Algebraic Coding Theory

Ramsey Rossmann

May 7, 2017

University of Puget Sound

Motivation

Goal

- Transmission across noisy channel
- Encoding and decoding schemes
- Detection vs. correction

Example

- Message: $u_1 u_2 \cdots u_k$, $u_i \in \mathbb{Z}_2$.
- Encoding: $u_1 u_1 u_1 u_1 u_2 u_2 u_2 u_2 \cdots u_k u_k u_k u_k$.
- Decoding:

$$0000 \to 0$$
$$0001 \to 0$$
$$0011 \to ?$$
$$\vdots$$

Measurements

How "good" is a code:

- How many errors are corrected?
- How many errors are detected?
- How accurate are the corrections?
- How efficient is the code?
- How easy are encoding and decoding?

Setup

- **Message**: k-bit binary string $u_0 u_1 \cdots u_k$ or vector $\mathbf{u}$.
- **Codeword**: n-bit binary string $x_0 x_1 \cdots x_n$ or vector $\mathbf{x}$.
- **Encoding function** $E : \mathbb{Z}_2^k \to \mathbb{Z}_2^n$
- **Decoding function** $D : \mathbb{Z}_2^n \to \mathbb{Z}_2^k$
- **Code** $\mathscr{C} = \mathrm{Im}(E)$. Also, the set of codewords.
- $(n, k)-$**block code**: a code that encodes messages of length k into codewords of length n.

Characteristics

- The **distance** between $\mathbf{x}$ and $\mathbf{y}$, $d(\mathbf{x}, \mathbf{y})$: number of bits in which $\mathbf{x}$ and $\mathbf{y}$ differ.
- The **minimum distance** of a code $\mathscr{C}$, $d_{\min}(\mathscr{C})$: minimum of all distances $d(\mathbf{x}, \mathbf{y})$ for all $\mathbf{x} \neq \mathbf{y}$ in $\mathscr{C}$.
- The **weight** of a codeword $\mathbf{x}$, $\mathrm{w}(\mathbf{c})$, is the number of 1s in $\mathbf{x}$.
- A code is **t-error-detecting** if, whenever there are at most t errors and at least 1 error in a codeword, the resulting word is not a codeword.
- A decoding function uses **maximum-likelihood decoding** if it decodes a received word $\mathbf{x}$ into a codeword $\mathbf{y}$ such that $d(\mathbf{x}, \mathbf{y}) \leq d(\mathbf{x}, \mathbf{z})$ for all codewords $\mathbf{z} \neq \mathbf{y}$.
- A code is **t-error-correcting** if maximum-likelihood decoding corrects all errors of size t or less.

Preliminary Results

Theorem

$d_{min}(\mathscr{C}) = \min\{w(\mathbf{x}) | \mathbf{x} \neq \mathbf{0}\}$.

Theorem

A code $\mathscr{C}$ *is exactly* t*-error-detecting if and only if* $d_{min}(\mathscr{C}) = t + 1$.

Theorem

A code $\mathscr{C}$ *is* t*-error-correcting if and only if* $d_{min}(\mathscr{C}) = 2t + 1$ *or* $2t + 2$.

Linear Codes

Consider the code $\mathscr{C}$ given by the following encoding function:

- $E : \mathbb{Z}_2^3 \to \mathbb{Z}_2^6$ given by $E\left(\begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix}\right) = \begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ u_1 + u_2 \\ u_1 + u_3 \\ u_2 + u_3 \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{bmatrix}$.
- **Parity-check bit**: $x_4 = u_1 + u_2$.
- Minimum distance: $d_{\min}(\mathscr{C}) = \min\{\mathrm{w}(\mathbf{x}) | \mathbf{x} \neq \mathbf{0}\} = 3$
  $(1, 0, 0) \mapsto (1, 0, 0, 1, 1, 0)$
  $(0, 1, 0) \mapsto (0, 1, 0, 1, 0, 1)$
  $(0, 0, 1) \mapsto (0, 0, 1, 0, 1, 1)$
- 2-error-detecting
- 1-error-correcting

Encoding

Consider the $\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$.

For some $\mathbf{u} \in \mathbb{Z}_2^3$,

$$\mathbf{Gu} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix} = \begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ u_1 + u_2 \\ u_1 + u_3 \\ u_2 + u_3 \end{bmatrix}.$$

Then, $\mathscr{C} = \{\mathbf{Gu} | \mathbf{u} \in \mathbb{Z}_2^3\}$, so $\mathbf{G}$ is the **generator matrix** for $\mathscr{C}$.

Error-detection

For the **parity-check matrix H**, consider

$$\mathbf{Hx} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{bmatrix} = \begin{bmatrix} x_1 + x_2 + x_4 \\ x_1 + x_3 + x_5 \\ x_2 + x_3 + x_6 \end{bmatrix}.$$

- If $\mathbf{Hx} = \mathbf{0}$, then no errors are detected.
- If $\mathbf{Hx} \neq \mathbf{0}$, then at least one error occurred.

Thus, $\mathscr{C} = \mathcal{N}(\mathbf{H}) \subset \mathbb{Z}_2^3$.

Definition

Let $\mathbf{H}$ be an $(n-k)\times n$ binary matrix of rank $n-k$. The null space of $\mathbf{H}$, $\mathcal{N}(\mathbf{H})\subset\mathbb{Z}_2^n$, forms a code $\mathscr{C}$ called a **linear** $(n,k)-$**code** with parity-check matrix $\mathbf{H}$.

Theorem

Linear codes are linear.

Proof.

For codeword $\mathbf{x}$ and $\mathbf{y}$, we know $\mathbf{Hx}=\mathbf{0}$ and $\mathbf{Hy}=\mathbf{0}$. Then, if $c\in\mathbb{Z}_2$,

$$\mathbf{H}(\mathbf{x}+\mathbf{y})=\mathbf{Hx}+\mathbf{Hy}=\mathbf{0}+\mathbf{0}=\mathbf{0}.$$

$$\mathbf{H}(c\mathbf{x})=c\mathbf{Hx}=c\mathbf{0}=0.$$

□

Linear Codes

Theorem

A linear code $\mathscr{C}$ is an additive group.

Proof.

For codewords $\mathbf{x}$ and $\mathbf{y}$ in $\mathscr{C}$ and parity-check matrix $\mathbf{H}$,

- $\mathbf{H0} = \mathbf{0} \Rightarrow \mathscr{C} \neq \emptyset$
- $\mathbf{H}(\mathbf{x} - \mathbf{y}) = \mathbf{Hx} - \mathbf{Hy} = \mathbf{0} - \mathbf{0} = \mathbf{0} \Rightarrow \mathbf{x} - \mathbf{y} \in \mathscr{C}$.

Thus, $\mathscr{C}$ is a subgroup of $\mathbb{Z}_2^n$. □

Coset Decoding

If we detect an error, how can we decode it?

For received $\mathbf{x}$, we know $\mathbf{x} = \mathbf{c} + \mathbf{e}$:

- Original codeword $\mathbf{c}$
- Transmission error $\mathbf{e}$

Then,

$$\mathbf{Hx} = \mathbf{H}(\mathbf{c} + \mathbf{e}) = \mathbf{Hc} + \mathbf{He} = \mathbf{0} + \mathbf{He} = \mathbf{He}.$$

Minimal error corresponds to $\mathbf{e}$ with minimal weight. To decode,

1. Calculate $\mathbf{Hx}$ to determine coset.
2. Pick coset representative $\mathbf{e}$ with minimal weight.
3. Decode to $\mathbf{x} - \mathbf{e}$.

Assessment

Performance:

- $n - k$ parity-check bits
- Flexible minimum distance:

$$d_{\min}(\mathscr{C}) = \min_{\mathbf{c} \in \mathscr{C} \setminus \{\mathbf{0}\}} \mathrm{w}(\mathbf{c}).$$

- As $d_{\min}(\mathscr{C})$ increases, the number of codewords decreases.
- Slow decoding:

$$[\mathbb{Z}_2^n : \mathscr{C}] = \frac{|\mathbb{Z}_2^n|}{|\mathscr{C}|} = \frac{2^n}{2^k} = 2^{n-k} \text{ cosets.}$$

Polynomial Codes

Definition

A code $\mathscr{C}$ is a **cyclic code** if for every codeword $u_0u_1 \dots u_{n-1}$, the shifted word $u_{n-1}u_1u_2 \dots u_{n-2}$ is also a codeword in $\mathscr{C}$.

Now, consider $u_0u_1 \cdots u_{n-1}$ as $f(x) = u_0 + u_1x + \cdots + u_{k-1}x^{k-1}$ where $f(x) \in \mathbb{Z}_2[x]/\langle x^k - 1\rangle$.

Definition

For $g(x) \in \mathbb{Z}_2[x]$ with degree $n - k$, a code $\mathscr{C}$ is a **polynomial code** if each codeword corresponds to a polynomial in $\mathbb{Z}_2[x]$ of degree less than n divisible by $g(x)$.

A message $f(x) = u_0 + u_1x + \cdots + u_{k-1}x^{k-1}$ is encoded to $g(x)f(x)$.

Example

Let $g(x) = 1 + x + x^3$ (irreducible). Then

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

is the generator matrix that corresponds to the ideal generated by $g(x)$. Similarly,

$$\mathbf{H} = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$

is the parity-check matrix for this code.

Generalization

If $g(x) = g_0 + g_1 x + \cdots + g_{n-k} x^{n-k}$, $h(x) = h_0 + h_1 x + \cdots + h_k x^k$, and $g(x)h(x) = x^n - 1$, then the polynomial code generated by $g(x)$ has

$$\mathbf{G} = \begin{bmatrix} g_0 & 0 & \cdots & 0 \\ g_1 & g_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ g_{n-k} & g_{n-k-1} & \cdots & g_0 \\ 0 & g_{n-k} & \cdots & g_1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & g_{n-k} \end{bmatrix}$$

$$\mathbf{H}_{(n-k)\times n} = \begin{bmatrix} 0 & \cdots & 0 & 0 & h_k & \cdots & h_0 \\ 0 & \cdots & 0 & h_k & \cdots & h_0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ h_k & \cdots & h_0 & 0 & 0 & \cdots & 0 \end{bmatrix}.$$

Results for Polynomial Codes

Theorem

A linear code $\mathscr{C}$ in $\mathbb{Z}_2^n$ is cyclic if and only if it is an ideal in $\mathbb{Z}[x]/\langle x^n - 1\rangle$.

Thus, we have a **minimal generator polynomial** for a code polynomial code $\mathscr{C}$.

Theorem

Let $\mathscr{C} = \langle g(x)\rangle$ be a cyclic code in $\mathbb{Z}_2[x]/\langle x^n - 1\rangle$ and suppose that ω is a primitive nth root of unity over $\mathbb{Z}_2$. If s consecutive powers of ω are roots of $g(x)$, then $d_{min}(\mathscr{C}) \geq s + 1$.

Conclusions

- Linear codes: simple, straightforward, computationally slow.
- Polynomial codes: more structured, faster and more complicated.
- Other considerations:
  - More algebra
  - Where and when errors occur
  - Combinatorics
  - Sphere-packing

References

1. Richard W. Hamming. *Coding and Information Theory.* Prentice-Hall, Inc., 1980.
2. Raymond Hill. *A First Course in Coding Theory.* Clarendon Press, 1999.
3. Thomas W. Judson. *Abstract Algebra: Theory and Applications.* Orthogonal Publishing L3C, 2018.
4. Rudolf Lidl and Gunter Pilz. *Applied Abstract Algebra.* Springer, 2008.
5. F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes.* Elsevier Science Publishers B.V., 1988.
6. Steven Roman. *Coding and Information Theory.* Springer-Verlag, 1992.