Geometric representations of linear codes

Pavel Rytíř

Department of Applied Mathematics
Charles University in Prague
Advisor: Martin Loebl

November 22, 2011
Discrete Math Seminar - Simon Fraser University

Linear code

Linear code $\mathcal{C}$ of length n and dimension d over field $\mathbb{F}$

- Linear subspace of dimension d of vector space $\mathbb{F}^n$
- $W_{\mathcal{C}}(x) := \sum_{c \in \mathcal{C}} x^{w(c)}$, $w(c)$ number of non-zero entries

Puncturing $\mathcal{C}$ along S

- $S \subseteq \{1, \ldots, n\}$, $\mathcal{C}/S = \{(c_i | i \notin S)_{i=1}^{n} | c \in \mathcal{C}\}$
- The puncturing $\mathcal{C}$ along S means deleting the entries indexed by S from $\mathcal{C}$.
- $\mathcal{C}/\{1\} = \{(c_2, c_3, \ldots, c_n) | (c_1, c_2, \ldots, c_n) \in \mathcal{C}\}$

Motivation

Incidence matrix $A = (A_{ij})$ of graph G

$$A_{ij} := \begin{cases} 1 & \text{if vertex } v_i \text{ belongs to edge } e_j, \\ 0 & \text{otherwise.} \end{cases}$$

$$\begin{array}{cc} & e_j \\ v_i & \begin{pmatrix} \quad & & \quad \\ & 1 & \\ & & \end{pmatrix} \end{array}$$

- The cycle space $\mathcal{C}$ of a graph G is the kernel of A over $GF(2)$.
- Graph G embedded as one dimensional simplicial complex in $\mathbb{R}^3$ may be considered as geometric representation of $\mathcal{C}$.
- **It is useful**: For graph G of fixed genus, there exists a polynomial algorithm for computation of $W_{\mathcal{C}}(x)$ by Galluccio and Loebl. This algorithm uses geometric properties of G namely embedding on closed Riemann surfaces.

2D simplicial complexes

- Are there geometric representation of linear codes that are not cycle spaces of graphs?

2D simplicial complexes

- Are there geometric representation of linear codes that are not cycle spaces of graphs?
- My representations will be two dimensional simplicial complexes.

2D simplicial complex Δ

- $\Delta = \{\text{vertices}, \text{edges}, \text{triangles}\}$
- Every face of a simplex from Δ belongs to Δ
- Intersection of every two simplices of Δ is a face of both

2D simplicial complexes

Incidence matrix $A = (A_{ij})$ of Δ

$$A_{ij} := \begin{cases} 1 & \text{if edge } e_i \text{ belongs to triangle } t_j, \\ 0 & \text{otherwise.} \end{cases}$$

$$\begin{array}{cc} & t_j \\ e_i & \begin{pmatrix} \quad & \quad & \quad \\ & 1 & \\ & & \end{pmatrix} \end{array}$$

Cycle space $\ker \Delta$ of Δ over $\mathbb{F}$

- $\ker \Delta = \{x | A_\Delta x = 0\}$

Linear code $\mathcal{C}$ is triangular representable if:

- There exists a triangular configuration Δ s. t. $\mathcal{C} = \ker \Delta / S$ for some set S
- There is a bijection between $\mathcal{C}$ and $\ker \Delta$

Linear code $\mathcal{C}$ is triangular representable if:

- There exists a triangular configuration Δ s. t. $\mathcal{C} = \ker \Delta / S$ for some set S
- There is a bijection between $\mathcal{C}$ and $\ker \Delta$

Do we need two dimensional simplicial complexes?

Lets try $\mathcal{C}$ is graphic representable if:

- There exists a graph G s. t. $\mathcal{C} = \ker G / S$ for some set S
- The class of linear codes that are cycle spaces of graphs is closed under operation of puncturing.
- If $\mathcal{C}$ is not cycle space of a graph, there is no such graph G

My results

Theorem

Let $\mathcal{C}$ be a linear code over rationals or over $GF(p)$, where p is a prime. Then $\mathcal{C}$ is triangular representable.

Theorem

If $\mathcal{C}$ is over $GF(p)$, where p is a prime, then there exists a triangular representation Δ such that: if $\sum_{i=0}^{m} a_i x^i$ is the weight enumerator of $\ker \Delta$ then

$$W_{\mathcal{C}}(x) = \sum_{i=0}^{m} a_i x^{(i \bmod e)},$$

where $e = (\text{number of punctured coordinates}) / \dim \mathcal{C}$.

My results

Theorem

Let $\mathbb{F}$ be a field different from rationals and $GF(p)$, where p is a prime. Then there exists a linear code over $\mathbb{F}$ that is not triangular representable.

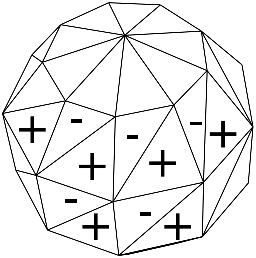
Work in progress

My work immediately raises the following questions:

- Which binary codes can be represented by 2D simplicial complex embeddable into $\mathbb{R}^3$? (every 2D complex can be embedded into $\mathbb{R}^5$)
- Relation with permanents and determinants of 3D matrices (tensors).
- Application of the geometric representations to the Ising problem.

A trivial one dimensional code

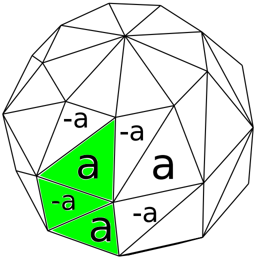
The most trivial case is a code generated by a vector that contains only entries $a, -a$. $\mathcal{C} = \text{span}(\{(a, a, -a, \ldots, a)\})$. This code is represented by the following complex:



This is a triangulation of a 2-dimensional sphere by triangles such that there is an assignment of $+$ and $-$ to triangles such that every edge is incident with $+$ and $-$ triangle. For every k there exists such triangulation with l triangles, $l > k$.

An example of triangular representation Δ of $\mathcal{C} = \mathrm{span}(\{(a, -a, a)\})$

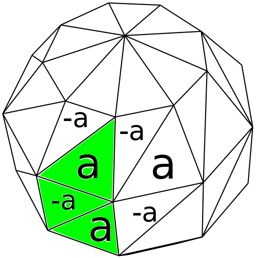
- I assign to $+$ triangles value a and to $-$ triangles value $-a$.
- Equation given by the row of the incidence matrix indexed by any edge e has form $a - a = 0$.



- $\mathcal{C} = \ker \Delta / \{$ non-green triangles $\}$
- $\dim \mathcal{C} = \dim \ker \Delta = 1$

An example of triangular representation Δ of $\mathcal{C} = \text{span}(\{(a, -a, a)\})$

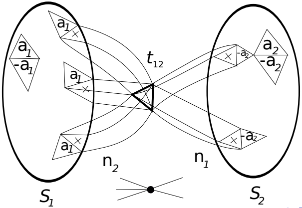
- Let p be the field characteristic. The weight enumerator of $\ker \Delta$ equals $W_\Delta(x) = 1 + (p-1)x^k$, k is the number of triangles of Δ.



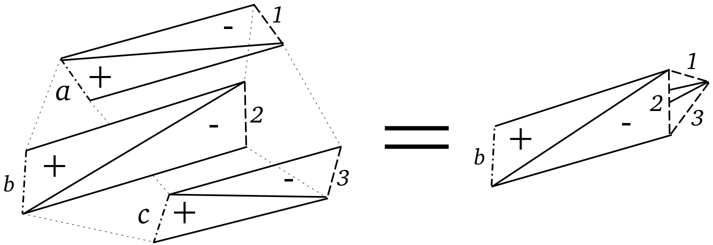
- $W_{\mathcal{C}}(x) = 1 + (p-1)x^{(k \bmod (k-3))} = 1 + (p-1)x^3$

Representation Δ of a code $\mathcal{C}$ over primefield generated by a vector of form $(a_1, a_2, -a_1, -a_2, \dots)$

- Here I need that the field is a primefield. I use that the additive group of every primefield is cyclic.
- $\mathcal{C}$ is generated by a vector that contains only four different elements $a_1, a_2, -a_1, -a_2$. $a_1 = n_1 \times g$ and $a_2 = n_2 \times g$ for some generator g of the cyclic group.
- Such a code can be represented by two triangular spheres interconnected by tunnels.

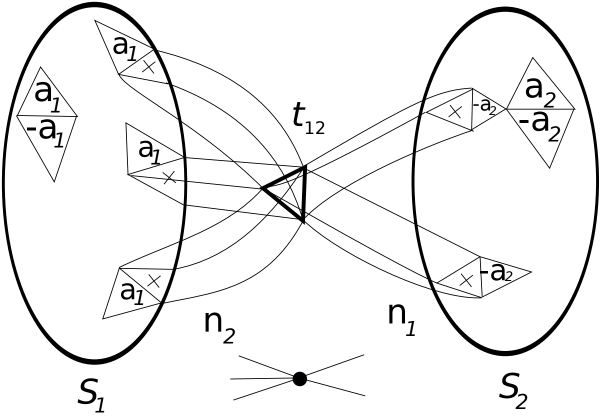


Triangular tunnel

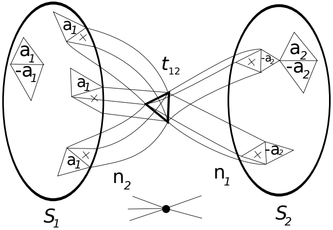


Representation Δ of $\mathcal{C} = \text{span}(\{(a_1, a_2, -a_1, -a_2, \ldots)\})$

$a_1 = n_1 \times g$, $a_2 = n_2 \times g$, g generator of the additive group

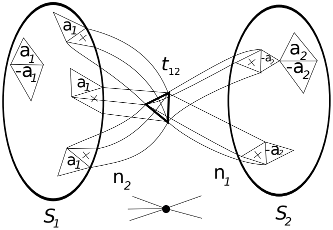


Representation Δ of $\mathcal{C} = \text{span}(\{(a_1, a_2, -a_1, -a_2, \ldots)\})$



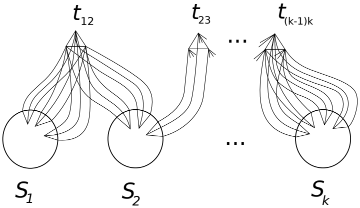
- The equation indexed by the edges different from the middle empty triangle are $a_1 - a_1 = 0$ or $a_1 - a_1 = 0$.
- The equation indexed by the edges of the middle empty triangle are
  $n_2 \times a_1 - n_1 \times a_2 = n_2 \times (n_1 \times g) - n_1 \times (n_2 \times g) = 0$.
- So the generating vector belongs to $\ker \Delta$

Representation Δ of $\mathcal{C} = \mathrm{span}(\{(a_1, a_2, -a_1, -a_2, \dots)\})$



- The equations $a_1 = x$ and $a_2 = x$ have obviously unique solutions a_1 and a_2, respectively.
- The equation $n_2 \times a_1 = n_1 \times x$ has unique solution a_2, since the additive group has a prime or an infinite order.
- Therefore $\dim \ker \Delta = \dim \mathcal{C} = 1$.

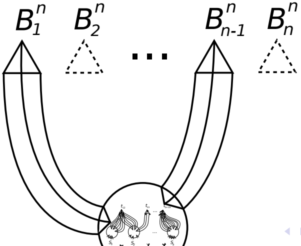
Representation Δ of a code C over primefield generated by a vector of form $(a_1, a_2, \ldots, a_k, -a_1, \ldots)$



- This code can be represented by k triangular spheres interconnected by tunnels analogously as in the previous case.
- I supposed that all $a_i \neq 0$. If the generator of the code contains zeros, I add to the representation one isolated triangle for each zero entry.
- I can represent all one dimensional codes over primefields.

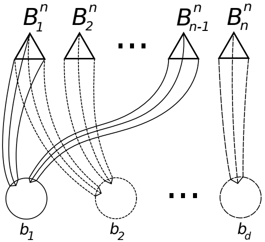
More dimensional codes

- Let $\mathcal{C}$ be a code over a primefield and let $B = \{b_1, \ldots, b_d\}$ be a basis of $\mathcal{C}$.
- For every b_i I construct a representation Δ_{b_i} that represents the code span$(\{b_i\})$, as in the previous steps.
- Let $B^n = \{B_1^n, \ldots, B_n^n\}$ be the triangles of Δ_{b_i} that correspond to the entries of b_i.
  span$(\{b_i\}) = \ker \Delta_{b_i}/(\text{non-}B^n \text{ triangles})$.
- I deform every Δ_{b_i} so that the triangles B^n are in this position.



More dimensional codes

The representation of $\mathcal{C}$ with respect to B is $\Delta_B^{\mathcal{C}} = \cup_{i=1}^{d} \Delta_{b_i}$.



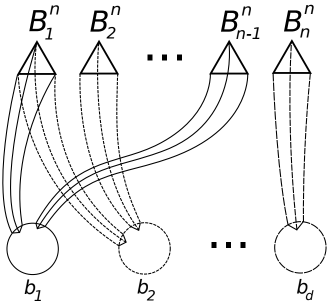
The solutions of equations indexd by edges of B^n triangles are all linear combinations of solutions of each part Δ_{b_i}, $i = 1, \ldots, d$.

Theorem

- $\ker \Delta_B^{\mathcal{C}} / (\text{non-}B^n \text{ triangles}) = \mathcal{C}$
- $\dim \ker \Delta_B^{\mathcal{C}} = \dim \mathcal{C}$

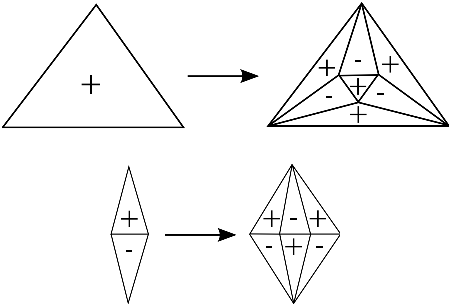
Weight enumerator, balanced representations

I can make the representation such that $|\Delta_{b_i}| - w(b_i) = e$ for all $i = 1, \ldots, d$ and e is greater than the length of $\mathcal{C}$.
Such representation is called balanced.

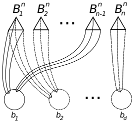


Balanced representation exists

I can apply the following subdivisions, the first increase the number of triangles by 6 and the second by 4.

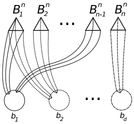


Weight enumerator, balanced representations



- Let $\mathcal{C}$ be a code and $\Delta_B^{\mathcal{C}}$ be its balanced representation with respect to a basis B
- Let $c = \sum_{b \in B} \alpha_b b$. I define a mapping $f : \mathcal{C} \mapsto \ker \Delta_B^{\mathcal{C}}$ as $f(c) := \sum_{b \in B} \alpha_b \Delta_b$
- Combination degree of c is the number of non-zero α_b's $(deg(c))$
- Let $b \in B$, then $w(f(b)) = w(b) + e$
- Let $c \in \mathcal{C}$, then $w(f(c)) = w(c) + deg(c)e$
- $w(f(c)) \bmod e = (w(c) + deg(c)e) \bmod e = w(c)$
- Note that, $w(c) < e$ for every c

Weight enumerator, balanced representations



if $\sum_{i=0}^{m} a_i x^i$ is the weight enumerator of $\Delta_B^{\mathcal{C}}$ then

$$W_{\mathcal{C}}(x) = \sum_{i=0}^{m} a_i x^{(i \bmod e)},$$

where $e = (\text{number of non-}B^n \text{ triangles}) / \dim \mathcal{C}$

My results

Theorem

Let $\mathbb{F}$ be a field different from rationals and $GF(p)$, where p is a prime. Then there exists a linear code over $\mathbb{F}$ that is not triangular representable.

Non-representable code

- Let $GF(4) = \{0, 1, x, 1 + x\}$.
- The linear code over $GF(4)$ generated by vector $(1, x)$ is not triangular representable.
- By an algebraic argument there is no $0, 1$ matrix with the dimension of kernel equals one and having a vector of form $(1, x, *, *, \ldots, *)$ in the kernel.

Thank you for your attention