{aligned} \tag{4.9}
$$

We shall prove the opposite inequality. Let $\{a_v\}$ be a set of non-negative integers which satisfy (3.3) with b replaced by R and

$$
\sum a_v = m_k(R). \tag{4.10}
$$

We regard $(\mathbb{Z}/2)^k$ as a subspace of $(\mathbb{Z}/2)^{k+1}$ in a natural way and define a'_v for $v \in (\mathbb{Z}/2)^{k+1}$ by

$$
a'_v := \begin{cases} Q+a_v & \text{for } v \in (\mathbb{Z}/2)^k \backslash \{0\}, \\ Q+1 & \text{for } v \notin (\mathbb{Z}/2)^k. \end{cases} \tag{4.11}
$$

We shall check that the set $\{a'_v\}$ of non-negative integers satisfies (3.3) with b replaced by

$$
b' := (2^k-1)Q+2^{k-1}+R. \tag{4.12}
$$

Let $u \in (\mathbb{Z}/2)^{k+1} \backslash \{0\}$ and denote by $u^\perp$ the kernel of the homomorphism $(u,\ )\colon (\mathbb{Z}/2)^{k+1} \to \mathbb{Z}/2$, which is a codimension 1 subspace of $(\mathbb{Z}/2)^{k+1}$. We distinguish two cases.

Case 1. The case where $u^\perp = (\mathbb{Z}/2)^k$. It follows from (4.10) and (4.11) that

$$
\begin{aligned}
\sum_{(u,v)=0} a'_v &= \sum (Q+a_v)\\
&= (2^k-1)Q + \sum a_v\\
&= (2^k-1)Q + m_k(R).
\end{aligned} \tag{4.13}
$$

Here $m_k(R) \leqq 2R$ by (3.7) and since $R \leqq 2^{k-1}-2$, we obtain

$$
m_k(R) \leqq 2^{k-1}+R.
$$

This together with (4.12) and (4.13) shows that $\sum_{(u,v)=0} a'_v \leqq b'$.

Case 2. The case where $u^\perp \neq (\mathbb{Z}/2)^k$. Since both $u^\perp$ and $(\mathbb{Z}/2)^k$ are codimension 1 subspaces of $(\mathbb{Z}/2)^{k+1}$ and they are different, the intersection $u^\perp \cap (\mathbb{Z}/2)^k$ is a codimension 1 subspace of $(\mathbb{Z}/2)^k$ and hence the number of elements in $u^\perp\backslash(\mathbb{Z}/2)^k$ is 2^{k-1}. Therefore, it follows from (4.11) and (4.12) that

$$\begin{aligned}\sum_{(u,v)=0} a'_v &= \sum_{v\in u^\perp\cap(\mathbb{Z}/2)^k} a'_v + \sum_{v\in u^\perp\backslash(\mathbb{Z}/2)^k} a'_v \\ &= \sum_{v\in u^\perp\cap(\mathbb{Z}/2)^k} (Q+a_v) + \sum_{v\in u^\perp\backslash(\mathbb{Z}/2)^k} (Q+1) \\ &= (2^k-1)Q + \sum_{v\in u^\perp\cap(\mathbb{Z}/2)^k} a_v + 2^{k-1} \\ &\leqq (2^k-1)Q + R + 2^{k-1} = b'\end{aligned}$$

where the inequality above follows from the fact that the set $\{a_v\}$ satisfies (3.3) with b replaced by R.

The above two cases prove that the set $\{a'_v\}$ satisfies (3.3) with b replaced by b'. Finally it follows from (4.10) and (4.11) that

$$\begin{aligned}\sum_{v\in(\mathbb{Z}/2)^{k+1}\backslash\{0\}} a'_v &= \sum_{v\in(\mathbb{Z}/2)^k\backslash\{0\}} (Q+a_v) + \sum_{v\notin(\mathbb{Z}/2)^k} (Q+1) \\ &= (2^{k+1}-1)Q + \sum_{v\in(\mathbb{Z}/2)^k\backslash\{0\}} a_v + 2^k \\ &= (2^{k+1}-1)Q + m_k(R) + 2^k.\end{aligned}$$

This implies the following desired opposite inequality

$$m_{k+1}((2^k-1)Q + 2^{k-1} + R) \geqq (2^{k+1}-1)Q + 2^k + m_k(R)$$

and completes the proof of (4.7). □

5. $m_k(b)$ FOR $b \leqq k+1$

In this section we will find the values of $m_k(b)$ for $b \leqq k+1$. We treat the case where $b \leqq k-1$ first.

Theorem 5.1. *For any $k \geqq 2$, we have*

$$m_k(b) = \begin{cases} b & \text{if } b \leqq k-2, \\ b+2 & \text{if } b = k-1. \end{cases}$$

Proof. (1) The case where $b \leqq k-2$. Let a_v's be non-negative integers which satisfy (3.3). Suppose that there are more than b positive integers a_v's and choose $b+1$ out of them. Since $b+1 \leqq k-1$, v's for the chosen $b+1$ positive a_v's are contained in some codimension 1 subspace of $(\mathbb{Z}/2)^k$; so the sum of those $b+1$ positive a_v's must be less than or equal to b by (3.3), which is a contradiction. Therefore there are at most b positive a_v's. Since $b \leqq k-2$, v's for the positive a_v's are contained in some codimension 1 subspace of $(\mathbb{Z}/2)^k$; so $\sum a_v \leqq b$ by (3.3) and this proves $m_k(b) \leqq b$. On the other hand, it is clear that $m_k(b) \geqq b$, so $m_k(b) = b$ when $b \leqq k-2$.

(2) The case where $b = k-1$. In this case we can use the matrix interpretation of $m_k(b)$, see the Remark following Lemma 3.5. The following argument is essentially same as Lemma 2.5. Let A be a $k \times m$ matrix where any k column vectors span $(\mathbb{Z}/2)^k$. We may assume that the first k column vectors are the standard basis, so $A = (\mathbf{e}_1, \dots, \mathbf{e}_k, \mathbf{a}_{k+1}, \dots, \mathbf{a}_m)$. Since any $k-1$ vectors from $\mathbf{e}_1, \dots, \mathbf{e}_k$ together with $\mathbf{a}_j$ span $(\mathbb{Z}/2)^k$, $\mathbf{a}_j$ must be $\sum_{i=1}^k \mathbf{e}_i$. Therefore m must be less than or equal to $k+1$ and this shows $m_k(k-1) \leqq k+1$. On the other hand, since any k column vectors in $(\mathbf{e}_1, \dots, \mathbf{e}_k, \sum \mathbf{e}_i)$ span $(\mathbb{Z}/2)^k$, $m_k(k-1) \geqq k+1$. This proves $m_k(k-1) = k+1$. □

Theorem 5.2. *If $b = k$, then*

$$m_k(b) = \begin{cases} b+4 & \text{if } k = 2,3,4, \\ b+2 & \text{if } k \geqq 5. \end{cases}$$

Proof. Since $m_2(2) = 6$ by (3.9) and $m_3(3) = 7$ by (3.8), the theorem is proven when $k = 2, 3$. One can easily check that any 5 columns in this matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

span $(\mathbb{Z}/2)^4$, so $m_4(4) \geqq 8$. On the other hand, using Lemma 4.2, we obtain

$$m_4(4) \leqq m_3(3) + 1 = 8.$$

Thus $m_4(4) = 8$ and the theorem is proven when $k = 4$.

Since $m_k(k-1) = k+1$ by Theorem 5.1, it follows from Lemma 4.1 (1) that

$$m_k(k) \geqq m_k(k-1) + 1 = k+2.$$

In the sequel it suffices to prove that if $m_k(k) \geqq k+3$, then $k \leqq 4$.

Suppose $m_k(k) \geqq k+3$. Then there is a $k \times (k+3)$ matrix A with entries in $\mathbb{Z}/2$ such that any $k+1$ column vectors in A span $(\mathbb{Z}/2)^k$. We may assume that $A = (\mathbf{e}_1, \dots, \mathbf{e}_k, \mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3)$ as before. Denote by $\mathbf{a}^i$ the i-th row vector in the submatrix $(\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3)$. Since any $k+1$ column vectors in A span $(\mathbb{Z}/2)^k$, we see that

$$\begin{pmatrix} \mathbf{a}^i \\ \mathbf{a}^j \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

up to permutations of column vectors at the right hand side. This must occur for any $1 \leqq i < j \leqq k$ but one can easily see that this is impossible when $k \geqq 5$. □

Theorem 5.3. *If $b = k + 1$, then*

$$m_k(b) = \begin{cases} b+6 & \text{if } k = 2, \\ b+4 & \text{if } 3 \leqq k \leqq 11, \\ b+2 & \text{if } k \geqq 12. \end{cases}$$

Proof. Since $m_2(3) = 9$ by (3.9), the theorem is proven when $k = 2$.

Using Lemma 4.2 repeatedly, we have

(5.1)
$$m_{11}(12) \leqq m_{10}(11)+1 \leqq m_9(10)+2 \leqq \cdots \leqq m_3(4)+8 \leqq m_2(2)+10 = 16$$

where we used (3.9) at the last identity. On the other hand, it follows from Theorem 2.7 that

$$s_{\mathbb{R}}(16, 13) = s_{\mathbb{R}}(15, 13) = [15 - \log_2(15 + 1)] = 11$$

and hence $m_{11}(12) \geqq 16$ by Lemma 3.5. Therefore $m_{11}(12) = 16$ and all the inequalities in (5.1) must be equalities, proving the second case in the theorem.

Similarly, it follows from Theorem 2.7 that

$$s_{\mathbb{R}}(16, 14) = [16 - \log_2(16 + 1)] = 11$$

and hence $m_{12}(13) \leqq 15$ by Lemma 3.5. On the other hand, it follows from Theorem 5.2 and Corollary 4.3 that

$$15 = m_{13}(13) \leqq m_{12}(13).$$

Therefore $m_{12}(13) = 15$.

Suppose $k \geqq 12$. Then using Lemma 4.2 repeatedly, we have

$$m_k(k + 1) \leqq m_{k-1}(k) + 1 \leqq \cdots \leqq m_{12}(13) + k - 12 = k + 3$$

where we used the fact $m_{12}(13) = 15$ just shown above. On the other hand, it follows from Lemma 4.1 (1) and Theorem 5.2 that

$$m_k(k + 1) \geqq m_k(k) + 1 = k + 3.$$

Therefore $m_k(k + 1) = k + 3$ when $k \geqq 12$, proving the last case in the theorem. □

6. Further computations of $m_k(b)$

In this section we will make some more computations of $m_k(b)$ by combining the results in the previous sections. All of the results provide supporting evidence to the Conjecture stated in Section 4.

Proposition 6.1. *If* $R \leqq k-1$*, then*

$$m_k((2^{k-1}-1)Q+R) = (2^k-1)Q + m_k(R)$$

where

$$m_k(R) = \begin{cases} R & \text{if } R \leqq k-2, \\ R+2 & \text{if } R = k-1. \end{cases}$$

by Theorem 5.1.

Proof. When $R = 0$, the proposition follows from (3.8) since $m_k(0) = 0$. So we may assume $1 \leqq R \leqq k-1$. We prove the proposition by induction on k. Since $m_2(b) = 3b$ by (3.9), the proposition holds when $k = 2$. Suppose the proposition holds for $k = \ell - 1$. It follows from (3.8), Lemmas 4.1, 4.2 and the induction assumption that

$$\begin{aligned} (2^\ell - 1)Q + m_\ell(R) &= m_\ell((2^{\ell-1}-1)Q) + m_\ell(R) \\ &\leqq m_\ell((2^{\ell-1}-1)Q + R) \\ &\leqq m_{\ell-1}((2^{\ell-1}-1)Q + R - Q - 1) + Q + 1 \\ &= m_{\ell-1}((2^{\ell-2}-1)2Q + R - 1) + Q + 1 \\ &= (2^{\ell-1}-1)2Q + m_{\ell-1}(R-1) + Q + 1 \\ &= (2^\ell - 1)Q + m_{\ell-1}(R-1) + 1. \end{aligned} \tag{6.1}$$

Here since $R \leqq \ell - 1$, we have $m_\ell(R) = m_{\ell-1}(R-1) + 1$ by Theorem 5.1. Therefore the first and last terms in (6.1) are same, so the first inequality in (6.1) must be an equality, which proves the proposition when $k = \ell$, completing the induction step. □

The following corollary follows from Proposition 6.1 by taking $k = 3$.

Corollary 6.2.

$$m_3(3Q+R) = \begin{cases} 7Q & \text{if } R = 0, \\ 7Q+1 & \text{if } R = 1, \\ 7Q+4 & \text{if } R = 2. \end{cases}$$

Combining Proposition 6.1 with Proposition 4.4, one can improve Proposition 6.1 as follows.

Theorem 6.3. *Let* $0 \leqq \ell \leqq k-2$*. If* $0 \leqq r \leqq k-\ell-1$*, then*

$$m_k((2^{k-1}-1)Q + 2^{k-1} - 2^{k-1-\ell} + r) = (2^k-1)Q + 2^k - 2^{k-\ell} + m_{k-\ell}(r)$$

where

$$m_{k-\ell}(r) = \begin{cases} r & \text{if } r \leqq k-\ell-2, \\ r+2 & \text{if } r = k-\ell-1. \end{cases}$$

by Theorem 5.1.

Proof. By Proposition 6.1, we have

(6.2)
$$m_k((2^{k-1}-1)Q+r) = (2^k-1) = (2^k-1)Q+m_k(r) \quad \text{for } 0 \leqq r \leqq k-1.$$

Therefore, it follows from (4.8) in Proposition 4.4 that

(6.3)
$$m_{k+\ell}((2^{k+\ell-1}-1)Q+2^{k+\ell-1}-2^{k-1}+r) = (2^{k+\ell}-1)Q+2^{k+\ell}-2^k+m_k(r)$$

for any non-negative integer ℓ. Rewriting $k+\ell$ as k, the identity (6.3) turns into the identity in the theorem and the condition $0 \leqq r \leqq k-1$ in (6.2) turns into the condition $0 \leqq r \leqq k-\ell-1$ in the theorem. □

Proposition 6.4. *If $R = k+1$ and $4 \leqq k \leqq 11$, then*

$$m_k((2^{k-1}-1)Q+R) = (2^k-1)Q+m_k(R)$$

where $m_k(R) = R+4$ by Theorem 5.3.

Proof. First we prove the proposition when $k = 4$. In this case $R = 5$. It follows from Lemma 4.2 and Corollary 6.2 that

$$\begin{aligned} m_4((2^3-1)Q+5) &\leqq m_3(7Q+5-Q-1)+Q+1 \\ &= 7(2Q+1)+1+Q+1 = 15Q+9 \end{aligned}$$

while it follows from (4.1), (3.8) and Theorem 5.3

$$\begin{aligned} m_4((2^3-1)Q+5) &\geqq m_4((2^3-1)Q)+m_4(5) \\ &= (2^4-1)Q+9 = 15Q+9. \end{aligned}$$

This proves the proposition when $k = 4$.

Suppose that the proposition holds for $k-1$ with $4 \leqq k-1 \leqq 10$. Then it follows from Lemma 4.2 and the induction assumption that

$$\begin{aligned} m_k((2^{k-1}-1)Q+R) &\leqq m_{k-1}((2^{k-1}-1)Q+R-Q-1)+Q+1 \\ &= m_{k-1}((2^{k-2}-1)2Q+R-1)+Q+1 \\ &= (2^{k-1}-1)2Q+(R-1)+4+Q+1 \\ &= (2^k-1)Q+R+4 \end{aligned}$$

while it follows from (4.1), (3.8) and Theorem 5.3

$$\begin{aligned} m_k((2^{k-1}-1)Q+R) &\geqq m_k((2^{k-1}-1)Q)+m_k(R) \\ &= (2^k-1)Q+R+4. \end{aligned}$$

These show that $m_k((2^{k-1}-1)Q+R) = (2^k-1)Q+R+4$, completing the induction step. □

Similarly to Theorem 6.3, Proposition 6.4 can be improved as follows by combining it with Proposition 4.4. The proof is same as that of Theorem 6.3, so we omit it.

Theorem 6.5. *Let* $0 \leqq \ell \leqq k-2$. *If* $4 \leqq k-\ell \leqq 11$, *then*

$$m_k((2^{k-1}-1)Q+2^{k-1}-2^{k-\ell-1}+k-\ell+1) = (2^k-1)Q+2^k-2^{k-\ell}+k-\ell+5.$$

Example 6.6. Below is a table of values of $m_k((2^{k-1}-1)Q+R)$ for $k = 2, 3, 4, 5, 6$.

$R\backslash k$	2	3	4	5	6
0	3Q	7Q	15Q	31Q	63Q
1		7Q+1	15Q+1	31Q+1	63Q+1
2		7Q+4	15Q+2	31Q+2	63Q+2
3			15Q+5	31Q+3	63Q+3
4			15Q+8	31Q+6	63Q+4
5			15Q+9	31Q+7 or 9	63Q+7
6			15Q+12	31Q+10	63Q+8 or 10
7				31Q+11 or 13	63Q+11
8				31Q+16	63Q+12 or 14
9				31Q+17	63Q+13, 15 or 17
10				31Q+18	63Q+14, 16 or 18
11				31Q+21	63Q+15, 17 or 19
12				31Q+24	63Q+20 or 22
13				31Q+25	63Q+21, 23 or 25
14				31Q+28	63Q+24 or 26
15					63Q+27 or 29
16					63Q+32
17					63Q+33
18					63Q+34
19					63Q+35
20					63Q+38
21					63Q+39 or 41
22					63Q+42
23					63Q+43 or 45
24					63Q+48
25					63Q+49
26					63Q+50
27					63Q+53
28					63Q+56
29					63Q+57
30					63Q+60

TABLE 1. $m_k((2^{k-1}-1)Q+R)$ for $k = 3, 4, 5, 6$

The values above for $k = 2, 3, 4$ can be obtained from Theorem 6.3 although they are obtained from (3.9) when $k = 2$ and from Corollary 6.2) when $k = 3$. Similarly, the values for $k = 5$ can be obtained from Theorem 6.3 except the three cases where $R = 5, 6, 7$. The case where $R = 6$ follows from Theorem 6.5 (or Proposition 6.4). As for the case where $R = 5$, $m_5(15Q+5)$ must lie in between $31Q+7$ and $31Q+9$ because $m_5(15Q+4) = 31Q+6$, $m_5(15Q+6) = 31Q+10$ and $m_k(b+1) \geqq m_k(b)+1$ as in Corollary 4.1, and the value $31Q+8$ would be excluded because $m_k(b) \equiv b \pmod 2$ by Theorem 3.6. As for the case where $R = 7$, the same argument shows that $m_5(15Q+7) = 31Q+11, 13$ or 15. But the value $31Q + 15$ would be excluded by (3.7). A similar argument shows the values above when $k = 6$. In fact we also use Proposition 8.1 proved later for $R = 12, 13, 14$ and 15.

Finally we note that $m_5(5) = 7$ and $m_6(6) = 8$ by Theorem 5.2 although we could not determine the values of $m_5(15Q+5)$ and $m_6(31Q+6)$ for $Q \geqq 1$ as shown above.

7. Upper and lower bounds of $m_k(b)$

We continue to use the expression

$$b = (2^{k-1} - 1)Q + R$$

where Q and R are non-negative integers and $0 \leqq R \leqq 2^{k-1} - 2$. Here are naive upper and lower bounds of $m_k(b)$.

Lemma 7.1. $(2^k - 1)Q + R \leqq m_k(b) \leqq (2^k - 1)Q + 2R$, *i.e. if we denote* $m_k(b) = (2^k - 1)Q + S$, *then* $R \leqq S \leqq 2R$.

Proof. We take $a_v = Q+R$ for one v and $a_v = Q$ for all other v's. These satisfy (3.3) and $\sum a_v = (2^k - 1)Q + R$, proving the lower bound. The upper bound is a restatement of the upper bound in (3.7). □

Remark. It easily follows from Lemma 7.1 that $\lim_{b\to\infty} m_k(b)/b = (2^k - 1)/(2^{k-1} - 1)$, so $m_k(b)$ is approximately $(2^k - 1)b/(2^{k-1} - 1)$ when b is large.

The bounds in Lemma 7.1 are best possible in the sense that both $S = R$ and $S = 2R$ occur and it is easy to see when $S = R$ occurs. In this section we improve the lower bound in Lemma 7.1 and see when the lower and upper bounds are attained. The following answers the question of when $S = R$ occurs.

Proposition 7.2. *Let* $b = (2^{k-1}-1)Q+R$ *and* $m_k(b) = (2^k-1)Q+S$. *Then* $S = R$ *if and only if* $R \leqq k - 2$.

Proof. The "if part" follows from Theorem 6.1. Suppose $R \geqq k - 1$. Then it follows from Lemma 4.1, (3.8) and Theorem 5.1 that

$$\begin{aligned}(2^k - 1)Q + S = m_k(b) &= m_k((2^{k-1} - 1)Q + R) \\ &\geqq m_k(2^{k-1} - Q) + m_k(k - 1) + m_k(R - k + 1) \\ &\geqq (2^k - 1)Q + (k + 1) + (R - k + 1) \\ &= (2^k - 1)Q + R + 2\end{aligned}$$

and hence $S \geqq R + 2$, proving the "only if" part. □

We shall study when $S = 2R$ occurs and improve the lower bound in Lemma 7.1 in the rest of this section. Remember that the polyhedron $P(b)$ defined by $(2^k - 1)$ inequalities

$$\sum_{(u,v)=0} a_v \leqq b \quad \text{for each } u \in (\mathbb{Z}/2)^k \backslash \{0\}$$

has the point $x = (a_v)$ with $a_v = b/(2^{k-1} - 1)$ as the unique vertex and the $(2^k - 1)$ hyperplanes

$$H^u(b) = \{(a_v) \in \mathbb{R}^{2^k-1} \mid \sum_{(u,v)=0} a_v = b\} \quad \text{for } u \in (\mathbb{Z}/2)^k \backslash \{0\}$$

are in general position. We set

$$H(m) = \{(a_v) \in \mathbb{R}^{2^k-1} \mid \sum a_v = m\}.$$

Lemma 3.4 tells us that the intersection $P(b) \cap H(m)$ is non-empty if and only if $m \leqq (2^k - 1)b/(2^{k-1} - 1)$, and that it is the one point x if $m = (2^k - 1)b/(2^{k-1} - 1)$ and a simplex of dimension $2^k - 2$ if $m < (2^k - 1)b/(2^{k-1} - 1)$.

Lemma 7.3. *Let $u \in (\mathbb{Z}/2)^k \backslash \{0\}$. Then the v-th coordinate a_v^u of a vertex $P^u = H(m) \cap (\cap_{u' \neq u} H^{u'})$ of $P(b) \cap H(m)$ is given by*

$$a_v^u = \begin{cases} 2b - m + (m - b)/2^{k-2} & \text{if } (u, v) \neq 0, \\ m - 2b & \text{if } (u, v) = 0. \end{cases}$$

In other words, if $b = (2^{k-1} - 1)Q + R$ and $m = (2^k - 1)Q + S$, then

$$a_v^u = \begin{cases} Q + 2R - S + (S - R)/2^{k-2} & \text{if } (u, v) \neq 0, \\ Q + S - 2R & \text{if } (u, v) = 0. \end{cases}$$

Proof. Fix $u \in (\mathbb{Z}/2)^k \backslash \{0\}$. For each $u' \in (\mathbb{Z}/2)^k \backslash \{0\}$ we consider an equation

$$\sum_{(u',v')=0} a_{v'}^u = b \tag{7.1}$$

where v' runs over elements with $(u', v') = 0$ in the sum.

The following argument is similar to the latter half of the proof of Lemma 3.4. For v with $(u, v) \neq 0$, we take sum of (7.1) over all non-zero u' with $(u', v) = 0$. Then we obtain

$$(2^{k-1} - 1)a_v^u + (2^{k-2} - 1) \sum_{v' \neq v} a_{v'}^u = (2^{k-1} - 1)b. \tag{7.2}$$

(Note that $a^u_{v'}$ with $v' \neq v$ appears in the equation (7.1) for u' with $(u', v) = (u', v') = 0$, so it appears $(2^{k-2} - 1)$ times.) Since $a^u_v + \sum_{v' \neq v} a^u_{v'} = m$, we plug $\sum_{v' \neq v} a^u_{v'} = m - a^u_v$ in (7.2) to obtain

$$
\begin{aligned}
a^u_v &= \frac{1}{2^{k-2}}\big\{(2^{k-1} - 1)b - (2^{k-2} - 1)m\big\} \\
&= 2b - m + \frac{1}{2^{k-2}}(m - b).
\end{aligned}
\tag{7.3}
$$

For v with $(u, v) = 0$, we take sum of (7.1) over all non-zero u' with $(u', v) = 0$ and $u' \neq u$. Since the number of such u' is $2^{k-1} - 2$, we obtain

$$
(2^{k-1} - 2)a^u_v + (2^{k-2} - 1) \sum_{v' \neq v} a^u_{v'} - \sum_{v' \neq v, (u,v')=0} a^u_{v'} = (2^{k-1} - 2)b. \tag{7.4}
$$

Here

$$
\sum_{v' \neq v} a^u_{v'} = m - a^u_v \tag{7.5}
$$

and

$$
\begin{aligned}
\sum_{v' \neq v, (u,v')=0} a^u_{v'} &= m - a^u_v - \sum_{(u,v') \neq 0} a^u_{v'} \\
&= m - a^u_v - 2^{k-1}\Big(2b - m + \frac{1}{2^{k-2}}(m - b)\Big) \\
&= (2^{k-1} - 1)m - (2^k - 2)b - a^u_v
\end{aligned}
\tag{7.6}
$$

where we used (7.3) for v' at the second identity. Plugging (7.5) and (7.6) in (7.4), we obtain

$$
2^{k-2}a^u_v - 2^{k-2}m + (2^k - 2)b = (2^{k-1} - 2)b
$$

and hence $a^u_v = m - 2b$. □

Proposition 7.4. *Let $b = (2^{k-1} - 1)Q + R$ and $m_k(b) = (2^k - 1)Q + S$. If $S = 2R$, then $R = 2^{k-1} - 2^{k-1-\ell}$ for some $0 \leqq \ell \leqq k - 2$.*

Proof. Suppose $S = 2R$. Then it follows from Lemma 7.3 that the v-th coordinate a^u_v of the vertex P^u of $P(b) \cap H(m_k(b))$ is given by

$$
a^u_v = \begin{cases} Q + R/2^{k-2} & \text{if } (u, v) \neq 0, \\ Q & \text{if } (u, v) = 0. \end{cases}
$$

Since $m_k(b) = (2^k - 1)Q + S$ and $S = 2R$ by assumption, there is a lattice point on the simplex $P(b) \cap H(m_k(b))$. The simplex is the convex hull of the vertices P^u, so there exist non-negative real numbers t_u's with $\sum t_u = 1$ such that $\sum t_u P^u$ is a lattice point, i.e.

$$\sum t_u a_v^u = \sum_{(u,v)\neq 0} t_u(Q+R/2^{k-2}) + \sum_{(u,v)=0} t_u Q = Q + (\sum_{(u,v)\neq 0} t_u)R/2^{k-2} \in \mathbb{Z}$$

for any v. This means that $(\sum_{(u,v)\neq 0} t_u)R/2^{k-2} = 0$ or 1, i.e.

$$\sum_{(u,v)\neq 0} t_u = 0 \quad \text{or} \quad 2^{k-2}/R \quad \text{for any } v \tag{7.7}$$

because $0 \leqq R \leqq 2^{k-1} - 2$ and $\sum_{(u,v)\neq 0} t_u \leqq 1$. On the other hand,

$$\sum_v \sum_{(u,v)\neq 0} t_u = 2^{k-1} \tag{7.8}$$

because each t_u appears 2^{k-1} times in the sum above and $\sum t_u = 1$. It follows from (7.7) and (7.8) that there are exactly $2R$ numbers of v's such that $\sum_{(u,v)\neq 0} t_u \neq 0$, in other words, there are exactly $2^k - 1 - 2R$ numbers of v's such that $\sum_{(u,v)\neq 0} t_u = 0$. The identity $\sum_{(u,v)\neq 0} t_u = 0$ implies that $t_u = 0$ for all u with $(u, v) \neq 0$ since $t_u \geqq 0$. Based on these observations, we introduce

$U :=$ the linear span of $U_0 := \{u \mid t_u \neq 0\}$,

$V :=$ the linear span of $V_0 := \{v \mid t_u = 0 \quad \text{for } \forall u \text{ such that } (u, v) \neq 0\}$.

If $v \in V_0$, then it follows from the definition of U_0 and V_0 that $(u, v) = 0$ for any $u \in U_0$ and hence $(u, v) = 0$ for any $u \in U$ since U is the linear span of U_0. This implies that $(u, v) = 0$ for any $u \in U$ and $v \in V$ since V is the linear span of V_0. It follows that

$$\dim U \leqq k - \dim V. \tag{7.9}$$

We note that V contains at least $2^k - 1 - 2R$ non-zero elements by the observation made above.

Suppose that

$$2^{k-1} - 2^{k-1-\ell} \leqq R < 2^{k-1} - 2^{k-1-(\ell+1)} \text{ for some } 0 \leqq \ell \leqq k-2. \tag{7.10}$$

(Note that R lies in the inequality (7.10) for some ℓ because $0 \leqq R \leqq 2^{k-1} - 2$.) Then, since $2^{k-\ell-1} - 1 < 2^k - 1 - 2R$ and V contains at least $2^k - 1 - 2R$ non-zero elements, V contains at least $2^{k-\ell-1}$ non-zero elements and hence $\dim V \geqq k - \ell$. This together with (7.9) shows

$$\dim U \leqq \ell \tag{7.11}$$

Since the bilinear form (,) is non-degenerate, there is a subspace W of $(\mathbb{Z}/2)^k$ such that $\dim W = \dim U$ and the bilinear form (,) restricted to $U \times W$ is still non-degenerate. We take sum of (7.7) over all non-zero $v \in W$. In this sum, each t_u for $u \in U \backslash \{0\}$ appears $2^{\dim W - 1}$ times. Since $\dim W = \dim U$ and $\sum_{u \in U \backslash \{0\}} t_u = 1$, we obtain

$$2^{\dim U - 1} \leqq (2^{\dim U} - 1) 2^{k-2} / R$$

and hence

$$R \leqq (2^{\dim U} - 1) 2^{k - \dim U - 1} \leqq 2^{k-1} - 2^{k-\ell-1} \tag{7.12}$$

where we used (7.11) at the latter inequality. Then (7.10) and (7.12) show that $R = 2^{k-1} - 2^{k-1-\ell}$, proving the proposition. □

It turns out that the converse of Proposition 7.4 holds, i.e. $S = 2R$ can be attained when $R = 2^{k-1} - 2^{k-1-\ell}$. In fact, we can prove the following.

Proposition 7.5. *Let $b = (2^{k-1} - 1)Q + R$ and let $2^{k-1} - 2^{k-1-\ell} \leqq R < 2^{k-1} - 2^{k-1-(\ell+1)}$ for some $0 \leqq \ell \leqq k-2$. Then*

$$m_k(b) \geqq (2^k - 1)Q + R + 2^{k-1} - 2^{k-1-\ell}.$$

In particular, if $R = 2^{k-1} - 2^{k-1-\ell}$ for some $0 \leqq \ell \leqq k-2$, then $m_k(b) \geqq (2^k - 1)Q + 2R$.

Proof. We take

$$m = (2^k - 1)Q + R + 2^{k-1} - 2^{k-1-\ell}$$

and find a lattice point in the simplex $P(b) \cap H(m)$ with non-negative coordinates. Set

$$r = R - 2^{k-1} + 2^{k-1-\ell}.$$

The v-th coordinate a_v^u of the vertex P^u of $P(b) \cap H(m)$ is given by

$$a_v^u = \begin{cases} Q + r + 2 - 2^{1-\ell} & \text{if } (u, v) \neq 0, \\ Q - r & \text{if } (u, v) = 0 \end{cases} \tag{7.13}$$

by Lemma 7.3. Set

$$L = 2 - 2^{1-\ell}. \tag{7.14}$$

Any point in $P(b) \cap H(m)$ can be expressed as $\sum_{u \in (\mathbb{Z}/2)^k \backslash \{0\}} t_u P^u$ with $t_u \geqq 0$ and $\sum t_u = 1$, and we find from (7.13) that its v-th coordinate

a_v is given by

$$\begin{aligned}a_v =&(\sum_{(u,v)\neq 0} t_u)(Q+r+L)+(\sum_{(u,v)=0} t_u)(Q-r)\\ =&(\sum t_u)Q+(1-\sum_{(u,v)=0} t_u)(r+L)+(\sum_{(u,v)=0} t_u)(-r)\\ =&Q+r+L-(\sum_{(u,v)=0} t_u)(2r+L).\end{aligned}\tag{7.15}$$

We take a codimension 1 subspace V of $(\mathbb{Z}/2)^k$ and an ℓ-dimensional subspace U of V arbitrarily and define

$$t_u = \begin{cases} \frac{2r}{2r+L}\frac{1}{2^{k-1}} & \text{for } u \notin V, \\ \frac{L}{2r+L}\frac{1}{2^{\ell}-1} & \text{for } u \in U\backslash\{0\}, \\ 0 & \text{otherwise.}\end{cases}\tag{7.16}$$

Then $t_u \geqq 0$ and $\sum t_u = 1$. We shall check that a_v in (7.15) is a non-negative integer. We denote by $v^\perp$ the codimension 1 subspace of $(\mathbb{Z}/2)^k$ consisting of elements w such that $(v,w)=0$ and distinguish three cases according to the position of $v^\perp$ relative to V and U.

Case 1. The case where $v^\perp = V$. In this case,

$$\sum_{(u,v)=0} t_u = \frac{L}{2r+L}\frac{1}{2^\ell-1}(2^\ell-1) = \frac{L}{2r+L},$$

so $a_v = Q+r$ by (7.15).

Case 2. The case where $v^\perp \neq V$ and $v^\perp \supset U$. In this case, $v^\perp \cap V$ is of dimension $k-2$ and

$$\sum_{(u,v)=0} t_u = \frac{2r}{2r+L}\frac{1}{2^{k-1}}2^{k-2} + \frac{L}{2r+L}\frac{1}{2^\ell-1}(2^\ell-1) = \frac{r+L}{2r+L},$$

so $a_v = Q$ by (7.15).

Case 3. The case where $v^\perp \neq V$ and $v^\perp \not\supset U$. In this case, $v^\perp \cap V$ is of dimension $k-2$ and $v^\perp \cap U$ is of dimension $\ell-1$ and hence

$$\begin{aligned}\sum_{(u,v)=0} t_u &= \frac{2r}{2r+L}\frac{1}{2^{k-1}}2^{k-2} + \frac{L}{2r+L}\frac{1}{2^\ell-1}(2^{\ell-1}-1)\\ &= \frac{r+L-1}{2r+L}\end{aligned}$$

where we used (7.14) at the second identity, so $a_v = Q+1$ by (7.15).

In any case a_v is a non-negative integer, so $\sum_{u\in(\mathbb{Z}/2)^k\backslash\{0\}} t_u P^u$ with t_u in (7.16) is a lattice point in $P(b)\cap H(m)$ with non-negative coordinates. This proves the proposition. □

Now we are ready to prove the latter theorem in the Introduction.

Theorem 7.6. *Let* $b = (2^{k-1} - 1)Q + R$. *If* $2^{k-1} - 2^{k-1-\ell} \leqq R < 2^{k-1} - 2^{k-1-(\ell+1)}$ *for some* $0 \leqq \ell \leqq k-2$, *then*

$$(2^k - 1)Q + R + 2^{k-1} - 2^{k-1-\ell} \leqq m_k(b) \leqq (2^k - 1)Q + 2R$$

where the lower bound is attained if and only if $R - (2^{k-1} - 2^{k-1-\ell}) \leqq k-\ell-2$ *and the upper bound is attained if and only if* $R = 2^{k-1} - 2^{k-1-\ell}$.

Proof. The inequality and the statement on the upper bound follows from Propositions 7.4 and 7.5. Moreover, Theorem 6.3 shows that the lower bound is attained if $R - (2^{k-1} - 2^{k-1-\ell}) \leqq k - \ell - 2$. Suppose $R - (2^{k-1} - 2^{k-1-\ell}) \geqq k - \ell - 1$ and set

$$D = R - (2^{k-1} - 2^{k-1-\ell}) - (k - \ell - 1). \tag{7.17}$$

Then it follows from Lemma 4.1 and Theorem 6.3 that

$$\begin{aligned} m_k(b) &= m_k((2^{k-1} - 1)Q + R) \\ &= m_k((2^{k-1} - 1)Q + 2^{k-1} - 2^{k-1-\ell} + k - \ell - 1 + D) \\ &\geqq m_k((2^{k-1} - 1)Q + 2^{k-1} - 2^{k-1-\ell} + k - \ell - 1) + m_k(D) \\ &\geqq (2^k - 1)Q + 2^k - 2^{k-\ell} + k - \ell + 1 + D \\ &= (2^k - 1)Q + R + 2^{k-1} - 2^{k-\ell-1} + 2 \end{aligned}$$

where we used (7.17) at the last identity. Therefore the lower bound is not attained if $R - (2^{k-1} - 2^{k-1-\ell}) \geqq k - \ell - 1$. □

8. A slight improvement of lower bounds

When $R \leqq 2^{k-2} - 1$, the lower bound of $m_k(b)$ in Theorem 7.6 is nothing but $(2^k - 1)Q + R$ and this is an obvious lower bound. In this section we improve the lower bound when $2^{k-2} - 4 \leqq R \leqq 2^{k-2} - 1$.

Proposition 8.1. *If k is odd, then*

(1) $m_k(2^{k-1} - 1)Q + 2^{k-2} - 1) \geqq (2^k - 1)Q + 2^{k-1} - k$,
(2) $m_k(2^{k-1} - 1)Q + 2^{k-2} - 2) \geqq (2^k - 1)Q + 2^{k-1} - k - 1$.

If k is even, then

(1) $m_k(2^{k-1} - 1)Q + 2^{k-2} - 1) \geqq (2^k - 1)Q + 2^{k-1} - k + 1$,
(2) $m_k(2^{k-1} - 1)Q + 2^{k-2} - 2) \geqq (2^k - 1)Q + 2^{k-1} - k - 2$,
(3) $m_k(2^{k-1} - 1)Q + 2^{k-2} - 3) \geqq (2^k - 1)Q + 2^{k-1} - 2k + 1$,
(4) $m_k(2^{k-1} - 1)Q + 2^{k-2} - 4) \geqq (2^k - 1)Q + 2^{k-1} - 2k$.

Proof. In any case it suffices to prove the inequality when $Q = 0$ by Lemma 4.1 (2). We recall how $m_k(2^{k-2}) = 2^{k-1}$ is obtained. Choose any non-zero element $u_0 \in (\mathbb{Z}/2)^k$ and define

$$a_v = \begin{cases} 1 & \text{if } (u_0, v) \neq 0, \\ 0 & \text{if } (u_0, v) = 0. \end{cases} \tag{8.1}$$

Then

$$\sum_{(u,v)=0} a_v = \begin{cases} 2^{k-2} & \text{if } u \neq u_0, \\ 0 & \text{if } u = u_0 \end{cases}$$

and $\sum a_v = 2^{k-1}$. This attains $m_k(2^{k-2}) = 2^{k-1}$.

We take

$$u_0 = (1, \dots, 1)^t.$$

Then $(u_0, v) = 0$ if and only if the number of 1 in the components of v is even. Let

$$V_1 := \{\mathbf{e}_1, \dots, \mathbf{e}_k\} \subset (\mathbb{Z}/2)^k$$

$$V_2 := \begin{cases} V_1 \cup \{u_0\} & \text{for } k \text{ odd}, \\ V_1 \cup \{u_0 - \mathbf{e}_1, u_0 - \mathbf{e}_2\} & \text{for } k \text{ even}, \end{cases}$$

and define for $q = 1, 2$

$$a_v^{(q)} := \begin{cases} 1 & \text{if } (u_0, v) \neq 0 \text{ and } v \notin V_q, \\ 0 & \text{otherwise}. \end{cases}$$

One can check that $\sum_{(u,v)=0} a_v^{(q)} \leqq 2^{k-2} - q$ for any non-zero $u \in (\mathbb{Z}/2)^k$. Clearly

$$\sum a_v^{(q)} = \begin{cases} 2^{k-1} - k & \text{when } q = 1, \\ 2^{k-1} - k - 1 & \text{when } q = 2 \text{ and } k \text{ is odd}, \\ 2^{k-1} - k - 2 & \text{when } q = 2 \text{ and } k \text{ is even}. \end{cases}$$

This together with the congruence $m_k(b) \equiv b \pmod 2$ in Theorem 3.6 (applied when $q = 1$ and k is even) implies the inequalities (1) and (2) in the proposition.

The proof of the inequality (4) is similar. Assume k is even and let

$$V_4 := V_1 \cup \{u_0 - \mathbf{e}_1, \dots, u_0 - \mathbf{e}_k\}$$

and define

$$a_v^{(4)} := \begin{cases} 1 & \text{if } (u_0, v) \neq 0 \text{ and } v \notin V_4, \\ 0 & \text{otherwise}. \end{cases}$$

One can check that $\sum_{(u,v)=0} a_v^{(4)} \leqq 2^{k-2}-4$ for any non-zero $u \in (\mathbb{Z}/2)^k$ (where we use the assumption on k being even) and $\sum a_v^{(4)} = 2^{k-1}-2k$. Therefore

$$m_k(2^{k-2}-4) \geqq 2^{k-1}-2k$$

which implies the inequality (4) in the proposition. The inequality (3) follows from (4) since $m_k(b+1) \geqq m_k(b)+1$. □

9. Some observation on the Conjecture

The Conjecture in Section 4 says that

$$m_k((2^{k-1}-1)Q+R) = (2^k-1)Q+m_k(R)$$

and this is equivalent to saying

$$m_k(b+2^{k-1}-1) = m_k(b)+2^k-1. \tag{9.1}$$

In this section, we prove (9.1) when b is large, to be more precise, we prove the following.

Theorem 9.1. *Let $b=(2^{k-1}-1)Q+R$. If*

$$Q \geqq \begin{cases} R & \text{when} \quad 0 \leqq R \leqq 2^{k-2}-1, \\ R-2^{k-2} & \text{when} \quad 2^{k-2} \leqq R \leqq 2^{k-1}-2, \end{cases}$$

(*this is the case when $b \geqq (2^{k-1}-1)(2^{k-2}-1)$*), *then*

$$m_k(b+2^{k-1}-1) = m_k(b)+2^k-1.$$

Proof. By Lemma 4.1 (2), it suffices to prove

$$m_k(b+2^{k-1}-1) \leqq m_k(b)+2^k-1. \tag{9.2}$$

Remember the polyhedron $P(b)$ defined by (2^k-1) inequalities

$$\sum_{(u,v)=0} a_v \leqq b \quad \text{for each } u \in (\mathbb{Z}/2)^k \backslash \{0\}. \tag{9.3}$$

We will find m such that the intersection of $P(b+2^{k-1}-1)$ with a half space $H^+(m)$ in $\mathbb{R}^{2^k-1}$ defined by

$$H^+(m) = \{\sum a_v \geqq m\}$$

has a lattice point with coordinates $\geqq 1$.

Case 1. The case where $0 \leqq R \leqq 2^{k-2}-1$. In this case we take

$$m = (2^k-1)(Q+1)+R.$$

Since

$$b+2^{k-1}-1 = (2^{k-1}-1)(Q+1)+R,$$

the coordinates of a vertex (except the vertex x of $P(b+2^{k-1}-1)$) in $P(b+2^{k-1}-1)\cap H^+(m)$ are either $Q+1+R$ or $Q+1-R$ by Lemma 7.3, so those vertices are lattice points and their coordinates are greater than or equal to 1 since $Q \geqq R$ by assumption. We know

$$m_k(b+2^{k-1}-1) \geqq (2^k-1)(Q+1)+R$$

by Lemma 7.1, so any lattice point (a_v) in (9.3) with b replaced by $b+2^{k-1}-1$, at which $\sum a_v$ attains the maximum value $m_k(b+2^{k-1}-1)$, lies in $P(b+2^{k-1}-1)\cap H^+(m)$ and hence $a_v \geqq 1$ for every v. Since $\{a_v-1\}$ is a set of non-negative integers which satisfy (9.3) and

$$\sum(a_v-1) = m_k(b+2^{k-1}-1)-(2^k-1),$$

it follows from the definition of $m_k(b)$ that

$$m_k(b+2^{k-1}-1)-(2^k-1) \leqq m_k(b),$$

proving the desired inequality (9.2).

Case 2. The case where $2^{k-2} \leqq R \leqq 2^{k-1}-2$. In this case we take

$$m = (2^k-1)(Q+1)+R+2^{k-2}.$$

Then the coordinates of a vertex (except the vertex x) in $P(b+2^{k-1}-1)\cap H^+(m)$ are either $Q+2+R-2^{k-2}$ or $Q+1-R+2^{k-2}$ by Lemma 7.3, so those vertices are lattice points and their coordinates are greater than or equal to 1 since $Q \geqq R-2^{k-2}$ by assumption. We know

$$m_k(b+2^{k-1}-1) \geqq (2^k-1)(Q+1)+R+2^{k-2}$$

by Proposition 7.5, so any lattice point (a_v) in (9.3) with b replaced by $b+2^{k-1}-1$, at which $\sum a_v$ attains the maximum value $m_k(b+2^{k-1}-1)$, lies in $P(b+2^{k-1}-1)\cap H^+(m)$ and hence $a_v \geqq 1$ for every v. The remaining argument is same as in Case 1 above. □

Appendix

Below is a table of values of $s_{\mathbb{R}}(m,p)$ for $2 \leqq p \leqq 18$ and $2 \leqq m \leqq 40$.

$m\backslash p$	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2	2																
3	2	3															
4	1	3	4														
5	1	2	4	5													
6	1	2	3	5	6												
7	1	1	3	4	6	7											
8	1	1	2	4	4	7	8										
9	1	1	2	2	4	5	8	9									
10	1	1	1	2	3	5	6	9	10								
11	1	1	1	2	3	4	6	7	10	11							
12	1	1	1	2	2	4	$* \leqq 5$	7	8	11	12						
13	1	1	1	1	2	3	*	$* \leqq 6$	8	9	12	13					
14	1	1	1	1	2	3	4	*	$* \leqq 7$	9	10	13	14				
15	1	1	1	1	2	2	4	5	*	$* \leqq 8$	10	11	14	15			
16	1	1	1	1	1	2	2	5	*	*	$* \leqq 9$	11	11	15	16		
17	1	1	1	1	1	2	2	3	$* \geqq 5$	*	*	$* \leqq 10$	11	12	16	17	
18	1	1	1	1	1	2	2	3	3	$* \geqq 5$	*	*	*	12	13	17	18
19	1	1	1	1	1	1	2	2	3	4	*	*	*	*	13	14	18
20	1	1	1	1	1	1	2	2	3	4	5	*	*	*	*	14	15
21	1	1	1	1	1	1	2	2	3	3	5	*	*	*	*	*	15
22	1	1	1	1	1	1	1	2	2	3	4	*	*	*	*	*	*
23	1	1	1	1	1	1	1	2	2	2	4	5	*	*	*	*	*
24	1	1	1	1	1	1	1	2	2	2	3	5	*	*	*	*	*
25	1	1	1	1	1	1	1	1	2	2	3	3	$* \geqq 5$	*	*	*	*
26	1	1	1	1	1	1	1	1	2	2	2	3	4	*	*	*	*
27	1	1	1	1	1	1	1	1	2	2	2	3	4	*	*	*	*
28	1	1	1	1	1	1	1	1	1	2	2	3	3	$* \geqq 5$	*	*	*
29	1	1	1	1	1	1	1	1	1	2	2	2	3	4	*	*	*
30	1	1	1	1	1	1	1	1	1	2	2	2	2	4	5	*	*
31	1	1	1	1	1	1	1	1	1	1	2	2	2	3	5	6	*
32	1	1	1	1	1	1	1	1	1	1	2	2	2	3	3	6	*
33	1	1	1	1	1	1	1	1	1	1	2	2	2	2	3	3	$* \geqq 6$
34	1	1	1	1	1	1	1	1	1	1	1	2	2	2	3	3	4
35	1	1	1	1	1	1	1	1	1	1	1	2	2	2	3	3	4
36	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	3	3
37	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	3
38	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	3
39	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	3
40	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2

Table 2. $s_{\mathbb{R}}(m,p)$ for $2 \leqq p \leqq 18,\ 2 \leqq m \leqq 40$

Since $s_{\mathbb{R}}(m,1) = 1$, the case where $p = 1$ is omitted. Remember that $s_{\mathbb{R}}(m,p) = 1$ if and only if $m \geqq 3p-2$ by Theorem 3.1 and that The values of $s_{\mathbb{R}}(m,p)$ for $p = m-1, m-2$ and $m-3$ can be obtained from Theorems 2.4 and 2.7. The other values can be obtained from Table 1 in Section 6 and the fact that $s_{\mathbb{R}}(m,p) = k$ for $k \geqq 2$ if and only if $m_{k+1}(p-1) < m \leqq m_k(p-1)$ (Lemma 3.5). The asterisk $*$ in a box means that the value is unknown. Finally we note that $s_{\mathbb{R}}(m,p)$ increases as p increases while it decreases as m increases (Proposition 2.3).

Acknowledgment. The authors thank Suyoung Choi for his help to find $k \times m$ matrices which realize $s_{\mathbb{R}}(m, p) = k$ for small values of m and p.

References

[1] V. M. Buchstaber, *Lectures on toric topology*, Trends in Mathematics, Information Center for Mathematical Sciences, vol. 11, No. 1 (2008), 1–55.

[2] V. M. Buchstaber and T. E. Panov, *Torus Actions and Their Applications in Topology and Combinatorics*, University Lecture, vol. **24**, Amer. Math. Soc., Providence, R.I., 2002.

[3] M. W. Davis and T. Januszkiewicz, *Convex polytopes, Coxeter orbifolds and torus actions*, Duke Math. J. **62** (1991), 417–451.

[4] M. Harada, Y. Karshon, M. Masuda and T. Panov (eds), *Toric Topology*, Proc. of the International Conference held at Osaka City University in 2006, Contemp. Math. 460 (2008).

Department of Mathematics, Osaka City University, Sumiyoshi-ku, Osaka 558-8585, Japan.

E-mail address: m09sa024@ex.media.osaka-cu.ac.jp

E-mail address: masuda@sci.osaka-cu.ac.jp