Linear Codes from the Axiomatic Viewpoint

Jay A. Wood

Department of Mathematics
Western Michigan University
http://homepages.wmich.edu/∼jwood/

Noncommutative rings and their applications, IV
University of Artois, Lens
June 11, 2015

“And now for something completely different.”
—John Cleese (1969)

8. Simplicial complexes coming from linear codes

- Paper by T. Johnsen and H. Verdure (2014).
- Simplicial complexes, Stanley-Reisner rings.
- Alexander dual.
- Parity check matrix or generator matrix?
- Poset of subspaces of $M^\sharp$.
- Possible resolution of Stanley-Reisner ring.
- Good case: one-weight code.
- Examples.
- Effect of puncturing.
- Effect of higher multiplicities.

Setting for this lecture

- Linear codes over a finite field, $\mathbb{F}_2$ in examples.
- Motivated by "Stanley-Reisner resolution of constant weight linear codes," by T. Johnsen and H. Verdure, Des. Codes Cryptogr. (2014), 72: 471–481.
- This is work in progress.

Simplicial complexes

- Let E be a finite set, say $E = \{1, 2, \ldots, n\}$.
- An abstract **simplicial complex** Δ is a collection of subsets of E that is closed under taking subsets. I.e., if $\sigma \in \Delta$ and $\tau \subseteq \sigma$, then $\tau \in \Delta$.
- Elements of Δ are called **faces**, and maximal faces (under inclusion) are called **facets**.

Polynomial ring

- Let k be any field, $E = \{1, 2, \ldots, n\}$.
- Polynomial ring $S = k[x_1, \ldots, x_n]$.
- Notation: for $\sigma \subseteq E$, write $x^\sigma = \prod_{i \in \sigma} x_i$. ($x^\emptyset = 1$.)
- Fine grading: S is $\mathbb{N}^n$-graded by exponents.
- Coarse grading: S is $\mathbb{N}$-graded by total degree.
- Can then have finely-graded or coarsely-graded modules over S.

Stanley-Reisner ring

- Given a simplicial complex Δ, the **Stanley-Reisner ideal** $I_\Delta \subseteq S$ is generated by $\{x^\sigma : \sigma \notin \Delta\}$.
- The **Stanley-Reisner ring** is $R_\Delta = S/I_\Delta$.
- One goal: determine minimal free resolution of R_Δ as a finely- or coarsely-graded S-module.
- Field of "combinatorial commutative algebra."

Alexander dual

- Complement: if $\sigma \subseteq E$, define $\bar{\sigma} = E \setminus \sigma$.
- Given a simplicial complex Δ, define its **Alexander dual**:
$$\Delta^{\vee} = \{\bar{\sigma} : \sigma \notin \Delta\}.$$
- If $D_\Delta = \{\bar{\sigma} : \sigma \in \Delta\}$, then $\Delta^{\vee} = \{\tau : \tau \notin D_\Delta\}$.
- Also, $D_{\Delta^{\vee}} = \{\bar{\tau} : \tau \in \Delta^{\vee}\} = \{\sigma : \sigma \notin \Delta\}$, which provides the exponents for generators of I_Δ.

Simplicial complex from parity check matrix

- Suppose a linear code $C \subseteq \mathbb{F}_q^n$ is given by a parity check matrix H. If $\dim C = m$, then H is an $(n-m) \times n$ matrix, and $c \in C$ if and only if $Hc^T = 0$.
- Let $E = \{1, 2, \ldots, n\}$, thought of as the position numbers of the columns of H.
- Define $\Delta_H = \{\sigma \subseteq E :$ $\sigma\text{-columns of } H \text{ are linearly independent}\}$.
- In fact, Δ_H is a matroid.

Using generator matrix instead

- If C has generator matrix G, then G has size $m \times n$. The columns of G represent coordinate functionals $\lambda_i \in M^\sharp = \mathrm{Hom}_{\mathbb{F}_q}(M, \mathbb{F}_q)$. Think C as image of $\Lambda : M \to \mathbb{F}_q^n$.
- Define $\Delta_G = \{\bar{\tau} : \tau\text{-columns of } G \text{ span } M^\sharp\}$.
- Then observe, for later use, that $\Delta_G^\vee = \{\tau : \tau\text{-columns of } G \text{ do not span } M^\sharp\}$.

Δ_G equals Δ_H

The following statements are equivalent:

- $\sigma \in \Delta_H$.
- σ-columns of H are linearly independent.
- If $c \in \mathbb{F}_q^n$ has support in σ and $Hc^T = 0$, then $c = 0$.
- If $c \in C$ has support in σ, then $c = 0$.
- If $x \in M$ has $x\lambda_i = 0$ for $i \in \bar{\sigma}$, then $x = 0$.
- $(\mathrm{Span}\{\lambda_i : i \in \bar{\sigma}\})^\circ = 0$; i.e., $\bar{\sigma}$-columns span $M^\sharp$.
- $\sigma \in \Delta_G$.

Poset of subspaces of $M^\sharp$

- Recall that the Alexander dual of Δ_G was $\Delta_G^\vee = \{\tau : \tau\text{-columns of } G \text{ do not span } M^\sharp\}$.
- If $\tau \in \Delta_G^\vee$, then what space do the τ-columns span?
- For every proper subspace $L \subseteq M^\sharp$, define

$$\tau_L = \{i : \lambda_i \in L\}.$$

- As L varies over the maximal proper subspaces of $M^\sharp$, the τ_L include all the facets of $\Delta_G^\vee$.
- Then the $\bar{\tau}_L$, L maximal, provide the exponents for the generators of I_Δ.

Example 1

- One weight code of dimension 3 over $\mathbb{F}_2$ has generator matrix

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

- There are seven 2-dimensional subspaces $L \subseteq M^\sharp$, and seven 1-dimensional subspaces. The τ_L are: $246, 145, 347, 123, 257, 167, 356$; $1, 2, 3, 4, 5, 6, 7$; and $\emptyset$.

Possible resolution of Stanley-Reisner ring

- Notation: for $\sigma \subseteq E$, write $S(-\sigma)$ for a free finely-graded S-module isomorphic to Sx^σ.
- It seems to be the case that the following is a (non-minimal) free resolution of R_{Δ_G}:

$$0 \leftarrow R_{\Delta_G} \leftarrow S \leftarrow \bigoplus_{L\,\text{codim}\,1} S(-\bar{\tau}_L) \leftarrow$$

$$\cdots \leftarrow \bigoplus_{L\,\text{codim}\,d} S(-\bar{\tau}_L)^{q^{\binom{d}{2}}} \leftarrow$$

$$\cdots \leftarrow \bigoplus_{L\,\text{codim}\,m} S(-\bar{\tau}_L)^{q^{\binom{m}{2}}} \leftarrow 0.$$

Good case: one-weight code

- Johnsen and Verdure show that the complex above is a minimal free resolution of R_{Δ_G} when C is a linear one-weight code.
- This involves a careful analysis of the subcodes of a one-weight code and the use of Hochster's formula for the Betti numbers of a minimal resolution in terms of the reduced homology of certain subcomplexes.

Example 1 again (a)

- One weight code of dimension 3 over $\mathbb{F}_2$ has generator matrix

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

- There are seven 2-dimensional subspaces $L \subseteq M^\sharp$, and seven 1-dimensional subspaces. The τ_L are: $246, 145, 347, 123, 257, 167, 356$; $1, 2, 3, 4, 5, 6, 7$; and $\emptyset$.

Example 1 (b)

- The respective $\bar{\tau}_L$ have cardinalities $4, 6, 7$, respectively.
- The data suggest, and Macaulay 2 confirms, a minimal coarse resolution:

$$0 \leftarrow R_\Delta \leftarrow S \leftarrow S(-4)^7 \leftarrow S(-6)^{14} \leftarrow S(-7)^8 \leftarrow 0.$$

Example 2 (a)

- Now consider the code of dimension 3 obtained by puncturing column 7:

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

- The τ_L are: $246, 145, 34, 123, 25, 16, 356$; $1, 2, 3, 4, 5, 6, \emptyset$; $\emptyset$. (Delete any 7 from previous listing.)

Example 2 (b)

- These data would suggest a (non-minimal) coarse resolution:

$$
\begin{aligned}
0 \leftarrow R_\Delta \leftarrow S \leftarrow S(-3)^4 \oplus S(-4)^3 \\
\leftarrow S(-5)^{12} \oplus S(-6)^2 \leftarrow S(-6)^8 \leftarrow 0.
\end{aligned}
$$

- The minimal coarse resolution from Macaulay 2:

$$
\begin{aligned}
0 \leftarrow R_\Delta \leftarrow S \leftarrow S(-3)^4 \oplus S(-4)^3 \\
\leftarrow S(-5)^{12} \leftarrow S(-6)^6 \leftarrow 0.
\end{aligned}
$$

Example 3 (a)

- This time, duplicate the last column in the one-weight code:

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

- Now the τ_L are: $246, 145, 3478, 123, 2578, 1678, 356$; $1, 2, 3, 4, 5, 6, 78$; and $\emptyset$. (Anytime there is a 7, also include an 8.)

Example 3 (c)

- These data would suggest a coarse resolution:

$$
\begin{aligned}
0 \leftarrow R_\Delta \leftarrow S \leftarrow S(-4)^3 \oplus S(-5)^4 \\
\leftarrow S(-6)^2 \oplus S(-7)^{12} \leftarrow S(-8)^8 \leftarrow 0.
\end{aligned}
$$

- This agrees with what one gets from Macaulay 2.

Effect of puncturing

- If a column is removed (punctured), say column j, then the number of columns is smaller. Call the original code C and the punctured code C'.
- Set $E' = E \setminus \{j\}$. Then $\tau'_L = \tau_L \cap E'$.
- Note that $\bar{\tau}'_L = E' \setminus \tau'_L = \bar{\tau}_L \cap E'$.
- Thus $|\bar{\tau}'_L| = |\bar{\tau}_L|$ when $j \in \tau_L$, and $|\bar{\tau}'_L| = |\bar{\tau}_L| - 1$ when $j \notin \tau_L$.
- This explains the shifts in degrees in Example 2.

Effect of higher multiplicities

- Now duplicate column j. Set $E' = E \cup \{j^*\}$.
- If $j \in \tau_L$, then $\tau'_L = \tau_L \cup \{j^*\}$. If $j \notin \tau_L$, then $\tau'_L = \tau_L$.
- Thus $|\bar{\tau}'_L| = |\bar{\tau}_L|$ when $j \in \tau_L$, and $|\bar{\tau}'_L| = |\bar{\tau}_L| + 1$ when $j \notin \tau_L$.
- This explains the shifts in degrees in Example 3.

Interpretation of coarse grading degrees

- At homological degree i, the smallest coarse grading degree is the generalized Hamming weight for C in dimension i. (Chen) That is, among the subcodes of C of dimension i, the smallest support length.
- A subcode $D \subseteq C$ is determined by its annihilator $L \subseteq M^\sharp$: codewords vanishing on τ_L belong to D. Such codewords have support contained in $\bar{\tau}_L$.

Codes over rings

- Most of the ideas presented should make sense for linear codes over rings or even over modules.
- One twist: in the proposed free resolution, the modules in homological degree i corresponded to subspaces $L \subseteq M^\sharp$ of codimension i. For codes over rings or modules, there may not be a way to assign degrees or dimensions to $L \subseteq \mathrm{Hom}_R(M, A)$.
- Perhaps there is a more general limit coming from viewing the terms in the complex as a functor on the poset of submodules of $\mathrm{Hom}_R(M, A)$.

Category of linear codes

- In 1998, Ed Assmus proposed a category of linear codes. Morphisms are defined as homomorphisms that do not increase the Hamming distance.
- Is $C \mapsto \Delta_C$ a functor from the category of linear codes to the category of simplicial complexes? If not, is there a way to fix it?

Thank you

- Thanks again to André Leroy for organizing the conference and his hospitality.
- Thank you, conference participants, for your kind attention, your questions, and your (gentle) harassment.

Thank you

- Thanks again to André Leroy for organizing the conference and his hospitality.
- Thank you, conference participants, for your kind attention, your questions, and your (gentle) harassment.
- Repeat after me: Frobenius, character, portrait, landscape, isometry.