

On the weight distribution of hermitian codes

Marco Pellegrini

April 20, 2006

Hermitian codes are very interesting AG codes; they have a lot of good properties. They can be defined as follows:

Let q be a power of a prime, F the field \mathbb{F}_{q^2} ; the *hermitian curve* \mathcal{H} is the curve defined over F by the affine equation

$$x^{q+1} = y^q + y \tag{1}$$

This curve has genus $g = q(q - 1)/2$ and has $n = q^3$ rational points, denoted by P_1, \dots, P_n ; more precisely, for each $x \in F$, the equation (1) has exactly q distinct solutions in F . The curve has also one point at infinity Q , so that it has $q^3 + 1$ points rational over F , that is the maximum allowed by Weyl bound for a curve X defined over a field \mathbb{F}_a :

$$|X(\mathbb{F}_a)| \leq 1 + a + 2g\sqrt{a}$$

Let m an integer such that $0 \leq m \leq n + 2g - 2 = q^3 + q^2 - q - 2$; we can define the *hermitian code* $C(q, m)$ using the general Goppa construction: let $D = \sum_{i=1}^n P_i$ and $G = mQ$, so that D and G have disjoint support; let $L(G)$ be the vector space of rational function on \mathcal{H} , whose divisor of poles is bounded by G ; then $C(q, m)$ is defined by

$$C(q, m) = \{(f(P_1), \dots, f(P_n)) \in F^n \mid f \in L(G)\}$$

So we obtain codes over F of length n ; the dimension k and the minimum distance d can easily be determined. For $m < 0$ the code has only the zero word, and for $m > q^3 + q^2 - q - 2$ the code is equal to the whole F^n . Notice that for each k such that $0 < k < n$ there is a (non-trivial) hermitian code with length n and dimension k .

The vector space $L(mQ)$ can be generated by a set of monomial functions

$$\{x^r y^s \mid qr + (q + 1)s \leq m\}$$

in order to obtain a basis, using the equation (1), we can suppose $0 \leq s \leq q - 1$, so that

$$L(mQ) = \langle x^r y^s \mid qr + (q + 1)s \leq m, r \geq 0, 0 \leq s \leq q - 1 \rangle$$

this allows us to easily write generator matrices. Moreover, we have that $C(q, m)^\perp = C(q, q^3 + q^2 - q - 2 - m)$, so that the parity check matrix of a hermitian code is the transposed of the generator matrix of another hermitian code, thus we can easily write it.

Despite of all these good properties, the problem of finding the weight distribution of hermitian codes is computationally very hard. We propose a new approach, that was successfully used for cyclic codes, and we think that it can be extended to other AG codes. Using the parity check matrix, for each integer w such that $0 \leq w \leq n$, we write a system of polynomial equations, whose solutions are exactly all the codewords of weight w of a hermitian code. We don't attempt to solve the system, but computing a Gröbner basis for the 0-dimensional ideal I generated by the polynomials of the system, and then computing the dimension of the ring of polynomials modulo I , we obtain the number of solutions of the system, from which we obtain the number of codewords of weight w . Here is how it's done.

Consider the parity check matrix H of a hermitian code C , that is the $n \times (n - k)$ matrix such that for any $z \in F^n$ we have

$$z \in C \Leftrightarrow zH = 0$$

Since H is the transposed of the generator matrix of a hermitian code, we know that

$$H = \begin{pmatrix} g_1(P_1) & \dots & g_{n-k}(P_1) \\ \dots & \dots & \dots \\ g_1(P_n) & \dots & g_{n-k}(P_n) \end{pmatrix}$$

where functions g_j are the $n - k$ monomials of the form $x^r y^s$ that generate the vector space associated to the code of dimension $n - k$. We define $S = \{g_1, \dots, g_{n-k}\}$. So the condition $zH = 0$ can be written as

$$\forall j = 1, \dots, n - k \quad \sum_{i=1}^n z_i g_j(P_i) = 0 \quad (2)$$

Now suppose that a codeword z has weight w ; we denote by z_1, \dots, z_w the non-zero coordinates of z . Then the system to find all codewords of weight w is

$$\forall (r, s) \mid x^r y^s \in S \quad \sum_{i=1}^w z_i x_i^r y_i^s = 0 \quad (3)$$

$$\forall i = 1, \dots, w \quad x_i^{q+1} - y_i^q - y_i = 0 \quad (4)$$

$$\forall i = 1, \dots, w \quad z_i^{q^2-1} - 1 = 0 \quad (5)$$

$$\forall i = 1, \dots, w \quad x_i^{q^2} - x_i = 0 \quad (6)$$

$$\forall i = 1, \dots, w \quad y_i^{q^2} - y_i = 0 \quad (7)$$

$$\forall (i, j) \mid i \neq j \quad ((x_i - x_j)^{q^2-1} - 1)((y_i - y_j)^{q^2-1} - 1) = 0 \quad (8)$$

Equations (3) are the same as (2), since in the sum we can omit the zero terms. Equations (4) indicate that every point (x_i, y_i) belongs to \mathcal{H} . Equations (5) indicate that every z_i belongs to F and is different from 0. Equations (6) and (7) indicate, respectively, that every x_i and every y_i belongs to F . Note that we can eliminate equations (7), because all the q solutions y_i of (4) belong to F . However, we still need equations (5) and (6), called *field equations*, to ensure that the ideal I be 0-dimensional.

Finally, we need equations (8) to eliminate improper solutions that don't correspond to any codeword. In fact, we can associate a codeword to a solution of the system in the following way: let $(x_1, \dots, x_w, y_1, \dots, y_w, z_1, \dots, z_w)$ be a solution; for each $i = 1, \dots, w$, the point (x_i, y_i) is a point P_{r_i} of \mathcal{H} , with $1 \leq r_i \leq n$. If all P_{r_i} are different, we can construct a codeword that has the (non-zero) value z_i at the position r_i , and 0 at other positions, thus this is a codeword of weight w ; but if for $i \neq j$ we have $P_{r_i} = P_{r_j}$, that is $x_i = x_j$ and $y_i = y_j$, we cannot set the w values z_i in w different positions, thus we cannot obtain a codeword of weight w . To avoid this situation, we need that for each (i, j) , with $i \neq j$, we have $P_{r_i} \neq P_{r_j}$, that is $x_i \neq x_j$ or $y_i \neq y_j$, that is $x_i - x_j$ or $y_i - y_j$ are non-zero elements of F , and this gives us equations (8).

In this way, to each solution of the system we can associate a codeword, and vice versa. Of course, different codewords correspond to different solutions. But if we take a solution of the system and we make a permutation of indexes $1, \dots, w$, we have a different solution (because all P_{r_i} are distinct) that correspond to the same codeword. So, to get the exact number of codewords of weight w , we need to divide the number of solutions of the system by $w!$.

Now the problem is to compute the number of solutions of the system (3-8). We used the Singular computer algebra system to find a Gröbner basis for the ideal I generated by the polynomials of the system, and to compute the dimension of the ring of polynomials modulo I .

Here there is the weight distribution of all hermitian codes with $q = 2$ (we have $n = 8$):

code \ weight	k	0	1	2	3	4	5	6	7	8
$C(2, 0)$	1	1	0	0	0	0	0	0	0	3
$C(2, 2)$	2	1	0	0	0	0	0	12	0	3
$C(2, 3)$	3	1	0	0	0	0	24	12	24	3
$C(2, 4)$	4	1	0	0	0	18	96	24	96	21
$C(2, 5)$	5	1	0	0	24	90	240	264	312	93
$C(2, 6)$	6	1	0	12	96	390	768	1356	1056	417
$C(2, 7)$	7	1	0	84	336	1470	3360	5124	4368	1641

And here there is a part of the weight distribution for some codes with $q = 4$:

code \ weight	k	0	1	2	3	4	...
...
$C(4, 59)$	54	1	0	0	0	0	...
$C(4, 60)$	55	1	0	0	0	240	...
$C(4, 61)$	56	1	0	0	0	240	...
$C(4, 62)$	57	1	0	0	0	240	...
$C(4, 63)$	58	1	0	0	0	14640	...
$C(4, 65)$	59	1	0	0	960	17520	...
$C(4, 66)$	60	1	0	0	960	490320	...
$C(4, 67)$	61	1	0	0	29760	7949520	...
$C(4, 70)$	62	1	0	1440	551040	125745840	...
$C(4, 71)$	63	1	0	30240	8749440	2010965040	...

The main problem of this approach is that the time necessary to find a Gröbner basis grows up with the number of variables of the equations, that is $3w$. We tried to decompose the set of solutions, adding equations like $x_i = 0$ or $x_i^{\frac{q^2-1}{p-1}} = a$, where p is the characteristic of F and a is a non-zero element of the prime field of F , and writing different systems to cover all possibilities; this can be done cleanly because, even if the variables are in F , the coefficients of the equations are all in the prime field; this reduced the total time needed to compute some values of the table for $q = 4$ by a factor $10^3 \sim 10^4$.

The author thanks his supervisors: C. Traverso and M. Sala.

Marco Pellegrini
Dipartimento di Matematica
Largo Bruno Pontecorvo 5
56127 Pisa
Italy
e-mail: pellegrini@mail.dm.unipi.it