AG codes; codes over rings

Recall: Let χ be a non-singular projective curve over $\mathbb{F}_q$. The free abelian group generated by the points of χ is called the divisor group of the curve. A element D of the group, called a divisor on χ, is a finite formal sum $\sum_{P\in\chi(\mathbb{F}_q)} n_P P$ of points on χ. The support of D is $\text{supp}(D) := \{P \mid n_P \neq 0\}$. Two divisors $D = \sum n_P P$ and $D' = \sum n'_P P$ are added as

$$D + D' = \sum_{P\in\chi(\mathbb{F}_q)} (n_P + n'_P)P.$$

If n_P for all P, the divisor D is effective $(D \geq 0)$. The degree of D is $\sum n_P \deg P$.

The **space of rational functions associated to** D is

$$L(D) := \{f \in \mathbb{F}_q(C) \mid \text{div }(f) + D \geq 0\} \cup \{0\}.$$

Let $P = (P_1, P_2, \ldots, P_n)$ be a set of n distinct $\mathbb{F}$-rational points on the curve. The map $\phi : L(D) \longrightarrow \mathbb{F}_q^n$ with $f \mapsto (f(P_1), \ldots, f(P_n))$ is linear, hence the image $\phi(L(D))$ is a linear code over $\mathbb{F}_q$. We denote this code by $C(\chi, P, D)$, the **algebraic geometric code** associated to χ, P and D.

parameters of $C(\chi, P, D)$

The map ϕ is injective (i.e. its kernel is $\{0\}$), therefore the dimension of $C(\chi, P, D)$ is dim $L(D)$.

If deg $D > 2g - 2$ (where g is the genus of χ), by the Riemann-Roch Theorem, $k = \dim C(\chi, P, D) = \deg D + 1 - g$.

Let d be the minimum distance of $C(\chi, P, D)$. Then there is a rational function $f \in L(D)$ such that $\phi(f) = (f(P_1), \ldots, f(P_n))$ has weight $d > 0$. Assume $f(P_i) \neq 0$ for $i = 1, \ldots, d$ and $f(P_i) = 0$ for $i = d + 2, \ldots, n$.
Thus $f \in L(D - P_{d+1} - P_{d+2} - \cdots - P_n)$. (i.e. div $(f) + D - \sum_{i=d+1}^{n} P_i \geq 0$). This means the divisor $D - \sum_{i=d+1}^{n} P_i$ has non-negative degree. So deg $D - (n - d) \geq 0$, therefore $d \geq n - \deg D$.

Theorem. Let χ be a non-singular projective curve over $\mathbb{F}_q$, with genus g. Let P be a set of n distinct $\mathbb{F}_q$-rational points on χ, and let D be a divisor on χ such that $2g - 2 < \deg D < n$. Then $C(\chi, P, D)$ is a linear code of length n, dimension $=$ $\deg D + 1 - g$ and minimum distance d where $d \geq n - \deg D$.

Recall the Singleton Bound: $d + k \leq n + 1$. Combining this with $d \geq n - \deg D$ and $k = \deg D + 1 - g$, we get $n + 1 - g \leq d + k \leq n + 1$.

Hence, if the underlying curve has genus $= 0$ (i.e. built from the projective line), the AG code is an MDS code.

generator matrix of $C(\chi, P, D)$

Let $\{f_1, f_2, \ldots, f_k\}$ be a basis for $L(D)$. Since the AG code $C(\chi, P, D)$ is the image of $L(D)$ under ϕ, it has basis $\{\phi(f_1), \phi(f_2), \ldots, \phi(f_k)\}$. Thus a generator matrix for $C(\chi, P, D)$ is:

$$G = \begin{bmatrix} f_1(P_1) & f_1(P_2) & \ldots & f_1(P_n) \\ f_2(P_1) & f_2(P_2) & \ldots & f_2(P_n) \\ \vdots & \vdots & & \vdots \\ f_k(P_1) & f_k(P_2) & \ldots & f_k(P_n) \end{bmatrix}.$$

Let $C = C(\chi, P, D)$. Under some conditions, we get the relative parameters

$$R_C = \frac{k}{n} = \frac{\deg D + 1 - g}{n} \text{ and } \delta_C = \frac{d}{n} \geq \frac{n - \deg D}{n}$$

We want $R_C + \delta_C$ large:

$$\begin{aligned} R_C + \delta_C &\geq \frac{\deg D + 1 - g}{n} + \frac{n - \deg D}{n} \\ &= \frac{n}{n} + \frac{1}{n} - \frac{g}{n} \end{aligned}$$

For long codes, we consider the limit as n increases.
(Correspondingly, a sequence of AG codes with increasing length.)

To construct these codes, we need a sequence of curves χ_i, with genus g_i, a set of n_i points P_i on χ_i and a chosen divisor D_i on χ_i.
So, $\lim_{n\to\infty}(R+\delta) \geq 1 - \lim_{i\to\infty} \frac{g_i}{n_i}$
Since we want $(R+\delta)$ big, we want $\lim_{n\to\infty} \frac{g}{n}$ as small as possible.
For a curve χ of genus g over $\mathbb{F}_q$, let $N_q(\chi) := \#\chi(\mathbb{F}_q)$

For $g \geq 0$, let $N_q(g)$ be the number of points on the largest possible curve over $\mathbb{F}_q$ with genus g. Define

$$A(q) := \lim_{g\to\infty} \frac{N_q(g)}{g}$$

Suppose we have a sequence of curves χ_i over $\mathbb{F}_q$ with genus g_i and size N_i such that $\lim_{i\to\infty} \frac{N_i}{g_i} = A(q)$.

For each i , choose $Q_i \in \chi_i(\mathbb{F}_q)$, and set $P_i = \chi_i(\mathbb{F}_q) \setminus \{Q_i\}$. Pick $r_i \in \mathbb{N}$ such that $2g_i - 2 < r_i < N_i - 1 = \#P_i$.

Consider the AG code $C_i = C(\chi_i, P_i, r_i Q_i)$ which has parameters $[N_i, r_i + 1 - g_i, d_i]$ with $d_i \geq N_i - 1 + r_i$.

If R_i and δ_i are the relative parameters of C_i, then

$$\begin{aligned} R_i + \delta_i &\geq \tfrac{r_i+1-g_i}{N_i-1} + \tfrac{N_i-1-r_i}{N_i-1} \\ &= \tfrac{N_i-g_i}{N_i-1} \\ &= 1 + \tfrac{1}{N_i-1} + \tfrac{g_i}{N_i-1} \end{aligned}$$

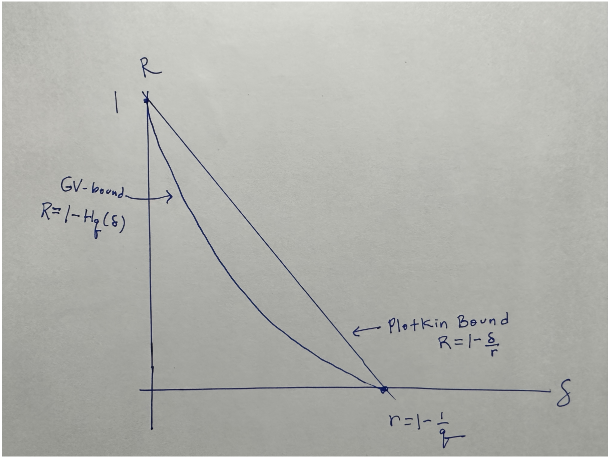
Let $R := \lim_{i\to\infty} R_i$ and $\delta := \lim_{i\to\infty} \delta_i$. We get

$$\begin{aligned} R + \delta &\geq 1 - \tfrac{1}{A(q)} \\ R &\geq -\delta + 1 - \tfrac{1}{A(q)} \end{aligned}$$

Recall: $\alpha_q(\delta) := \limsup_{n\to\infty} \frac{1}{n} \log A_q(n, \lfloor \delta n \rfloor)$.

Thus $\alpha_q(\delta) \geq -\delta + 1 - \frac{1}{A(q)}$.

The line $R = -\delta + 1 - \frac{1}{A(q)}$ has negative slope, hence will intersect the GV bound at 0, 1 or 2 points.



So we need to look at the value of $A(q)$.

Given genus g, how big can $\chi(\mathbb{F}_q)$? Since

$$\mathbb{P}^2(\mathbb{F}_q) = \{(\alpha : \beta : 1) \mid \alpha, \beta \in \mathbb{F}_q\} \cup \{(\alpha : 1 : 0) \mid \alpha \in \mathbb{F}_q\} \cup \{(1 : 0 : 0)\}$$

the size of plane curves has upper bound $q^2 + q + 1$.

In general, if χ is a non-singular projective curve of genus g over $\mathbb{F}_q$, then $\mid \#\chi(\mathbb{F}_q) - (q+1) \mid \leq 2g\sqrt{q}$. (Hasse-Weil)

A curve that meets the bound (i.e. $\#\chi(\mathbb{F}_q) = q + 1 + 2g\sqrt{q}$) is "maximal". Here is J.P. Serre's improvement of the Hasse-Weil bound :

$$\mid \#\chi(\mathbb{F}_q) - (q+1) \mid \leq g\lfloor 2\sqrt{q} \rfloor.$$

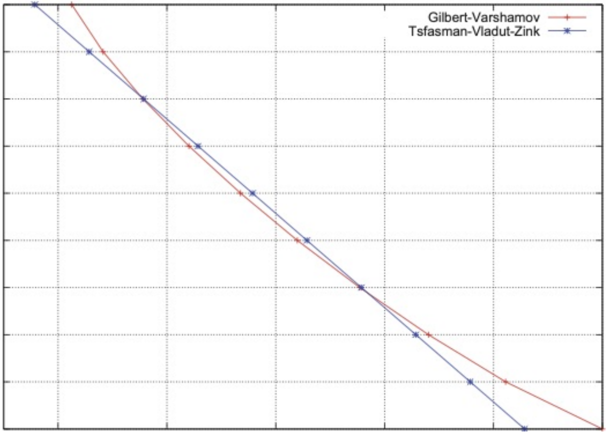
Theorem. (Drinfeld, Vladut). If q is a prime power, then $A(q) \leq \sqrt{q} - 1$.

Theorem. (Ihara, Tsfasman, Vladut, Zink) Let $q = p^{2m}$. There exists a sequence of curves χ_i over $\mathbb{F}_q$ with genus g_i such that $\lim_{i \to \infty} \frac{\#\chi_i(\mathbb{F}_q)}{g_i} = \sqrt{q} - 1$.

Theorem. (Tsfasman, Vladut, Zink) Let q be a perfect square. Then
$\alpha_q(\delta) \geq -\delta + 1 - \frac{1}{\sqrt{q}-1}$.

This gives us the line that will intersect the GV bound at exactly 2 points, when $q \geq 49$.

The Tsfasman-Vladut-Zink line, $R = -\delta + 1 - \frac{1}{\sqrt{q}-1}$ intersects the GV bound at 2 points, whenever $q \geq 49$.



non-linear codes

Let A be an alphabet. If A is a field, a linear code over A is a subspace of A^n. If a subset of A^n is not a vector space, it is a non-linear code over A.

It is known that there is no binary linear code $[16, 8, 6]_2$. But in

1967, a binary but non-linear $(16, 2^8, 6)$ code was found by Nordstrom and Robinson. The code has a high degree of regularity and symmetry.

Generalizations of the Nordstrom-Robinson code were found later:

Preparata codes (for $m \geq 2$) : $(2^{2m}, 2^{2^{2m}-4m}, 6)$
Kerdock codes (for $m \geq 2$): $(2^{2m}, 2^{4m}, 2^{2m-1} - 2^{m-1})$.

Codes over finite rings

Generalizations of Nordstrom-Robinson code: Preparata, Kerdock codes, etc.

Recent interest in codes over **rings** is due to the discovery that certain non-linear binary codes can be constructed as images of codes over the finite ring $\mathbb{Z}_4 := \mathbb{Z}/4\mathbb{Z}$.

Definition. The *Gray map* $\phi : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2^2$ is given by

$$0 \longmapsto 00, \ 1 \longmapsto 01, \ 2 \longmapsto 11, \ 3 \longmapsto 10.$$

We can extend this to $\phi : \mathbb{Z}_4^n \longmapsto\longrightarrow \mathbb{Z}_2^{2n}$.

Theorem. *(Hammons, Kumar, Calderbank, Sloane and Solé, 1992)* Let $(\mathcal{O})$ (the "octacode") be the linear $(2^3, 256, 6)_{\mathbb{Z}_4}$ code with generator matrix

$$G = \begin{bmatrix} 3 & 3 & 2 & 3 & 1 & 0 & 0 & 0 \\ 3 & 0 & 3 & 2 & 3 & 1 & 0 & 0 \\ 3 & 0 & 0 & 3 & 2 & 3 & 1 & 0 \\ 3 & 0 & 0 & 0 & 3 & 2 & 3 & 1 \end{bmatrix}.$$

Then $\phi((\mathcal{O}) =$ Nordstrom-Robinson code.

Theorem. *(Hammons, Kumar, Calderbank, Sloane and Solé, 1992)* Let $(\mathcal{O})$ (the "octacode") be the linear $(2^3, 256, 6)_{\mathbb{Z}_4}$ code with generator matrix

$$G = \begin{bmatrix} 3 & 3 & 2 & 3 & 1 & 0 & 0 & 0 \\ 3 & 0 & 3 & 2 & 3 & 1 & 0 & 0 \\ 3 & 0 & 0 & 3 & 2 & 3 & 1 & 0 \\ 3 & 0 & 0 & 0 & 3 & 2 & 3 & 1 \end{bmatrix}.$$

Then $\phi((\mathcal{O}) =$ Nordstrom-Robinson code. The non-linear binary codes are Gray map images of linear codes over $\mathbb{Z}_4$.

Further reading

1) Høholdt, van Lint, and Pellikaan. *Algebraic geometry codes*, in Handbook of Coding Theory (Pless, Huffman and Brualdi, eds.), Vol. 1, (1998).

2) Katsman, Tsfasman, and Vladut. "Modular curves and codes with a polynomial construction". IEEE Trans. Inform. Theory **30(2)** (1984), 353-355.

3) Tsfasman, Vladut, and Zink. "Modular curves, Shimura curves, and Goppa Codes, better than the Varshamov-Gilbert bound". *Math. Nachrichten,* **109** *(1982), 21-28.*

4) van Lint, and van der Geer. "Introduction to coding theory and algebraic geometry", DMV Seminar, Vol. 12, Birkhauser (1988)

5) Hammons, Kumar, Calderbank, Sloane, Sole. "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes", IEEE Trans. Inform. Theory **IT-40** *(1994), 301-319.*