LE MATEMATICHE
Vol. LX (2005) – Fasc. I, pp. 3–12

GEOMETRIC GOPPA CODES ON FERMAT CURVES

ANTONINO GIORGIO SPERA

We consider a class of codes defined by Goppa's algebraic-geometric construction on Fermat curves. Automorphisms and decoding of such codes are investigated.

1. Introduction.

This paper is concerned with Geometric Goppa codes, nowadays also called algebraic-geometric codes, which were introduced by V.D. Goppa in 1977 ([5], [6]) using algebraic curves over finite fields. We construct a class of such codes associated with some Fermat curves. Precisely, if q is a prime power and $\mathbf{F}_q$ denotes the finite field of order q, we take into consideration Fermat curves over $\mathbf{F}_q$ of degree m with $q \equiv 1 \pmod{6m}$. Such a curve $\mathbf{C}_m$ is absolutely irreducible and smooth. The case where $m = \frac{q-1}{s}$, s is a positive integer which is divisible by 6 and (q, s) is a circular pair (see [1] and [10]), was considered by H. Kiechle in [10] where the $\mathbf{F}_q$-rational points were determined. We investigate, in section 3, the automorphisms of $\mathbf{C}_m$ showing that each of them is defined over $\mathbf{F}_q$. Moreover we analyse the orbits of the automorphism group of $\mathbf{C}_m$ on the $\mathbf{F}_q$-rational point set of $\mathbf{C}_m$. There are at

Entrato in redazione il 27 Febbraio 2003.

2000 Methematics Subject Classification: Primary 94B27, Secondary 11G20.

Key words:Code,Curve, Finite field, Automorphism.

Research supported by the Italian MURST (progetto 40% ”Strutture geometriche, combinatoria e loro applicazione”).

least two orbits V_1 and V_2 which have order $3m$ and $2m^2$ respectively. Next, considering the rational divisors $D = \sum_{i=1}^{2m^2} P_i$ and $A = r(\sum_{j=1}^{3m} Q_j)$, where $V_1 = \{Q_1, Q_2, ..., Q_{3m}\}$, $V_2 = \{P_1, P_2, \ldots, P_{2m^2}\}$ and r is a positive integer, we obtain a linear code which admits an automorphism group of order $6m^2$. Furthermore this group has a subgroup which is regular on $suppD$. In section 4, using the automorphisms of the code, we are able to embed the code as a left ideal of a group algebra in order to get an easy decoding of the constructed code.

2. Notations and basic results.

Let $\mathbf{F}_q$ be the finite field of order $q = p^l$, where p is a prime number and l a positive integer. Suppose $\mathbf{X}$ is an absolutely irreducible, non-singular, projective curve defined over $\mathbf{F}_q$ and let $g(\mathbf{X})$ be its genus. We denote by $Aut(\mathbf{X})$ the automorphism group of $\mathbf{X}$ and by $Aut_{\mathbf{F}_q}(\mathbf{X})$ the subgroup of $Aut(\mathbf{X})$ of $\mathbf{F}_q$-automorphisms of $\mathbf{X}$.

It is known that $Aut(\mathbf{X})$ always is finite if $g(\mathbf{X}) > 1$ (see [11]) and H. Stichtenoth proved the following result.

Theorem 2.1 ([16])**.** *If* $\mathbf{X}$ *is not the Hermitian curve and* $g(\mathbf{X}) > 1$ *then* $|Aut(\mathbf{X})| \leq 16\, g(\mathbf{X})^4$.

Suppose m is a positive integer, $m > 1$, which is relatively prime to p. The Fermat curve of degree m over $\mathbf{F}_q$ is the projective plane curve $\mathbf{C}_m$ defined by the homogeneous equation

$$X^m + Y^m = Z^m \tag{1}$$

A Fermat curve of degree $q+1$ is called Hermitian curve.
Since p does not divides m, $\mathbf{C}_m$ is easily seen to be absolutely irreducible and non-singular, so its genus is

$$g(\mathbf{C}_m) = \frac{1}{2}(m-1)(m-2)$$

Theorem 2.2. ([11]). *Let* $q = p^l$, $m \geq 4$ *a positive integer with* $(m, p) = 1$ *and* $\mathbf{C}_m$ *the Fermat curves of degree* m.

i) If $m \neq q+1$, *then* $|Aut(\mathbf{C}_m)| = 6m^2$.
ii) If $m = q+1$, *then* $|Aut(\mathbf{C}_m)| = q^3(q^2-1)(q^3+1)$, $Aut(\mathbf{C}_m) = Aut_{\mathbf{F}_{q^2}}(\mathbf{C}_m)$ *and it is isomorphic to the projective unitary group* $PGU(3, q^2)$.

Note that in the $ii)$ case of the above theorem, $\mathbf{C}_m$ is an Hermitian curve.

For a curve $\mathbf{X}$ over $\mathbf{F}_q$, $\mathbf{X}(\mathbf{F}_q)$ denotes the set of $\mathbf{F}_q$-rational points of $\mathbf{X}$ and $N(\mathbf{X})$ the cardinality of $\mathbf{X}(\mathbf{F}_q)$. The well-known Hasse-Weil bound states that

$$|N(\mathbf{X}) - (q+1)| \leq 2\, g(\mathbf{X})\sqrt{q}. \tag{2}$$

$\mathbf{X}$ is said to be a maximal curve if the upper bound in (2) is attained. It is known (see [13], [7]) that Hermitian curves are the only maximal curves of genus $\frac{1}{2}(q-1)q$ over $\mathbf{F}_{q^2}$. For some Fermat curves Garcia and Voloch gave in [4] an upper bound which is better than Hasse-Weil bound.

Consider the Fermat curve $\mathbf{C}_m$ over $\mathbf{F}_q$ and suppose that $q \equiv 1 \pmod{6m}$. Then $(\mathbf{F}_q)^* = \mathbf{F}_q \backslash \{0\}$ has some element of order $6m$. If β is a such element, we set

$$\begin{gathered} V_1 = \{(\beta^{6i}, 0, 1) | i = 0, 1, ..., m-1\} \cup \\ \{(0, \beta^{6i}, 1) | i = 0, 1, ..., m-1\} \cup \\ \{(\beta^{6i+3}, 1, 0) | i = 0, 1, ..., m-1\} \; and \\ V_2 = \{(1, \beta^{6i+2}, \beta^{6j+1}) | i, j = 0, 1, ..., m-1\} \cup \\ \{(1, \beta^{6i-2}, \beta^{6j-1}) | i, j = 0, 1, ..., m-1\}. \end{gathered}$$

It easy to show that $V_1 \cup V_2 \subseteq \mathbf{C}_m(\mathbf{F}_q)$.

Now let $s \geq 2$ be an integer and q, as before, a power of a prime number. The ordered pair (q, s) is said to be circular (see [1]) if s divides $q-1$ and the subgroup Φ of $(\mathbf{F}_q)^*$ of order s satisfies

$$|(\Phi a + b) \cap (\Phi c + d)| \leq 2$$

for all $a, b, c, d \in \mathbf{F}_q$ with $\Phi a \neq \Phi c$ or $b \neq d$.

For example, it is known that the pair $(q^2, q+1)$ is circular for every prime power q. For more information and tables on circular pairs see [1]. For a circular pair (q, s), consider the Fermat curve $\mathbf{C}_m$ of degree $m = \frac{q-1}{s}$. It was proved (see [9] and [10]) that if 6 divides s (and so $q \equiv 1 \pmod{6m}$), then $\mathbf{C}_m$ has exactly $n = 2m^2 + 3m$ rational points over $\mathbf{F}_q$. More precisely, there was shown the following result.

Theorem 2.3. *Let (q, s) be a circular pair, $m = \frac{q-1}{s}$ and suppose that 6 divides s. Then the set of $\mathbf{F}_q$-rational points $\mathbf{C}_m(\mathbf{F}_q)$ of the Fermat curve $\mathbf{C}_m$ is $\mathbf{C}_m(\mathbf{F}_q) = V_1 \cup V_2$.*

Now we recall some basic facts about geometric Goppa codes (cf. [5], [12], [14]). Let $\mathbf{X}$ be an (absolutely irreducible, smooth, projective) curve over $\mathbf{F}_q$. If $P_1, P_2, ..., P_n$ are n pairwise distinct rational points of $\mathbf{X}$, let D be the divisor defined by

$$D = P_1 + P_2 + ... + P_n$$

and A be a rational divisor on $\mathbf{X}$ with $suppD \cap suppA = \emptyset$. Moreover, if $\mathbf{F}_q(\mathbf{X})$ denotes the field of $\mathbf{F}_q$-rational functions on $\mathbf{X}$, set

$$L(A) = \{z \in \mathbf{F}_q(\mathbf{X})^* \mid div(z) \geq -A\} \cup \{0\}.$$

Here as usual, $div(z)$ denotes the principal divisor associated with the function z. The geometric Goppa code $C(A, D)$ associated with A and D is defined by

$$C(A, D) = \{(z(P_1), z(P_2), ..., z(P_n)) \mid z \in L(A)\}.$$

With this notations we have (see [12] or [14]) the following theorem.

Theorem 2.4. *If* $2g(\mathbf{X}) - 2 < degA < n$*, then* $C(A, D)$ *is a* q*-ary* $[n, k, d]$*-linear code where* $k = degA + 1 - g(\mathbf{X})$ *and* $d \geq n - degA$.

It is known that the symmetric group S_n acts on $\mathbf{F}_q^n$ in the following way:

$$\tau(a_1, a_2, ..., a_n) = (a_{\tau(1)}, a_{\tau(2)}, ..., a_{\tau(n)})$$

for every $\tau \in S_n$ and $(a_1, a_2, ..., a_n) \in \mathbf{F}_q^n$. We define the automorphism group of the code $C(A, D)$ by

$$Aut(C(A, D)) = \{\tau \in S_n \mid \tau(c) \in C(A, D) \;\; for \;\; every \;\; c \in C(A, D)\}.$$

The group $Aut_{\mathbf{F}_q}(\mathbf{X})$ acts on the rational divisor group $Div(\mathbf{X})$ of $\mathbf{X}$ via

$$\rho(\sum n_p P) = \sum n_p \rho(P)$$

if $\sum n_p P \in Div(\mathbf{X})$ and $\rho \in Aut_{\mathbf{F}_q}(\mathbf{X})$. So the stabilizer of A and D,

$$(Aut_{\mathbf{F}_q}(\mathbf{X}))_{A,D} = \{\rho \in Aut_{\mathbf{F}_q}(\mathbf{X}) \mid \rho(D) = D \; and \; \rho(A) = A\},$$

is a subgroup of $Aut_{\mathbf{F}_q}(\mathbf{X})$ and each of its elements ρ induces an automorphism of $C(A, D)$ by

$$\rho(x(P_1), x(P_2), ..., x(P_n)) = (x(\rho(P_1)), x(\rho(P_2)), ..., x(\rho(P_n)))$$

where $(x(P_1), x(P_2), ..., x(P_n)) \in C(A, D)$. Moreover, it was shown in [15] (see also [14]) the following result.

Theorem 2.5.

a) If $n > 2\,g(\mathbf{X}) + 2$, then $(Aut_{\mathbf{F}_q}(\mathbf{X}))_{A,D}$ is isomorphic to a subgroup of $Aut(C(A, D))$.

b) If $g(\mathbf{X}) = 0$, $A > 0$ and $deg A \leq n - 3$, then $Aut(C(A, D))$ is isomorphic to $(Aut_{\mathbf{F}_q}(\mathbf{X}))_{A,D}$. So, being $Aut_{\mathbf{F}_q}(\mathbf{X})$ isomorphic to the projective linear group $PGL(2, q)$, any automorphism of $C(A, D)$ is induced by a projective linear map.

3. Fermat codes.

First we determine the automorphisms of a Fermat curve $\mathbf{C}_m$ over $\mathbf{F}_q$ in the case where $q \equiv 1 \pmod{6m}$, showing that each of them is defined over $\mathbf{F}_q$. As in section 2, let $\beta \in \mathbf{F}_q^*$ be a element of order $6m$ and consider the projective linear transformation σ associated with the matrix

$$\begin{pmatrix} 0 & \beta^3 & 0 \\ 0 & 0 & \beta^6 \\ 1 & 0 & 0 \end{pmatrix}.$$

Suppose $P = (a, b, c)$ is a points of $\mathbf{C}_m$. We have that $\sigma(P) = (\beta^3 b, \beta^6 c, a)$ is on $\mathbf{C}_m$ too. In fact, $(\beta^3 b)^m) + (\beta^6 c)^m = a^m$ if and only if $\beta^{3m} b^m + c^m = a^m$ if and only if $P \in \mathbf{C}_m$ being $\beta^{3m} = -1$. So $\sigma \in Aut_{\mathbf{F}_q}(\mathbf{C}_m)$. Of course if α is the projective linear transformation that switches a and b in each point (a, b, c) of the plane, α is a $\mathbf{F}_q$-automorphism of $\mathbf{C}_m$ and the group $H = \langle \alpha, \sigma \rangle$ is a $\mathbf{F}_q$-automorphism group of $\mathbf{C}_m$. Moreover, since α and σ have order two and three respectively, it is easy to see that $H = \langle \alpha, \sigma \rangle$ is isomorphic to the symmetric group S_3. Consider now the projective linear transformation $\gamma(i, j)$, i,j = 0,1,...,m-1, associated with the matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \beta^{6i} & 0 \\ 0 & 0 & \beta^{6j} \end{pmatrix}.$$

Since $\gamma(i, j)(P) = (a, \beta^{6i} b, \beta^{6j} c)$ if $P = (a, b, c)$, we have that $P \in \mathbf{C}_m$ if and only if $\gamma(i, j)(P) \in \mathbf{C}_m$. So

$$L = \{\gamma(i, j) \mid i, j = 0, 1, ..., m - 1\}$$

is clearly an abelian group of $\mathbf{F}_q$-automorphisms of $\mathbf{C}_m$ of order m^2. Since H normalises L and $H \cap L = \{1\}$, we get $\bar{G} = HL$ is a $\mathbf{F}_q$-automorphism group of $\mathbf{C}_m$ of order $6m^2$. Now by i) of the Theorem 2.2, we have that

$$Aut(\mathbf{C}_m) = \bar{G} = HL \tag{3}$$

being $m \neq q + 1$; so $Aut(\mathbf{C}_m) = Aut_{\mathbf{F}_q}(\mathbf{C}_m)$. Therefore we get the following proposition.

Proposition 3.1. *Let $\mathbf{C}_m$ be a Fermat curve over $\mathbf{F}_q$ of degree $m \geq 4$ such that $q \equiv 1$ (mod $6m$). Then $Aut(\mathbf{C}_m) = Aut_{\mathbf{F}_q}(\mathbf{C}_m)$.*

With notations as above we set

$$G = \langle \alpha, L \rangle.$$

Let $\mathbf{C}_m(\mathbf{F}_q)$ be the set of $\mathbf{F}_q$-rational points of $\mathbf{C}_m$ and suppose again that $q \equiv 1$ (mod $6m$). Then $\mathbf{C}_m(\mathbf{F}_q) \supseteq V_1 \cup V_2$ where V_1 and V_2 are as in section 2.

Proposition 3.2. *Let q, m and $\mathbf{C}_m$ be as in the previous proposition. Then $Aut(\mathbf{C}_m)$ admits at least two orbits on $\mathbf{C}_m(\mathbf{F}_q)$, namely V_1 and V_2. Moreover, G is a subgroup of $Aut(\mathbf{C}_m)$ which is regular on V_2.*

Proof. By (3) we have $Aut(\mathbf{C}_m) = \bar{G} = HL$ where $H = \langle \alpha, \sigma \rangle$ and $L = \{\gamma(i, j) \mid i, j = 0, 1, ..., m-1\}$. Consider the point $P = (1, \beta^2, \beta) \in V_2$. Since $\gamma(i, j)(P) = (1, \beta^{6i+2}, \beta^{6j+1})$ and $\alpha\gamma(i, j)(P) = (\beta^{6i+2}, 1, \beta^{6j+1}) = (1, \beta^{6(m-i)-2}, \beta^{6(m-i+j)-1})$ for every $\gamma(i, j) \in L \subset \bar{G}$, we have that V_2 is contained in the $\bar{G}$-orbit $P^{\bar{G}}$ of P. Moreover the stabilizer $\bar{G}_P$ of P is the subgroup generated by the automorphism $\sigma\gamma(m-1, m-1)$ which has order 3. So $P^{\bar{G}} = V_2$ being $|P^{\bar{G}}| = \frac{|\bar{G}|}{|\bar{G}_P|} = \frac{6m^2}{3} = 2m^2 = |V_2|$. Now it is easy to see that the subgroup $M = \{\gamma(j, j) \mid j = 0, 1, ..., m-1\}$ of $\bar{G}$ acts regularly on the points set $\Delta_1 = \{(\beta^{6i}, 0, 1) \mid i = 0, 1, ..., m-1\}$ and so Δ_1 and $\alpha(\Delta_1)$ are contained in the same $\bar{G}$-orbit of $\bar{G}$. But M is also regular on $\Delta_2 = \{(\beta^{6i+3}, 1, 0) \mid i = 0, 1, ..., m-1\}$ and, as $\sigma((\beta^3, 1, 0)) = (1, 0, 1) \in \Delta_1$, we get V_1 is contained in the orbit $Q^{\bar{G}}$ where $Q = (1, 0, 1)$. Further the stabilizer of Q is $\bar{G}_Q = T \cup S$ where $T = \{\gamma(i, 0) \mid i = 0, 1, ..., m-1\}$ and $S = \{\alpha\sigma\gamma(i, m-1) \mid i = 0, 1, ..., m-1\}$. So $|\bar{G}_Q| = 2m$ being $T \cap S = \emptyset$. Hence $|Q^{\bar{G}}| = \frac{|\bar{G}|}{|\bar{G}_Q|} = \frac{6m^2}{2m} = 3m$ and we obtain that $Q^{\bar{G}} = V_1$. Now the group $G = \langle \alpha, L \rangle$ is regular on V_2 since $G \subseteq \bar{G}$, $G \cap \bar{G}_P = 1$ and $|G| = 2m^2$. $\square$

In the following for $\mathbf{C}_m$ we always suppose that $q \equiv 1$ (mod $6m$). We now construct a class of geometric Goppa codes on Fermat curves which admit enough large groups of automorphisms. Consider the subsets of rational points V_1 and V_2 of $\mathbf{C}_m$ and let $N = 2m^2$ and

$$D = \sum_{i=1}^{N} P_i$$

where $P_1, P_2, ..., P_N$ are the points of V_2 in a fixed order. Further we consider the divisor $A = r \sum Q_j$ where the Q_j's are the points of V_1 and r is a positive integer. Thus we have $deg A = 3rm$ and for

$$\frac{m}{3} - 1 < r < 2\frac{m}{3}$$

the geometric Goppa code $C(A, D)$ has parameters (see Theorem 2.4) N, k, d with

$$k = 3rm + 1 - \frac{(m-1)(m-2)}{2} \quad and \quad d \geq m(2m - 3r).$$

In the following we will denote the constructed q-ary linear code $C(A, D)$ by $C(r, m)$.

Example 3.3. If we consider the Fermat curve $\mathbf{C}_4$ defined over $\mathbf{F}_{25}$, then $C(r, 4)$ is a 25-[32,10,20]-code for $r = 1$ and a 25-[32,22,8]-code for $r = 2$. In the first case is not difficult to show that the following ten functions

$$1, \frac{x}{y}, \frac{x}{z}, \frac{y}{z}, \frac{y}{x}, \frac{z}{x}, \frac{z}{y}, \frac{y^2}{xz}, \frac{z^2}{xy}, \frac{x^2}{yz}$$

form a basis for the space $L(A)$. So it is possible to have a generator matrix for the code $C(1, 4)$.

Theorem 3.4. *If $m \geq 4$ and $\frac{m}{3} - 1 < r < 2\frac{m}{3}$, then the q-ary code $C(r, m)$ constructed on the Fermat curve $\mathbf{C}_m$ admits an automorphism group of order $6m^2$ which is isomorphic to $Aut(\mathbf{C}_m)$. Moreover it has a subgroup acting regularly on $suppD$.*

Proof. Let $\mathbf{C}_m$ be the Fermat curve with $q \equiv 1 \pmod{6m}$. By Proposition 3.1 $Aut(\mathbf{C}_m) = Aut_{\mathbf{F}_q}(\mathbf{C}_m)$ and, by Theorem 2.2, $|Aut(\mathbf{C}_m)| = 6m^2$ since $m \geq 4$. Moreover by Proposition 3.2, $Aut_{\mathbf{F}_q}(\mathbf{C}_m) = (Aut_{\mathbf{F}_q}(\mathbf{C}_m))_{A,D}$ since $suppD = V_2$ and $suppA = V_1$. Now, $N = 2m^2 > (m-1)(m-2) + 2 = 2g(\mathbf{C}_m) + 2$ and so, by a) of Theorem 2.5, $Aut_{\mathbf{F}_q}(\mathbf{C}_m) = (Aut_{\mathbf{F}_q}(\mathbf{C}_m))_{A,D}$ is, up to isomorphism, a subgroup of the automorphism group of $C(r, m)$. Now, by Proposition 3.2, the subgroup G of $Aut_{\mathbf{F}_q}(\mathbf{C}_m)$ is regular on $suppD = V_2$. □

Remark 3.5. We note that in the case where (q, s) is a circular pair with $s = 6s'$ for some integer s' and $m = \frac{q-1}{s} \geq 4$, then by Theorem 2.3 $\mathbf{C}_m(\mathbf{F}_q) = V_1 \cup V_2$ and so the q-ary code $C(r, m)$ constructed in the above theorem cannot be enlarged further.

4. Decoding.

In order to have an easy decoding for our codes, we will embed them into group algebras.
Let $C(r, m)$ be the code constructed in the previous section where $\frac{m-3}{3} < r < \frac{2m}{3}$, $m =\geq 4$ and $q \equiv 1 \pmod{6m}$. Moreover consider the automorphism group G of $C(r, m)$ which is regular on suppD (see Theorem 3.4). The vector space $\mathbf{F}_q^N$ is isomorphic to $\mathbf{F}_q[G]$ since $|G| = N$ being G regular on $suppD = \{P_1, P_2, ..., P_N\}$. For every $i = 1, 2, ..., N$ let ρ_i be the unique element of G such that $\rho_i(P_1) = P_i$. Now we consider the $\mathbf{F}_q$-linear isomorphism $\phi : \mathbf{F}_q^N \longrightarrow \mathbf{F}_q[G]$, defined by

$$\phi(a_1, a_2, ..., a_N) = \sum_{i=1}^{N} a_i \rho_i \tag{4}$$

for every $(a_1, a_2, ..., a_N) \in \mathbf{F}_q^N$. So we can identify our code $C(r, m)$ to $\phi(C(r, m)) = \{\sum_{i=1}^{N} x(P_i)\rho_i \mid x \in L(A)\}$. After this identification we have that G acts on $\phi(C(r, m))$ in the following way

$$\rho(\sum_{i=1}^{N} x(P_i)\rho_i) = \sum_{i=1}^{N} x(\rho P_i)\rho_i \tag{5}$$

for every $\rho \in G$ and $\sum_{i=1}^{N} x(P_i)\rho_i \in \phi(C(r, m))$. Now we are able to prove the following

Proposition 4.1. *The code $C(r, m)$ is, up to isomorphism, a left ideal in the group algebra $\mathbf{F}_q[G]$.*

Proof. We will prove that $\phi(C(r, m))$ is a left ideal of the group algebra $\mathbf{F}_q[G]$. In order to show this it is enough to prove that $\rho \circ \sum_{i=1}^{N} x(P_i)\rho_i \in \phi(C(r, m))$ for any $\rho \in G$ and $\sum_{i=1}^{N} x(P_i)\rho_i \in \phi(C(r, m))$ where $\circ$ denotes the multiplication in $\mathbf{F}_q[G]$. But

$$\rho \circ \sum_{i=1}^{N} x(P_i)\rho_i = \sum_{i=1}^{N} x(P_i)(\rho\rho_i) = \sum_{i=1}^{N} x(\rho_i P_1)(\rho\rho_i) \tag{6}$$

and if we set $\rho_j = \rho\rho_i$ then $\rho_i = \rho^{-1}\rho_j$ and so from (5) we get $\rho \circ \sum_{i=1}^{N} x(P_i)\rho_i = \sum_{j=1}^{N} x(\rho^{-1}\rho_j P_1)\rho_j = \sum_{j=1}^{N} x(\rho^{-1}P_j)\rho_j = \rho^{-1}(\sum_{j=1}^{N} x(P_j)\rho_j) \in \phi(C(r, m))$ because of (4) and $\rho^{-1} \in G$. $\square$

Now we are able to give a easy decoding of $C(r, m)$ in the case where $p \neq 2$. In fact in this case the group algebra $\mathbf{F}_q[G]$ considered above is semisimple by Maschke's theorem because of $char\mathbf{F}_q = p$ does not divide $|G| = 2m^2 = 2\frac{(q-1)^2}{s^2}$. Thus any left ideal of $\mathbf{F}_q[G]$ is generated by an idempotent (see for instance [2]). Let $\phi(C(r, m))$ be generated by the idempotent e and consider its orthogonal idempotent $u = 1 - e$. An element $c \in \phi(C(r, m))$ if and only if $c \circ u = 0$. If we define the syndrome as the map $S : \mathbf{F}_q[G] \longrightarrow \mathbf{F}_q[G]$ defined by $S(v) = v \circ u$ for every $v \in \mathbf{F}_q[G]$, we have that c is a code word if and only if its syndrome is equal to zero. In case $v = c + a$ with $c \in \phi(C(r, m))$ and a having at most

$$t \leq \frac{(d-1)}{2} \tag{7}$$

coordinates different to zero (where d is the minimal distance of the code), then the syndrome is $S(v) = v \circ u = (c + a) \circ u = a \circ u$. But if $\mathbf{A}$ denotes the set of vectors of $\mathbf{F}_q[G]$ with at most t coordinates different from zero, the restricted map

$$S : \mathbf{A} \longrightarrow \mathbf{F}_q[G]$$

is injective (see [3]) since if $a, b \in \mathbf{A}$, $S(a) = S(b)$ if and only if $a - b = (a - b) \circ e$. Thus $a - b \in \mathbf{F}_q[G] \circ e = \phi(C(r, m))$. But the weight of $a - b$ is : $w(a - b) \leq w(a) + w(b) \leq 2t \leq d - 1$ by (6). So $a - b = 0$ that is $a = b$. Therefore the error vector a, and so the code word c, is uniquely determined.

REFERENCES

[1] J.R. Clay, *Nearrings, Genesis and Applications,* Oxford Science Publications, 1992.

[2] Y.A. Drozd - V.V. Kirichenko, *Finite Dimensional Algebras,* Springer-Verlag, Berlin, Heidelberg, 1994.

[3] I. Damgard - P. Landrock, *Codes and Ideals in Group Algebras,* Preprint n. 12, Math. Inst. Aarhus Univ. (1986/87).

[4] A. Garcia - J.F. Voloch, *Fermat Curves over Finite Fields,* J. Number Theory, 30 (1988), pp. 345–356.

[5] V.D. Goppa, *Codes on Algebraic Curves,* (Russian), Dokl. Akad. Nauk SSSR, 259 (1981), pp. 1289–1290.

[6] V.D. Goppa, *Algebraic-Geometric Codes,* Math. USSR Izvestia, 21 –1 (1983), pp. 75–91.

[7] J W.P. Hirschfeld - L. Storme - J.A. Thas - J.F. Voloch, *A Characterization of Hermitian curves,* J. Geometry, 41 (1991), pp. 72–78.

[8] J.P. Hansen, *Codes on the Klein Quartic, Ideals and Decoding,* IEEE Trans. Inform. Theory Vol. IT-33, n. 6 (1987), pp. 923-925.

[9] W.F. Ke - H. Kiechle, *On the Solutions of the Equation* $x^m + y^m - z^m = 1$ *in a Finite field,* Proc. Am. Math. Soc., 123 (1995), pp. 1331–1339.

[10] H. Kiechle, *Points in Fermat curves over Finite Fields,* Contem. Math., 168 (1994), pp. 181–183.

[11] H.W. Leopoldt, *Über die Automorphismengruppe des Fermatkörpers,* J. Number Theory, 56 (1996), pp. 256–282.

[12] C.J. Moreno, *Algebraic Curves over Finite Fields,* Cambridge University Press, 1993.

[13] H.-G. Rück - H. Stichtenoth, *A Characterization of Hermitian function fields over Finite Fields,* J. Reine Angew, 459 (1994), pp 185-188.

[14] H. Stichtenoth, *Algebraic Function Fields and Codes,* Springer-Verlag, Berlin, Heidelberg, New York, 1993.

[15] H. Stichtenoth, *On Automorphisms of Geometric Goppa codes,* J. Algebra, 130 (1990), pp. 113–121.

[16] H. Stichtenoth, *The Fermat curves in Characteristic p,* Contem. Math., 225 (1999), pp. 123–129.

[17] H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik, I, II,* Arch. Math., 24 (1973), pp. 527–544, pp. 615–631.

Dipartimento di Matematica ed Applicazioni,
Via Archirafi 34, 90123 Palermo (ITALY)
e-mail: spera@dipmat.math.unipa.it