Self-Dual Binary Codes from Small Covers and Simple Polytopes
— A joint work with Bo Chen and Zhi Lü

Li Yu

Department of Mathematics, Nanjing University

International Conference on Combinatorial and Toric Homotopy

August 24–28, 2015, Singapore
A binary linear code $C$ of length $l$ — a linear subspace of the $l$-dimensional linear space $\mathbb{F}_2^l$ over $\mathbb{F}_2$.

The Hamming weight of an element $u = (u_1, \ldots, u_l) \in \mathbb{F}_2^l$, denoted by $wt(u)$, is the number of nonzero components $u_i$ in $u$. The Hamming distance $d(u, v)$ of any elements $u, v \in C$ is defined by

$$d(u, v) = wt(u - v).$$

The minimum of the distances $d(u, v)$ for all $u, v \in C$, $u \neq v$, is called the minimum distance of $C$. It is also equal to the minimal Hamming weight of all the nonzero elements in $C$.

A binary code $C \subset \mathbb{F}_2^l$ is called type $[l, k, d]$ if $\dim_{\mathbb{F}_2} C = k$ and the minimum distance of $C$ is $d$. 
The inner product $\langle , \rangle$ on $\mathbb{F}_2^l$ is defined by:

$$\langle u, v \rangle := \sum_{i=1}^{l} u_i v_i, \; u = (u_1, \ldots, u_l), \; v = (v_1, \ldots, v_l) \in \mathbb{F}_2^l.$$ 

Note that

$$\langle u, u \rangle = \sum_{i=1}^{l} u_i, \; u = (u_1, \ldots, u_l) \in \mathbb{F}_2^l.$$
Self-dual Binary Code

Any binary linear code $C$ in $\mathbb{F}_2^l$ has a 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 $\dim_{\mathbb{F}_2} C + \dim_{\mathbb{F}_2} C^\perp = n$. We call $C$ self-dual if $C = C^\perp$.

If $C$ is self-dual, we have:

- The code length $l = 2 \dim_{\mathbb{F}_2} C$ must be even;
- For any $u \in C$, the Hamming weight $wt(u)$ is an even integer;
- The minimum distance of $C$ is an even integer.
m-involutins on manifolds

An involution \( \tau \) on a manifold \( M \) is called an \( m \)-involution if
- \( \tau \) only has isolated fixed points, and
- the number of fixed points of \( \tau \) is equal to \( \sum_i b_i(M; \mathbb{F}_2) \).

Let \( G_\tau = \langle \tau \rangle \cong \mathbb{Z}_2 \). Then we can show that

(a) The number of fixed points \(|M^{G_\tau}| = 2r, r \geq 1\).

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

\[
H^*_{G_\tau}(M; \mathbb{F}_2) = H^*(M; \mathbb{F}_2) \otimes H^*(BG_\tau; \mathbb{F}_2).
\]
The inclusion of the fixed point set, \( \iota : M^{G_\tau} \hookrightarrow M \), induces a monomorphism

\[
\iota^* : H^*_{G_\tau}(M; \mathbb{F}_2) \rightarrow H^*_{G_\tau}(M^{G_\tau}; \mathbb{F}_2) \cong \mathbb{F}_2^{2r} \otimes \mathbb{F}_2[t].
\]

So the image of \( H^*_{G_\tau}(M; \mathbb{F}_2) \) in \( \mathbb{F}_2^{2r} \otimes \mathbb{F}_2[t] \) under the map \( \iota^* \) is isomorphic to \( H^*_{G_\tau}(M; \mathbb{F}_2) \) as graded algebras. Define

\[
V_k^M = \{ y \in \mathbb{F}_2^{2r} \mid y \otimes t^k \in \text{Im}(\iota^*) \} \subset \mathbb{F}_2^{2r}, \ k = 0, \cdots, n.
\]

We have a filtration:

\[
\mathbb{F}_2 \cong V_0^M \subset V_1^M \subset \cdots \subset V_{n-2}^M \subset V_{n-1}^M = \mathcal{V}_{2r} \subset V_n^M = \mathbb{F}_2^{2r}
\]

where \( \mathcal{V}_{2r} = \{ x = (x_1, \ldots, x_{2r}) \in \mathbb{F}_2^{2r} \mid \langle x, x \rangle = 0 \} \).
Binary Codes Constructed from $m$-involutions

By the localization theorem for equivariant cohomology,

$$H^k(M^n; \mathbb{F}_2) \cong V^M_k / V^M_{k-1}, \ 0 \leq k \leq n. \quad (1.1)$$

So we have: $\dim_{\mathbb{F}_2} V^M_k = \sum_{j=0}^{k} b_j(M; \mathbb{F}_2)$. Moreover, we have

$$(V^M_k)\perp = V^M_{n-1-k}. \quad (1.2)$$

This is because $V^M_{n-1-k}$ is perpendicular to $V^M_k$ with respect to $\langle \ , \rangle$ and by the Poincaré duality of $M$, we have

$$\dim_{\mathbb{F}_2} V^M_k + \dim_{\mathbb{F}_2} V^M_{n-1-k} = \sum_{j=0}^{n} b_j(M; \mathbb{F}_2) = 2r.$$
Each $V^M_k$ above can be thought of as a binary code in $\mathbb{F}_2^{2r}$. So when $n$ is odd, $V^M_{\frac{n-1}{2}}$ is a self-dual binary code in $\mathbb{F}_2^{2r}$.

**Theorem [Puppe 2001]**
For any $m$-involution $\tau$ on a closed manifold $M^n$ where $n$ is odd, we obtain a self-dual binary code $V^M_{\frac{n-1}{2}}$ from the localization of $H^*_G(M^n; \mathbb{F}_2)$ to the fixed point sets.

**Theorem [Puppe-Kreck 2012]**
Any self-dual binary code can be obtained from an $m$-involution on some closed 3-manifold in the above way.
Self-dual binary codes $\leftrightarrow$ \(m\)-involutions on manifolds

**Problem:** Construct \(m\)-involutions on manifolds? (Not easy)

Small covers — closed \(n\)-manifold with locally standard \((\mathbb{Z}_2)^n\)-actions whose orbit space is a simple convex polytope.

They are introduced by Davis-Januszkiewicz (1991 Duke. Math. J.) as an analogue of toric manifolds.
Suppose $M^n$ is a small cover whose orbit space under the locally standard $(\mathbb{Z}_2)^n$-action is $P^n$ (a simple $n$-polytope). Let

$$\pi : M^n \rightarrow P^n \text{ (the orbit map).}$$

For any facet $F_i$ of $P^n$, the isotropy subgroup of $\pi^{-1}(F_i) \subset M^n$ under the $(\mathbb{Z}_2)^n$-action is a rank one subgroup of $(\mathbb{Z}_2)^n$ generated by a nonzero element, say $g_{F_i} \in (\mathbb{Z}_2)^n$. Then we obtain a map

$$\lambda_{M^n} : \mathcal{F}(P^n) \longrightarrow (\mathbb{Z}_2)^n$$

$$F_i \longmapsto g_{F_i}$$

We call $\lambda_{M^n}$ the characteristic function associated to $M^n$. 
Conversely, Davis-Januszkiewicz showed that up to equivariant homeomorphism, $M^n$ can be recovered from $(P^n, \lambda_{M^n})$ by

$$M^n = P^n \times (\mathbb{Z}_2)^n / \sim \quad (1.3)$$

where $(p, g) \sim (p', g')$ if and only if $p = p'$ and $g^{-1}g' \in G_p$ where

$$G_p = \text{ the subgroup of } (\mathbb{Z}_2)^n \text{ generated by } \{\lambda_{M^n}(F) \mid p \in F\}$$

Many topological invariants (fundamental group, cohomology groups, characteristic classes etc.) can be explicitly computed from the combinatorics of $P^n$ and $\lambda$. For example,

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

where $(h_0(P^n), h_1(P^n), ..., h_n(P^n))$ is the $h$-vector of $P^n$
1 Backgrounds
2 Main Results
1.1 Binary Linear Codes
1.2 Self-Dual Binary Codes from $m$-Involutions on Manifolds
1.3 Small Covers

Self-dual binary codes

Small covers

Follow Puppe-Kreck

Davis - Januszkiewicz

Simple polytopes

Li Yu
Self-Dual Binary Codes from Small Covers and Simple Polytopes
Let $\pi : M^n \rightarrow P^n$ be a small cover and $\lambda : \mathcal{F}(P^n) \rightarrow (\mathbb{Z}_2)^n$ be its characteristic function. Any $g \neq 0 \in (\mathbb{Z}_2)^n$ determines an involution $\tau_g$ on $M^n$, called a regular involution on $M^n$.

**Theorem [Chen-Lü-Yu]**

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 $\text{Im}(\lambda)$ of $\lambda$ is a basis of $(\mathbb{Z}_2)^n$ (which implies that $P^n$ is $n$-colorable).
A simple polytope is \textit{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.

**Theorem [Joswig 2002]**

Let \( P^n \) be an \( n \)-dimensional simple polytope. 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) Each \( k \)-face of \( P^n \) is \( k \)-colorable.
Let $\pi : M^n \rightarrow P^n$ be an $n$-dimensional small cover which admits a regular $m$-involution. Then by our preceding discussions,

- $P^n$ is an $n$-dimensional $n$-colorable simple polytope.
- The characteristic function $\lambda$ of $M^n$ satisfies: $\text{Im}(\lambda) = \{e_1, \cdots, e_n\}$ is a basis of $(\mathbb{Z}_2)^n$.
- $\tau_{e_1+\cdots+e_n}$ is an $m$-involution on $M^n$.
- Suppose $P^n$ has $2r$ vertices. There is a filtration

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

In particular, when $n$ is odd, $C_{M^n} := V_{\frac{n-1}{2}}^M \subset \mathbb{F}_2^{2r}$ is a self-dual binary code determined by $(M^n, \tau_{e_1+\cdots+e_n})$. 
Let \( \{v_1, \cdots, v_{2r}\} \) be all the vertices of \( P^n \). Any face \( f \) of \( P^n \) determines an element \( \xi_f \in \mathbb{F}_2^{2r} \) where the \( i \)-th entry of \( \xi_f \) is 1 if and only if \( v_i \) is a vertex of \( f \).

For example, \( \xi_{v_i} = (0, \cdots, 1, \cdots, 0) \), \( \xi_{P^n} = 1 = (1, \cdots, 1) \in \mathbb{F}_2^{2r} \).
Main Theorem [Chen-Lü-Yu]

Let $\pi : M^n \to P^n$ be an $n$-dimensional small cover which admits a regular $m$-involution where $n$ is odd. For any $0 \leq k \leq n$,

$$V^M_k = \text{Span}_{F_2} \{\xi_f ; f \text{ is a codimension-}k \text{ face of } P^n\}$$

- The self-dual binary code $C_{M^n} = V^M_{n-1}$ is spanned by

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

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

$$\min\{\#(\text{vertices of } f) ; f \text{ is a } \frac{n+1}{2}-\text{dimensional face of } P^n\}.$$
A linear basis of $V^M_k$

- Choose a generic height function $\phi$ on $P^n$. Using $\phi$, one makes the 1-skeleton of $P^n$ into a directed graph by orienting each edge so that $\phi$ increases along it.

- For any face $f$ of $P^n$ with dimension $> 0$, $\phi|_f$ assumes its maximum (or minimum) at a vertex. Since $\phi$ is generic, each face $f$ of $P^n$ of a unique “top” and a unique “bottom” vertex.

- For any vertex $v$, let $m(v)$ denote the number of incident edges which point toward $v$, and let $f_v$ be the smallest face of $P^n$ which contains all the inward pointing edges incident to $v$. It is clear that $\dim(f_v) = m(v)$. 
§1 Backgrounds
§2 Main Results

§2.1 m-involutions on Small Covers
§2.2 Self-dual Codes from Small Covers
§2.3 Binary Codes from General Simple Polytopes
§2.4 Properties of n-colorable simple n-polytopes
§2.5 Minimum Distance

Li Yu
Self-Dual Binary Codes from Small Covers and Simple Polytopes
Fact

The number of vertices $v$ of $P^n$ with $m(v) = k$ is equal to $h_k(P^n)$.

Proposition

Let $\pi : M^n \rightarrow P^n$ be an $n$-dimensional small cover which admits a regular $m$-involution where $n$ is odd. For any $0 \leq k \leq n$, the linear space $V^M_k$ has a basis defined by

$$A_k = \{ \xi_{f_v} ; v \text{ is any vertex of } P^n \text{ with } n-k \leq m(v) \leq n, \} \subset (\mathbb{F}_2)^{2r}.$$

So in particular, $A_{\frac{n-1}{2}}$ is a basis of $C_{M^n} = V_{\frac{n-1}{2}}^M$. 
Given an arbitrary $n$-dimensional simple polytope $P^n$, let the vertices of $P^n$ be $v_1, \cdots, v_l$. Then for any $0 \leq k \leq n$, the following definition still makes sense.

$$\mathcal{B}_k(P^n) := \text{Span}_{\mathbb{F}_2}\{\xi_f ; f \text{ is a codimension-}k \text{ face of } P\} \subset \mathbb{F}_2^l.$$ 

Question:
For what simple polytope $P^n$ and what $0 \leq k \leq n$, is the $\mathcal{B}_k(P^n)$ a binary self-dual code?
**Theorem [Chen-Lü-Yu]**

Let $P$ be an $n$-dimensional simple polytope. Then $B_k(P)$ is a self-dual code if and only if $P$ is $n$-colorable, $n$ is odd and $k = \frac{n-1}{2}$.

Therefore, the set of self-dual binary codes we can obtain from simple polytopes agree with those obtained from small covers!


**Proposition [Chen-Lü-Yu]**

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 $\mathcal{F}_1, \ldots, \mathcal{F}_n$ of the set $\mathcal{F}(P^n)$ of all facets, such that for each $1 \leq i \leq n$, all the facets in $\mathcal{F}_i$ are pairwise disjoint and $\sum_{F \in \mathcal{F}_i} \xi_F = 1$ (i.e., each vertex of $P^n$ is incident to exactly one facet from every $\mathcal{F}_i$).
3. $\mathcal{B}_0(P^n) \subset \mathcal{B}_1(P^n) \subset \cdots \subset \mathcal{B}_{n-1}(P^n) \subset \mathcal{B}_n(P^n) \cong \mathbb{F}_2^{|V(P^n)|}$.
4. $\mathcal{B}_{n-2}(P^n) \subset \mathcal{B}_{n-1}(P^n)$.
5. $\dim_{\mathbb{F}_2} \mathcal{B}_1(P^n) = m - n + 1$. 

Li Yu  
Self-Dual Binary Codes from Small Covers and Simple Polytopes
Proposition [Chen-Lü-Yu]

Let $P^n$ be an $n$-colorable simple $n$-polytope. For any codimension-$k$ face $f$ of $P^n$. Then $|V(P^n)| \geq 2^k |V(f)|$.
Moreover, $|V(P^n)| = 2^k |V(f)|$ if and only if $P = f \times [0, 1]^k$.

Corollary

For any $n$-colorable simple $n$-polytope $P^n$, we must have $|V(P^n)| \geq 2^n$. In particular, $|V(P^n)| = 2^n$ if and only if $P^n = [0, 1]^n$ (the $n$-dimensional cube).
Minimum Distance of Self-Dual Codes from Simple Polytopes

Proposition [Chen-Lü-Yu]

For a 3-dimensional 3-colorable simple polytope $P^3$, the minimum distance of the self-dual code $\mathcal{B}_1(P^3)$ is always equal to 4.

Conjecture: For an $n$-colorable simple $n$-polytope $P^n$ where $n$ is odd, the minimum distance of the self-dual binary code $\mathcal{B}_{\frac{n-1}{2}}(P^n)$ is equal to

$$\min\{\#(\text{vertices of } f) ; f \text{ is a } \frac{n+1}{2}-\text{-dimensional face of } P^n\}.$$
End of Talk

August 24, 2015

Singapore National University