Feng-Rao distances in Arf and inductive semigroups

José I. Farrán Pedro A. García-Sánchez

International Meeting on Numerical Semigroups – Levico Terme

July 5th, 2016

Outline

Error-correcting codes

Parameters

- Alphabet $\mathcal{A} = \mathbb{F}_q$
- Code $C \subseteq \mathbb{F}_q^n$
- Dimension $\dim C = k \leq n$

Hamming distance

- The Hamming distance in $\mathbb{F}_q^n$ is defined by

$$d(\mathbf{x}, \mathbf{y}) \doteq \sharp\{i \mid x_i \neq y_i\}$$

- The minimum distance of C is

$$d \doteq d(C) \doteq \min\{d(\mathbf{c}, \mathbf{c}') \mid \mathbf{c}, \mathbf{c}' \in C, \;\; \mathbf{c} \neq \mathbf{c}'\}$$

- The parameters of a code are $C \equiv [n, k, d]_q$
- d is connected with the error correction capacity of the code, so that it is important either
  - the exact value of d, or
  - a lower-bound for d
- In the case of AG codes some numerical semigroup helps ...

One-point AG Codes

- χ "curve" over a finite field $\mathbb{F} \equiv \mathbb{F}_q$
- P and $P_1, \ldots, P_n$ "rational" points of χ
- C_m^* image of the linear map

$$\begin{array}{rcccl} ev_D & : & \mathcal{L}(mP) & \longrightarrow & \mathbb{F}^n \\ & & f & \mapsto & (f(P_1), \ldots, f(P_n)) \end{array}$$

- C_m the orthogonal code of C_m^*
  with respect to the canonical bilinear form

$$\langle \mathbf{a}, \mathbf{b} \rangle \doteq \sum_{i=1}^{n} a_i b_i$$

- If we assume that $2g - 2 < m < n$, then the parameters of C_m are
  - $k = n - m + g - 1$
  - $d \geq m + 2 - 2g$ (Goppa bound)

  by using the Riemann-Roch theorem

Weierstrass semigroups

The Goppa bound can actually be improved by using the Weierstrass semigroup of χ at the point p

$$\Gamma_P \doteq \{m \in \mathbb{N} \mid \exists f \text{ with } (f)_\infty = mP\}$$

Note that $\Gamma_P = \mathbb{N} \setminus \{\ell_1, \ldots, \ell_g\}$ where g is the genus of χ and the numbers ℓ_i are called the Weierstrass gaps of χ at P

- $k = n - k_m$, where $k_m \doteq \sharp(\Gamma_P \cap [0, m])$ (note that $k_m = m + 1 - g$ for $m >> 0$)
- $d \geq \delta(m+1)$ (the so-called Feng–Rao distance)
- We have an improvement, since $\delta(m+1) \geq m + 2 - 2g$, and they coincide for $m >> 0$

Generalized Hamming weights

- Define the support of a linear code C as

$$\mathrm{supp}(C) := \{i \mid c_i \neq 0 \text{ for some } \mathbf{c} \in C\}$$

- The r-th generalized weight of C is defined by

$$\mathrm{d}_r(C) := \min\{\sharp\,\mathrm{supp}(C') \mid C' \leq C \text{ with } \dim(C') = r\}$$

- The above definition only makes sense if $r \leq k$, where $k = dim(C)$
- The set of numbers $\mathrm{GHW}(C) := \{\mathrm{d}_1, \ldots, \mathrm{d}_k\}$ is called the weight hierarchy of the code C
- It is possible to generalize the generalized Feng-Rao distance for higher order r, and for a one-point AG code C_m one has

$$d_r(C_m) \geq \delta_{FR}^r(m+1)$$

(the details on Feng-Rao distances are given later)

Feng-Rao distance

Let $S = \{\rho_1 = 0 < \rho_2 < \cdots\}$ be a numerical semigroup of genus g and conductor c

- The Feng–Rao distance in S is defined as

$$\delta_{FR}(m) := \min\{\nu(m') \mid m' \geq m, \quad m' \in S\}$$

where $\nu(m') := \sharp N(m')$ and

$$N(m') := \{(a, b) \in S^2 \mid a + b = m'\}$$

- Basic results:
  (i) $\nu(m) = m + 1 - 2g + D(m)$ for $m \geq c$, where

$$D(m) \doteq \sharp\{(x, y) \mid x, y \notin S \text{ and } x + y = m\}$$

  (ii) $\nu(m) = m + 1 - 2g$ for $m \geq 2c - 1$
  (iii) $\delta_{FR}(m) \geq m + 1 - 2g \doteq d^*(m - 1) \quad \forall m \in S$,
  "and equality holds for $m \geq 2c - 1$"

Generalized Feng-Rao distances

- The classical Feng-Rao distance corresponds to $r = 1$ in the following definition:
  - Let S be a numerical semigroup. For any integer $r \geq 1$, the *r-th Feng-Rao distance* of S is defined by

$$\delta_{FR}^{r}(m) :=$$

$$\min\{\nu(m_1, \ldots, m_r) \mid m \leq m_1 < \cdots < m_r, \quad m_i \in S\}$$

  - where $\nu(m_1, \ldots, m_r) := \sharp N(m_1, \ldots, m_r)$ and

$$N(m_1, \ldots, m_r) := N(m_1) \cup \cdots \cup N(m_r)$$

Feng-Rao numbers

- There exists a certain constant $E_r = \mathrm{E}(S,r)$, depending on r and S, such that

$$\delta_{FR}^r(m) = m + 1 - 2g + E_r$$

  for $m \geq 2c - 1$
- This constant is called the *r-th Feng-Rao number* of S
- Furthermore, $\delta_{FR}^r(m) \geq m + 1 - 2g + \mathrm{E}(S,r)$ for $m \geq c$, and equality holds if S is symmetric and $m = 2g - 1 + \rho$ for some $\rho \in S \setminus \{0\}$
- We may consider $\mathrm{E}(S,1) = 0$
- If $g = 0$ then $\mathrm{E}(S,r) = r - 1$

Feng-Rao numbers

We summarize some general properties of the Feng-Rao numbers, for $r \geq 2$ and S fixed, with $g \geq 1$:

1. The function $\mathrm{E}(S, r)$ is non-decreasing in r
2. $r \leq \mathrm{E}(S, r) \leq \rho_r$
3. If furthermore $r \geq c$, then $\mathrm{E}(S, r) = \rho_r = r + g - 1$

Computing the Feng-Rao numbers is hard, even in simple examples

- $\mathrm{E}(S, 2)$ can be computed with an algorithm based on Apéry sets
- If $S = \langle a, b \rangle$ then $\mathrm{E}(S, r) = \rho_r$, and hence by symmetry
  1. $\delta^r_{FR}(m) = \rho_r + \rho_k$ if $m = 2g - 1 + \rho_k$ with $k \geq 2$
  2. $\delta^r_{FR}(m) \geq \rho_r + \ell_i$ if $m = 2g - 1 + \ell_i$, where $\ell_i \in \mathrm{G}(S)$ is a gap of S
- $\mathrm{E}(S, r)$ is also known for semigroups generated by intervals

Arf semigroups

- Let $S = \{\rho_1 = 0 < \rho_2 < \cdots\}$, and assume that $c = \rho_r$ is the conductor, so that $g = c - r + 1$ is the genus
- S is called an Arf semigroup if $\rho_i + \rho_j - \rho_k \in S$ for every $i, j, k \in \mathbb{N}$ with $i \geq j \geq k$
- Notice that if $\rho_i \geq c$, then for every $i \geq j \geq k$ one has $\rho_i + \rho_j - \rho_k \in S$, so that the Arf condition only needs to be imposed in the range $k \leq j \leq i < r$
- We can call to such a sequence $0 = \rho_1 < \cdots < \rho_r = c$ satisfying the Arf condition an Arf sequence
- Let $S = \{\rho_1 = 0 < \rho_2 < \cdots\}$ be a numerical semigroup; for each $i \geq 1$ define

$$S^{(i)} = \{\rho_k - \rho_i \geq 0 \mid \rho_k \in S\}$$

- Note that not always $S^{(i)}$ is a semigroup
- In fact, $S^{(i)}$ is a semigroup for all i if and only if S is Arf (and all the $S^{(i)}$ are Arf, as a consequence)

The Feng-Rao distance in Arf semigroups

- For $i >> 0$ one gets $S^{(i)} = \mathbb{N}$
- We could call these $S^{(i)}$ "derivatives" of S
- For the reverse construction, get an Arf sequence

$$0 = \rho_1 < \rho_2 < \cdots < \rho_r = c$$

  and define $d_k = \rho_{k+1} - \rho_k$ for $k = 1, \ldots, r-1$
- Now we start from $\Gamma = S^{(r)} = \mathbb{N}$ and iterate the construction

$$\Gamma_* = \{0\} \cup (d + \Gamma)$$

  for $d = d_{r-1}, d_{r-2}, \ldots, d_1$, obtaining $S^{(r-1)}, S^{(r-2)}, \ldots, S^{(1)} = S$
- Using this construction, one can prove recursively for S being Arf:
  1. $\nu(c + \rho_i - 1) = 2(i-1)$ for $i = 2, \ldots, r$
  2. $\delta_{FR}(m) = 2(i-1)$ if $c + \rho_{i-1} \leq m \leq c + \rho_i - 1$, for $i = 2, \ldots, r$

Inductive semigroups

- Starting with $S_0 = \mathbb{N}$ (that is Arf) we can iterate n times the following construction:

$$S_k = a_k \cdot S_{k-1} \cup (c_k + \mathbb{N})$$

- Notice that if S_k is Arf then also S_{k+1} is Arf
- Thus, every semigroup constructed as above is always Arf
- Question: which Arf semigroups cannot be constructed in this way?
- For the sake of regularity, we impose extra conditions:

$$a_k \geq 2, \quad \text{and} \quad c_k = a_k b_k \quad \text{with} \quad b_k \geq c_{k-1}$$

- These semigroups are called inductive
- Ordinary semigroups are inductive, with $n = 1$ and $b_1 = 1$

The Feng-Rao distance for inductive semigroups

- Inductive semigroups $\Gamma \equiv \Gamma_n$ are very comfortable to work with, since we can easily enumerate their elements
- Assume that $n \geq 1$, set $\lambda_1 = b_1$ and $\lambda_{i+1} = b_{i+1} - a_i b_i$ for $i \geq 2$
- From the sequences $(a_1, \ldots, a_n)$ and $(\lambda_1, \ldots, \lambda_n)$ we can retrieve $b_1 = \lambda_1$ and $b_{i+1} = \lambda_{i+1} + a_i b_i$
- For $i \in \{1, \ldots, n\}$, define $A_i = \prod_{j=i}^{n} a_i$
  (A_1 is the multiplicity of Γ_n, and $1 < A_n < \cdots < A_1$)
- The numerical semigroup Γ is a disjoint union of the following sets:
  - $\Lambda^1 = \{0, A_1, 2A_1, \ldots, \lambda_1 A_1\}$
  - $\Lambda^2 = b_1 A_1 + \{A_2, 2A_2, \ldots, \lambda_2 A_2\}$
  - ...
  - $\Lambda^n = b_{n-1} A_{n-1} + \{A_n, 2A_n, \ldots, \lambda_n A_n\}$
  - $\Lambda^{n+1} = (a_n b_n + 1) + \mathbb{N}$
- In [Campillo–Farrán–Munuera] the Feng-Rao distance is made explicit in terms of the above parameters

The second Feng-Rao number for inductive semigroups

- Our purpose is now to compute the second Feng-Rao number of inductive semigroups [García–Farrán]
- To that end, we recall the following technical result from [Farrán–Munuera]:

$$\mathrm{E}(\Gamma, 2) = \min\{\sharp \mathrm{Ap}(\Gamma, x) \mid 1 \leq x \leq \rho_2\}$$

where the Apéry set of the semigroup Γ related to x is

$$\mathrm{Ap}(\Gamma, x) = \{y \in \Gamma \mid y - x \notin \Gamma\}$$

- It is known that $\sharp \mathrm{Ap}(\Gamma, x) = x$ if and only if $x \in \Gamma$ (in this case, the set $\mathrm{Ap}(\Gamma, x) \setminus \{0\}) \cup \{x\}$ is a very nice generating system of Γ)
- If x is a gap of Γ, then $\sharp \mathrm{Ap}(\Gamma, x) > x$

The second Feng-Rao number for inductive semigroups

- By studying the behaviour of $\sharp \mathrm{Ap}(\Gamma, x)$ in subintervals and multiples, one reduces the computations to

$$\mathrm{E}(\Gamma, 2) = \min\{\sharp S_1, \sharp S_{A_n}, \sharp S_{A_{n-1}}, \ldots, \sharp S_{A_2}, \sharp S_{A_1}\}$$

- In fact, we found an explicit formula for these numbers:

$$\sharp S_1 = \lambda_1 + \cdots + \lambda_n + 1$$

where $\lambda_1 = b_1$ and

$$\sharp S_{A_{n-k}} = \lambda_1 + \cdots + \lambda_{n-k-1} + A_{n-k}$$

for $k \in \{0, \ldots, n-1\}$

- Every of the above numbers can be reached as minimum, so that this formula is sharp
- It can be applied to towers of function fields ...

Towers of Function Fields

- Consider the tower of function fields $(\mathcal{T}_n)$ over $\mathbb{F}_{q^2}$, where $\mathcal{T}_1 = \mathbb{F}_{q^2}(x_1)$ and for $n \geq 2$, $\mathcal{T}_n$ is obtained from $\mathcal{T}_{n-1}$ by adjoining a new element x_n satisfying

$$x_n^q + x_n = \frac{x_{n-1}^q}{x_{n-1}^{q-1} + 1}.$$

- Let Q_n be the rational place on $\mathcal{T}_n$ that is the unique pole of x_1 ; then the Weierstrass semigroups Γ_n of $\mathcal{T}_n$ at Q_n are inductive: $\Gamma_1 = \mathbb{N}$, and for $n \geq 2$,

$$\Gamma_n = q \cdot \Gamma_{n-1} \cup \{m \in \mathbb{N} \mid m \geq c_n\},$$

where

$$c_n = \begin{cases} q^n - q^{\frac{n+1}{2}} & \text{if } n \text{ is odd,} \\ q^n - q^{\frac{n}{2}} & \text{if } n \text{ is even.} \end{cases}$$

- We apply the above formulas, with $a_1 = 1$ and $\lambda_1 = 0$, as follows . . .

Towers of Function Fields

- First note that $a_n = q$ for all $n \geq 2$, and

$$b_n = \frac{c_n}{a_n} = \begin{cases} q^{n-1} - q^{\frac{n-1}{2}} & \text{if } n \text{ is odd} \\ q^{n-1} - q^{\frac{n-2}{2}} & \text{if } n \text{ is even} \end{cases}$$

so that $\lambda_2 = b_2 = q - 1$

- For $n \geq 3$, we have

$$\lambda_n = b_n - c_{n-1} = \begin{cases} 0 & \text{if } n \text{ is odd} \\ (q-1)q^{\frac{n-2}{2}} & \text{if } n \text{ is even} \end{cases}$$

- As a consequence, by writing $n = 2m + b$ with $b \in \{0, 1\}$:
  (1) $A_{n-k} = q^{k+1}$, for $0 \leq k \leq n-2$.
  (2) $\sharp S_{q^{n-1}} = q^{n-1}$.
  (3) $\sharp S_1 = q^m = q^{\lfloor \frac{n}{2} \rfloor}$.
  (4) If $n = 2m$, then for $i \in \{1, \ldots, n-2\}$, $\sharp S_{q^i} = (q^{\lfloor m - \frac{i}{2} \rfloor} - 1) + q^i$.
  (5) If $n = 2m + 1$, then for $i \in \{1, \ldots, n-2\}$, $\sharp S_{q^i} = (q^{\lceil m - \frac{i}{2} \rceil} - 1) + q^i$.

Towers of function fields

- Extra reduction: the second Feng-Rao number of the Weierstrass semigroup Γ_n of the function field $\mathcal{T}_n$ at Q_n is given by the minimum of the following numbers:

$$\sharp S_1 = q^{\lfloor \frac{n}{2} \rfloor}$$
$$\sharp S_{q^{n-1}} = q^{n-1}$$
$$\sharp S_{q^{n-1-2k}} = (q^k - 1) + q^{n-1-2k}, \text{ for } k \in \{1, \ldots, \lfloor \tfrac{n}{2} \rfloor - 1\}$$

- Thus we conclude that:
  (1) $\mathrm{E}(\Gamma_1, 2) = 1$.
  (2) $\mathrm{E}(\Gamma_2, 2) = \mathrm{E}(\Gamma_3, 2) = q$.
  (3) $\mathrm{E}(\Gamma_4, 2) = 2q - 1$.
  (4) $\mathrm{E}(\Gamma_5, 2) = q^2$.
  (5) For $n \geq 6$, $\mathrm{E}(\Gamma_n, 2) = q^{\lceil \frac{n-1}{3} \rceil} + q^{n-1-2\lceil \frac{n-1}{3} \rceil} - 1$.

Thank you