Algebraic & Geometric Topology 18 (2018) 2729–2767

Self-dual binary codes from small covers and simple polytopes

BO CHEN
ZHI LÜ
LI YU

The work of Volker Puppe and Matthias Kreck exhibited some intriguing connections between the algebraic topology of involutions on closed manifolds and the combinatorics of self-dual binary codes. On the other hand, the work of Michael Davis and Tadeusz Januszkiewicz brought forth a topological analogue of smooth, real toric varieties, known as "small covers", which are closed smooth manifolds equipped with some actions of elementary abelian 2–groups whose orbit spaces are simple convex polytopes. Building on these works, we find various new connections between all these topological and combinatorial objects and obtain some new applications to the study of self-dual binary codes, as well as colorability of polytopes. We first show that a small cover M^n over a simple n–polytope P^n produces a self-dual code in the sense of Kreck and Puppe if and only if P^n is n–colorable and n is odd. Then we show how to describe such a self-dual binary code in terms of the combinatorics of P^n. Moreover, we can construct a family of binary codes $\mathfrak{B}_k(P^n)$, for $0 \le k \le n$, from an arbitrary simple n–polytope P^n. Then we give some necessary and sufficient conditions for $\mathfrak{B}_k(P^n)$ to be self-dual. A spinoff of our study of such binary codes gives some new ways to judge whether a simple n–polytope P^n is n–colorable in terms of the associated binary codes $\mathfrak{B}_k(P^n)$. In addition, we prove that the minimum distance of the self-dual binary code obtained from a 3–colorable simple 3–polytope is always 4.

57M60, 57R91, 57S25, 94B05

1 Introduction

As described by Rains and Sloane in [23], self-dual codes are an important class of linear codes for both theoretical and practical reasons. It is a fundamental problem to classify self-dual codes of modest lengths and determine the largest minimum weight among self-dual codes of that length. Much work has been done towards classifying self-dual codes over $\mathbb{F}_q$ for $q = 2$ and 3, where $\mathbb{F}_q$ denotes the finite field of order q. Codes over $\mathbb{F}_2$ are called *binary* and all codes in this paper are binary. The dual code $C^{\perp}$

Published: 22 August 2018 DOI: 10.2140/agt.2018.18.2729

of a binary code C of length l is defined as $C^{\perp} := \{u \in \mathbb{F}_2^l \mid \langle u, c\rangle = 0 \text{ for all } c \in C\}$, where $\langle\, ,\rangle$ is the standard inner product. A binary code C is called *self-dual* if $C = C^{\perp}$.

Puppe [22] found an interesting connection between closed manifolds and self-dual binary codes. It was shown in [22] that an involution τ on an odd-dimensional closed manifold M with "maximal number of isolated fixed points" $\big($ie with only isolated fixed points and the number of fixed points satisfying $|M^{\tau}| = \dim_{\mathbb{F}_2}\big(\bigoplus_i H^i(M;\mathbb{F}_2)\big)\big)$ determines a self-dual binary code of length $|M^{\tau}|$. Such an involution τ is called an m–*involution*. Conversely, Kreck and Puppe [17] proved a somewhat surprising theorem that any self-dual binary code can be obtained from an m–involution on some closed 3–manifold. Hence it is an interesting problem for us to search for m–involutions on closed manifolds. But in practice it is very difficult to construct all possible m–involutions on a given manifold.

On the other hand, Davis and Januszkiewicz [8] introduced a class of closed smooth manifolds M^n with locally standard actions of the elementary 2–group $\mathbb{Z}_2^n$, called *small covers*, whose orbit space is an n–dimensional simple convex polytope P^n in $\mathbb{R}^n$. They showed that many geometric and topological properties of a small cover M^n can be explicitly described in terms of the combinatorics of P^n and some characteristic function on P^n determined by the $\mathbb{Z}_2^n$–action. For example, the k^{th} mod 2 Betti number of M^n is equal to $h_k(P^n)$, where $(h_0(P^n), h_1(P^n), \dots, h_n(P^n))$ is the *h–vector* of P^n.

Note that any nonzero element $g \in \mathbb{Z}_2^n$ determines a nontrivial involution on the small cover M^n, denoted by τ_g. We call τ_g a *regular involution* on M^n. So whenever τ_g is an m–involution on M^n, where n is odd, we obtain a self-dual binary code from (M^n, τ_g).

Motivated by the work of Kreck and Puppe and the work of Davis and Januszkiewicz, our purpose in this paper is to explore the connection between the theory of binary codes and the combinatorics of simple polytopes via the topology of small covers. First, we can tell when a small cover M^n over an n–dimensional simple polytope P^n has a regular m–involution by the following theorem.

Theorem 3.2 *Let λ be the characteristic function determined by a small cover M^n over a simple n–polytope P^n. Then the following statements are equivalent:*

(a) *There exists a regular* m*–involution on M^n.*

(b) *There exists a regular involution on M^n with only isolated fixed points.*

(c) *The image* $\operatorname{Im}\lambda \subseteq \mathbb{Z}_2^n$ *of λ consists of exactly n elements* (which implies that P^n is n–colorable) *and so they form a basis of $\mathbb{Z}_2^n$.*

A polytope is called *n–colorable* if we can color all the facets of the polytope by n different colors so that any neighboring facets are assigned different colors. Note if λ and λ' are both characteristic functions over a simple polytope P^n that satisfy condition (c) in Theorem 3.2, the small covers M^n and N^n determined by (P^n,λ) and (P^n,λ') are equivalent in the sense that there is a homeomorphism $f\colon M^n \to N^n$ and a $\sigma \in \mathrm{GL}(n,\mathbb{Z}_2)$ such that $f(g\cdot x)=\sigma(g)\cdot f(x)$ for any $g\in\mathbb{Z}_2^n$ and $x\in M^n$. This implies that up to equivalence of binary codes, the self-dual binary code C_{M^n} obtained from a regular m–involution on an n–dimensional small cover M^n over P^n (which has to be n–colorable, with n odd) is essentially determined by the polytope P^n. Moreover, we can spell out the code C_{M^n} directly from the combinatorics of P^n as follows.

Let the vertex set of P^n be $\{v_1,\dots,v_{2r}\}$. Here the number of vertices of P^n must be even because P^n is n–colorable (see Joswig [15]). Any face f of P^n determines an element $\xi_f\in\mathbb{F}_2^{2r}$, where the i^{th} entry of ξ_f is 1 if and only if v_i is a vertex of f. In particular,

$$\xi_{P^n}=\underline{1}=(1,\dots,1)\in\mathbb{F}_2^{2r},$$

and $\{\xi_{v_1},\dots,\xi_{v_{2r}}\}$ is a linear basis of $\mathbb{F}_2^{2r}$. We define a sequence of binary codes by

$$\mathfrak{B}_k(P^n):=\mathrm{Span}_{\mathbb{F}_2}\{\xi_f\mid f \text{ is a codimension-}k\text{ face of } P^n\}\subseteq\mathbb{F}_2^{2r}\quad\text{for } 0\le k\le n.$$

By a close examination of the localization of the equivariant cohomology of a small cover M^n to its fixed-point set (in the proof of Theorem 4.3), we obtain in Corollary 4.5 that the self-dual binary code C_{M^n} is equivalent to $\mathfrak{B}_{(n-1)/2}(P^n)$. This builds a direct connection between the combinatorics of simple polytopes and self-dual binary codes. An interesting consequence of this connection is that we can detect various properties of such self-dual binary codes from the combinatorics of the corresponding polytopes. This might help us construct self-dual binary codes with certain prescribed properties.

The key idea of the proof of Theorem 4.3 is understanding the image of the localization of the equivariant cohomology $H^*_{G_\tau}(M^n;\mathbb{F}_2)\to H^*_{G_\tau}((M^n)^{G_\tau};\mathbb{F}_2)$ to the fixed points, where G_τ is the $\mathbb{Z}_2$–subgroup generated by the regular m–involution on M^n, in terms of the localization map $H^*_{\mathbb{Z}_2^n}(M^n;\mathbb{F}_2)\to H^*_{\mathbb{Z}_2^n}((M^n)^{\mathbb{Z}_2^n};\mathbb{F}_2)$ of the whole $\mathbb{Z}_2^n$–action on M^n. Indeed, we have a commutative diagram (see (12))

$$\begin{tikzcd}
H^*_{\mathbb{Z}_2^n}(M^n;\mathbb{F}_2) \arrow[r, "\phi^*"] \arrow[d, "i_4^*"'] & H^*_{G_\tau}(M^n;\mathbb{F}_2) \arrow[d, "i_3^*"] \\
H^*_{\mathbb{Z}_2^n}((M^n)^{\mathbb{Z}_2^n};\mathbb{F}_2) \arrow[r, "\psi^*"'] & H^*_{G_\tau}((M^n)^{G_\tau};\mathbb{F}_2)
\end{tikzcd}$$

where we can show that ϕ^* is a group epimorphism. So the image of the localization map i_3^* is the image of the composite map $\psi^* \circ i_4^*$. Then we use some results on small covers from Davis and Januszkiewicz [8] to give an explicit description of i_4^* and derive Theorem 4.3. The reader is referred to Allday and Puppe [2] for the basic theory of equivariant cohomology, localization and classifying spaces.

Note that the definition of $\mathfrak{B}_k(P^n)$ depends only on the combinatorial structure of P^n and makes perfect sense for general simple polytopes (not necessarily n–colorable). For a general simple polytope P^n, we can show (see Proposition 5.3) that $\dim_{\mathbb{F}_2} \mathfrak{B}_k(P^n) \geq h_0(P^n) + \cdots + h_k(P^n)$ for any $0 \leq k \leq n$. Moreover, we can detect some properties of P^n from the family of codes $\{\mathfrak{B}_k(P^n)\}_{0 \leq k \leq n}$. For example, it is shown in the following proposition that we can tell whether P^n is n–colorable by simply computing the dimension of $\mathfrak{B}_1(P^n)$.

Proposition 5.5 *Let P^n be an n–dimensional simple polytope with m facets. Then $\dim_{\mathbb{F}_2} \mathfrak{B}_1(P^n) = m - n + 1$ if and only if P^n is n–colorable.*

There is a special class of binary codes called doubly even codes, which are intensively studied by both mathematicians and engineers. A binary code C is called *doubly even* if the Hamming weight of any codeword in C is divisible by 4. Doubly even self-dual binary codes are of particular importance both theoretically and practically. We can determine which kind of n–colorable simple n–polytopes can produce a doubly even self-dual binary code in our approach. This gives us a purely combinatorial way to construct doubly even self-dual binary codes. But unfortunately, we find that some famous binary codes of this type such as the extended Golay code and the extended quadratic residue code cannot be obtained from any n–colorable simple n–polytope.

The paper is organized as follows. In Section 2, we introduce the basic notions and facts about binary codes and simple polytopes that we use. Additionally, we briefly explain the procedure of obtaining self-dual binary codes, as described by Puppe in [22], from m–involutions on closed manifolds. In Section 3, we first recall some basic facts of small covers and then investigate when a small cover can admit a regular m–involution (see Theorem 3.2). In Section 4, we spell out the self-dual binary code from a small cover with a regular m–involution (see Corollary 4.5). It turns out that the self-dual binary code depends only on the combinatorial structure of the underlying simple polytope. In Section 5, we study the properties of the family of binary codes $\mathfrak{B}_k(P^n)$, $0 \leq k \leq n$, associated to any simple n–polytope P^n. A spinoff of our study produces several new criteria to judge whether P^n is n–colorable in terms of the associated binary codes $\mathfrak{B}_k(P^n)$ (see Proposition 5.5 and Proposition 5.6). In Section 6, we will give some necessary and sufficient conditions for $\mathfrak{B}_k(P^n)$ to be self-dual codes for general simple polytopes P^n (see Theorem 6.2). In Section 7, we prove that the minimum distance of the self-dual binary code obtained from any 3–colorable simple 3–polytope is always 4 (see Proposition 7.1). In Section 8, we investigate some special properties of n–colorable simple n–polytopes. In Section 9, we study what kind of doubly even binary codes can be obtained from n–colorable simple n–polytopes. In particular, we show that the extended Golay code and the extended quadratic residue code cannot be obtained from any n–colorable simple n–polytopes.

2 Preliminaries

Here we collect some necessary information about binary codes and simple polytopes and briefly explain the construction of self-dual binary codes from m–involutions on manifolds.

2.1 Self-dual binary codes

A (linear) *binary code* C of length l is a linear subspace of the l–dimensional linear space $\mathbb{F}_2^l$ over $\mathbb{F}_2$ (the binary field). The *Hamming weight* of an element $u=(u_1,\dots,u_l)\in\mathbb{F}_2^l$, denoted by $\mathrm{wt}(u)$, is the number of nonzero coordinates u_i in u. Any element of C is called a *codeword*. The *Hamming distance* $d(u,v)$ between any two codewords $u,v\in C$ is defined by

$$d(u,v)=\mathrm{wt}(u-v).$$

The minimum of the Hamming distances $d(u,v)$ for all $u,v\in C$, where $u\neq v$, is called the *minimum distance* of C (which also equals the minimum Hamming weight of nonzero elements in C). A binary code $C\subseteq\mathbb{F}_2^l$ is called *type* $[l,k,d]$ if $\dim_{\mathbb{F}_2} C=k$ and the minimum distance of C is d. We call two binary codes in $\mathbb{F}_2^l$ *equivalent* if they differ only by a permutation of coordinates.

A *generator matrix* for a binary code C is a binary matrix whose rows form a basis for C. Then the codewords of C are all of the linear combinations of the rows of this matrix, that is, C is the row space of its generator matrix.

The standard bilinear form $\langle\ ,\ \rangle$ on $\mathbb{F}_2^l$ is defined by

$$\langle u,v\rangle:=\sum_{i=1}^{l}u_iv_i \quad \text{for } u=(u_1,\dots,u_l),\ v=(v_1,\dots,v_l)\in\mathbb{F}_2^l.$$

Note that $\langle u, v\rangle = \frac{1}{2}(\mathrm{wt}(u)+\mathrm{wt}(v)-\mathrm{wt}(u+v)) \bmod 2$ for any $u, v \in \mathbb{F}_2^l$, and

$$\langle u, u\rangle = \sum_{i=1}^{l} u_i \quad \text{for } u = (u_1, \dots, u_l) \in \mathbb{F}_2^l.$$

Any linear binary code C in $\mathbb{F}_2^l$ has the *dual code* $C^\perp$ defined by

$$C^\perp := \{u \in \mathbb{F}_2^l \mid \langle u, c\rangle = 0 \text{ for all } c \in C\}.$$

It is clear that $\dim_{\mathbb{F}_2} C + \dim_{\mathbb{F}_2} C^\perp = l$. We call C *self-dual* if $C = C^\perp$. For a self-dual binary code C, we can easily show the following:

- The length $l = 2\dim_{\mathbb{F}_2} C$ must be even.
- For any $u \in C$, the Hamming weight $\mathrm{wt}(u)$ is an even integer since $\langle u, u\rangle = 0$.
- The minimum distance of C is an even integer.

Self-dual binary codes play an important role in coding theory and have been studied extensively (see [23] for a detailed survey).

2.2 Simple polytopes

A (convex) polytope P is the convex hull of a finite set of points in some Euclidean space. The dimension of P is the dimension of the affine hull of these points. We refer to n–dimensional convex polytopes simply as n–polytopes. Two polytopes P and Q are *combinatorially equivalent* ($P \simeq Q$) if there is a bijection between their faces preserving the inclusion relation. An n–polytope P^n is called *simple* if each vertex of P^n is the intersection of exactly n distinct *facets* (codimension-one faces) of P^n. Any 0–face of P^n is called a *vertex* and any 1–face of P^n is called an *edge*. Let $V(P^n)$ denote the set of vertices of P.

Let $f_i(P^n)$ be the number of i–faces of P^n. The vector $(f_0(P^n), f_1(P^n), \dots, f_n(P^n))$ is called the *f–vector* of P^n. Let $h_k(P^n)$ be the coefficient of t^{n-k} in the polynomial $\sum_{i=0}^{n} f_i(P^n)(t-1)^i$. Then the vector $(h_0(P^n), h_1(P^n), \dots, h_n(P^n))$ is called the *h–vector* of P^n. It is easy to see that $h_0(P^n) = 1$, $h_1(P^n) = f_{n-1}(P^n) - n$ and

$$\sum_{i=0}^{n} h_i(P^n) = f_0(P^n) = |V(P^n)|,$$

where $|V(P^n)|$ is the number of vertices of P^n. For a general simple n–polytope P^n, there are many relations among the $h_k(P^n)$. Indeed, the famous g–theorem (see [5, Section 1.3]) characterizes all possible integer vectors that are the h–vector of some simple polytope.

Definition For positive integers a and i, define $a^{\langle i\rangle}=\binom{a_i+1}{i+1}+\binom{a_{i-1}+1}{i}+\cdots+\binom{a_j+1}{j+1}$ and $0^{\langle i\rangle}=0$, where $a=\binom{a_i}{i}+\binom{a_{i-1}}{i-1}+\cdots+\binom{a_j}{j}$ is the unique *binomial i–expansion* of a with $a_i>a_{i-1}>\cdots>a_j\geq j\geq 1$.

Theorem (g–theorem) *An integer vector $(h_0,h_1,\dots,h_n)$ is the h–vector of a simple n–polytope if and only if the following conditions are satisfied:*

(i) ***Dehn–Sommerville relations*** $h_i=h_{n-i}$ *for* $0\leq i\leq n$.

(ii) $h_0\leq h_1\leq\cdots\leq h_{[n/2]}$ *for* $0\leq i\leq n/2$.

(iii) $h_0=1$ *and* $h_{i+1}-h_i\leq(h_i-h_{i-1})^{\langle i\rangle}$ *for* $1\leq i\leq[n/2]-1$.

Our study of binary codes in Section 5 leads to some new criteria to judge whether a simple n–polytope is n–colorable. The following are some known descriptions of n–colorable simple n–polytopes due to Joswig [15].

Theorem 2.1 [15, Theorem 16 and Corollary 21] *Let P^n be an n–dimensional simple polytope, where $n\geq 3$. The following statements are equivalent:*

(a) *P^n is n–colorable.*

(b) *Each 2–face of P^n has an even number of vertices.*

(c) *Each face of P^n with dimension greater than 0 (including P^n itself) has an even number of vertices.*

(d) *Any proper k–face of P^n is k–colorable.*

2.3 Binary codes from m–involutions on manifolds

Let τ be an involution on a closed connected n–dimensional manifold M which has only isolated fixed points. Let $G_\tau\cong\mathbb{Z}_2$ denote the binary group generated by τ. By Conner [7, page 82], the number $|M^{G_\tau}|$ of the fixed-point set M^{G_τ} of G_τ must be even. So we assume that $|M^{G_\tau}|=2r$, where $r\geq 1$, in the following discussion. By [2, Proposition (1.3.14)], the following statements are equivalent:

(a) $|M^{G_\tau}|=\sum_{i=0}^n b_i(M;\mathbb{F}_2)$ (ie τ is an m–involution).

(b) $H^*_{G_\tau}(M;\mathbb{F}_2)$ is a free $H^*(BG_\tau;\mathbb{F}_2)$–module, so
$$H^*_{G_\tau}(M;\mathbb{F}_2)=H^*(M;\mathbb{F}_2)\otimes H^*(BG_\tau;\mathbb{F}_2).$$

(c) The inclusion of the fixed-point set, $\iota\colon M^{G_\tau}\hookrightarrow M$, induces a monomorphism
$$\iota^*\colon H^*_{G_\tau}(M;\mathbb{F}_2)\to H^*_{G_\tau}(M^{G_\tau};\mathbb{F}_2)\cong\mathbb{F}_2^{2r}\otimes\mathbb{F}_2[t].$$

Next we assume that τ is an m–involution on M. So the image of $H^*_{G_\tau}(M;\mathbb{F}_2)$ in $\mathbb{F}_2^{2r}\otimes\mathbb{F}_2[t]$ under the localization map ι^* is isomorphic to $H^*_{G_\tau}(M;\mathbb{F}_2)$ as graded algebras. It is shown in [6; 22] that the image $\iota^*(H^*_{G_\tau}(M;\mathbb{F}_2))$ can be described in the following way. For any vectors $x=(x_1,\dots,x_{2r})$ and $y=(y_1,\dots,y_{2r})$ in $\mathbb{F}_2^{2r}$, define

$$x\circ y=(x_1y_1,\dots,x_{2r}y_{2r}).$$

It is clear that $\mathbb{F}_2^{2r}$ forms a commutative ring with respect to the two operations $+$ and $\circ$. Actually, $(\mathbb{F}_2^{2r},+,\circ)$ is a boolean ring. Notice that $x\circ x=x$ for any $x\in\mathbb{F}_2^{2r}$. Let

$$\mathcal{V}_{2r}=\left\{x=(x_1,\dots,x_{2r})\in\mathbb{F}_2^{2r}\;\middle|\;\langle x,x\rangle=\sum_{i=1}^{2r}x_i=0\in\mathbb{F}_2\right\}. \tag{1}$$

Then $\mathcal{V}_{2r}$ is a $(2r-1)$–dimensional linear subspace of $\mathbb{F}_2^{2r}$. Note that for any $u\in\mathcal{V}_{2r}$, the Hamming weight $\mathrm{wt}(u)$ of u is an even integer. The following lemma is immediate from our definitions.

Lemma 2.2 *Let C be a binary code in $\mathbb{F}_2^{2r}$ with $\dim_{\mathbb{F}_2}C=r$. Then the following statements are equivalent:*

(C1) *C is self-dual.*

(C2) *$\langle x,y\rangle=0$ for any $x,y\in C$.*

(C3) *$x\circ y\in\mathcal{V}_{2r}$ for any $x,y\in C$.*

Moreover, let

$$\begin{aligned} V_k^M&=\{y\in\mathbb{F}_2^{2r}\mid y\otimes t^k\in\mathrm{Im}(\iota^*)\}\subseteq\mathbb{F}_2^{2r}\quad\text{for } k=0,\dots,n;\\ V_{-1}^M&=\{0\}.\end{aligned} \tag{2}$$

By the localization theorem for equivariant cohomology (see [2]), we have isomorphisms

$$H^k(M;\mathbb{F}_2)\cong V_k^M/V_{k-1}^M\quad\text{for } 0\le k\le n. \tag{3}$$

Theorem 2.3 [6, Theorem 3.1; 22, page 213] *For any $0\le k\le n$, we have*

$$\dim_{\mathbb{F}_2}V_k^M=\sum_{j=0}^k b_j(M;\mathbb{F}_2).$$

In addition, $H^*_{G_\tau}(M;\mathbb{F}_2)$ is isomorphic to the graded ring

$$\mathcal{R}_M=V_0^M+V_1^Mt+\cdots+V_{n-2}^Mt^{n-2}+V_{n-1}^Mt^{n-1}+\mathbb{F}_2^{2r}(t^n+t^{n+1}+\cdots),$$

where the ring structure of $\mathcal{R}_M$ is given by the following:

(a) $\mathbb{F}_2 \cong V_0^M \subseteq V_1^M \subseteq \cdots \subseteq V_{n-2}^M \subseteq V_{n-1}^M = \mathcal{V}_{2r} \subseteq V_n^M = \mathbb{F}_2^{2r}$, *where* V_0^M *is generated by* $\underline{1} = (1, \dots, 1) \in \mathbb{F}_2^{2r}$.

(b) *For* $d = \sum_{i=0}^{n-1} i d_i < n$ *with each* $d_i \geq 0$, *the composition* $v_{\omega_{d_0}} \circ \cdots \circ v_{\omega_{d_{n-1}}}$ *is in* V_d^M, *where*

$$v_{\omega_{d_i}} = v_1^{(i)} \circ \cdots \circ v_{d_i}^{(i)} \quad \text{for some } v_j^{(i)} \in V_i^M.$$

The operation $\circ$ *on* $\mathbb{F}_2^{2r}$ *corresponds to the cup product in* $H^*_{G_\tau}(M;\mathbb{F}_2)$.

Each V_k^M above can be thought of as a binary code in $\mathbb{F}_2^{2r}$. Theorem 2.3 and the Poincaré duality of M imply that

$$\dim_{\mathbb{F}_2} V_k^M + \dim_{\mathbb{F}_2} V_{n-1-k}^M = \sum_{j=0}^{n} b_j(M;\mathbb{F}_2) = 2r. \tag{4}$$

In addition, V_{n-1-k}^M is perpendicular to V_k^M with respect to $\langle\ ,\ \rangle$. This is because

$$H_G^k(M;\mathbb{F}_2) \cong V_k^M t^k \quad \text{and} \quad H_G^{n-k-1}(M;\mathbb{F}_2) \cong V_{n-k-1}^M t^{n-k-1}.$$

So for any $x \in V_k^M$ and $y \in V_{n-k-1}^M$, we have that $xt^k \cup yt^{n-k-1} = (x \circ y)t^{n-1}$ belongs to $H_G^{n-1}(M;\mathbb{F}_2) \cong \mathcal{V}_{2r} t^{n-1}$ by Theorem 2.3(b). Then, by Lemma 2.2, $x \circ y \in \mathcal{V}_{2r}$ implies $\langle x, y \rangle = 0$. So we have $V_{n-1-k}^M \subseteq (V_k^M)^\perp$. Moreover, $\dim_{\mathbb{F}_2} V_{n-1-k}^M = \dim_{\mathbb{F}_2} (V_k^M)^\perp$ by (4). This implies that

$$(V_k^M)^\perp = V_{n-1-k}^M. \tag{5}$$

Corollary 2.4 $V_k^M \subseteq \mathbb{F}_2^{2r}$ *is self-dual if and only if* $\dim_{\mathbb{F}_2} V_k^M = \sum_{j=0}^{k} b_j(M;\mathbb{F}_2) = r$.

Proof The necessity is trivial. If $\dim_{\mathbb{F}_2} V_k^M = r$, then $\dim_{\mathbb{F}_2} V_{n-1-k}^M = r$ by (4). But by Theorem 2.3(a), we have either $V_k^M \subseteq V_{n-1-k}^M$ or $V_{n-1-k}^M \subseteq V_k^M$. Then V_k^M and V_{n-1-k}^M must be equal since they have the same dimension. So by (5), $(V_k^M)^\perp = V_{n-1-k}^M = V_k^M$. Hence V_k^M is self-dual. □

3 Small covers with m–involutions

3.1 Small covers

Following [8], an n–dimensional *small cover* is a closed n–manifold M^n with a locally standard $\mathbb{Z}_2^n$–action whose orbit space is homeomorphic to an n–dimensional simple convex polytope P^n, where "locally standard" means that this $\mathbb{Z}_2^n$–action on M^n is locally isomorphic to the standard faithful representation of $\mathbb{Z}_2^n$ on $\mathbb{R}^n$ (ie the n–fold Cartesian product of the natural representation of $\mathbb{Z}_2$ on $\mathbb{R}$). Let $\pi\colon M^n \to P^n$ be the orbit map. Let $\mathcal{F}(P^n)$ denote the set of all facets of P^n. For any facet F of P^n, the isotropy subgroup of $\pi^{-1}(F)$ in M^n with respect to the $\mathbb{Z}_2^n$–action is a rank-1 subgroup of $\mathbb{Z}_2^n$ generated by an element of $\mathbb{Z}_2^n$, denoted by $\lambda(F)$. Then we obtain a map $\lambda\colon \mathcal{F}(P^n) \to \mathbb{Z}_2^n$, called the *characteristic function* associated to M^n, which maps the n facets meeting at each vertex of P^n to n linearly independent elements in $\mathbb{Z}_2^n$. It is shown in [8] that up to equivariant homeomorphisms, M^n can be recovered from (P^n, λ) in a canonical way (see (8)). Moreover, many algebraic topological invariants of a small cover $\pi\colon M^n \to P^n$ can be easily computed from (P^n, λ). Here is a list of facts on the cohomology rings of small covers proved in [8]:

(R1) Let $b_i(M^n; \mathbb{F}_2)$ be the i^{th} mod 2 Betti number of M^n. Then

$$b_i(M^n; \mathbb{F}_2) = h_i(P^n) \quad \text{for } 0 \le i \le n,$$

where $(h_0(P^n), h_1(P^n), \dots, h_n(P^n))$ is the h–vector of P^n.

(R2) Let $(M^n)^{\mathbb{Z}_2^n}$ denote the fixed-point set of the $\mathbb{Z}_2^n$–action on M^n. Then

$$|(M^n)^{\mathbb{Z}_2^n}| = \sum_{i=0}^{n} b_i(M^n; \mathbb{F}_2) = \sum_{i=0}^{n} h_i(P^n) = |V(P^n)|.$$

(R3) The equivariant cohomology $H^*_{\mathbb{Z}_2^n}(M^n; \mathbb{F}_2)$ is isomorphic as graded rings to the Stanley–Reisner ring of P^n

$$H^*_{\mathbb{Z}_2^n}(M^n; \mathbb{F}_2) \cong \mathbb{F}_2(P^n) = \mathbb{F}_2[a_{F_1}, \dots, a_{F_m}]/\mathcal{I}_{P^n}, \tag{6}$$

where $F_1, \dots, F_m$ are all the facets of P^n and $a_{F_1}, \dots, a_{F_m}$ are of degree 1, and $\mathcal{I}_{P^n}$ is the ideal generated by all square-free monomials of $a_{F_{i_1}} \cdots a_{F_{i_s}}$ with $F_{i_1} \cap \cdots \cap F_{i_s} = \varnothing$ in P^n.

(R4) The mod 2 cohomology ring satisfies

$$H^*(M^n; \mathbb{F}_2) \cong \mathbb{F}_2[a_{F_1}, \dots, a_{F_m}]/\mathcal{I}_P + J_\lambda,$$

where J_λ is an ideal determined by λ. In particular, $H^*(M^n; \mathbb{F}_2)$ is generated by degree-1 elements.

3.2 Spaces constructed from simple polytopes with $\mathbb{Z}_2^r$–colorings

Let P^n be an n–dimensional simple polytope in $\mathbb{R}^n$. For any $r \geq 0$, a $\mathbb{Z}_2^r$–coloring on P^n is a map $\mu\colon \mathcal{F}(P^n) \to \mathbb{Z}_2^r$. For any facet F of P^n, we call $\mu(F)$ the *color of* F. Since P^n is simple, any codimension-k face of P^n is the intersection of a unique collection of k facets of P^n. Let $f = F_1 \cap \cdots \cap F_k$ be a codimension-k face of P^n, where $F_1, \dots, F_k \in \mathcal{F}(P^n)$. Define

$$G_f^{\mu} = \text{the subgroup of } \mathbb{Z}_2^r \text{ generated by } \mu(F_1), \dots, \mu(F_k). \tag{7}$$

Additionally, let G^{μ} be the subgroup of $\mathbb{Z}_2^r$ generated by $\{\mu(F) \mid F \in \mathcal{F}(P^n)\}$. The rank of G^{μ} is called the *rank of* μ, denoted by $\operatorname{rank}(\mu)$. It is clear that $\operatorname{rank}(\mu) \leq r$.

For any point $p \in P^n$, let $f(p)$ denote the unique face of P^n that contains p in its relative interior. Then we define a space associated to (P^n, μ) by

$$M(P^n, \mu) = P^n \times \mathbb{Z}_2^r / \sim, \tag{8}$$

where $(p, g) \sim (p', g')$ if and only if $p = p'$ and $g' - g \in G^{\mu}_{f(p)}$. Note the following:

- $M(P^n, \mu)$ is a closed manifold if μ is *nondegenerate* (ie $\mu(F_1), \dots, \mu(F_k)$ are linearly independent whenever $F_1 \cap \cdots \cap F_k \neq \varnothing$).
- $M(P^n, \mu)$ has $2^{r-\operatorname{rank}(\mu)}$ connected components. So $M(P^n, \mu)$ is connected if and only if $\operatorname{rank}(\mu) = r$.
- There is a canonical $\mathbb{Z}_2^r$–action on $M(P^n, \mu)$ defined by

  $$h \cdot [(x, g)] = [(x, g + h)] \quad \text{for } x \in P^n \text{ and } g, h \in \mathbb{Z}_2^r.$$

  Let $\pi_{\mu}\colon M(P^n, \mu) \to P^n$ be the map sending any $[(x, g)] \in M(P^n, \mu)$ to $x \in P^n$.

For any face f of P^n with $\dim(f) \geq 1$, let $r(f) = r - \operatorname{rank}(G_f^{\mu})$ and

$$\eta_f\colon \mathbb{Z}_2^r \to \mathbb{Z}_2^r / G_f^{\mu} \cong \mathbb{Z}_2^{r(f)}$$

be the quotient homomorphism. Then μ induces a $\mathbb{Z}_2^{r(f)}$–coloring μ_f on f by

$$\mu_f(F \cap f) := \eta_f(\mu(F)), \quad \text{where } F \in \mathcal{F}(P^n) \text{ and } \dim(F \cap f) = \dim(f) - 1. \tag{9}$$

It is easy to see that $\pi_{\mu}^{-1}(f)$ is homeomorphic to $M(f, \mu_f)$.

Example 3.1 Suppose $\pi\colon M^n \to P^n$ is a small cover with characteristic function λ. Then M^n is homeomorphic to $M(P^n, \lambda)$. For any face f of P^n, we have that $\pi^{-1}(f) \cong M(f, \lambda_f)$ is a closed connected submanifold of M^n (called a *facial submanifold* of M^n) which is a small cover over f.

3.3 Small covers with regular m–involutions

Let $\pi\colon M^n \to P^n$ be a small cover over an n–dimensional simple polytope P^n and $\lambda\colon \mathcal{F}(P^n) \to \mathbb{Z}_2^n$ be its characteristic function. Let us discuss under what conditions there exists a regular m–involution on M^n.

Theorem 3.2 *The following statements are equivalent:*

(a) *There exists a regular* m*–involution on M^n.*

(b) *There exists a regular involution on M^n with only isolated fixed points.*

(c) *The image $\operatorname{Im}\lambda \subseteq \mathbb{Z}_2^n$ of λ consists of exactly n elements* (which implies that P^n is n–colorable) *and so they form a basis of $\mathbb{Z}_2^n$.*

Proof (a)$\Rightarrow$(b) By definition, an m–involution only has isolated fixed point.

(b)$\Rightarrow$(c) Suppose there exists $g \in \mathbb{Z}_2^n$ such that the fixed points of τ_g on M^n are all isolated. Let v be an arbitrary vertex on P^n and $F_1, \dots, F_n$ be the n facets meeting at v. By the construction of small covers, $\pi^{-1}(v) = p$ is a fixed point of the whole group $\mathbb{Z}_2^n$. Let $U \subseteq M$ be a small neighborhood of p. Since the action of $\mathbb{Z}_2^n$ on M^n is locally standard, we observe that for $h = \lambda(F_{i_1}) + \cdots + \lambda(F_{i_s}) \in \mathbb{Z}_2^n$, where $1 \le i_1 < \cdots < i_s \le n$, the dimension of the fixed-point set of τ_h in U is equal to $n - s$. Then, since the fixed points of τ_g are all isolated, we must have that $g = \lambda(F_1) + \cdots + \lambda(F_n)$. Next, take an edge of P^n with two endpoints v_1 and v_2. Since P^n is simple, there are $n+1$ facets $F_1, \dots, F_n, F_n'$ such that $v_1 = F_1 \cap \cdots \cap F_{n-1} \cap F_n$ and $v_2 = F_1 \cap \cdots \cap F_{n-1} \cap F_n'$. Then $\lambda(F_1) + \cdots + \lambda(F_{n-1}) + \lambda(F_n) = g = \lambda(F_1) + \cdots + \lambda(F_{n-1}) + \lambda(F_n')$, which implies $\lambda(F_n) = \lambda(F_n')$. Since the 1–skeleton of P^n is connected, we can deduce the image $\operatorname{Im}\lambda$ of λ consists of n elements of $\mathbb{Z}_2^n$ which form a basis of $\mathbb{Z}_2^n$.

(c)$\Rightarrow$(a) Suppose $\operatorname{Im}\lambda = \{g_1, \dots, g_n\}$ is a basis of $\mathbb{Z}_2^n$. Then, by the construction of small covers, the fixed-point set of the regular involution $\tau_{g_1+\dots+g_n}$ on M^n is

$$(M^n)^{\mathbb{Z}_2^n} = \{\pi^{-1}(v) \mid v \in V(P^n)\}.$$

So the number of fixed points of $\tau_{g_1+\cdots+g_n}$ is equal to the number of vertices of P^n, which is known to be $h_0(P^n)+h_1(P^n)+\cdots+h_n(P^n)$. Then, by result (R1) in Section 3.1, $\tau_{g_1+\cdots+g_n}$ is an m–involution on M^n. □

Remark It should be pointed out that for an n–colorable simple n–polytope P^n, the image of a characteristic function $\lambda\colon \mathcal{F}(P^n)\to\mathbb{Z}_2^n$ might consist of more than n elements of $\mathbb{Z}_2^n$. In that case, the small cover defined by P^n and λ admits no regular m–involutions. So Theorem 3.2 only tells us that if an n–dimensional small cover M^n over P^n admits a regular m–involution, then P^n is n–colorable. But the converse is not true.

4 Self-dual binary codes from small covers

Let $\pi\colon M^n\to P^n$ be an n–dimensional small cover which admits a regular m–involution. By the proof of Theorem 3.2, P^n is an n–dimensional n–colorable simple polytope with an even number of vertices. Let $\{v_1,\dots,v_{2r}\}$ be all the vertices of P^n. The characteristic function λ of M^n satisfies the following: $\operatorname{Im}(\lambda)=\{e_1,\dots,e_n\}$ is a basis of $\mathbb{Z}_2^n$. By Theorem 3.2, $\tau_{e_1+\cdots+e_n}$ is an m–involution on M^n. So by the discussion in Section 2.3, we obtain a filtration

$$\mathbb{F}_2\cong V_0^{M^n}\subseteq V_1^{M^n}\subseteq\cdots\subseteq V_{n-2}^{M^n}\subseteq V_{n-1}^{M^n}=\mathcal{V}_{2r}\subseteq V_n^{M^n}=\mathbb{F}_2^{2r}.$$

According to Theorem 2.3 and property (R1) of small covers,

$$\dim_{\mathbb{F}_2}V_k^{M^n}=\sum_{j=0}^{k}b_j(M^n;\mathbb{F}_2)=\sum_{j=0}^{k}h_j(P^n)\quad\text{for } 0\le k\le n.$$

So, since $h_j(P^n)>0$ for all $0\le j\le n$, we have $V_0^{M^n}\subsetneq V_1^{M^n}\subsetneq\cdots\subsetneq V_{n-1}^{M^n}\subsetneq V_n^{M^n}=\mathbb{F}_2^{2r}$. Note that $V_k^{M^n}$ is self-dual in $\mathbb{F}_2^{2r}$ if and only if $V_k^{M^n}=(V_k^{M^n})^{\perp}=V_{n-1-k}^{M^n}$, by (5). Then $V_k^{M^n}$ is self-dual if and only if $k=n-1-k$ (ie n is odd and $k=(n-1)/2$). So we have proved the following proposition:

Proposition 4.1 *Let $\pi\colon M^n\to P^n$ be an n–dimensional small cover which admits a regular* m*–involution. Then $V_k^{M^n}$ is a self-dual code if and only if n is odd and $k=(n-1)/2$.*

In the remaining part of this section, we will describe each $V_k^{M^n}$, for $0\le k\le n$, explicitly in terms of the combinatorics of P^n. First, any face f of P^n determines an element $\xi_f \in \mathbb{F}_2^{2r}$, where the i^{th} entry of ξ_f is 1 if and only if v_i is a vertex of f. Note that for any faces $f_1, \dots, f_s$ of P^n, we have

$$\xi_{f_1 \cap \cdots \cap f_s} = \xi_{f_1} \circ \cdots \circ \xi_{f_s}, \tag{10}$$

and define a sequence of binary codes $\mathfrak{B}_k(P^n) \subseteq \mathbb{F}_2^{2r}$ as follows:

$$\mathfrak{B}_k(P^n) := \mathrm{Span}_{\mathbb{F}_2}\{\xi_f \mid f \text{ is a codimension-}k \text{ face of } P^n\} \quad \text{for } 0 \le k \le n. \tag{11}$$

Remark Changing the ordering of the vertices of P^n only causes the coordinate changes in $\mathbb{F}_2^n$. So up to equivalences of binary codes, each $\mathfrak{B}_k(P^n)$ is uniquely determined by P^n.

Lemma 4.2 *For any n–colorable simple n–polytope P^n with $2r$ vertices, we have*

$$\mathfrak{B}_0(P^n) \subseteq \mathfrak{B}_1(P^n) \subseteq \cdots \subseteq \mathfrak{B}_{n-1}(P^n) = \mathcal{V}_{2r} \subseteq \mathfrak{B}_n(P^n) \cong \mathbb{F}_2^{2r}.$$

Proof By definition, P^n can be colored by n colors $\{e_1, \dots, e_n\}$. Choosing an arbitrary color, say e_j, we observe that each vertex of P^n is contained in exactly one facet of P^n colored by e_j. This implies that

$$\xi_{P^n} = \xi_{F_1} + \cdots + \xi_{F_s},$$

where $F_1, \dots, F_s$ are all the facets of P^n colored by e_j. So $\mathfrak{B}_0(P^n) \subseteq \mathfrak{B}_1(P^n)$. Moreover, by Theorem 2.1(d), the facets $F_1, \dots, F_s$ are $(n-1)$–dimensional simple polytopes which are $(n-1)$–colorable. So by repeating the above argument, we can show that $\mathfrak{B}_1(P^n) \subseteq \mathfrak{B}_2(P^n)$ and so on. Now it remains to show $\mathfrak{B}_{n-1}(P^n) = \mathcal{V}_{2r}$.

By definition, $\mathfrak{B}_{n-1}(P^n)$ is spanned by $\{\xi_f \mid f \text{ is an edge (or 1–face) of } P^n\}$. So it is obvious that $\mathfrak{B}_{n-1}(P^n) \subseteq \mathcal{V}_{2r}$. Let $\{v_1, \dots, v_{2r}\}$ be all the vertices of P^n. It is easy to see that $\mathcal{V}_{2r}$ is spanned by $\{\xi_{v_i} + \xi_{v_j} \mid 1 \le i \ne j \le 2r\}$. Then, since there exists an edge path on P^n between any two vertices v_i and v_j of P^n, we have that $\xi_{v_i} + \xi_{v_j}$ belongs to $\mathfrak{B}_{n-1}(P^n)$. So $\mathcal{V}_{2r} \subseteq \mathfrak{B}_{n-1}(P^n)$. This finishes the proof. □

Later we will prove that the condition in Lemma 4.2 is also sufficient for an n–dimensional simple polytope to be n–colorable (see Proposition 5.6).

Theorem 4.3 *Let $\pi\colon M^n \to P^n$ be an n–dimensional small cover which admits a regular* m*–involution. For any $0 \le k \le n$, the space $V_k^{M^n}$ coincides with $\mathfrak{B}_k(P^n)$.*

Corollary 4.4 *Let P^n be an n–colorable simple n–polytope with $2r$ vertices. Then*

$$\dim_{\mathbb{F}_2} \mathfrak{B}_k(P^n) = \sum_{i=0}^{k} h_i(P^n) \quad \text{for } 0 \le k \le n.$$

If n is odd, then $\mathfrak{B}_k(P^n)$ is a self-dual code in $\mathbb{F}_2^{2r}$ if and only if $k=(n-1)/2$. If n is even, $\mathfrak{B}_k(P^n)$ cannot be a self-dual code in $\mathbb{F}_2^{2r}$ for any $0 \le k \le n$.

Proof Let M^n be a small cover over P^n whose characteristic function $\lambda\colon \mathcal{F}(P^n) \to \mathbb{Z}_2^n$ satisfies the condition that the image $\mathrm{Im}(\lambda)$ is a basis $\{e_1,\dots,e_n\}$ in $\mathbb{Z}_2^n$. Then, by Theorem 4.3, $\mathfrak{B}_k(P^n)$ coincides with V_k^M. So this corollary follows from Theorem 2.3, property (R1) in Section 3.1 and Proposition 4.1. □

Corollary 4.5 *Let $\pi\colon M^n \to P^n$ be an n–dimensional small cover which admits a regular* m*–involution, where n is odd. Then the self-dual binary code $C_{M^n} = V_{(n-1)/2}^{M^n} = \mathfrak{B}_{(n-1)/2}(P^n)$ is spanned by*

$$\{\xi_f \mid f \text{ is any face of } P^n \text{ with } \dim(f) = (n+1)/2\}.$$

So the minimum distance of C_{M^n} is less than or equal to

$$\min\{\#(\text{vertices of } f) \mid f \text{ is an } ((n+1)/2)\text{–dimensional face of } P^n\}.$$

Problem For any n–dimensional small cover M^n that admits a regular m–involution, where n is odd, determine the minimum distance of the self-dual binary code C_{M^n}.

We will see in Proposition 7.1 that when $n=3$, the minimum distance of C_{M^n} is always equal to 4. For higher dimensions, it seems to us that the minimum distance of C_{M^n} should be equal to $\min\{\#(\text{vertices of } f) \mid f \text{ is an } ((n+1)/2)\text{–dimensional face of } P^n\}$. But the proof is not clear to us. Some examples supporting this statement can be found in Example 9.2.

In the following, we are going to prove Theorem 4.3. For brevity, let

$$\tau = \tau_{e_1+\dots+e_n} \quad \text{and} \quad G_\tau = \langle e_1 + \dots + e_n \rangle \cong \mathbb{Z}_2.$$

By the construction of M^n, all the fixed points of τ on M^n are $\tilde{v}_1,\dots,\tilde{v}_{2r}$, where

$$\tilde{v}_i = \pi^{-1}(v_i) \in M^n \quad \text{for } i = 1,\dots,2r.$$

Proof of Theorem 4.3 According to result (R4) of Section 3.1, the cohomology ring $H^*(M^n;\mathbb{F}_2)$ of M^n is generated as an algebra by $H^1(M^n;\mathbb{F}_2)$. So as an algebra over $H^*(BG_\tau;\mathbb{F}_2)=\mathbb{F}_2[t]$, the equivariant cohomology ring $H^*_{G_\tau}(M^n;\mathbb{F}_2)=H^*(M^n;\mathbb{F}_2)\otimes H^*(BG_\tau;\mathbb{F}_2)$ is generated by elements of degree 1. In addition, the operation $\circ$ on $\mathbb{F}_2^{2r}$ corresponds to the cup product in $H^*_{G_\tau}(M^n;\mathbb{F}_2)$. So we obtain from Theorem 2.3 that, for any $1\le k\le n$,

$$V_k^{M^n}=\underbrace{V_1^{M^n}\circ\cdots\circ V_1^{M^n}}_{k}.$$

On the other hand, there is a similar structure on $\mathfrak{B}_k(P^n)$ as well.

Claim 1 $\quad \mathfrak{B}_k(P^n)=\underbrace{\mathfrak{B}_1(P^n)\circ\cdots\circ\mathfrak{B}_1(P^n)}_{k}\quad$ for $1\le k\le n$.

Indeed, for any k different facets $F_{i_1},\dots,F_{i_k}$ of P^n, their intersection $F_{i_1}\cap\cdots\cap F_{i_k}$ is either empty or a face of codimension k. So by (10), we have $\xi_{F_{i_1}}\circ\cdots\circ\xi_{F_{i_k}}=\xi_{F_{i_1}\cap\cdots\cap F_{i_k}}\in\mathfrak{B}_k(P^n)$. If there are repetitions of facets in $F_{i_1},\dots,F_{i_k}$, we have $\xi_{F_{i_1}}\circ\cdots\circ\xi_{F_{i_k}}\in\mathfrak{B}_l(P^n)$ for some $l<k$ (because $x\circ x=x$ for any $x\in\mathbb{F}_2^{2r}$). But since P^n is n–colorable in our case, we have $\mathfrak{B}_l(P^n)\subseteq\mathfrak{B}_k(P^n)$ by Lemma 4.2. Conversely, any codimension-k face f of P^n can be written as $f=F_{i_1}\cap\cdots\cap F_{i_k}$, where $F_{i_1},\dots,F_{i_k}$ are k different facets of P^n. So $\xi_f=\xi_{F_{i_1}\cap\cdots\cap F_{i_k}}=\xi_{F_{i_1}}\circ\cdots\circ\xi_{F_{i_k}}$. Claim 1 is proved.

So, to prove Theorem 4.3, it is sufficient to prove that $V_1^{M^n}=\mathfrak{B}_1(P^n)$, ie $V_1^{M^n}$ is spanned by the set $\{\xi_F\mid F\text{ is any facet of }P^n\}$. Next, we examine the localization of $H^1_{\mathbb{Z}_2^n}(M^n;\mathbb{F}_2)$ to $H^1_{\mathbb{Z}_2^n}((M^n)^{\mathbb{Z}_2^n};\mathbb{F}_2)$ more carefully. Let $\mathcal{F}(P^n)=\{F_1,\dots,F_m\}$ be the set of all facets of P^n. By our previous notation, the regular involution $\tau=\tau_{e_1+\cdots+e_n}$ on M^n only has isolated fixed points:

$$(M^n)^{G_\tau}=(M^n)^{\mathbb{Z}_2^n}=\{\tilde v_1,\dots,\tilde v_{2r}\}.$$

Clearly the inclusion $G_\tau\hookrightarrow\mathbb{Z}_2^n$ induces diagonal maps $\Delta_E\colon EG_\tau\to E\mathbb{Z}_2^n$ and $\Delta_B\colon BG_\tau\to B\mathbb{Z}_2^n$ such that the following diagram commutes:

$$\begin{tikzcd} EG_\tau \arrow[r, "\Delta_E"] \arrow[d] & E\mathbb{Z}_2^n \arrow[d] \\ BG_\tau \arrow[r, "\Delta_B"] & B\mathbb{Z}_2^n \end{tikzcd}$$

Since $(M^n)^{G_\tau} = (M^n)^{\mathbb{Z}_2^n}$ consists of isolated points, we have a commutative diagram

$$\begin{tikzcd}
EG_\tau \times (M^n)^{G_\tau} \arrow[rrr, "\Delta_E \times \mathrm{id}"] \arrow[dr, "i_1"] \arrow[ddd] & & & E\mathbb{Z}_2^n \times (M^n)^{\mathbb{Z}_2^n} \arrow[dl, "i_2"'] \arrow[ddd] \\
& EG_\tau \times M^n \arrow[r, "\Delta_E \times \mathrm{id}"] \arrow[d] & E\mathbb{Z}_2^n \times M^n \arrow[d] & \\
& EG_\tau \times_{G_\tau} M^n \arrow[r, "\phi"] & E\mathbb{Z}_2^n \times_{\mathbb{Z}_2^n} M^n & \\
EG_\tau \times_{G_\tau} (M^n)^{G_\tau} \arrow[rrr, "\Delta_B \times \mathrm{id} = \psi"'] \arrow[ur, "i_3"] & & & E\mathbb{Z}_2^n \times_{\mathbb{Z}_2^n} (M^n)^{\mathbb{Z}_2^n} \arrow[ul, "i_4"']
\end{tikzcd}$$

where ϕ is the map induced by $\Delta_E \times \mathrm{id}$, and i_1, i_2, i_3 and i_4 are all inclusions. Furthermore, we have the following commutative diagram, where $i_3^* \circ \phi^* = \psi^* \circ i_4^*$:

$$\begin{tikzcd}
H^*_{\mathbb{Z}_2^n}(M^n;\mathbb{F}_2) \arrow[r, "\phi^*"] \arrow[d, "i_4^*"'] & H^*_{G_\tau}(M^n;\mathbb{F}_2) \arrow[d, "i_3^*"] \\
H^*_{\mathbb{Z}_2^n}((M^n)^{\mathbb{Z}_2^n};\mathbb{F}_2) \arrow[r, "\psi^*"'] & H^*_{G_\tau}((M^n)^{G_\tau};\mathbb{F}_2)
\end{tikzcd} \tag{12}$$

Note that i_3^* and i_4^* are injective, and

$$H^*_{\mathbb{Z}_2^n}((M^n)^{\mathbb{Z}_2^n};\mathbb{F}_2) \cong \bigoplus_{v \in V(P^n)} H^*_{\mathbb{Z}_2^n}(\tilde{v};\mathbb{F}_2),$$
$$H^*_{G_\tau}((M^n)^{G_\tau};\mathbb{F}_2) \cong \bigoplus_{v \in V(P^n)} H^*_{G_\tau}(\tilde{v};\mathbb{F}_2),$$

where $\tilde{v} = \pi^{-1}(v)$ is the fixed point corresponding to a vertex $v \in V(P^n)$. Then, by the facts that $H^*_{\mathbb{Z}_2^n}(\tilde{v};\mathbb{F}_2) \cong H^*(B\mathbb{Z}_2^n;\mathbb{F}_2)$ and $H^*_{G_\tau}(\tilde{v};\mathbb{F}_2) \cong H^*(BG_\tau;\mathbb{F}_2)$, we can regard ψ^* as a direct sum:

$$\psi^* = \bigoplus_{v \in V(P^n)} \Delta_B^*. \tag{13}$$

We know $H^*(B\mathbb{Z}_2^n;\mathbb{F}_2) = \mathbb{F}_2[t_1,\dots,t_n]$ with $\deg t_i = 1$, and $H^*(BG_\tau;\mathbb{F}_2) = \mathbb{F}_2[t]$ with $\deg t = 1$ (see [2, Section 1]). For each $1 \le i \le n$, let $G_i = \langle e_i \rangle \cong \mathbb{Z}_2$. Clearly,

$$H^*(BG_i;\mathbb{F}_2) = \mathbb{F}_2[t_i] \quad \text{for } 1 \le i \le n \qquad \text{and} \qquad \mathbb{Z}_2^n = G_1 \times \cdots \times G_n.$$

For any $1 \le i \le n$, let $\zeta_i\colon G_i \to G_\tau$ be the group isomorphism sending $e_i \to e_1 + \cdots + e_n$, and let $\rho_i\colon \mathbb{Z}_2^n \to G_i$ be the projection sending e_j to 0 for any $1 \le j \ne i \le n$. Let $\theta\colon G_\tau \hookrightarrow \mathbb{Z}_2^n$ be the inclusion map. It is clear that

$$\rho_i \circ \theta \circ \zeta_i = \mathrm{id}_{G_i} \quad \text{for } 1 \le i \le n.$$

Let $B_{\zeta_i}\colon BG_i \to BG_\tau$ and $B_{\rho_i}\colon B\mathbb{Z}_2^n \to BG_i$ be the maps between the classifying spaces induced, respectively, by ζ_i and ρ_i. Then, since there is a functorial construction of classifying spaces of groups (see [20]), we can assume $B_{\rho_i} \circ \Delta_B \circ B_{\zeta_i} = \mathrm{id}_{BG_i}$ (recall that $\Delta_B\colon BG_\tau \to B\mathbb{Z}_2^n$ is induced by θ). So for any $1 \le i \le n$, we have

$$\mathrm{id}^*_{BG_i} = B^*_{\zeta_i} \circ \Delta^*_B \circ B^*_{\rho_i}\colon H^1(BG_i;\mathbb{F}_2) \to H^1(B\mathbb{Z}_2^n;\mathbb{F}_2) \to H^1(BG_\tau;\mathbb{F}_2) \to H^1(BG_i;\mathbb{F}_2).$$

Obviously, we have $B^*_{\rho_i}(t_i) = t_i$ for any $1 \le i \le n$. In addition, we can assert $B^*_{\zeta_i}(t) = t_i$ since $B^*_{\zeta_i}$ is an isomorphism, and t and t_i are the unique generators of $H^1(BG_\tau;\mathbb{F}_2)$ and $H^1(BG_i;\mathbb{F}_2)$, respectively. Then $t_i = B^*_{\zeta_i} \circ \Delta^*_B \circ B^*_{\rho_i}(t_i) = B^*_{\zeta_i} \circ \Delta^*_B(t_i)$ implies

$$\Delta^*_B(t_i) = t \quad \text{for } 1 \le i \le n. \tag{14}$$

Our strategy here is to understand the image of the localization map i_3^* in terms of ψ^* and i_4^*. So we need to show that ϕ^* is surjective.

Claim 2 The homomorphism ϕ^* is surjective.

Indeed, according to [8, Theorem 4.12], the E_2–term of the Serre spectral sequence of the fibration $E\mathbb{Z}_2^n \times_{\mathbb{Z}_2^n} M^n \to B\mathbb{Z}_2^n$ collapses and we have

$$H^*_{\mathbb{Z}_2^n}(M^n;\mathbb{F}_2) \cong H^*(M^n;\mathbb{F}_2) \otimes H^*(B\mathbb{Z}_2^n;\mathbb{F}_2).$$

This means that the small cover M^n is *equivariantly formal* (see [10] for the definition). Meanwhile, we already know that $H^*_{G_\tau}(M^n;\mathbb{F}_2) = H^*(M^n;\mathbb{F}_2) \otimes H^*(BG_\tau;\mathbb{F}_2)$. So the surjectivity of ϕ^* follows from the surjectivity of $\Delta^*_B\colon H^*(B\mathbb{Z}_2^n;\mathbb{F}_2) \to H^*(BG_\tau;\mathbb{F}_2)$, which is implied by (14). Claim 2 is proved.

Remark The surjectivity of restriction map to the equivariant cohomology with respect to a subgroup is known for many equivariant formal situations. For example, an explicit statement of the surjectivity result in case of real torus actions is contained in [1, Theorem 5.7].

By Claim 2, the image of the localization $i_3^*\colon H^*_{G_\tau}(M^n;\mathbb{F}_2) \to H^*_{G_\tau}((M^n)^{G_\tau};\mathbb{F}_2)$ is

$$\mathrm{Im}(i_3^*) = \mathrm{Im}(i_3^* \circ \phi^*) = \mathrm{Im}(\psi^* \circ i_4^*). \tag{15}$$

For any fixed point $\tilde{v} \in (M^n)^{\mathbb{Z}_2^n}$, the inclusion $i_{\tilde{v}}\colon \{\tilde{v}\} \hookrightarrow M^n$ induces a homomorphism

$$i_{\tilde{v}}^*\colon H^*_{\mathbb{Z}_2^n}(M^n;\mathbb{F}_2) \cong \mathbb{F}_2[a_{F_1},\dots,a_{F_m}]/I \\ \to H^*_{\mathbb{Z}_2^n}(\{\tilde{v}\};\mathbb{F}_2) \cong H^*(B\mathbb{Z}_2^n;\mathbb{F}_2) = \mathbb{F}_2[t_1,\dots,t_n].$$

Then we can write

$$i_4^* = \bigoplus_{v\in V(P^n)} i_{\tilde{v}}^*. \tag{16}$$

Since we already know how to compute ψ^* from (13) and (14), it remains to understand each $i_{\tilde{v}}^*$ for us to compute $\mathrm{Im}(i_3^*)$. This is given in the following lemma.

Lemma 4.6 *Let λ be the characteristic function of the small cover M^n such that $\mathrm{Im}(\lambda) = \{e_1,\dots,e_n\}$ is a basis of $\mathbb{Z}_2^n$. Suppose F is a facet of P^n with $\lambda(F) = e_j$ for some $1 \le j \le n$. Then, for any vertex v of P^n, the fixed point $\tilde{v} = \pi^{-1}(v) \in (M^n)^{\mathbb{Z}_2^n}$ satisfies*

$$i_{\tilde{v}}^*(a_F) = \begin{cases} t_j & \text{if } v \in F, \\ 0 & \text{if } v \notin F. \end{cases}$$

Proof Let $M_F = \pi^{-1}(F)$. Let $M_{\mathbb{Z}_2^n} = E\mathbb{Z}_2^n \times_{\mathbb{Z}_2^n} M^n$ and $(M_F)_{\mathbb{Z}_2^n} = E\mathbb{Z}_2^n \times_{\mathbb{Z}_2^n} M_F$ be the Borel constructions of M^n and M_F, respectively. According to the discussion in [8, Section 6.1], a_F is the first Stiefel–Whitney class $w_1(L_F)$ of a line bundle L_F over $M_{\mathbb{Z}_2^n}$. Moreover, the restriction of L_F to $M_{\mathbb{Z}_2^n} \setminus (M_F)_{\mathbb{Z}_2^n}$ is a trivial line bundle.

For any fixed point $\tilde{v}$ of M^n, let $L_{\tilde{v}}$ denote the restriction of the line bundle L_F to the Borel construction $\{\tilde{v}\}_{\mathbb{Z}_2^n} = E\mathbb{Z}_2^n \times_{\mathbb{Z}_2^n} \{\tilde{v}\}$.

If a vertex v is not in F, so that $\tilde{v} \notin M_F$, then $L_{\tilde{v}}$ is a trivial line bundle over $\{\tilde{v}\}_{\mathbb{Z}_2^n}$. So we have

$$0 = w_1(L_{\tilde{v}}) = i_{\tilde{v}}^*(w_1(L_F)) = i_{\tilde{v}}^*(a_F).$$

For any vertex $v \in F$, let $\mathfrak{p}_{\tilde{v}}\colon M^n \to \{\tilde{v}\}$ be the constant map. Clearly $\mathfrak{p}_{\tilde{v}} \circ i_{\tilde{v}} = \mathrm{id}_{\{\tilde{v}\}}$. The induced maps $\mathfrak{p}_{\tilde{v}}^*$ and $i_{\tilde{v}}^*$ on the equivariant cohomology give

$$\begin{tikzcd} \mathrm{id}\colon & H^1_{\mathbb{Z}_2^n}(\{\tilde{v}\}) \arrow[r, "\mathfrak{p}_{\tilde{v}}^*"] \arrow[d, equal] & H^1_{\mathbb{Z}_2^n}(M^n) \arrow[r, "i_{\tilde{v}}^*"] \arrow[d, equal] & H^1_{\mathbb{Z}_2^n}(\{\tilde{v}\}) \arrow[d, equal] \\ \mathrm{id}\colon & \mathrm{span}\{t_1,\dots,t_n\} \arrow[r, "\mathfrak{p}_{\tilde{v}}^*"] & \mathrm{span}\{a_{F_1},\dots,a_{F_m}\} \arrow[r, "i_{\tilde{v}}^*"] & \mathrm{span}\{t_1,\dots,t_n\} \end{tikzcd} \tag{17}$$

Let λ be the characteristic function of the small cover $\pi\colon M^n \to P^n$. We can regard λ as a linear map $\lambda\colon \mathbb{Z}_2^m = \mathrm{span}\{F_1, \dots, F_m\} \to \mathbb{Z}_2^n = \mathrm{span}\{e_1, \dots, e_n\}$, which is represented by an $n \times m$ matrix $A = (\lambda(F_1), \dots, \lambda(F_m))$. Since $\tilde{v}$ is a fixed point of the $\mathbb{Z}_2^n$–action on M^n, we can identify the map $\mathfrak{p}_{\tilde{v}}^*$ in (17) with $p^*\colon H^1(B\mathbb{Z}_2^n) \to H^1_{\mathbb{Z}_2^n}(M^n)$, where $p\colon E\mathbb{Z}_2^n \times_{\mathbb{Z}_2^n} M^n \to B\mathbb{Z}_2^n$ is the projection. Then, by the analysis of p^* in [8, pages 438–439], we have

$$\mathfrak{p}_{\tilde{v}}^*(t_j) = \lambda^*(t_j) = \sum_{\substack{\lambda(F_l)=e_j\\ 1\le l\le m}} a_{F_l}, \tag{18}$$

where $\lambda^*\colon \mathrm{span}\{t_1, \dots, t_n\} \to \mathrm{span}\{a_{F_1}, \dots, a_{F_m}\}$ is the dual of λ, which is represented by the transpose A^t of A. So we obtain

$$t_j = i_{\tilde{v}}^*(\mathfrak{p}_{\tilde{v}}^*(t_j)) = i_{\tilde{v}}^*\Bigg(\sum_{\substack{\lambda(F_l)=e_j\\ 1\le l\le m}} a_{F_l}\Bigg) = \sum_{\substack{\lambda(F_l)=e_j\\ 1\le l\le m}} i_{\tilde{v}}^*(a_{F_l}) = \sum_{\substack{F_l\ni v,\, \lambda(F_l)=e_j\\ 1\le l\le m}} i_{\tilde{v}}^*(a_{F_l}). \tag{19}$$

Observe that among all the n facets of P^n containing v, there is only one facet (ie F) colored by e_j. So we obtain from (19) that

$$\sum_{\substack{F_l\ni v,\, \lambda(F_l)=e_j\\ 1\le l\le m}} i_{\tilde{v}}^*(a_{F_l}) = i_{\tilde{v}}^*(a_F) = t_j.$$

The lemma is proved. □

Now for an arbitrary facet F of P^n, suppose $\lambda(F) = e_j$. We get from Lemma 4.6 that

$$i_4^*(a_F) = \bigoplus_{v\in V(P^n)} i_{\tilde{v}}^*(a_F) = \sum_{v\in F} t_j \cdot \xi_v = t_j \cdot \xi_F. \tag{20}$$

Recall that ξ_v denotes the vector in $\mathbb{F}_2^{2r} = \mathbb{F}_2^{|V(P^n)|}$ with 1 at the coordinate corresponding to the vertex v and zero everywhere else. Combining (20) with (13) and (14), we obtain

$$\psi^* i_4^*(a_F) = t \cdot \xi_F. \tag{21}$$

So $\psi^* i_4^*(H^1_{\mathbb{Z}_2^n}(M^n; \mathbb{F}_2)) = t \cdot \mathfrak{B}_1(P^n)$ since ψ^* and i_4^* are graded ring homomorphisms. Then, by (15), we have $\mathrm{Im}(i_3^*) = \mathrm{Im}(\psi^* \circ i_4^*) = t \cdot \mathfrak{B}_1(P^n)$. This implies that $V_1^{M^n} = \mathfrak{B}_1(P^n)$. So we complete the proof of Theorem 4.3. □

5 Binary codes from general simple polytopes

The definition of $\mathfrak{B}_k(P^n)$ in (11) clearly makes sense for an arbitrary n–dimensional simple polytope P^n. We call $\mathfrak{B}_k(P^n) \subseteq \mathbb{F}_2^{|V(P^n)|}$ the *codimension-k face code of* P^n. It is obvious that $\mathfrak{B}_0(P^n) = \{\underline{0}, \underline{1}\} \cong \mathbb{F}_2$, and $\mathfrak{B}_n(P^n) \cong \mathbb{F}_2^{|V(P^n)|}$, where

$$\underline{0} = (0, \dots, 0) \quad \text{and} \quad \underline{1} = (1, \dots, 1).$$

If we choose an ordering of all the vertices of P^n, we can write down a generator matrix for $\mathfrak{B}_k(P^n)$.

Example 5.1 Under the labeling of the vertices of the 6–gon prism P^3 in Figure 1, the following 6×12 binary matrix is a generator matrix of $\mathfrak{B}_1(P^3)$, where the first row of the matrix is the codeword corresponding to the top facet of P^3:

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

Next, we study some properties of $\mathfrak{B}_k(P^n)$. The arguments in the rest of this section are completely combinatorial and are independent from the discussion of equivariant cohomology and small covers in the previous sections. First, note that the last part of the proof of Lemma 4.2 indicates the following result for general simple polytopes.

Proposition 5.2 *For any n–dimensional simple polytope P^n, we have*

$$\mathfrak{B}_{n-1}(P^n) = \{u \in \mathbb{F}_2^{|V(P^n)|} \mid \mathrm{wt}(u) \textit{ is even}\}.$$

So $\dim_{\mathbb{F}_2} \mathfrak{B}_{n-1}(P^n) = |V(P^n)| - 1$.

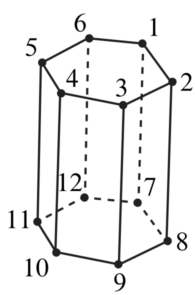

Figure 1: A 6–gon prism

Proof For any 1–face f of P^n, its Hamming weight satisfies $\mathrm{wt}(\xi_f)=2$. So $\mathfrak{B}_{n-1}(P^n)$ is a linear subspace of $\{u\in\mathbb{F}_2^{|V(P^n)|}\mid \mathrm{wt}(u)\text{ is even}\}$. Conversely, we have that $\{u\in\mathbb{F}_2^{|V(P^n)|}\mid \mathrm{wt}(u)\text{ is even}\}$ is linearly spanned by $\{\xi_v+\xi_{v'}\mid v,v'\in V(P^n)\}$, where ξ_v is defined similarly as in Section 4. Then, since there always exists an edge path on P^n between any two vertices v and v' of P^n, we have that $\xi_v+\xi_{v'}$ belongs to $\mathfrak{B}_{n-1}(P^n)$. This proves the proposition. □

In the following proposition, we obtain a lower bound on the dimension of $\mathfrak{B}_k(P^n)$.

Proposition 5.3 *For any n–dimensional simple polytope P^n, we have*

$$\dim_{\mathbb{F}_2}\mathfrak{B}_k(P^n)\ge h_0(P^n)+\cdots+h_k(P^n)\quad \text{for } 0\le k\le n.$$

Proof Using the Morse-theoretical argument in [4], we can define a generic height function ϕ on P^n that makes the 1–skeleton of P^n into a directed graph by orienting each edge so that ϕ increases along it. Then, for any face f of P^n with dimension greater than 0, the restriction $\phi|_f$ assumes its maximum (or minimum) at a vertex. Since ϕ is generic, each face f of P^n has a unique "top" and a unique "bottom" vertex. For each vertex v of P^n, we define the *index* $\mathrm{ind}(v)$ of v to be the number of incident edges of P^n that point towards v. A simple argument (see [4, page 115 or 5, page 13]) shows that for any $0\le j\le n$, the number of vertices of P^n with index j equals $h_j(P^n)$.

Now fix an integer $0\le k\le n$. For any vertex v of P^n with $0\le \mathrm{ind}(v)\le k$, there are exactly $n-\mathrm{ind}(v)$ incident edges of P^n that point away from v. So there are $\binom{n-\mathrm{ind}(v)}{n-k}$ codimension-k faces of P^n that are incident to v and take v as their (unique) "bottom" vertex. Choose an arbitrary one such face at v, denoted by f_v^{n-k}.

Claim $\{\xi_{f_v^{n-k}}\mid 0\le \mathrm{ind}(v)\le k \text{ and } v\in V(P^n)\}$ is a linearly independent subset of $\mathfrak{B}_k(P^n)$.

Otherwise there would exist vertices $v_1,\dots,v_s$ of P^n with $0\le\mathrm{ind}(v_i)\le k$ for $1\le i\le s$, so that $\xi_{f_{v_1}^{n-k}}+\cdots+\xi_{f_{v_s}^{n-k}}=0$. Without loss of generality, we can assume $\phi(v_1)<\cdots<\phi(v_s)$. Then, among $f_{v_1}^{n-k},\dots,f_{v_s}^{n-k}$, only $f_{v_1}^{n-k}$ is incident to the vertex v_1. From this fact, we obtain $\xi_{v_1}\circ(\xi_{f_{v_1}^{n-k}}+\cdots+\xi_{f_{v_s}^{n-k}})=\xi_{v_1}\circ\xi_{f_{v_1}^{n-k}}=\xi_{v_1}=0$, which is absurd.

This claim implies that $\dim_{\mathbb{F}_2}\mathfrak{B}_k(P^n)$ is greater than or equal to the number of vertices of P^n whose indices are less than or equal to k. Hence $\dim_{\mathbb{F}_2}\mathfrak{B}_k(P^n)\ge h_0(P^n)+\cdots+h_k(P^n)$. □

Remark Suppose P^n is an n–colorable simple n–polytope. Then the dimension of $\mathfrak{B}_k(P^n)$ is exactly $h_0(P^n)+\cdots+h_k(P^n)$ by Corollary 4.4. So by the claim in the proof of Proposition 5.3, $\{\xi_{f_v^{n-k}} \mid 0 \le \operatorname{ind}(v) \le k,\ v \in V(P^n)\}$ is actually a linear basis for $\mathfrak{B}_k(P^n)$. This gives us an interesting way to write a linear basis of $\mathfrak{B}_k(P^n)$ from a generic height function on P^n. In particular when n is odd, we can obtain a linear basis of the self-dual binary code $\mathfrak{B}_{(n-1)/2}(P^n)$ in this way.

Corollary 5.4 *Let P^n be an n–dimensional simple polytope with m facets. Then*

$$\dim_{\mathbb{F}_2} \mathfrak{B}_1(P^n) \ge m-n+1.$$

Moreover, for any vertex v of P^n, let F_v be an arbitrary facet of P^n containing v and $F_1,\dots,F_{m-n}$ be all the facets of P^n not containing v. Then $\xi_{F_v},\xi_{F_1},\dots,\xi_{F_{m-n}} \in \mathfrak{B}_1(P^n)$ are linearly independent.

Proof Since $h_0(P^n)=1$ and $h_1(P^n)=m-n$, Proposition 5.3 tells us that

$$\dim_{\mathbb{F}_2} \mathfrak{B}_1(P^n) \ge h_0(P^n)+h_1(P^n) = m-n+1.$$

For any vertex v of P^n, we can define a height function ϕ as in the proof of Proposition 5.3 so that v is the unique "bottom" vertex of P^n relative to ϕ. Then v is the only vertex of index 0. For each $1 \le i \le m-n$, let v_i be the bottom vertex of F_i relative to ϕ. Then $v_1,\dots,v_{m-n}$ are exactly all the vertices of index 1 relative to ϕ. This is because the index of v_i relative to ϕ is clearly 1 for any $1 \le i \le m-n$ while the index 1 vertices of P^n is equal to $h_1(P^n)=m-n$. So by the claim in the proof of Proposition 5.3 for $k=1$, we have that $\xi_{F_v},\xi_{F_1},\dots,\xi_{F_{m-n}}$ are linearly independent in $\mathfrak{B}_1(P^n)$. $\square$

Next let us look at what happens when $\dim_{\mathbb{F}_2} \mathfrak{B}_1(P^n) = m-n+1$.

Proposition 5.5 *Let P^n be an n–dimensional simple polytope with m facets. Then $\dim_{\mathbb{F}_2} \mathfrak{B}_1(P^n) = m-n+1$ if and only if P^n is n–colorable.*

Proof Let $\{F_1,\dots,F_m\}$ be all the facets of P^n. Suppose P^n is n–colorable. Then we can use n different colors, say $\mathfrak{c}_1,\dots,\mathfrak{c}_n$, to color all the facets of P^n so that any neighboring facets have different colors. Define

$$\mathcal{F}_i = \{F \in \mathcal{F}(P^n) \mid F \text{ is colored by } \mathfrak{c}_i\} \quad \text{for } i=1,\dots,n.$$

By the definition of n–colorable, each vertex of P^n is incident to exactly one facet in $\mathcal{F}_i$. So we have

(22) $$\bigcup_{F\in\mathcal{F}_i} V(F)=V(P^n) \quad\text{and}\quad \sum_{F\in\mathcal{F}_i}\xi_F=\sum_{v\in V(P^n)}\xi_v=\underline{1}.$$

Without loss of generality, assume that the facets $F_1,\dots,F_n$ meet at a vertex of P^n and that F_i is colored by $\mathfrak{c}_i$ for $1\le i\le n$. So by our definition, $F_i\in\mathcal{F}_i$ for $1\le i\le n$. For each $1\le i\le n-1$, we claim that ξ_{F_i} can be written as a linear combination of elements in $\{\xi_{F_n},\xi_{F_{n+1}},\dots,\xi_{F_m}\}$. Indeed, it follows from (22) that

(23) $$\sum_{F\in\mathcal{F}_i}\xi_F+\sum_{F\in\mathcal{F}_n}\xi_F=\underline{1}+\underline{1}=\underline{0}.$$

Observe that for any $1\le i\le n-1$, we have

$$\{\xi_F \mid F\in\mathcal{F}_i\}\subseteq\{\xi_{F_i},\xi_{F_n},\xi_{F_{n+1}},\dots\xi_{F_m}\},$$
$$\{\xi_F \mid F\in\mathcal{F}_n\}\subseteq\{\xi_{F_i},\xi_{F_n},\xi_{F_{n+1}},\dots\xi_{F_m}\}.$$

So (23) implies that $\{\xi_{F_i},\xi_{F_n},\xi_{F_{n+1}},\dots\xi_{F_m}\}$ is linearly dependent. In addition, we know from Corollary 5.4 that $\{\xi_{F_n},\xi_{F_{n+1}},\dots\xi_{F_m}\}$ is linearly independent. So ξ_{F_i} is a linear combination of $\xi_{F_n},\xi_{F_{n+1}},\dots,\xi_{F_m}$. This implies that $\{\xi_{F_n},\xi_{F_{n+1}},\dots,\xi_{F_m}\}$ is a basis of $\mathfrak{B}_1(P^n)$. So $\dim_{\mathbb{F}_2}\mathfrak{B}_1(P^n)=m-n+1$.

Conversely, suppose $\dim_{\mathbb{F}_2}\mathfrak{B}_1(P^n)=m-n+1$. If P^n is not n–colorable, by Theorem 2.1 there exists a 2–face f^2 of P^n which has an odd number of vertices, say $v_1,\dots,v_{2k+1}$. Without loss of generality, assume that $f^2=F_1\cap\dots\cap F_{n-2}$ and $v_1=F_1\cap F_2\cap\dots\cap F_n$. By Corollary 5.4, $\{\xi_{F_n},\xi_{F_{n+1}},\dots,\xi_{F_m}\}$ is a basis of $\mathfrak{B}_1(P^n)$. Without loss of generality, we may assume the following (see Figure 2):

$$\begin{aligned}
v_1&=f^2\cap F_{n-1}\cap F_n,\\
v_2&=f^2\cap F_n\cap F_{n+1},\\
&\ \ \vdots\\
v_i&=f^2\cap F_{n+i-2}\cap F_{n+i-1},\\
&\ \ \vdots\\
v_{2k}&=f^2\cap F_{n+2k-2}\cap F_{n+2k-1},\\
v_{2k+1}&=f^2\cap F_{n+2k-1}\cap F_{n-1}.
\end{aligned}$$

Assume that there exists $\epsilon_i\in\mathbb{F}_2$ for $i=1,n,\dots,m$ such that

(24) $$\epsilon_1\xi_{F_1}+\epsilon_n\xi_{F_n}+\epsilon_{n+1}\xi_{F_{n+1}}+\dots+\epsilon_m\xi_{F_m}=\underline{0}.$$

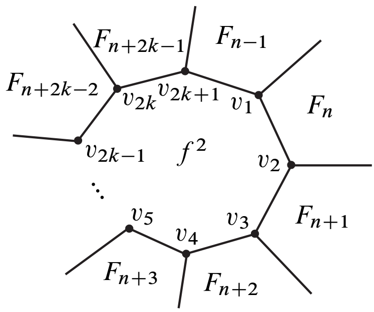

Figure 2: A 2–face f^2 with an odd number of vertices

By taking the inner product with ξ_{v_i} on both sides of (24) for each $1 \le i \le 2k+1$, we get

$$(25)\qquad \begin{cases} \epsilon_1 + \epsilon_n = 0, \\ \epsilon_1 + \epsilon_n + \epsilon_{n+1} = 0, \\ \epsilon_1 + \epsilon_{n+1} + \epsilon_{n+2} = 0, \\ \quad\vdots \\ \epsilon_1 + \epsilon_{n+i-2} + \epsilon_{n+i-1} = 0, \\ \quad\vdots \\ \epsilon_1 + \epsilon_{n+2k-2} + \epsilon_{n+2k-1} = 0, \\ \epsilon_1 + \epsilon_{n+2k-1} = 0. \end{cases}$$

The coefficient matrix of the above linear system is a $(2k+1) \times (2k+1)$ matrix over $\mathbb{F}_2$:

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & \cdots & 0 & 0 & 0 \\ & & & & & \vdots & & & \\ 1 & 0 & 0 & 0 & 0 & \cdots & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{pmatrix}_{(2k+1)\times(2k+1)}$$

It is easy to show that the determinant of this matrix is 1. So the linear system (25) only has the trivial solution, which implies that $\xi_{F_1}, \xi_{F_n}, \dots, \xi_{F_m}$ are linearly independent. Then we have $\dim_{\mathbb{F}_2} \mathfrak{B}_1(P^n) \ge m-n+2$. But this contradicts our assumption that $\dim_{\mathbb{F}_2} \mathfrak{B}_1(P^n) = m-n+1$. So the proposition is proved. $\square$

From the above discussion, we can derive several new criteria to judge whether a simple n–polytope P^n is n–colorable in terms of the associated binary codes $\{\mathfrak{B}_k(P^n)\}_{0\le k\le n}$.

Proposition 5.6 *Let P^n be an n–dimensional simple polytope with m facets. Then the following statements are equivalent:*

(1) *P^n is n–colorable.*

(2) *There exists a partition $\mathcal{F}_1,\dots,\mathcal{F}_n$ of the set $\mathcal{F}(P^n)$ of all facets such that for each $1\le i\le n$, all the facets in $\mathcal{F}_i$ are pairwise disjoint and $\sum_{F\in\mathcal{F}_i}\xi_F=\underline{1}$ (ie each vertex of P^n is incident to exactly one facet from every $\mathcal{F}_i$).*

(3) $\mathfrak{B}_0(P^n)\subseteq\mathfrak{B}_1(P^n)\subseteq\cdots\subseteq\mathfrak{B}_{n-1}(P^n)\subseteq\mathfrak{B}_n(P^n)\cong\mathbb{F}_2^{|V(P^n)|}$.

(4) $\mathfrak{B}_{n-2}(P^n)\subseteq\mathfrak{B}_{n-1}(P^n)$.

(5) $\dim_{\mathbb{F}_2}\mathfrak{B}_1(P^n)=m-n+1$.

Proof It is easy to verify the above equivalences when $n\le 2$. So we assume $n\ge 3$ below. In the proof of Proposition 5.5, we have proved $(1)\Rightarrow(2)$ and $(1)\Leftrightarrow(5)$.

Now we show that $(2)\Rightarrow(3)$. By (2), we clearly have

$$\mathfrak{B}_0(P^n)\subseteq\mathfrak{B}_1(P^n)\quad\text{and}\quad\mathfrak{B}_{n-1}(P^n)\subseteq\mathfrak{B}_n(P^n).$$

It remains to show that $\mathfrak{B}_k(P^n)\subseteq\mathfrak{B}_{k+1}(P^n)$ for each $1\le k\le n-2$. Let f^{n-k} be a codimension-k face of P^n. Without the loss of generality, we assume that

$$f^{n-k}=F_1\cap F_2\cap\cdots\cap F_k,\quad\text{where } F_i\in\mathcal{F}_i \text{ for } i=1,\dots,k.$$

For each $j=k+1,\dots,n$, we have that

$$\sum_{F\in\mathcal{F}_j}\xi_{F\cap f^{n-k}}=\sum_{F\in\mathcal{F}_j}\xi_F\circ\xi_{f^{n-k}}=\xi_{f^{n-k}}\circ\Bigl(\sum_{F\in\mathcal{F}_j}\xi_F\Bigr)=\xi_{f^{n-k}}\circ\underline{1}=\xi_{f^{n-k}}.$$

In the above equality, if $F\cap f^{n-k}=\varnothing$, then $\xi_{F\cap f^{n-k}}=\xi_\varnothing=\underline{0}$. If $F\cap f^{n-k}\ne\varnothing$, then $F\cap f^{n-k}$ is a face of codimension $k+1$. So $\xi_{F\cap f^{n-k}}\in\mathfrak{B}_{k+1}(P^n)$. Thus we get $\xi_{f^{n-k}}=\sum_{F\in\mathcal{F}_j}\xi_{F\cap f^{n-k}}\in\mathfrak{B}_{k+1}(P^n)$. This completes the proof of $(2)\Rightarrow(3)$.

It is trivial that $(3)\Rightarrow(4)$. Next we show $(4)\Rightarrow(1)$. Assume $\mathfrak{B}_{n-2}(P^n)\subseteq\mathfrak{B}_{n-1}(P^n)$. Notice that the number of nonzero coordinates in any vector in $\mathfrak{B}_{n-1}(P^n)$ must be even. So for any 2–face f^2 of P^n, we have $\xi_{f^2}\in\mathfrak{B}_{n-2}(P^n)\subseteq\mathfrak{B}_{n-1}(P^n)$, which implies that f^2 has an even number of vertices. Hence P^n is n–colorable by Theorem 2.1. □

6 Self-dual binary codes from general simple polytopes

In this section we discuss under what conditions $\mathfrak{B}_k(P^n)$, where $0 \le k \le n$, can be a self-dual code in $\mathbb{F}_2^{|V(P^n)|}$. It is clear that when the number of vertices $|V(P^n)|$ of P^n is odd, $\mathfrak{B}_k(P^n)$ cannot be a self-dual code for any k.

Lemma 6.1 *Let P^n be an n–dimensional simple polytope with $n \ge 3$. Assume that $\mathfrak{B}_k(P^n)$ is a self-dual code. Then $\underline{1} \in \mathfrak{B}_k(P^n)$ and $0 < 2k < n$.*

Proof From [6, Corollary 3.1] it is easy to see that $\underline{1} \in \mathfrak{B}_k(P^n)$. Obviously, $k = 0$ is impossible since $\dim \mathfrak{B}_0(P^n) = h_0(P^n) = 1$ and $n \ge 3$. If $2k \ge n$, then at any vertex v of P^n there exist two codimension-k faces f_1 and f_2 of P^n such that $f_1 \cap f_2 = v$. But then $\langle \xi_{f_1}, \xi_{f_2} \rangle = 1$, which contradicts the assumption that $\mathfrak{B}_k(P^n)$ is self-dual. We can also prove $2k < n$ using Proposition 5.3. Indeed, since $\mathfrak{B}_k(P^n)$ is self-dual, we can deduce from Proposition 5.3 that

$$\dim_{\mathbb{F}_2} \mathfrak{B}_k(P^n) = \frac{|V(P^n)|}{2} = \frac{h_0(P^n) + \cdots + h_n(P^n)}{2} \ge h_0(P^n) + \cdots + h_k(P^n). \tag{26}$$

Then, since $h_i(P^n) > 0$ and $h_i(P^n) = h_{n-i}(P^n)$ (Dehn–Sommerville relations) for all $0 \le i \le n$, we must have $2k < n$. □

Theorem 6.2 *For an n–dimensional simple polytope P^n with $n \ge 3$, the binary code $\mathfrak{B}_k(P^n)$ is self-dual if and only if the following two conditions are satisfied:*

(a) *$|V(P^n)|$ is even and $\dim_{\mathbb{F}_2} \mathfrak{B}_k(P^n) = |V(P^n)|/2$.*

(b) *All faces of codimensions $k, \dots, 2k$ in P^n have an even number of vertices.*

Proof If $\mathfrak{B}_k(P^n)$ is a self-dual code, then (a) obviously holds. Let $|V(P^n)| = 2r$. For any face f of codimension l, where $k \le l \le 2k$, we can always write $f = f_1 \cap f_2$, where f_1 and f_2 are faces of codimension k. In particular if f is of codimension k, we just let $f_1 = f_2 = f$. Then $\xi_f = \xi_{f_1} \circ \xi_{f_2} \in \mathcal{V}_{2r}$ since $\mathfrak{B}_k(P^n)$ is self-dual (see Lemma 2.2). This implies that the number of vertices of f is even.

Conversely, suppose $\mathfrak{B}_k(P^n)$ satisfies (a) and (b). For any codimension-k faces f and f' of P^n, either $f \cap f' = \varnothing$ or the codimension of $f \cap f'$ is between k and $2k$. Then, by (b), the number of vertices of $f \cap f'$ is even, which implies that $\langle \xi_f, \xi_{f'} \rangle = 0$. Then, by Lemma 2.2, $\mathfrak{B}_k(P^n)$ is self-dual in $\mathbb{F}_2^{|V(P^n)|}$. Note that by (26), condition (a) implies $0 < 2k < n$ when $n \ge 3$. □

Remark When $k \geq (n-2)/2$ (where $n \geq 3$), condition (b) in Theorem 6.2 implies that the polytope P^n is n–colorable. But if $k < (n-2)/2$, condition (b) cannot guarantee that P^n is n–colorable. For example let $P^n = \Delta^2 \times [0,1]^{n-2}$, where $n \geq 3$ and Δ^2 is the 2–simplex. Then P^n satisfies condition (b) for all $k < (n-2)/2$ because any face of P^n with dimension greater than 2 has an even number of vertices. But by Theorem 2.1(b), P^n is not n–colorable since Δ^2 is a 2–face of P^n.

Problem For an arbitrary simple polytope P^n, determine the dimension of $\mathfrak{B}_k(P^n)$ for all $0 \leq k \leq n$.

We have seen in Corollary 4.4 that when a simple n–polytope P^n is n–colorable, the dimension of $\mathfrak{B}_k(P^n)$ can be expressed by the h–vector of P^n. But generally, we only know a lower bound of the dimension of $\mathfrak{B}_k(P^n)$ from Proposition 5.3.

Proposition 6.3 *Let P^n be a simple n–polytope with $2r$ vertices, m facets and $n \geq 3$.*

(a) *$\mathfrak{B}_k(P^3)$ is a self-dual code if and only if $k=1$ and P^3 is 3–colorable.*
(b) *$\mathfrak{B}_k(P^4)$ is never self-dual for any $0 \leq k \leq 4$.*
(c) *$\mathfrak{B}_k(P^5)$ is a self-dual code if and only if $k=2$ and P^5 is 5–colorable.*
(d) *When $n > 5$, if $\mathfrak{B}_k(P^n)$ is a self-dual code and $m > (n+1)(n-2)/(n-3)$, then $k \geq 2$.*

Proof For (a), by Corollary 4.4 it suffices to show that if $\mathfrak{B}_k(P^3)$ is a self-dual code, then $k=1$ and P^3 is 3–colorable. Assume that $\mathfrak{B}_k(P^3)$ is a self-dual code. Then, by Theorem 6.2, k must be 1 and any 2–face of P^3 has an even number of vertices. So P^3 is 3–colorable by Theorem 2.1. This proves (a).

For (b), assume that $\mathfrak{B}_k(P^4)$ is a self-dual code. By Theorem 6.2, k must be 1 and any 2–face has an even number of vertices. So P^4 is 4–colorable by Theorem 2.1. Then (b) follows from Corollary 4.4.

Now let $n \geq 5$ and assume that $\mathfrak{B}_k(P^n)$ is a self-dual code. Let $f_{k-1}(P^n)$ denote the number of codimension-k faces in P^n. Then, by [5, Theorems 1.33 and 1.37], we have

$$f_{k-1}(P^n) \leq \binom{m}{k} \quad \text{if } 2k < n \qquad \text{and} \qquad f_{n-1}(P^n) = 2r \geq (n-1)m-(n+1)(n-2).$$

By the fact that $\dim_{\mathbb{F}_2} \mathfrak{B}_k(P^n) \leq f_{k-1}(P^n)$, we obtain

$$\begin{aligned} (27) \qquad (n-1)m-(n+1)(n-2) &\leq 2r \\ &= 2\dim_{\mathbb{F}_2} \mathfrak{B}_k(P^n) = h_0(P^n) + \cdots + h_n(P^n) \\ &\leq 2\binom{m}{k}. \end{aligned}$$

If $k=1$, we have $m \le (n+1)(n-2)/(n-3)$. Thus, if $m > (n+1)(n-2)/(n-3)$, then $k \ge 2$. This proves (d).

Next we consider the case $n=5$ with $k=1$. In this case, we have $6 \le m \le 9$ and by Lemma 6.1, all 3–faces and 4–faces of P^n have an even number of vertices. Moreover, $\dim_{\mathbb{F}_2} \mathfrak{B}_k(P^n) \le f_{k-1}(P^n)$ implies that

$$r = h_0(P^5) + h_1(P^5) + h_2(P^5) = 1 + m - 5 + h_2(P^5) = m - 4 + h_2(P^5) \le m.$$

So we have $h_2(P^5) \le 4$. In addition, by the g–theorem, we have the following restrictions:

$$h_2(P^5) \ge h_1(P^5) = m - 5 \ge h_0(P^5) = 1;$$

$$(h_1(P^5) - h_0(P^5))^{\langle 1 \rangle} \ge h_2(P^5) - h_1(P^5),$$

so

$$(m-6)^{\langle 1 \rangle} = \binom{m-5}{2} \ge h_2(P^5) - (m-5),$$

which implies

$$h_2(P^5) \le \frac{(m-4)(m-5)}{2}.$$

Combining all these restrictions, we can list all such simple 5–polytopes in terms of their h–vectors as follows:

$$\begin{aligned}
h(P^5_1) &= (1,4,4,4,4,1) \quad \text{with } m = 9;\\
h(P^5_2) &= (1,3,4,4,3,1) \quad \text{with } m = 8;\\
h(P^5_3) &= (1,3,3,3,3,1) \quad \text{with } m = 8;\\
h(P^5_4) &= (1,2,3,3,2,1) \quad \text{with } m = 7;\\
h(P^5_5) &= (1,2,2,2,2,1) \quad \text{with } m = 7;\\
h(P^5_6) &= (1,1,1,1,1,1) \quad \text{with } m = 6.
\end{aligned}$$

Clearly, P^5_6 is just a 5–simplex. So P^5_6 should be excluded since each facet of P^5_6 is a 4–simplex which has an odd number of vertices. By [5, Theorem 1.37], a direct check shows that the dual polytopes of P^5_1, P^5_3 and P^5_5 are all stacked 5–polytopes. Then they can also be excluded since they all have at least one 4–simplex as a facet. Recall that a simplicial n–polytope S is called *stacked* if there is a sequence $S_0, S_1, \dots, S_l = S$ of simplicial n–polytopes such that S_0 is an n–simplex and S_{i+1} is obtained from S_i by adding a pyramid (ie gluing another n–simplex to one of its facets). Note that adding a pyramid is dual to “cutting a vertex” of a simple polytope (see [5, Definition 1.36]).

So a simple polytope dual to a stacked n–polytope can be obtained from an n–simplex by a sequence of vertex cuttings, which implies that the polytope has at least one n–simplex as a facet.

By [5, Theorem 1.33], we can directly check that P^5_4 is the dual polytope of a cyclic polytope $C^5(7)$. Let $\{F_1, \dots, F_7\}$ be the set of all facets of P^5_4. By the main theorem in [24], we can write all the 12 vertices $v_1, \dots, v_{12}$ of P^5_4 explicitly in terms of the intersections of its facets $F_1, \dots, F_7$ as follows:

$$\begin{aligned}
v_1 &= F_1 \cap F_2 \cap F_3 \cap F_4 \cap F_5, & v_2 &= F_1 \cap F_2 \cap F_3 \cap F_4 \cap F_7,\\
v_3 &= F_1 \cap F_2 \cap F_3 \cap F_6 \cap F_7, & v_4 &= F_1 \cap F_2 \cap F_5 \cap F_6 \cap F_7,\\
v_5 &= F_1 \cap F_4 \cap F_5 \cap F_6 \cap F_7, & v_6 &= F_3 \cap F_4 \cap F_5 \cap F_6 \cap F_7,\\
v_7 &= F_1 \cap F_3 \cap F_4 \cap F_5 \cap F_6, & v_8 &= F_2 \cap F_3 \cap F_4 \cap F_5 \cap F_7,\\
v_9 &= F_1 \cap F_2 \cap F_4 \cap F_5 \cap F_7, & v_{10} &= F_1 \cap F_3 \cap F_4 \cap F_6 \cap F_7,\\
v_{11} &= F_1 \cap F_2 \cap F_3 \cap F_5 \cap F_6, & v_{12} &= F_2 \cap F_3 \cap F_5 \cap F_6 \cap F_7.
\end{aligned}$$

We can easily see that each of F_1, F_3, F_5 and F_7 has 9 vertices, and each of F_2, F_4 and F_6 has 8 vertices. Thus, P^5_4 should be excluded as well.

Now the only case left to check is P^5_2. Note that the dual polytope of P^5_2 is a simplicial 5–polytope with 8 vertices and 16 facets. By the classification in [11, Section 6.3, pages 108–112], there are exactly 8 simplicial 5–polytopes with 8 vertices up to combinatorial equivalence. They are listed in [11, Section 6.3, page 112] in terms of standard contracted Gale diagrams. By examining those Gale diagrams, we find that only two of them (shown in Figure 3) give simplicial 5–polytopes with 8 vertices and 16 facets. Let Q_1 be the simplicial 5–polytope corresponding to the left diagram, and Q_2 to the right, in Figure 3. A simple calculation shows that $\dim_{\mathbb{F}_2} \mathfrak{B}_1(Q_1^*) = 6 \neq 8$ and Q_2^* has a facet with 11 vertices, where Q_1^* and Q_2^* are the dual polytopes of Q_1 and Q_2, respectively. Hence P^5_2 cannot be Q_1^* or Q_2^*. So P^5_2 should be excluded as well.

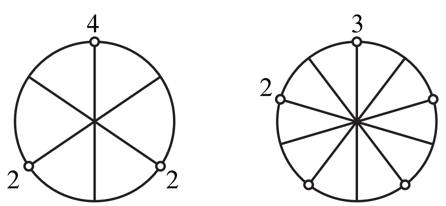

Figure 3: Two standard contracted Gale diagrams

Combining the above arguments, we can conclude that $\mathfrak{B}_1(P^5)$ is never self-dual. Therefore, if $\mathfrak{B}_k(P^5)$ is self-dual, k must be 2 and so P^5 is 5–colorable by Lemma 6.1. Then (c) follows from Corollary 4.4. □

Corollary 6.4 *For an n–dimensional simple polytope P^n with $2r$ vertices and m facets, if $\mathfrak{B}_k(P^n)$ is a self-dual code in $\mathbb{F}_2^{2r}$ and $r \geq \binom{m}{l}$ for some $l < (m-1)/2$, then $k \geq l$.*

Proof By (27), we have $\binom{m}{k} \geq r \geq \binom{m}{l}$. Then, since $2k < n \leq m-1$ (by Lemma 6.1), we obtain $k \geq l$. □

In general, judging the existence of self-dual codes $\mathfrak{B}_k(P^n)$ for a simple n–polytope P^n that is not n–colorable seems to be a quite hard problem when $n > 5$. On the other hand, Corollary 4.4 tells us that $2k$–colorable simple $2k$–polytopes cannot produce any self-dual codes. Then considering the statements in Proposition 6.3, it is reasonable to pose the following conjecture.

Conjecture *Let P^n be a simple n–polytope with $2r$ vertices and m facets, where $n \geq 3$. Then $\mathfrak{B}_k(P^n)$ is a self-dual code if and only if P^n is n–colorable, n is odd and $k = (n-1)/2$.*

7 Minimum distance of self-dual codes from 3–dimensional simple polytopes

Proposition 7.1 *For any 3–dimensional 3–colorable simple polytope P^3, the minimum distance of the self-dual code $\mathfrak{B}_1(P^3)$ is always equal to 4.*

Proof It is well known that any 3–dimensional simple polytope must have a 2–face with fewer than 6 vertices. Then, since P^3 is even, there must exist a 4–gon 2–face in P^3. So by Corollary 4.5, the minimum distance of $\mathfrak{B}_1(P^3)$ is less than or equal to 4. In addition, we know that the Hamming weight of any element in $\mathfrak{B}_1(P^3)$ is an even integer. So we only need to prove that for any collection of 2–faces $\{F_1, \dots, F_k\}$ of P^3, the Hamming weight of $\alpha = \xi_{F_1} + \cdots + \xi_{F_k} \in \mathfrak{B}_1(P^3)$ cannot be 2. We will use the following notation:

- Let $V(\alpha)$ denote the union of all the vertices of $F_1, \dots, F_k$.
- Let $\Gamma(\alpha)$ denote the union of all the vertices and edges of $F_1, \dots, F_k$. So $\Gamma(\alpha)$ is a graph with vertex set $V(\alpha)$.

A vertex v in $V(\alpha)$ is called *type* j if v is incident to exactly j facets in $F_1, \dots, F_k$. Then, since P^3 is simple, any vertex in $V(\alpha)$ is of type 1, type 2 or type 3 (see Figure 4). Suppose there are l_j vertices of type j in $V(\alpha)$ for $j = 1, 2, 3$. It is easy to see that the Hamming weight of α is equal to $l_1 + l_3$. Assume that $\mathrm{wt}(\alpha) = l_1 + l_3 = 2$. Then we have three cases for l_1 and l_3:

(a) $l_1 = 2$ and $l_3 = 0$; (b) $l_1 = 1$ and $l_3 = 1$; (c) $l_1 = 0$ and $l_3 = 2$.

Note that any vertex of type 2 or type 3 in $V(\alpha)$ meets exactly three edges in $\Gamma(\alpha)$. In other words, $\Gamma(\alpha)$ is a graph whose vertices are all 3–valent except the type-1 vertices. Let $\Gamma(P^3)$ denote the graph of P^3 (the union of all the vertices and edges of P^3) and let $\overline{\Gamma}(\alpha) = \Gamma(P^3) \backslash \Gamma(\alpha)$. Observe that $\Gamma(\alpha)$ meets $\overline{\Gamma}(\alpha)$ only at the type-1 vertices in $V(\alpha)$.

We now argue that none of the three cases for l_1 and l_3 is possible:

- In case (a), there are two type-1 vertices in $V(\alpha)$, denoted by v and v'. Then, since $\Gamma(\alpha)$ meets $\overline{\Gamma}(\alpha)$ only at $\{v, v'\}$, removing v and v' from the graph $\Gamma(P^3)$ will disconnect $\Gamma(P^3)$ (see Figure 4 for an example). But according to Balinski's theorem (see [3]), the graph of any 3–dimensional simple polytope is a 3–connected graph (ie removing any two vertices from the graph does not disconnect it). So (a) is impossible.
- In case (b), there is only one type-1 vertex in $V(\alpha)$, denoted by v. By an argument similar to that for case (a), removing v from the graph $\Gamma(P^3)$ will disconnect $\Gamma(P^3)$. This contradicts the 3–connectivity of $\Gamma(P^3)$. So (b) is impossible also.
- In case (c), there are no type-1 vertices in $V(\alpha)$. So $\Gamma(\alpha)$ is a 3–valent graph. This implies that $\Gamma(\alpha)$ is the whole 1–skeleton of P^3, and so $V(\alpha) = V(P^3)$. Then the Hamming weight satisfies $\mathrm{wt}(\alpha) = \mathrm{wt}(\xi_{F_1} + \cdots + \xi_{F_k}) = \mathrm{wt}(\underline{1}) = |V(P^3)| \geq 4$. But this contradicts our assumption that $\mathrm{wt}(\alpha) = 2$. So (c) is impossible.

Therefore, the Hamming weight of any element of $\mathfrak{B}_1(P^3)$ cannot be 2. This finishes the proof of the theorem. □

Remark It is shown in [14] that any 3–dimensional 3–colorable simple polytope can be obtained from the 3–dimensional cube via two kinds of operations. So it might be possible to classify all the self-dual binary codes obtained from 3–dimensional simple polytopes. But the classification seems to be very complicated.

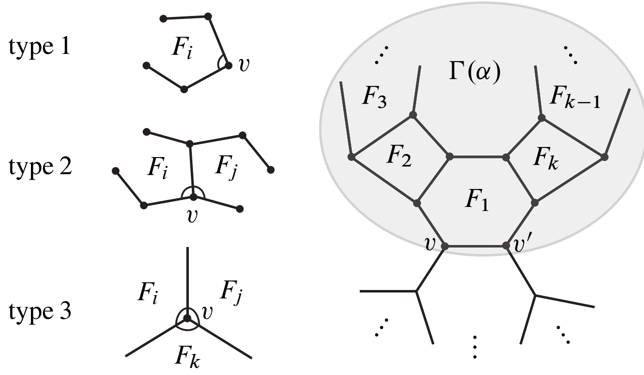

Figure 4: The graph of a simple 3–polytope

8 Properties of n–dimensional n–colorable simple polytopes

For brevity, we use the words "even polytope" to refer to an n–dimensional n–colorable simple polytope. Indeed, this term has already been used by Joswig [15].

Definition [21; 16, Remark 2] Let F be a facet of a simple polytope P and $V(F)$ be the set of vertices of F. Define a map $\Xi_F\colon V(F) \to V(P) \setminus V(F)$ as follows. For each $v \in V(F)$, there is exactly one edge e of P such that $e \not\subseteq F$ and $v \in e$ (since P is simple and F is codimension one). Let $\Xi_F(v)$ be the other endpoint of e.

Example 8.1 Let P be the 6–gon prism in Figure 1 and F be the facet of P with vertex set $\{3,4,9,10\}$. Then, by definition, $\Xi_F\colon \{3,4,9,10\} \to \{1,2,5,6,7,8,11,12\}$, where

$$\Xi(3) = 2, \quad \Xi(4) = 5, \quad \Xi(9) = 8, \quad \Xi(10) = 11.$$

Proposition 8.2 *For an even polytope P, the map Ξ_F is injective for any facet F of P.*

Proof Assume Ξ_F is not injective. There must exist two vertices $p_1, p_2 \in F$ and a vertex $v \notin F$ such that v is connected to both p_1 and p_2 by edges in P (see Figure 5). For $i = 1, 2$, let f_i be the edge with endpoints p_i and v. Suppose the dimension of P is n. Then there exist n facets $F_1, F_2, \dots, F_n$, distinct from F, such that

$$v = \bigcap_{i=1}^{n} F_i, \quad f_1 = \bigcap_{i=1}^{n-1} F_i \quad \text{and} \quad f_2 = \bigcap_{i=2}^{n} F_i.$$

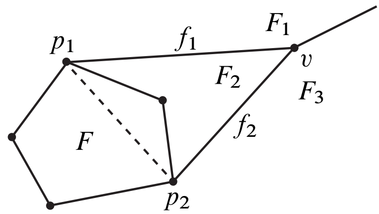

Figure 5: A facet F with Ξ_F noninjective

Then we have

$$p_1 = F \cap \left(\bigcap_{i=1}^{n-1} F_i \right) \quad \text{and} \quad p_2 = F \cap \left(\bigcap_{i=2}^{n} F_i \right).$$

Since P is n–colorable, we can color all the facets of P by n–colors $e_1, \dots, e_n$ such that no adjacent facets are assigned the same color. Suppose F_i is colored by e_i for $i = 1, \dots, n$. Then, at p_1, the facet F has to be colored by e_n, while at p_2, the facet F has to be colored by e_1, a contradiction. $\square$

Proposition 8.3 *Let P be an even polytope. For any facet F of P, we have*

$$|V(P)| \geq 2|V(F)|.$$

Moreover, $|V(P)| = 2|V(F)|$ if and only if $P \simeq F \times [0,1]$, where $[0,1]$ denotes a 1–simplex.

Proof By Proposition 8.2, the map $\Xi_F \colon V(F) \to V(P) \setminus V(F)$ is injective. Thus

$$|V(F)| \leq |V(P) \setminus V(F)| = |V(P)| - |V(F)|.$$

So $|V(P)| \geq 2|V(F)|$. If $|V(P)| = 2|V(F)|$, the injectivity of Ξ_F implies that $P \simeq F \times [0,1]$. $\square$

Corollary 8.4 *Let f be a codimension-k face of an even polytope P. Then $|V(P)| \geq 2^k |V(f)|$. Moreover, $|V(P)| = 2^k |V(f)|$ if and only if $P \simeq f \times [0,1]^k$.*

Corollary 8.5 *For any n–dimensional even polytope P, we must have $|V(P)| \geq 2^n$. In particular, $|V(P)| = 2^n$ if and only if $P \simeq [0,1]^n$* (the n–dimensional cube).

Corollary 8.6 *Suppose P is an n–dimensional even polytope, where $n \geq 4$. If there exists a facet F of P with $|V(P)| = 2|V(F)|$, then there exists a 3–face of P combinatorially equivalent to a 3–dimensional cube.*

Proof It is well known that any 3–dimensional simple polytope must have a 2–face f with fewer than 6 vertices. Now, since P is even, any 2–face of P must have an even number of vertices. So there exists a 4–gon face f in F, ie $f \simeq [0,1]^2$. Then, since $|V(P)| = 2|V(F)|$, we have $P \simeq F \times [0,1]$ by Corollary 8.4. So P has a 3–face combinatorially equivalent to $f \times [0,1] \simeq [0,1]^3$. □

Given any two even polytopes P_1 and P_2, we have the following constructions:

- The product $P_1 \times P_2$ is also an even polytope.
- If P_1 has the same dimension as P_2, we can choose a vertex v_1 of P_1 and a vertex v_2 of P_2 to form a new simple polytope $P_1 \#_{v_1,v_2} P_2$, called the *connected sum* of P_1 and P_2. Roughly speaking, $P_1 \#_{v_1,v_2} P_2$ is obtained by cutting off v_1 from P_1 and v_2 from P_2 and gluing the rest of P_1 to the rest of P_2 along the new simplex face (see [5, Construction 1.13]). By Theorem 2.1, $P_1 \#_{v_1,v_2} P_2$ is also an even polytope.

9 Doubly even binary codes

A binary code C is called *doubly even* if the Hamming weight of any codeword in C is divisible by 4. Doubly even self-dual codes are of special importance among binary codes and have been extensively studied. According to Gleason [9], the length of any doubly even self-dual code is divisible by 8. In addition, Mallows and Sloane [19] showed that if C is a doubly even self-dual code of length l, it is necessary that the minimum distance d of C satisfies $d \leq 4[l/24] + 4$. And C is called *extremal* if equality holds.

A somewhat surprising result of Zhang [26] tells us that an extremal doubly even self-dual binary code must have length less than or equal to 3928. However, the existence of extremal doubly even self-dual binary codes is only known for the following lengths (see [12] and [23, page 273]):

$$l = 8,\ 16,\ 24,\ 32,\ 40,\ 48,\ 56,\ 64,\ 80,\ 88,\ 104,\ 112,\ 136.$$

For example, the extended Golay code $\mathcal{G}_{24}$ is the only doubly even self-dual $[24,12,8]$ code, and the extended quadratic residue code QR_{48} is the only doubly even self-dual $[48,24,12]$ code (see [13]). In addition, the existence of an extremal doubly even self-dual code of length 72 is a long-standing open question (see [25] and [23, Section 12]).

The following proposition is an immediate consequence of Corollary 4.5 which gives us a way to construct doubly even self-dual codes from simple polytopes.

Proposition 9.1 *For an* $(2k+1)$*–dimensional even polytope* P*, the self-dual binary code* $\mathfrak{B}_k(P)$ *is doubly even if and only if the number of vertices of any* $(k+1)$*–dimensional face of* P *is divisible by* 4*.*

Definition We say that a self-dual binary code C can be *realized by an even polytope* if there exists a $(2k+1)$–dimensional even polytope P such that $C=\mathfrak{B}_k(P)$.

Example 9.2 Extremal doubly even self-dual binary codes of lengths 8 and 16 can be realized by the 3–cube and the 8–gon prism (8–gon $\times [0,1]$), respectively. In addition, the $(2k+1)$–dimensional cube realizes a doubly even code of type $[2^{2k+1}, 2^{2k}, 2^{k+1}]$ which is the *Reed–Muller code* $\mathcal{R}(k, 2k+1)$ (see [18, Section 4.5]). Moreover, we can use the product of an even polytope with the polytopes in the above examples to realize more doubly even self-dual binary codes with larger minimum distances.

Proposition 9.3 *The* $[24,12,8]$ *extended Golay code* $\mathcal{G}_{24}$ *cannot be realized by any even polytope.*

Proof Assume $\mathcal{G}_{24}$ can be realized by an n–dimensional even polytope P^n, where n is odd. Then P^n has 24 vertices. By Corollary 8.5, we have $24 \geq 2^n$, which implies $n=1$ or $n=3$. But $n=1$ is clearly impossible. And by Proposition 7.1, $n=3$ is also impossible since the minimal distance of $\mathcal{G}_{24}$ is 8. □

Proposition 9.4 *The* $[48,24,12]$ *extended quadratic residue code* QR_{48} *cannot be realized by any even polytope.*

Proof Suppose QR_{48} can be realized by an n–dimensional even polytope P^n. Then, by Corollary 8.5, we must have $n=1,3$ or 5. But by Proposition 7.1, n cannot be 1 or 3. If $n=5$, since $|V(P^5)|=48$, any 3–face of P^5 has to be an even polytope with 12 vertices by Corollary 8.4 and the fact that the minimum distance of QR_{48} is 12. Then P^5 is combinatorially equivalent to the product of a simple 3–polytope with $[0,1]^2$ by Corollary 8.4 again. This implies that P^5 has a 3–face combinatorially equivalent to a 3–cube. But this contradicts the fact that any 3–face of P^5 has 12 vertices. □

Proposition 9.5 *An extremal doubly even self-dual code of length* 72 (if one exists) *cannot be realized by any even polytope.*

Proof Assume that C is an extremal doubly even self-dual binary code of length 72 and C can be realized by an even polytope P. Then, by the definition of extremity, the minimum distance of C is 16 and P has 72 vertices. Moreover, we have that

(i) the dimension of P has to be 5 by Corollary 8.5 and Proposition 7.1;

(ii) any 3–face of P must be an even polytope with 16 vertices by Corollary 8.4 and Proposition 9.1.

Then any 4–face of P must have 32 or 36 vertices by Corollary 8.4. But neither is possible:

- If P has a 4–face F with 32 vertices, then $F \simeq f \times [0,1]$, where f is a 3–face with 16 vertices, by (ii) and Corollary 8.4. This implies that P has a 3–face combinatorially equivalent to a 3–cube by Corollary 8.6. But this contradicts (ii).

- If P has a 4–face F with 36 vertices, then $P \simeq F \times [0,1]$ by Corollary 8.4. So P has a 3–face combinatorially equivalent to a 3–cube by Corollary 8.6. This contradicts (ii) again.

So by the above argument, such an even polytope P does not exist. □

Acknowledgements This paper was inspired by a question on self-dual binary codes and small covers which was proposed to the authors by Professor Matthias Kreck during his visit to China in September 2012. The authors also want to thank the anonymous reviewers for some helpful information and suggestions. This work is supported in part by grants from NSFC (No. 11371093, No. 11371188, No. 11401233, No. 11431009, No. 11661131004) and PAPD (Priority Academic Program Development of Jiangsu Higher Education Institutions).

References

[1] **C Allday**, **M Franz**, **V Puppe**, *Equivariant cohomology, syzygies and orbit structure*, Trans. Amer. Math. Soc. 366 (2014) 6567–6589 MR

[2] **C Allday**, **V Puppe**, *Cohomological methods in transformation groups*, Cambridge Studies in Advanced Mathematics 32, Cambridge Univ. Press (1993) MR

[3] **M L Balinski**, *On the graph structure of convex polyhedra in n–space*, Pacific J. Math. 11 (1961) 431–434 MR

[4] **A Brøndsted**, *An introduction to convex polytopes*, Graduate Texts in Mathematics 90, Springer (1983) MR

[5] **V M Buchstaber**, **T E Panov**, *Torus actions and their applications in topology and combinatorics*, University Lecture Series 24, Amer. Math. Soc., Providence, RI (2002) MR

[6] **B Chen**, **Z Lü**, *Equivariant cohomology and analytic descriptions of ring isomorphisms*, Math. Z. 261 (2009) 891–908 MR

[7] **P E Conner**, *Differentiable periodic maps*, 2nd edition, Lecture Notes in Mathematics 738, Springer (1979) MR

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

[9] **A M Gleason**, *Weight polynomials of self-dual codes and the MacWilliams identities*, from "Actes du Congrès International des Mathématiciens, 3", Gauthier-Villars, Paris (1971) 211–215 MR

[10] **M Goresky**, **R Kottwitz**, **R MacPherson**, *Equivariant cohomology, Koszul duality, and the localization theorem*, Invent. Math. 131 (1998) 25–83 MR

[11] **B Grünbaum**, *Convex polytopes*, 2nd edition, Graduate Texts in Mathematics 221, Springer (2003) MR

[12] **M Harada**, *An extremal doubly even self-dual code of length* 112, Electron. J. Combin. 15 (2008) art. id. N33, 5 pages MR

[13] **S K Houghten**, **C W H Lam**, **L H Thiel**, **J A Parker**, *The extended quadratic residue code is the only* $(48, 24, 12)$ *self-dual doubly-even code*, IEEE Trans. Inform. Theory 49 (2003) 53–59 MR

[14] **I V Izmest'ev**, *Three-dimensional manifolds defined by a coloring of the faces of a simple polytope*, Mat. Zametki 69 (2001) 375–382 MR In Russian; translated in Mathematical Notes 69 (2001) 340–346

[15] **M Joswig**, *Projectivities in simplicial complexes and colorings of simple polytopes*, Math. Z. 240 (2002) 243–259 MR

[16] **G Kalai**, *A simple way to tell a simple polytope from its graph*, J. Combin. Theory Ser. A 49 (1988) 381–383 MR

[17] **M Kreck**, **V Puppe**, *Involutions on* 3*–manifolds and self-dual, binary codes*, Homology Homotopy Appl. 10 (2008) 139–148 MR

[18] **J H van Lint**, *Introduction to coding theory*, 2nd edition, Graduate Texts in Mathematics 86, Springer (1992) MR

[19] **C L Mallows**, **N J A Sloane**, *An upper bound for self-dual codes*, Information and Control 22 (1973) 188–200 MR

[20] **J Milnor**, *Construction of universal bundles, II*, Ann. of Math. 63 (1956) 430–436 MR

[21] **M A Perles**, *Results and problems on reconstruction of polytopes*, unpublished manuscript (1970)

[22] **V Puppe**, *Group actions and codes*, Canad. J. Math. 53 (2001) 212–224 MR

[23] **E M Rains**, **N J A Sloane**, *Self-dual codes*, from "Handbook of coding theory, I" (V S Pless, W C Huffman, R A Brualdi, editors), North-Holland, Amsterdam (1998) 177–294 MR

[24] **G C Shephard**, *A theorem on cyclic polytopes*, Israel J. Math. 6 (1968) 368–372 MR

[25] **N J A Sloane**, *Is there a $(72, 36)$ $d = 16$ self-dual code?*, IEEE Trans. Information Theory 19 (1973) 251 MR

[26] **S Zhang**, *On the nonexistence of extremal self-dual codes*, Discrete Appl. Math. 91 (1999) 277–286 MR

School of Mathematics and Statistics, Huazhong University of Science and Technology
Wuhan, China

School of Mathematical Sciences, Fudan University
Shanghai, China

Department of Mathematics and IMS, Nanjing University
Nanjing, China

bobchen@hust.edu.cn, zlu@fudan.edu.cn, yuli@nju.edu.cn

Received: 27 March 2017 Revised: 25 February 2018