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

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

Puncturing $C$ along $S$

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

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

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

- The cycle space $\mathcal{C}$ of a graph $G$ is the kernel of $A$ over $\mathbb{GF}(2)$.
- 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 $\Delta$

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

Background

2D simplicial complexes

Incidence matrix $A = (A_{ij})$ of $\Delta$

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

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

$$\ker \Delta = \{ x | A_\Delta x = 0 \}$$
Linear code $C$ is triangular representable if:

- There exists a triangular configuration $\Delta$ s. t. $C = \ker \Delta / S$ for some set $S$
- There is a bijection between $C$ and $\ker \Delta$
Linear code $C$ is triangular representable if:

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

Do we need two dimensional simplicial complexes?

Lets try $C$ is graphic representable if:

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

My results

Theorem

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

Theorem

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

$$W_C(x) = \sum_{i=0}^{m} a_i x^{i \mod e},$$

where $e = \frac{\text{(number of punctured coordinates)}}{\dim C}$. 
**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.
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 $a, -a$. $C = \text{span}(\{(a, a, -a, \ldots, a)\})$. 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 $\Delta$ of $C = \text{span}(\{(a, -a, a)\})$

- 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 $a - a = 0$.

$C = \ker \Delta/\{ \text{non-green triangles} \}$

$\text{dim } C = \text{dim } \ker \Delta = 1$
An example of triangular representation $\Delta$ of $C = \text{span}((a, -a, a))$

- 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 $\Delta$.

\[
W_C(x) = 1 + (p - 1)x^{(k \mod (k - 3))} = 1 + (p - 1)x^3
\]
Representation $\Delta$ of a code $C$ over prime field generated by a vector of form $(a_1, a_2, -a_1, -a_2, \ldots)$

- Here I need that the field is a prime field. I use that the additive group of every prime field is cyclic.
- $C$ 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 $\Delta$ of $\mathcal{C} = \text{span}(\{(a_1, a_2, -a_1, -a_2, \ldots)\})$

\[ a_1 = n_1 \times g, \quad a_2 = n_2 \times g, \quad g \text{ generator of the additive group} \]
Representation $\Delta$ of $C = \text{span}(\{(a_1, a_2, -a_1, -a_2, \ldots)\})$

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

- 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 $\dim \ker \Delta = \dim C = 1$. 
Representation $\Delta$ of a code $\mathcal{C}$ 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.
Let $C$ be a code over a primefield and let $B = \{b_1, \ldots, b_d\}$ be a basis of $C$.

For every $b_i$, I construct a representation $\Delta_{b_i}$ that represents the code $\text{span}(\{b_i\})$, as in the previous steps.

Let $B^n = \{B^n_1, \ldots, B^n_n\}$ be the triangles of $\Delta_{b_i}$ that correspond to the entries of $b_i$.

$\text{span}(\{b_i\}) = \ker \Delta_{b_i} / (\text{non-}B^n\text{ triangles})$.

I deform every $\Delta_{b_i}$ so that the triangles $B^n$ are in this position.
More dimensional codes

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

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

Theorem

- $\ker \Delta_B^C / (\text{non-}B^n \text{ triangles}) = \mathcal{C}$
- $\dim \ker \Delta_B^C = \dim \mathcal{C}$
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 $C$. 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.
Let $C$ be a code and $\Delta^C_B$ be its balanced representation with respect to a basis $B$.

Let $c = \sum_{b \in B} \alpha_b b$. Define a mapping $f : C \mapsto \ker \Delta^C_B$ as $f(c) := \sum_{b \in B} \alpha_b \Delta_b$.

Combination degree of $c$ is the number of non-zero $\alpha_b$'s ($\deg(c)$).

Let $b \in B$, then $w(f(b)) = w(b) + e$.

Let $c \in C$, then $w(f(c)) = w(c) + \deg(c)e$.

$w(f(c)) \mod e = (w(c) + \deg(c)e) \mod e = w(c)$.

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 $\Delta_C^B$ then

$$W_C(x) = \sum_{i=0}^{m} a_i x^{(i \mod e)},$$

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