# On the Feng-Rao distance for symmetric semigroups

J.I. Farrán

July 26, 1999

**Abstract**

We present some results on the Feng-Rao distance for symmetric semigroups. Such a distance is known to be a lower bound for the minimum distance of a one-point AG code by considering the Weierstrass semigroup at the corresponding point.

**Key words** – AG codes, Weierstrass semigroups, Feng-Rao distance.

## 1 Introduction

The Feng-Rao distance $\delta_{FR}(m)$ can be defined in terms of arithmetical relations among elements in a semigroup $S$. The value of $\delta_{FR}(m)$ is known for the case of telescopic semigroups (see [4]). Such semigroups are complete intersection, and hence a very special kind of symmetric semigroups.

In this paper, we show some general formulae for the Feng-Rao distance in the case of symmetric semigroups. For instance, we show how the formula

$$\delta_{FR}(m) = \min\{r \in S \mid r \geq m + 1 - 2g\} \qquad [@]$$

holds for most values $m \in S$ with $c \geq m \geq 2c - 1$, $c$ being the conductor of the semigroup $S$, and we also give a formula for the minimum element $m_0 \in S$ such that the formula [@] holds for $m > m_0$ . An estimate for $m_0$ was given for telescopic semigroups in [4].

The Feng-Rao distance is a good estimate for the minimum distance of one-point AG codes, which are defined as follows (see the details in [5]). Consider a non-singular projective algebraic curve $\chi$ defined over a finite field $\mathbb{F}$ such that $\chi$ is irreducible over $\overline{\mathbb{F}}$. Take $n+1$ different $\mathbb{F}$-rational points $P_1, \ldots, P_n$ and $P$ of the curve $\chi$, and take a positive integer $m$. Thus, one can consider the linear map

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

and define the linear code $C(m)$ as the dual space of $Im\,(ev_D)$. Denote by $d(m)$ the minimum distance of the linear code $C(m)$. From the *Riemann-Roch formula* is derived that

$$d(m) \geq m + 2 - 2g \doteq d^*(m)$$

if $2g - 2 < m < n$, where $g$ is the genus of the curve $\chi$. The integer $d^*(m)$ is called Goppa designed minimum distance of $C(m)$.

The main interest of these codes is that they can be decoded efficiently by the majority scheme of Feng and Rao algorithm given in [2], which corrects up to half the Feng-Rao distance of the Weierstrass semigroup $S = \Gamma_P$ of $\chi$ at $P$. More precisely, the procedure corrects up to $\left\lfloor \dfrac{\delta_{FR}(m') - 1}{2} \right\rfloor$ errors, where $m' = \min\{r \in S \mid r > m\}$. In particular, one has $d(m) \geq \delta_{FR}(m')$ [1]. On the other hand, it is known that $\delta_{FR}(m) \geq m + 1 - 2g = d^*(m-1)$ for all $m \in S$.

# 2 Computing the Feng-Rao distance

In the sequel, we consider numerical semigroups, i.e. subsemigroups $S$ of $\mathbb{N}$ such that $\sharp(\mathbb{N} \setminus S) < \infty$ and $0 \in S$. The number $g \doteq \sharp(\mathbb{N} \setminus S)$ is called the *genus* of the semigroup $S$. Since the genus is finite, there exists a (unique) element $c \in S$ such that $c - 1 \notin S$ and $c + l \in S$ for all $l \in \mathbb{N}$. The number $c$ is called the *conductor* of $S$, and one has $c \leq 2g$. Thus, the "last gap" of $S$ is $l_g \doteq c - 1 \leq 2g - 1$, where $k$ is called a gap of $S$ if $k \in \mathbb{N} \setminus S$.

On the other hand, notice that every $m \geq 2g$ is the $(m + 1 - g)$-th element of $S$, that is $\rho_{m+1-g}$ , according to the notations of [4]. Finally, the semigroup $S$ is called *symmetric* when $r \in S$ if and only if $c - 1 - r \notin S$, for all $r \in \mathbb{Z}$. This is equivalent to say $c = 2g$, that is to say $l_g = 2g - 1$.

**Definition 2.1** *For any semigroup $S \subseteq \mathbb{N}$ with $\sharp(\mathbb{N} \setminus S) < \infty$ and $0 \in S$, the Feng-Rao distance of $S$ is defined by the function*

$$\delta_{FR} \;:\; S \longrightarrow \mathbb{N}$$

$$m \mapsto \delta_{FR}(m) \doteq \min\{\nu(r) \mid r \geq m, \;\; r \in S\}$$

*where $\nu$ is the function*

$$\nu \;:\; S \longrightarrow \mathbb{N}$$

$$r \mapsto \nu(r) \doteq \sharp\{(a, b) \in S^2 \mid a + b = r\}$$

With the above notations, the following result summarizes some known facts about the functions $\nu$ and $\delta_{FR}$ for an arbitrary semigroup. One can check the details in [4].

[1] In fact, the idea of bounding the minimum distance with the aid of the Weierstrass semigroup is due to Goppa himself (see [3]).

**Proposition 2.2**

**(i)** $\delta_{FR}(0) = \nu(0) = 1$, *and* $2 \leq \nu(m), \delta_{FR}(m) \leq m+1$ *if* $m \in S \setminus \{0\}$.

**(ii)** $\nu(m) = m + 1 - 2g + D(m)$ *for* $m \geq c$, *where*

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

**(iii)** $\nu(m) = m + 1 - 2g$ *for all* $m \in S$ *with* $m \geq 2c - 1$.

**(iv)** $\delta_{FR}(m) \geq m + 1 - 2g \doteq d^*(m-1)$ *for all* $m \in S$, *and equality holds if moreover* $m \geq 2c - 1$.

In particular, it follows that $\delta_{FR}(m) = \nu(m) = m + 1 - 2g$ for all $m \in S$ such that $D(m) = 0$. On the other hand, since from **(iii)** one has that $\nu$ is an increasing function for $m \geq 2c - 1$ at most, the Feng-Rao distance is finitely determined by the values of $\nu$. In fact, for any $m \in S$ one has

$$\delta_{FR}(m) = \min\{\nu(m), \nu(m+1), \ldots, \nu(m')\}$$

where $m'$ is the least element in $S$ with $m' \geq m$ and such that $\nu(m') = m' + 1 - 2g$. Thus, elements $m' \in S$ with $D(m') = 0$ are interesting for calculations. Other interesting kind of elements in $S$ are those satisfying the equality

$$\delta_{FR}(m) = \min\{r \in S \mid r \geq m + 1 - 2g\} \qquad [@]$$

since the Feng-Rao distance for them is easy to compute in practice.

# 3 Symmetric semigroups

Now we compute the value of $\delta_{FR}(m)$ for many elements $m \in S$, $S$ being a symmetric semigroup. The underlying idea is searching for values $m \in S$ such that either $\delta_{FR}(m) = \nu(m) = d^*(m-1) = m + 1 - 2g$ or the formula [@] is satisfied; this formula will be called "minimum formula" in the sequel. Our results will partially cover lacks of those given in [4]. First, the following theorem provides us with a formula of $\delta_{FR}(m)$ for a certain range of values in $S$.

**Theorem 3.1** *Let $S$ be a symmetric semigroup. Then one has*

$$\delta_{FR}(m) = \nu(m) = m - l_g = m + 1 - 2g = e$$

*for all* $m = 2g - 1 + e$ *with* $e \in S \setminus \{0\}$.

*Proof:*

One easily checks that $D(m) = 0$ for such values. See [1] for an alternative proof in terms of Apéry sets.

□

Notice that theorem 3.1 trivially implies the formula [@] for $m = 2g - 1 + n$ with $n \in S \setminus \{0\}$, since $m + 1 - 2g = n \in S$. Thus, such formula holds for half of the elements in the interval $[c-1, 2c-2]$. However, theorem 3.1 is more precise than [@] for such values.

The "minimum formula" actually holds for many other elements in this interval. In order to show it, we define for each $m \in I \doteq [c, 2c-2]$ two integers $n, q$ given respectively by the equalities

$$m = n + c - 1 \quad , \quad n + q = c - 1$$

Then one has $m = 2c - 2 - q$, and $n \in S$ iff $q \notin S$. Moreover, from proposition 2.2 **(ii)** and the fact that $S$ is symmetric, it follows that

$$\nu(m) = n + \nu(q)$$

where $\nu(q) \doteq 0$ for $q \notin S$ [2].

Assume now that $n \notin S$ and let $n'$ be the least integer in $S$ such that $n' > n$. Consider the element $q'$ given by $n' + q' = c - 1$ and let $\delta = \delta(q) = q - q' = n' - n$ be the distance of $q$ (resp. $n$) to a gap (resp. non-gap) of $S$. Notice that $\delta(q) \leq e_0 - 1$, $e_0$ being the multiplicity of $S$ (that is the minimum of $S \setminus \{0\}$), since the interval $[n, n')$ consists of gaps and there are at most $e_0 - 1$ consecutive gaps in $S$.

**Theorem 3.2** *Let $S$ be a symmetric semigroup and $m \in I = [c, 2c-2]$. With notations as above, one has*

$$\delta_{FR}(m) = \min\{n + \nu(q), n + 1 + \nu(q-1), \ldots, n + \delta - 3 + \nu(q - \delta + 3), n'\} =$$

$$= \min\{\nu(m), nu(m+1), \ldots, \nu(m + \delta - 3), n'\}$$

*In particular, one has $\delta_{FR}(m) \leq n'$.*

*Proof:*

Since $n' \in S$ one has $\nu(c - 1 + n') = n'$; thus, from 2.2 **(iv)** and the definition of the Feng-Rao distance one has

$$\delta_{FR}(m) = \min\{\nu(m), nu(m+1), \ldots, \nu(m + \delta) = n'\}$$

But $\nu(m + \delta - 1) = n' - 1 + \nu(q' + 1) \geq n'$, since $q' + 1 \in S$. Moreover, $\nu(m + delta - 2) = n' - 2 + \nu(q' + 2) \geq n'$, since $q' + 2 \in S \setminus \{0\}$ and therefore $\nu(q' + 2) \geq 2$ (notice that $q'$ can be negative but only in the case $n' = c$, and in this case $q' = -1$). This proves the theorem.

$\square$

[2] In particular, if $n \in S$ one recovers $\nu(m) = n$, what gives a different proof of theorem 3.1.

**Corollary 3.3** *Let $S$ be a symmetric semigroup and $m \in I$. With notations as above, the minimum formula [@] holds for $m$ if and only if one has*

$$\nu(\overline{q}) \geq \delta(\overline{q})$$

*for every $\overline{q}$ in the interval $[q'+3, q]$.*

*In particular, this is satisfied for the cases $n \in S$, $\delta = \delta(q) = 1$ or 2, and when $\delta = 3$ but $q$ is not an irreducible element of $S$ (i.e. a non-zero element of $S$ which is not a sum of two non-zero elements of $S$).*

*Proof:*

It follows from theorems 3.1 and 3.2. Notice that $\nu(q) \geq 3$ if $\delta = 3$ and $q$ is not irreducible.

□

The condition in the above corollary is easy to check, in practice, for many values of $m$ (v.g. those with small values of $q$). However, by using Apéry systems it is always possible both checking this condition and computing $\nu(q)$ (see [1]).

Finally, let $q_0$ be the smallest integer in $S$ such that $\nu(q_0) < \delta(q_0)$, and set $q_0 = c-1$ if such an integer does not exist. From corollary 3.3 one has $q_0 \geq e_0+2$ and $q_0 = e_0+2$ if and only if $e_0, e_0+1, e_0+2 \in S$ and $e_0 > 2$. This happens, for instance, for the symmetric semigroup whose gaps are $1, 2, \ldots, g-1, 2g-1$, with $g \geq 3$. For a general symmetric semigroup, the value of $q_0$ is, in practice, much bigger.

Now, from proposition 2.2 **(iv)**, the minimum formula holds in the interval $[4g-1, \infty)$. In fact, from the above results one deduces the whole interval where this formula is satisfied.

**Corollary 3.4** *For a symmetric semigroup $S$, the minimum formula [@] is satisfied in the interval $(m_0, \infty)$, where $m_0 = 4g-2-q_0$, but it does not hold for $m_0$. In particular, this formula holds for $m \geq 4g-e_0-3$, since $m_0 \geq 4g-e_0-3$.*

*Proof:*

It follows from theorem 3.2, corollary 3.3 and the definition of $q_0$.

□

**Example 3.5**

- *For the semigroup $S = \langle 9, 12, 15, 17, 20, 23, 25, 28\rangle$ one has $c = 32$ and $q_0 = 25$, thus [@] is satisfied for $m \geq 38$.*

- *For the semigroup* $S = \langle 6, 8, 10, 17, 19 \rangle$ *one has* $c = 22$ *and* $q_0 = 19$*, thus* [@] *is satisfied for* $m \geq 24$*.*
- *For the semigroup* $S = \langle 8, 10, 12, 13 \rangle$ *one has* $c = 28$ *and* $q_0 = 25$*, thus* [@] *is satisfied for* $m \geq 31$*.*
- *For the semigroup* $S = \langle 6, 10, 15 \rangle$ *one has* $c = 30$ *and* $q_0 = 29$*, thus* [@] *is satisfied for* $m \geq 30$*.*

**Remark 3.6** *One can apply the above results for concrete examples of symmetric semigroups as complete intersection or telescopic. In principle, one would expect that the results of [4] can be improved with the aid of our formulas, which should be more explicit for such semigroups.*

*For example, if* $S$ *is generated by a telescopic sequence* $\{\delta_0, \delta_1, \ldots, \delta_h\}$*, and we assume moreover that* $\delta_h = \max\{\delta_0, \delta_1, \ldots, \delta_h\}$*, then the minimum formula* [@] *is true for every* $m \in [c, 2c-2]$ *in the interval* $[(4g-1)-(d_h-1)\delta_h, 4g-1)$*, i.e. one has* $q_0 \geq (d_h-1)\delta_h$ *. Also one has* $\delta_{FR}(m) = j+1$ *if* $(j-1)\delta_h < m \leq j\,\delta_h \leq (d_h-1)\delta_h$ *(see [4]). Hence, the Feng-Rao distance is unknown in general for the interval* $[(d_h-1)\delta_h + 1, (4g-2)-(d_h-1)\delta_h]$*.*

*This result is improved by corollary 3.4. For example, the telescopic semigroup* $S = \langle 8, 10, 12, 13 \rangle$ *the formula* [@] *is satisfied from* $m = 31$ *instead of* $m = 42$*, and for the telescopic semigroup* $S = \langle 6, 10, 15 \rangle$ *the formula* [@] *is satisfied from* $m = 30$ *instead of* $m = 44$*. Finally, notice also that one has*

$$\nu\left(\sum_{k=1}^{h} \lambda_k \delta_k\right) = (\lambda_1 - 1)(\lambda_2 - 1)\ldots(\lambda_h - 1)$$

# References


[1] A. Campillo and J.I. Farrán, *Computing Weierstrass semigroups and the Feng-Rao distance from singular plane models*, to appear in *Finite Fields and their Applications*.

[2] G.L. Feng and T.R.N. Rao, *Decoding algebraic-geometric codes up to the designed minimum distance*, IEEE Trans. Inform. Theory **39**, pp. 37-45 (1993).

[3] V.D. Goppa, *Geometry and codes*, Kluwer Academic Publishers (1988).

[4] C. Kirfel and R. Pellikaan, *The minimum distance of codes in an array coming from telescopic semigroups*, IEEE Trans. Inform. Theory **41**, pp. 1720-1732 (1995).

[5] M.A. Tsfasman and S.G. Vlăduţ, *Algebraic-geometric codes*, Math. and its Appl., vol. 58, Kluwer Academic Pub., Amsterdam (1991).