Self-dual Codes and Simple Polytopes

Bo Chen

School of Mathematics and Statistics, HUST
Jiont-work with Zhi Lü and Li Yu
bobchen@hust.edu.cn

Jan. 2014, Osaka

Binary Self-dual codes

Let $\mathbb{F} = \mathbb{Z}/2$.

Definition

- *A linear code C over $\mathbb{F}$ of length n is a linear subspace of $\mathbb{F}^n$.*

Binary Self-dual codes

Let $\mathbb{F} = \mathbb{Z}/2$.

Definition

- *A linear code C over $\mathbb{F}$ of length n is a linear subspace of $\mathbb{F}^n$.*
- *Hamming distance $d = min\{|c| : c \in C \setminus 0\}$.*

Binary Self-dual codes

Let $\mathbb{F} = \mathbb{Z}/2$.

Definition

- *A linear code C over $\mathbb{F}$ of length n is a linear subspace of $\mathbb{F}^n$.*
- *Hamming distance $d = min\{|c| : c \in C \setminus 0\}$.*
- *A linear code with type $[n, k, d]$ means it has length n, dimension k, and Hamming distance d.*

Binary Self-dual codes

Let $\mathbb{F} = \mathbb{Z}/2$.

Definition

- *A linear code C over $\mathbb{F}$ of length n is a linear subspace of $\mathbb{F}^n$.*
- *Hamming distance $d = min\{|c| : c \in C \setminus 0\}$.*
- *A linear code with type $[n, k, d]$ means it has length n, dimension k, and Hamming distance d.*
- *The dual of C, $C^\perp \triangleq \{u \in \mathbb{F}^n | \langle u, v\rangle = 0, \forall v \in C\}$.*

Binary Self-dual codes

Let $\mathbb{F} = \mathbb{Z}/2$.

Definition

- *A linear code C over $\mathbb{F}$ of length n is a linear subspace of $\mathbb{F}^n$.*
- *Hamming distance $d = min\{|c| : c \in C \setminus 0\}$.*
- *A linear code with type $[n, k, d]$ means it has length n, dimension k, and Hamming distance d.*
- *The dual of C, $C^\perp \triangleq \{u \in \mathbb{F}^n | \langle u, v\rangle = 0, \forall v \in C\}$.*
- *C is said to be self-dual, if $C^\perp = C$.*

Binary Self-dual codes

Let $\mathbb{F} = \mathbb{Z}/2$.

Definition

- *A linear code C over $\mathbb{F}$ of length n is a linear subspace of $\mathbb{F}^n$.*
- *Hamming distance $d = min\{|c| : c \in C \setminus 0\}$.*
- *A linear code with type $[n, k, d]$ means it has length n, dimension k, and Hamming distance d.*
- *The dual of C, $C^\perp \triangleq \{u \in \mathbb{F}^n | \langle u, v\rangle = 0, \forall v \in C\}$.*
- *C is said to be self-dual, if $C^\perp = C$.*

Remark

$[n, k, d]$ is self-dual, then n must be even, and $k = n/2$.

example

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

gives a generation matrix of a self-dual code of type [8,4,4].

Examples of self-dual codes: Golay code[24,12,8]

$$B = \begin{pmatrix} 110111000101 \\ 101110001011 \\ 011100010111 \\ 111000101101 \\ 110001011011 \\ 100010110111 \\ 000101101111 \\ 001011011101 \\ 010110111001 \\ 101101110001 \\ 011011100011 \\ 111111111110 \end{pmatrix}_{12\times 12}$$

$\begin{pmatrix} B \\ I \end{pmatrix}$ is a generation matrix of the well known extended Golay code.

Background

Puppe and Kreck ([Puppe][KP])

$\{$Involution on 3-manifolds with isolated fixed pts$\}$
$\longleftrightarrow$ $\{$self-dual codes$\}$

Background

Puppe and Kreck ([Puppe][KP])

{Involution on 3-manifolds with isolated fixed pts}
$\longleftrightarrow$ {self-dual codes}

- In case of dim=3, the equvi. cohomology are one-to-one corresponding to binary self-dual codes.[KP]

Background

Puppe and Kreck ([Puppe][KP])

{Involution on 3-manifolds with isolated fixed pts}
$\longleftrightarrow$ {self-dual codes}

- In case of dim=3, the equvi. cohomology are one-to-one corresponding to binary self-dual codes.[KP]
- For higher dimension case, only the odd dimension case gives self-dual codes.[Puppe][CL]

Background

Puppe and Kreck ([Puppe][KP])

{Involution on 3-manifolds with isolated fixed pts}
$\longleftrightarrow$ {self-dual codes}

- In case of dim=3, the equvi. cohomology are one-to-one corresponding to binary self-dual codes.[KP]
- For higher dimension case, only the odd dimension case gives self-dual codes.[Puppe][CL]
- $H^{[\frac{n}{2}]}_{\mathbb{Z}_2}(M^n)$ becomes a self-dual code.

Background

Puppe and Kreck ([Puppe][KP])

{Involution on 3-manifolds with isolated fixed pts}
$\longleftrightarrow$ {self-dual codes}

- In case of dim=3, the equvi. cohomology are one-to-one corresponding to binary self-dual codes.[KP]
- For higher dimension case, only the odd dimension case gives self-dual codes.[Puppe][CL]
- $H_{\mathbb{Z}_2}^{[\frac{n}{2}]}(M^n)$ becomes a self-dual code.
- [CL] gives a lower bound for number of self-dual codes.

Motivation

What can we do on the categary of small covers?

Motivation

What can we do on the categary of small covers?

- Does there exist a subgroup($\cong \mathbb{Z}_2$) action of a small cover, such that it fixed isolated points?

Motivation

What can we do on the categary of small covers?

- Does there exist a subgroup($\cong \mathbb{Z}_2$) action of a small cover, such that it fixed isolated points?
- If YES, How to compute the self-dual code, espcially by using the combinatoric of the polytope?

small cover with sub involution

Lemma

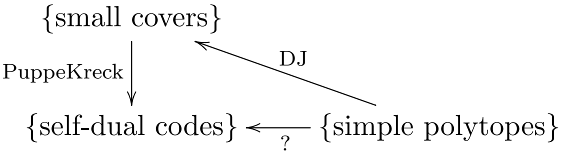
Let $\pi : M^n \to P^n$ be a small cover. Then there exists a generator $\beta \in (\mathbb{Z}_2)^n$ so that $M^{<\beta>}$ is isolated $\Longleftrightarrow$ λ_{M^n} is an n-coloring.

small cover with sub involution

Lemma

Let $\pi : M^n \to P^n$ be a small cover. Then there exists a generator $\beta \in (\mathbb{Z}_2)^n$ so that $M^{<\beta>}$ is isolated $\Longleftrightarrow$ λ_{M^n} is an n-coloring.

Furthermore $M^{<\beta>} = M^{(\mathbb{Z}_2)^n}$ and $\beta = \alpha_1 + \cdots + \alpha_n$, where $\alpha_1, \cdots, \alpha_n$ are all the colors in λ_{M^n}.


{small covers}
PuppeKreck
DJ
{self-dual codes}
?
{simple polytopes}

n-colorable simple n-polytope

Proposition

([Jos]) For any simple n-polytope P, the following statements are equivariant.

- *P can be colored by exact n colors.*

n-colorable simple n-polytope

Proposition

([Jos]) For any simple n-polytope P, the following statements are equivariant.

- *P can be colored by exact n colors.*
- *each 2-face of P has even number of vertices.*

n-colorable simple n-polytope

Proposition

([Jos]) For any simple n-polytope P, the following statements are equivariant.

- *P can be colored by exact n colors.*
- *each 2-face of P has even number of vertices.*
- *each k-face($k > 0$) of P has even number of vertices.*

n-colorable simple n-polytope

Proposition

([Jos]) For any simple n-polytope P, the following statements are equivariant.

- *P can be colored by exact n colors.*
- *each 2-face of P has even number of vertices.*
- *each k-face($k > 0$) of P has even number of vertices.*
- *each k-face can be colored by exact k colors.*

n-colorable simple n-polytope

Proposition

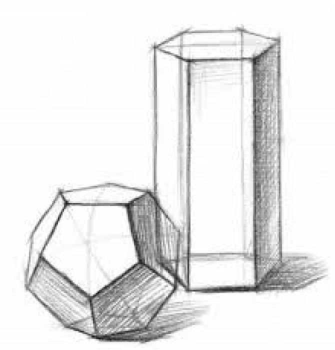
([Jos]) For any simple n-polytope P, the following statements are equivariant.

- *P can be colored by exact n colors.*
- *each 2-face of P has even number of vertices.*
- *each k-face($k > 0$) of P has even number of vertices.*
- *each k-face can be colored by exact k colors.*

Proposition

Let P^n be an n-colorable simple n-polytope.
Then $|V(P)| \geq 2^n$.
And $|V(P)| = 2^n \Leftrightarrow P = I^n$, the n-cube.

examples of n-colorable n-polytopes



compuation of self-dual codes

Let $\pi : M^n \to P^n$ be a small cover with n odd. Then $H^{[\frac{n}{2}]}_{\mathbb{Z}_2}(M)$ becomes a self-dual code.

- How to compute $H^*_{\mathbb{Z}_2}(M)$?

compuation of self-dual codes

Let $\pi : M^n \to P^n$ be a small cover with n odd. Then $H^{[\frac{n}{2}]}_{\mathbb{Z}_2}(M)$ becomes a self-dual code.

- How to compute $H^*_{\mathbb{Z}_2}(M)$?
- Is there a relation between such self-dual code and simple polytope P?

vertex-face incident vectors

Definition

For each face f of a polytope P, define a vector of face f,

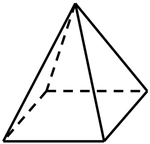
$$\zeta_f : V(P) \to \mathbb{Z}_2, p \mapsto \begin{cases} 1, & \text{if } p \in f; \\ 0, & \text{if } p \notin f. \end{cases}$$

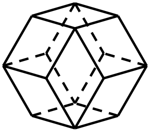
vertex-face incident vectors

Definition

For each face f of a polytope P, define a vector of face f,

$$\zeta_f : V(P) \to \mathbb{Z}_2, p \mapsto \begin{cases} 1, & \text{if } p \in f; \\ 0, & \text{if } p \notin f. \end{cases}$$





$\zeta_{f_0} = (1, 0, 1, 1, 0)$

graded Boolean ring of polytopes

Definition

$$\mathfrak{B}_k(P) \triangleq \begin{cases} span\{\zeta_f \mid f \text{ is a codim-}k \text{ face of } P\}, & if\ k \le n; \\ \mathcal{V}^* = Map(V(P), \mathbb{Z}_2) \cong \mathbb{Z}_2^s, & if\ k > n. \end{cases}$$

graded Boolean ring of polytopes

Definition

$$\mathfrak{B}_k(P) \triangleq \begin{cases} span\{\zeta_f \mid f \text{ is a codim-}k \text{ face of } P\}, & \text{if } k \leq n; \\ \mathcal{V}^* = Map(V(P), \mathbb{Z}_2) \cong \mathbb{Z}_2^s, & \text{if } k > n. \end{cases}$$

$$\mathfrak{B}(P) \triangleq \bigoplus_{k \geq 0} \mathfrak{B}_k \, t^k.$$

graded Boolean ring of polytopes

Definition

$$\mathfrak{B}_k(P) \triangleq \begin{cases} span\{\zeta_f \mid f \text{ is a codim-}k \text{ face of } P\}, & \text{if } k \le n; \\ \mathcal{V}^* = Map(V(P), \mathbb{Z}_2) \cong \mathbb{Z}_2^s, & \text{if } k > n. \end{cases}$$

$$\mathfrak{B}(P) \triangleq \bigoplus_{k \ge 0} \mathfrak{B}_k \, t^k.$$

Proposition

P^n *is* n*-colorable* $\iff \mathfrak{B}_0 \subset \mathfrak{B}_1 \subset \cdots \subset \mathfrak{B}_n$.

graded Boolean ring of polytopes

Definition

$$\mathfrak{B}_k(P) \triangleq \begin{cases} span\{\zeta_f \mid f \text{ is a } codim\text{-}k \text{ face of } P\}, & \text{if } k \le n; \\ \mathcal{V}^* = Map(V(P), \mathbb{Z}_2) \cong \mathbb{Z}_2^s, & \text{if } k > n. \end{cases}$$

$$\mathfrak{B}(P) \triangleq \bigoplus_{k \ge 0} \mathfrak{B}_k \, t^k.$$

Proposition

P^n is n-colorable $\iff \mathfrak{B}_0 \subset \mathfrak{B}_1 \subset \cdots \subset \mathfrak{B}_n$.
In this case, $\dim \mathfrak{B}_1(P) = m - n + 1$.

equivariant cohomology

Theorem

$$i^*(H^*_{\mathbb{Z}_2}(M)) = \mathfrak{B}(P),$$

where $i : M^{\mathbb{Z}_2} \hookrightarrow M$.

equivariant cohomology

Theorem

$$i^*(H^*_{\mathbb{Z}_2}(M)) = \mathfrak{B}(P),$$

where $i : M^{\mathbb{Z}_2} \hookrightarrow M$.

$$\begin{array}{ccc}
\mathbb{Z}_2(P) \cong H^*_{\mathbb{Z}_2^n}(M) & \xrightarrow{\phi^*} & H^*_{\mathbb{Z}_2}(M) \\
\downarrow i^* & \searrow g & \downarrow i^* \\
\bigoplus_{p\in V} \mathbb{Z}_2[t_1, \cdots, t_n] \cong H^*_{\mathbb{Z}_2^n}(V) & \xrightarrow[\phi^*_{|_V}]{} & H^*_{\mathbb{Z}_2}(V) \cong \bigoplus_{p\in V} \mathbb{Z}_2[t]
\end{array}$$

where $V = M^{\mathbb{Z}_2} = M^{\mathbb{Z}_2^n}$.

Theorem

For any n-colorable simple polytope P^n with n odd, there is a self-dual code

$$W = \mathfrak{B}_{[\frac{n}{2}]}(P) = span\{\zeta_f | f \text{ is a } \frac{n+1}{2}\text{-face of } P\}.$$

Self-dual codes risen from simple polytopes

Theorem

For any n-colorable simple polytope P^n with n odd, there is a self-dual code

$$W = \mathfrak{B}_{[\frac{n}{2}]}(P) = span\{\zeta_f | f \text{ is a } \frac{n+1}{2}\text{-face of } P\}.$$

Remark

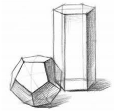
For the case $n = 3$, a basis of the self-dual code W risen from P^3 can be written down quickly:

$$\{\zeta_f | f \in \mathcal{F}(P^3) \setminus \{f_1, f_2\}\}$$

where f_1 and f_2 are any two faces with a common edge.

self-dual codes [12, 6, 4] risen from 6-prim

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}_{12\times 6}$$



properties of such self-dual codes

Proposition

Let W be a self-dual code realized by an n-colorable simple n-polytope(n is odd). Let W is of type $[l, l/2, d]$. Then $l \geq 2^n$. If $n = 3$, $d = 4$.

properties of such self-dual codes

Proposition

Let W be a self-dual code realized by an n-colorable simple n-polytope(n is odd). Let W is of type $[l, l/2, d]$. Then $l \geq 2^n$. If $n = 3$, $d = 4$.

Remark

Different polytopes may give same self-dual code. Take the connected sum of two 6-prim.

Corollary

Extended Golay code can not be realized by such a polytope.

Corollary

Extended Golay code can not be realized by such a polytope.

Proof.

Extended Golay code is of [24,12,8]. Suppose that it can be realized by an n-colorable simple n-polytope, then $24 \geq 2^n$, $n = 3$. In this case, the hamming distance $= 4$. Contradiction. □

Further questions

- Conjecture: $d = \min\{\zeta_f | f \text{is a } \frac{n+1}{2}\text{-face of } P\} \geq 2^{\frac{n+1}{2}}$, for any self-dual code W risen from P^n.

Further questions

- Conjecture: $d = \min\{\zeta_f | f \text{is a } \frac{n+1}{2}\text{-face of } P\} \geq 2^{\frac{n+1}{2}}$, for any self-dual code W risen from P^n.
- Inverse problem, i.e, which kind of self-dual code can be realized by such a simple polytope? How?

Reference

C. Allday, V. Puppe, *Cohomological methods in transformation groups*. In: Cambridge Studies in Advanced Mathematics, vol. 32. Cambridge University Press, London (1993).

B. Chen, Z. Lü, *Equivariant cohomology and analytic descriptions of ring isomorphisms*, Math. Z. 261 (2009), No. 4, 891–908.

M. Joswig, *Projectivities in simplicial complexes and colorings of simple polytopes*, Math. Z. 240 (2002), no. 2, 243–259.

M. Kreck and V. Puppe, *Involutions on 3-manifolds and self-dual, binary codes*, Homology, Homotopy Appl. 10 (2008), no. **2**, 139–148.

V. Puppe, *Group actions and codes*. Can. J. Math. l53, 212–224 (2001).

proof

$$
\begin{array}{ccc}
\mathbb{Z}_2(P) \cong H^*_{\mathbb{Z}_2^n}(M) & \xrightarrow{\phi^*} & H^*_{\mathbb{Z}_2}(M) \\
\downarrow i^* & \searrow g & \downarrow i^* \\
\bigoplus_{p\in V} \mathbb{Z}_2[t_1, \cdots, t_n] \cong H^*_{\mathbb{Z}_2^n}(V) & \xrightarrow[\phi^*_{|_V}]{} & H^*_{\mathbb{Z}_2}(V) \cong \bigoplus_{p\in V} \mathbb{Z}_2[t]
\end{array}
$$

proof

$$\begin{array}{ccc}
\mathbb{Z}_2(P) \cong H^*_{\mathbb{Z}_2^n}(M) & \xrightarrow{\phi^*} & H^*_{\mathbb{Z}_2}(M) \\
\Big\downarrow i^* & \searrow g & \Big\downarrow i^* \\
\bigoplus_{p\in V} \mathbb{Z}_2[t_1,\cdots,t_n] \cong H^*_{\mathbb{Z}_2^n}(V) & \xrightarrow[\phi^*_{|_V}]{} & H^*_{\mathbb{Z}_2}(V) \cong \bigoplus_{p\in V} \mathbb{Z}_2[t]
\end{array}$$

- $\phi^*_{|_V}(t_i) = t.$

proof

$$\begin{array}{ccc} \mathbb{Z}_2(P)\cong H^*_{\mathbb{Z}_2^n}(M) & \xrightarrow{\phi^*} & H^*_{\mathbb{Z}_2}(M) \\ \downarrow i^* & \searrow g & \downarrow i^* \\ \bigoplus_{p\in V}\mathbb{Z}_2[t_1,\cdots,t_n]\cong H^*_{\mathbb{Z}_2^n}(V) & \xrightarrow[\phi^*_{|V}]{} & H^*_{\mathbb{Z}_2}(V)\cong\bigoplus_{p\in V}\mathbb{Z}_2[t] \end{array}$$

- $\phi^*_{|V}(t_i) = t$.
- Suppose a facet F is colored by α_{i_0}. Then $i^*(a_F) = t_{i_0}\zeta_F$

proof

$$\begin{array}{ccc}
\mathbb{Z}_2(P) \cong H^*_{\mathbb{Z}_2^n}(M) & \xrightarrow{\quad \phi^* \quad} & H^*_{\mathbb{Z}_2}(M) \\
\downarrow i^* & \searrow g & \downarrow i^* \\
\bigoplus_{p\in V} \mathbb{Z}_2[t_1,\cdots,t_n] \cong H^*_{\mathbb{Z}_2^n}(V) & \xrightarrow[\phi^*_{|_V}]{} & H^*_{\mathbb{Z}_2}(V) \cong \bigoplus_{p\in V} \mathbb{Z}_2[t]
\end{array}$$

- $\phi^*_{|_V}(t_i) = t$.
- Suppose a facet F is colored by α_{i_0}. Then $i^*(a_F) = t_{i_0}\zeta_F$
- $g(a_F) = t\zeta_F$,

proof

$$\begin{array}{ccc}
\mathbb{Z}_2(P) \cong H^*_{\mathbb{Z}_2^n}(M) & \xrightarrow{\phi^*} & H^*_{\mathbb{Z}_2}(M) \\
\downarrow i^* & \searrow g & \downarrow i^* \\
\bigoplus_{p\in V} \mathbb{Z}_2[t_1,\cdots,t_n] \cong H^*_{\mathbb{Z}_2^n}(V) & \xrightarrow[\phi^*_{|V}]{} & H^*_{\mathbb{Z}_2}(V) \cong \bigoplus_{p\in V} \mathbb{Z}_2[t]
\end{array}$$

- $\phi^*_{|V}(t_i) = t$.
- Suppose a facet F is colored by α_{i_0}. Then $i^*(a_F) = t_{i_0}\zeta_F$
- $g(a_F) = t\zeta_F$,$g(H^1_{\mathbb{Z}_2^n}(M)) = \mathfrak{B}_1(P)$.

proof

$$\begin{array}{ccc}
\mathbb{Z}_2(P) \cong H^*_{\mathbb{Z}_2^n}(M) & \xrightarrow{\phi^*} & H^*_{\mathbb{Z}_2}(M) \\
\downarrow i^* & \searrow g & \downarrow i^* \\
\bigoplus_{p\in V} \mathbb{Z}_2[t_1,\cdots,t_n] \cong H^*_{\mathbb{Z}_2^n}(V) & \xrightarrow[\phi^*_{|V}]{} & H^*_{\mathbb{Z}_2}(V) \cong \bigoplus_{p\in V} \mathbb{Z}_2[t]
\end{array}$$

- $\phi^*_{|V}(t_i) = t$.
- Suppose a facet F is colored by α_{i_0}. Then $i^*(a_F) = t_{i_0}\zeta_F$
- $g(a_F) = t\zeta_F$,$g(H^1_{\mathbb{Z}_2^n}(M)) = \mathfrak{B}_1(P)$.
- dim $H^1_{\mathbb{Z}_2}(M) = m - n + 1 =$dim $g(H^1_{\mathbb{Z}_2^n}(M))$.

proof

$$\begin{array}{ccc}
\mathbb{Z}_2(P) \cong H^*_{\mathbb{Z}_2^n}(M) & \xrightarrow{\phi^*} & H^*_{\mathbb{Z}_2}(M) \\
\downarrow i^* & \searrow g & \downarrow i^* \\
\bigoplus_{p\in V} \mathbb{Z}_2[t_1,\cdots,t_n] \cong H^*_{\mathbb{Z}_2^n}(V) & \xrightarrow[\phi^*_{|_V}]{} & H^*_{\mathbb{Z}_2}(V) \cong \bigoplus_{p\in V} \mathbb{Z}_2[t]
\end{array}$$

- $\phi^*_{|_V}(t_i) = t$.
- Suppose a facet F is colored by α_{i_0}. Then $i^*(a_F) = t_{i_0}\zeta_F$
- $g(a_F) = t\zeta_F$,$g(H^1_{\mathbb{Z}_2^n}(M)) = \mathfrak{B}_1(P)$.
- dim $H^1_{\mathbb{Z}_2}(M) = m - n + 1 =$dim $g(H^1_{\mathbb{Z}_2^n}(M))$.
- i^* are injective.

proof

$$\begin{array}{ccc} \mathbb{Z}_2(P)\cong H^*_{\mathbb{Z}_2^n}(M) & \xrightarrow{\phi^*} & H^*_{\mathbb{Z}_2}(M) \\ \downarrow i^* & \searrow g & \downarrow i^* \\ \bigoplus_{p\in V}\mathbb{Z}_2[t_1,\cdots,t_n]\cong H^*_{\mathbb{Z}_2^n}(V) & \xrightarrow[\phi^*_{|V}]{} & H^*_{\mathbb{Z}_2}(V)\cong\bigoplus_{p\in V}\mathbb{Z}_2[t] \end{array}$$

- $\phi^*_{|V}(t_i) = t$.
- Suppose a facet F is colored by α_{i_0}. Then $i^*(a_F) = t_{i_0}\zeta_F$
- $g(a_F) = t\zeta_F$,$g(H^1_{\mathbb{Z}_2^n}(M)) = \mathfrak{B}_1(P)$.
- dim $H^1_{\mathbb{Z}_2}(M) = m - n + 1 =$dim $g(H^1_{\mathbb{Z}_2^n}(M))$.
- i^* are injective.
- Both are generated by degree one elements.