CIE6020/MAT3350
Selected Topics in Information Theory

Lecture 17: Algebraic Codes

4 April 2019

The Chinese University of Hong Kong, Shenzhen

Reed-Solomon Codes

Applications of Reed-Solomon Codes

- Burst error protection: in many scenarios, couple bits are treated as a symbol.
- Communications
- Storage
- Bar code

Reed-Solomon Codes

- The alphabet is the finite field $\mathbb{F}$ with q elements, where $q \geq n$.
- Let $\alpha_1, \dots, \alpha_n$ be n distinct elements of $\mathbb{F}$.
- Encoding:
  - For a message $\mathbf{m} = (m_0, \dots, m_{k-1})$, define polynomial

$$p_{\mathbf{m}}(x) = m_0 + m_1 x + \cdots + m_{k-1} x^{k-1}.$$

  - $\mathbf{m} \mapsto (p_{\mathbf{m}}(\alpha_1), \dots, p_{\mathbf{m}}(\alpha_n))$.
- Generator matrix:

$$G = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \end{bmatrix}$$

Decoding of Reed-Solomon Codes

- The Reed-Solomon code with above parameters is a $(n, k, n-k+1)$ code.
- Decoding algorithms:
  - Syndrome decoding (E.g. Berlekamp-Massey algorithm)
  - List decoding (Sudan and Guruswami's algorithms)
  - Soft decoding (Kötter and Vardy)

Welch-Berlekamp Algorithm

- Decoding problem:
  - Given: n pairs of field elements (α_i, r_i), $i = 1, \ldots, n$, and a parameter k.
  - Task: Find a polynomial $p(x)$ of degree less than k such that $p(\alpha_i) = r_i$ for at least $(n + k)/2$ values of $i \in \{1, \ldots, n\}$.

Welch-Berlekamp Algorithm

- Decoding problem:
  - Given: n pairs of field elements (α_i, r_i), $i = 1, \ldots, n$, and a parameter k.
  - Task: Find a polynomial $p(x)$ of degree less than k such that $p(\alpha_i) = r_i$ for at least $(n+k)/2$ values of $i \in \{1, \ldots, n\}$.
- Error polynomial $E(x)$
  - $p(\alpha_i) \neq r_i$ implies $E(\alpha_i) = 0$.
  - Given E, p can be computed efficiently.
  - Such an E exists: $E(x) = \prod_{i : r_i \neq p(\alpha_i)} (x - \alpha_i)$.
  - E has degree equal to the number t of errors and the most significant coefficient is 1.

Welch-Berlekamp Algorithm

- Decoding problem:
  - Given: n pairs of field elements (α_i, r_i), $i = 1, \ldots, n$, and a parameter k.
  - Task: Find a polynomial $p(x)$ of degree less than k such that $p(\alpha_i) = r_i$ for at least $(n+k)/2$ values of $i \in \{1, \ldots, n\}$.
- Error polynomial $E(x)$
  - $p(\alpha_i) \neq r_i$ implies $E(\alpha_i) = 0$.
  - Given E, p can be computed efficiently.
  - Such an E exists: $E(x) = \prod_{i : r_i \neq p(\alpha_i)} (x - \alpha_i)$.
  - E has degree equal to the number t of errors and the most significant coefficient is 1.
- Key equation: $r_i E(\alpha_i) = E(\alpha_i) p(\alpha_i)$ for $i = 1, \ldots, n$.

Welch-Berlekamp Algorithm

- Let $Q(x) = E(x)p(x)$, which has degree $k - 1 + t$.
- Take the unknown coefficients of Q and E as variables and solve the linear system

$$r_i E(\alpha_i) = Q(\alpha_i), i = 1, \ldots, n.$$

- Try $t = 0, 1, \ldots, (n - k)/2$.
- A solution exists, but may not be unique.

Singleton Bound

Theorem
For a block code $\mathcal{C} \subset \mathcal{A}^n$ satisfies

$$|\mathcal{C}| \leq q^{n-d_{\mathit{min}}+1}.$$

- Codes that achieve the Singleton bound is also called maximum distance separable (MDS) codes.
- Reed-Solomon codes are MDS.

MDS conjecture

- There exist linear MDS codes over $\mathbb{F}_q$ of length $n = q + 1$.

MDS conjecture

- There exist linear MDS codes over $\mathbb{F}_q$ of length $n = q + 1$.

$$G = \begin{bmatrix} 1 & 1 & \cdots & 1 & 0 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n & 0 \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 & \vdots \\ \vdots & \vdots & \ddots & \vdots & 0 \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} & 1 \end{bmatrix}$$

MDS conjecture

- There exist linear MDS codes over $\mathbb{F}_q$ of length $n = q + 1$.
- (Bush 1952) If $k \geq q + 1$, then for any MDS codes $n \leq k + 1$.

MDS conjecture

- There exist linear MDS codes over $\mathbb{F}_q$ of length $n = q + 1$.
- (Bush 1952) If $k \geq q + 1$, then for any MDS codes $n \leq k + 1$.

$$G = \begin{bmatrix} 1 & 0 & \cdots & 0 & 1 \\ 0 & 1 & \cdots & 0 & 1 \\ 0 & 0 & \ddots & \vdots & 1 \\ 0 & 0 & \cdots & 1 & 1 \end{bmatrix}$$

MDS conjecture

- There exist linear MDS codes over $\mathbb{F}_q$ of length $n = q + 1$.
- (Bush 1952) If $k \geq q + 1$, then for any MDS codes $n \leq k + 1$.
- (MDS conjecture, Segre 1955) If $k \leq q$ then for any MDS codes $n \leq q + 1$, unless $q = 2^h$ and $k = 3$ or $k = q - 1$, in which case $n \leq q + 2$.

MDS conjecture

- There exist linear MDS codes over $\mathbb{F}_q$ of length $n = q + 1$.
- (Bush 1952) If $k \geq q + 1$, then for any MDS codes $n \leq k + 1$.
- (MDS conjecture, Segre 1955) If $k \leq q$ then for any MDS codes $n \leq q + 1$, unless $q = 2^h$ and $k = 3$ or $k = q - 1$, in which case $n \leq q + 2$.

$$G = \begin{bmatrix} 1 & 1 & \cdots & 1 & 0 & 0 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_q & 0 & 1 \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_q^2 & 1 & 0 \end{bmatrix}$$

Greedy algorithms

Gilbert-Varshamov Bound (Sphere-Covering Bound)

Theorem

There exists a code $\mathcal{C} \subset \mathcal{A}^n$ such that

$$|\mathcal{C}| \geq \frac{q^n}{\sum_{i=0}^{d_{min}-1} \binom{n}{i} (q-1)^i}.$$

Gilbert-Varshamov Bound (Sphere-Covering Bound)

Theorem

There exists a code $\mathcal{C} \subset \mathcal{A}^n$ such that

$$|\mathcal{C}| \geq \frac{q^n}{\sum_{i=0}^{d_{\mathit{min}}-1} \binom{n}{i} (q-1)^i}.$$

Theorem

There exists a linear code $\mathcal{C} \subset \mathcal{A}^n$ with dimension k such that

$$k \geq n - \log_q \sum_{i=0}^{d_{\mathit{min}}-1} \binom{n}{i} (q-1)^i.$$

Asymptotic Gilbert-Varshamov Bound

- Let $\delta = d/n$.
- For a fixed rate r, $0 < r < 1$,

$$\delta^*(r) = \lim\sup_{n\to\infty} \max\{d(C)/n : C \in \mathcal{C}(n, 2^{\lfloor nr \rfloor})\}.$$

Theorem

$$h(\delta^*(r)) \geq 1 - r.$$

Proof.
Using G-V bound and $\binom{n}{n\delta} \approx 2^{nh(\delta)}$. $\square$