Goppa Codes and AG Codes

Jiyou Li
lijiyou@sjtu.edu.cn

Department of Mathematics, Shanghai Jiao Tong University

Dec. 2nd, 2014
Shannon’s Channel Coding Theorem

**Theorem (Shannon, 1948)**

In a discrete, memoryless, binary symmetric channel, let $V$ be the channel capacity defined by

$$V = 1 - H(p) = 1 - p \log \frac{1}{p} - (1 - p) \log \frac{1}{1-p},$$

where $p$ is the probability of a bit error (or flipping). For any $0 < R < V$, there is a code $C$ with information rate $R$ such that

$$P[A \text{ wrong decoding for a message } m] < e^{-n}.$$
Theorem (Gilbert-Varshamov bound)

Let $M_q(n, d)$ denote the maximum possible size such that there is an $(n, M_q(n, d), d)_q$ code. Then

$$M_q(n, d) \geq \frac{q^n}{1 + (q - 1) \binom{n}{1} + \cdots + (q - 1)^{d-1} \binom{n}{d-1}}.$$
Theorem (Asymptotic Gilbert-Shannon-Varshamov bound)

Define

\[ \alpha(\delta) = \lim_{n \to \infty} \sup log_q M_q(n, \delta n) \]

and for \( 0 \leq x < \frac{q-1}{q} \), define

\[ H_q(x) = x \log_q (q - 1) - x \log_q x - (1 - x) \log_q (1 - x). \]

If \( 0 < \delta \leq \frac{q-1}{q} \), then

\[ \alpha(\delta) \geq 1 - H_q(\delta). \]
Theorem (Asymptotic Gilbert-Shannon-Varshamov bound)

Define
\[
\alpha(\delta) = \lim_{n \to \infty} \sup \log_q M_q(n, \delta n) \frac{n}{n}
\]

and for \(0 \leq x < \frac{q-1}{q}\), define
\[
H_q(x) = x \log_q (q - 1) - x \log_q x - (1 - x) \log_q (1 - x).
\]

If \(0 < \delta \leq \frac{q-1}{q}\), then
\[
\alpha(\delta) \geq 1 - H_q(\delta).
\]

Recall that the Singleton bound gives
\[
\alpha(\delta) \leq 1 - \delta.
\]
Definition

Let $(n, q) = 1$ and $\mathbb{F}_{q^m} = \mathbb{F}_q(\beta)$, $\text{Ord}(\beta) = n$. $2 \leq t \leq n - 1$ is an integer. Then $q$-ary cyclic code of roots $\beta, \beta^2, \ldots, \beta^{t-1}$ is defined as

$$C = \{ c(x) \in \mathbb{F}_q[x], c(\beta) = c(\beta^2) = \cdots = c(\beta^{t-1}) = 0 \}$$

is called a **BCH** code of designed distance $t$. 
The parity check matrix $H$ of a $\text{BCH}$ code is given by

$$H = \begin{pmatrix}
1 & \beta & \beta^2 & \ldots & \beta^{n-1} \\
1 & \beta^2 & \beta^4 & \ldots & \beta^{(n-1)} \\
\vdots & \vdots & \ddots & \ddots & \vdots \\
1 & \beta^{t-1} & \beta^{2(t-1)} & \ldots & \beta^{(t-1)(n-1)}
\end{pmatrix}_{mt \times n}.$$
\[ c(x) \in C \iff c(\beta^i) = 0, \forall 1 \leq i \leq t - 1 \]

\[ \iff (z^n - 1) \left( \sum_{i=0}^{n-1} \frac{c_i}{z - \beta^{-i}} \right) \equiv 0 \pmod{z^{t-1}} \]

\[ \iff \sum_{i=0}^{n-1} \frac{c_i}{z - \beta^{-i}} \equiv 0 \pmod{z^{t-1}}. \]
Definition

Let $g(x)$ be a monic polynomial in $\mathbb{F}_{q^m}[x]$ with $\deg(g(x)) = t$. Let $L = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ with $\alpha_i$ are distinct and $g(\alpha_i) \neq 0$. Define the Goppa code $C(L, g(x))$ by

$$C = \{ c \in \mathbb{F}_q^n | \sum_{i=0}^{n-1} \frac{c_i}{x - \alpha_i} \equiv 0 \pmod{g(x)} \}.$$
Theorem

The Goppa code $C(L, g(x))$ defined as above has parameter $[n, k \geq n - mt, d \geq t + 1]$.

Proof.

$$H = \begin{pmatrix}
    h_0 & h_1 & \ldots & h_{n-1} \\
    h_0 \alpha_0 & h_1 \alpha_1 & \ldots & h_{n-1} \alpha_{n-1} \\
    \vdots & \vdots & \ddots & \vdots \\
    h_0 \alpha_0^{t-1} & h_1 \alpha_1^{t-1} & \ldots & h_{n-1} \alpha_{n-1}^{t-1}
\end{pmatrix}_{mt \times n},$$

where $h_i = g^{-1}(\alpha_i)$. 

$\square$
Let $g(x)$ be in $\mathbb{F}_{q^m}[x]$ with $\deg(g(x)) = t$. Let 
$L = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ with $\alpha_i$ being distinct. Consider a vector space $V \subseteq \mathbb{F}_{q^m}(x)$ such that 
(1). For each zero of $g(x)$, and every function $f(x)$ in $V$, $f(x)$ has at least the same multiplicities as $g(x)$ has on this zero; 
(2). Every function $f(x)$ in $V$ has no poles except in $L$ with multiplicity at most 1.

**Definition**

Define a code by

$$\{(\text{Res}_{\alpha_0} f, \text{Res}_{\alpha_1} f, \ldots, \text{Res}_{\alpha_{n-1}} f) \mid f \in V\}.$$ 

The Goppa code $\mathcal{C}(L, g(x))$ is defined as the subfield subcode over $\mathbb{F}_q$ of this codes.
Let $E/\mathbb{F}_q$ be a geometrically irreducible smooth projective curve of genus $g$ over the finite field $\mathbb{F}_q$ with the function field $\mathbb{F}_q(E)$.

Let $E(\mathbb{F}_q)$ be the set of all $\mathbb{F}_q$-rational points on $E$.

Let $D = \{P_1, P_2, \ldots, P_n\}$ be a proper subset of rational points $E(\mathbb{F}_q)$.

Denote $D$ by $D = P_1 + P_2 + \cdots + P_n$.

For a function $f(x) \in \mathbb{F}_q(E)$, let $\text{div}(f)$ be its divisor.
Let $G$ be a divisor of degree $m$ \((2g - 2 < m < n)\) such that 
\[ \text{Supp}(G) \cap D = \emptyset. \]

\[ \mathcal{L}(G) = \{ f \in \mathbb{F}_q(E) \mid \text{div}(f) \geq -G \} \cup \{0\}. \]

The AG code $\mathcal{C}(D, G)$ is defined to be the image of the following evaluation map:
\[ \text{ev} : \mathcal{L}(G) \rightarrow \mathbb{F}_q^n; \ f \mapsto (f(P_1), f(P_2), \ldots, f(P_n)). \]
The Riemann-Roch theorem asserts if \( m \geq 2g - 2 \), then
\[
\dim_{\mathbb{F}_q} \mathcal{L}(G) = m - g + 1.
\]
The Riemann-Roch theorem asserts if $m \geq 2g - 2$, then
$$\dim_{\mathbb{F}_q} \mathcal{L}(G) = m - g + 1.$$ 

By Riemann-Roch theorem, the AG code $\mathcal{C}(D, G)$ has parameters $[n, m - g + 1, d \geq n - m]$. 
AG codes-IV

Let $\Omega(E)$ be the space of rational differential form on $E$. Define

$$\Omega(D) = \{\omega \in \Omega(E) | \omega \geq -D\}.$$ 

The geometric Goppa code $C^*(D, G)$ is defined to be the image of the following evaluation map:

$$re : \Omega(G-D) \to \mathbb{F}_q^n; \omega \mapsto (\text{Res}_{P_1}(\omega), \text{Res}_{P_2}(\omega), \ldots, \text{Res}_{P_n}(\omega)).$$
Again by Riemann-Roch theorem, the Goppa code $C^*(D, G)$ has parameters $[n, n - m + g - 1, d \geq m - 2g + 2]$. 
Again by Riemann-Roch theorem, the Goppa code $C^*(D, G)$ has parameters $[n, n - m + g - 1, d \geq m - 2g + 2]$. $C(D, G)$ and $C^*(D, G)$ are dual codes.
Again by Riemann-Roch theorem, the Goppa code $\mathcal{C}^*(D, G)$ has parameters $[n, n - m + g - 1, d \geq m - 2g + 2]$.

$\mathcal{C}(D, G)$ and $\mathcal{C}^*(D, G)$ are dual codes.

Since, for any differential $\omega \in \Omega(E)$,

$$\sum_{P \in E} \text{Res}_P(\omega) = 0.$$
Let $E$ to the projective line over $\mathbb{F}_q$ and thus $g = 0$. Choose $G = m \cdot \infty = m \cdot (1 : 0)$, $P_i = (\alpha_i : 1)$. We then have

$$\mathcal{L}(G) = \{ f \in \mathbb{F}_q(E) \mid \text{div}(f) \geq -G \} \cup \{0\}$$

$$= \{ f(x) \in \mathbb{F}_q[x] \mid \deg(f(x)) \leq m \}.$$ 

This is the extended Reed-Solomon code.
Let $E$ to the projective line over $\mathbb{F}_{q^m}$ and thus $g = 0$. Let $P_i = (\alpha_i : 1), 1 \leq i \leq n - 1$. Define $D = P_0 + P_1 + \cdots + P_{n-1}$ and $G = (g)$.

**Definition**

The code $C^*(D, G)$ generated by

$$\{(\text{Res}_{\alpha_0} f, \text{Res}_{\alpha_1} f, \ldots, \text{Res}_{\alpha_{n-1}} f) \mid f \in \Omega(G - D)\}.$$ 

has the Goppa code $C(L, g(x))$ as the subfield subcode over $\mathbb{F}_q$. 

Li Jiyou
Let $E$ to the projective curve $x^3 + y^3 + z^3 = 0$ over $\mathbb{F}_2$. $\alpha$ is a generator in $\mathbb{F}_4$. Choose $G = 2 \cdot (0 : 1 : 1)$, $D = P_1 + P_2 + \cdots + P_8$, $P_1 = (0 : \alpha : 1)$, $P_2 = (0 : 1 + \alpha : 1)$, $P_3 = (1 : 0 : 1)$, $P_4 = (1 : 1 : 0)$, $P_5 = (\alpha : 0 : 1)$, $P_6 = (1 + \alpha : 0 : 1)$, $P_7 = (\alpha : 1 : 0)$, $P_8 = (\alpha + 1 : 1 : 0)$. One checks that 1 and $\frac{x}{y+z}$ are a basis of $L(G)$. We then have a $[8, 2, 6]_4$ AG code with the generator matrix

$$
\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 1 & \alpha & \alpha + 1 & \alpha & \alpha + 1
\end{pmatrix}.
$$
Corollary (Asymptotic bound of AG codes)

For $0 \leq \delta < \frac{q-1}{q}$ recall

$$\alpha(\delta) = \lim_{n \to \infty} \sup_{q} \frac{\log q M_q(n, \delta n)}{n}.$$ 

If $0 \leq \delta \leq \frac{q-1}{q}$, then

$$\alpha(\delta) \geq 1 - \delta - \frac{H_2(\delta)}{\log(q)} - o\left(\frac{1}{\log(q)}\right).$$

There are family of AG codes such that

$$\alpha(\delta) \geq 1 - \delta - \frac{1}{\sqrt{q-1}}.$$