3. A large Fermat code

From theorem 2.6 we know that the Fermat curve of degree nine is maximal over $F_{64}$, in fact it is a Hermite curve and there are 513 rational points. After determining rational points over some extensions of $F_2$ (prop.3.3), we may define a series of codes. Lenght and dimension of the codes follow immediately (prop.3.5). For one of the codes (def.3.6) we determine the minimum distance. The code appears to be of type $[513,485,15]$ (th.3.15), so the minimum distance is 14 above the design minimum distance.

3.1 Fermat curve. Let $X/F_2^{alg}$ denote the Fermat curve of degree nine, defined by $F(x,y,z) = x^9 + y^9 + z^9 = 0$. For the genus $g$ of $X$ we have (prop.1.6)
\[
g = \binom{8}{2} = 28
\]

Let $L,K$ be as in def.1.1, then with the adjunction formula (prop.1.7)
\[
K \sim 6L
\]

Finally let $\sigma$ denote the Frobenius on $X$, i.e.
\[
\sigma P = (x^2, y^2, z^2) \quad \text{for} \quad P = (x,y,z)
\]

3.2 Remark. The fields $F_4$, $F_8$, ..., $F_{64}$ may be interpreted as extensions of $F_2$ as follows

\[
\begin{align*}
F_4 &= F_2(\alpha^{21}) \equiv F_2(X)/(X^2+X+1) \quad , \alpha^{21} \rightarrow X \\
F_8 &= F_2(\alpha^{27}) \equiv F_2(X)/(X^3+X+1) \quad , \alpha^{27} \rightarrow X \\
F_{16} &= F_2(\gamma) \equiv F_2(X)/(X^4+X+1) \quad , \gamma \rightarrow X \\
F_{32} &= F_2(\beta) \equiv F_2(X)/(X^5+X^2+1) \quad , \beta \rightarrow X \\
F_{64} &= F_2(\alpha) \equiv F_2(X)/(X^6+X+1) \quad , \alpha \rightarrow X
\end{align*}
\]

With this choise $F_{64}$ is an extension of both $F_4$ and $F_8$. (One verifies immediately that the polynomials involved are irreducible and that the first two isomorphisms agree with the last one)

3.3 Proposition. Let $N$ be the 9-roots of unity in $F_{64}$, $N = \{1, \alpha^7, \ldots, \alpha^{56}\}$, and $\sigma$ the Frobenius as in def.3.1.
For the fields of rem. 3.2 the rational points on $X$ are given by

\[
\begin{align*}
F_2 & \quad \{ \tau \,(0:1:1) \mid \tau \in S_3 \} =: A \\
F_4 & \quad A \cup \{ \tau \,(0:1:\alpha^{21}) \mid \tau \in S_3 \} \\
F_8 & \quad A \cup \{ \tau \,(1:\alpha^{27}:\alpha^{18}) \mid \tau \in S_3 \} \\
F_{16} & \quad A \cup \{ \tau \,(0:1:\gamma^6) \mid \tau \in S_3 \} \\
F_{32} & \quad A \cup \{ \sigma^i \tau \,(1:\beta:\beta^{19}) \mid \tau \in S_3, i=0,1,\ldots,4 \} \\
F_{64} & \quad \{ \tau \,(0:1:\mu) \mid \tau \in S_3, \mu \in \mathbb{N} \} \cup \\
& \quad \{ (1:1:y:vz) \mid 1+y+9z=0, y,z \in F_8^+, \mu, v \in \mathbb{N} \}
\end{align*}
\]

For their number we obtain

\[
\begin{array}{cccccccc}
k & F_2 & F_4 & F_8 & F_{16} & F_{32} & F_{64} \\
\#X(k) & 3 & 9 & 9 & 9 & 33 & 513
\end{array}
\]

In particular $X$ is maximal over $F_{64}$.

Proof. All points given are on the curve and their number agree with the table. We show there are no more $0$.

$F_2, F_8$ and $F_{32}$ do not contain a primitive third root of unity. Therefore the map $x \rightarrow x^9$ is a bijection on these fields, yielding $\#X(k)=\#P^1(k)$, as in the table.

For $F_4$ and $F_{16}$ one has

\[
\begin{align*}
x \in F_4 & \quad \Rightarrow \quad x^9 \in \{0,1\} \\
x \in F_{16} & \quad \Rightarrow \quad x^9 \in \{0,1,\gamma^3,\gamma^6,\gamma^9,\gamma^{12}\} =: D
\end{align*}
\]

from which the case $F_4$ follows immediately. As for $F_{16}$, points $(x:y:z)$ with $xyz=0$, are just the points over $F_4$. To see that there are no new points, i.e. points with $xyz \neq 0$, it is sufficient to note $\gamma^3+1=\gamma^1$ (rem. 3.2) and $\gamma \not\in D$.

$F_{64}$ contains a primitive ninth root of unity and we find rational points by adjugating them to points over $F_2$ (obtaining $3 \times 9$ points) and the new points over $F_8$ (obtaining $6 \times 81$ points). Since their number equal the Weil upper bound, it is sufficient to verify that the points thus obtained are all different. This being a trivial verification, the proposition is proved.
3.4 Divisors on X. Write $P_1, P_2, \ldots, P_{513}$ for the points over $F_{64}$, say with $P_1=(0:1:1)$, $P_2=(1:0:1)$, $P_3=(1:1:0)$. With $(1: \beta : \beta^{19}) \in X(F_{32})$ and $\sigma$ the Frobenius we define $B_{i+1} = \sigma^i (1: \beta : \beta^{19})$, $i=0,1,\ldots,4$. Finally let $D$, $B$ and $G$ be divisors over $F_2$ on $X$, given by

\[
D = P_1 + P_2 + \ldots + P_{513} \\
B = B_1 + B_2 + B_3 + B_4 + B_5 \\
G = mB
\]

$11 \leq m \leq 102$

3.5 Proposition. The parameters of a Goppa code $C^*(D,G)$, $D$ and $G$ as in 3.4, satisfy

\[
\begin{align*}
n &= 513, \quad \text{length} \\
k &= 540 - m, \quad \text{dimension} \\
d^* &= 5m - 54, \quad \text{design minimum distance} \\
d^* &\leq d \leq d^* + 28, \quad \text{minimum distance}
\end{align*}
\]

Proof. We may use prop.1.11 to find

\[
\begin{align*}
n &= \deg(D) \\
k &= \deg(D-G) + g -1 \\
d^* &= \deg(G-K) \\
d^* &\leq d \leq d^* + g
\end{align*}
\]

Substitution of $\deg(D)=54, \deg(G)=5m, \deg(K)=54$ and $g=28$ yields the result $\diamondsuit$.

3.6 Definition. With $D$, $B$ the divisors of 3.4 and referring to the definition of a Goppa code (1.9) we define the code $C$ as the Goppa code $C^*(D,11B)$.

After proposition 3.5 it remains to determine the minimum distance of $C$. In preparation for theorem 3.15 we deduce some equivalences of divisors on $X$. The following lemma gives us the divisor, corresponding to a tangent at $X$. 
3.7 Lemma. Let $X/F_p^{a1g}$ be a Hermitian curve of degree $q+1$. On $X$ consider

$\phi : (x:y:z) \rightarrow (x^q:y^q:z^q)$

For any $P \in X(F_p^{a1g})$ the divisor $L_P$, cut out by the tangent at $P$ is given by

$L_P = qP + q^2P$

**Proof.** Say $P = (x_0:y_0:z_0)$. Points of $L_P$ are given by

\[
\begin{cases}
  x^{q+1} + y^{q+1} + z^{q+1} = 0 \\
  x_0^{q}x + y_0^{q}y + z_0^{q}z = 0
\end{cases}
\]

Suppose $q^2P = (x_1:y_1:z_1) \neq P$. Since $q^2P \in L_P$ points on $L_P$ are of the form

\[
(x_0 + \lambda(x_1-x_0) : y_0 + \lambda(y_1-y_0) : z_0 + \lambda(z_1-z_0))
\]

Substitution in $x^{q+1} + y^{q+1} + z^{q+1} = 0$ yields $\lambda = 0$ ($qx$), $\lambda = 1$ ($1x$). For $q^2P = P$ one verifies $L_P = (q+1)P$.

3.8 Corollary. On $X$ we have the equivalence of divisors ($B$ as in 3.4, $L$ as in def.1.1)

$9B \sim 5L$

**Proof.** We have

$5L \sim L_{B_1} + L_{B_2} + L_{B_3} + L_{B_4} + L_{B_5}$

and by the lemma

$L_{B_1} + L_{B_2} + L_{B_3} + L_{B_4} + L_{B_5} = 9B$

3.9 Lemma.

(a) The equation $F_2(x,y,z) := xy + xz + y^2 = 0$ determines the unique conic through $B_1,B_2,...,B_5$.

(b) There is a unique divisor $E$ on $X$, satisfying

$B + E \sim 2L \quad \& \quad E \geq 0$

(c) The divisor $E$ from (b) is a divisor over $F_2$ of degree 13, with one point of degree one and two points of degree six.
Proof. (a) $F_2$ is the unique solution of a system of linear equations. Unicity also follows from Bezout (th.1.8). (b) is consequence of (a).
(c) With $(a,b)$, points of $B + E$ are the solutions of
\[
\begin{cases}
  x^9 + y^9 + z^9 = 0 \\
  xy + xz + y^2 = 0
\end{cases}
\]
or, since a solution $(x:y:z)$ satisfies $x \neq 0$
\[
\begin{cases}
  1 + y^9 + y^{18} + y^{17} + y^{10} + y^9 = 0 \\
  (x:y:z) = (1:y:y+y^2)
\end{cases}
\]
(3.1)
and it suffices to give the factorisation of (3.1) over $F_2$
\[
y^{18} + y^{17} + y^{10} + 1 = (y^6 + y^5 + y^4 + y + 1)(y^6 + y^5 + 1) \times (y^5 + y^2 + 1)(y+1)
\]

3.10 Lemma.
(a) The equation $F_3(x,y,z) := x^2z + xyz + (y+z)^3 = 0$ determines the unique third degree curve, that touches $X$ at $B_1, B_2, ..., B_5$.
(b) There is a unique divisor $E'$ on $X$, satisfying
\[
2B + E' \sim 3L \quad \wedge \quad E' \geq 0
\]
(c) The divisor $E'$ from (b) is a divisor over $F_2$ of degree 17, with three points of degree one ($P_1 + 2P_2$) and a term that is either a point of degree 14 or the sum of two points of degree 7.

Proof.
(a) We look for a $F$ of the form
\[
F(x,y,z) = a_0x^3 + a_1x^2y + ... + a_9z^3
\]
From the proof of lem.3.9(c) we see
\[
[B_1, B_2, ..., B_5] = \{ (1:y:y+y^2) \} y^5 + y^2 + 1 = 0
\]
with $y^5 + y^2 + 1$ irreducible over $F_2$. Hence $F$ is of the form
\[
F(1,y,y+y^2) = (b_0y+b_1)(y^5 + y^2 + 1)
\]
\[b_0, b_1 \in F_2^{\text{alg}}\]
Comparing coefficients of powers of $y$ in the last equation leads to seven
equations in twelve unknowns $(a_0,a_1,\ldots,a_9,b_0,b_1)$. One obtains easily, with $F_2$ as
in lem.3.9(a),

$$F(x,y,z) = c_0F_2x + c_1F_2y + c_2F_2z + c_3(x^3+xyz+yz^2) +
+ c_4(x^2+y^2z+yz^2+z^3)$$

Let $X'$ be the curve determined by $F(x,y,z)=0$ and for a non-singular point $P$ of
$X'$ let $L'_P$ be the tangent of $P$ at $X'$. With lem.3.7 it suffices to choose
c_0,c_1,\ldots,c_4 such that $\varphi^2P\in L'_P$ for $P\in \{B_1,B_2,\ldots,B_5\}$. As a unique solution we
obtain $F = x^2z + xyz + (y+z)^3$. (b) follows from (a)
(c) With $(a,b)$, points of $2B + E'$ are the solutions of

$$\begin{cases}
\begin{alignat*}{2}
x^9 + y^9 + z^9 &= 0 \quad (3.2) \\
x^2z + xyz + (y+z)^3 &= 0 \quad (3.3)
\end{alignat*}
\end{cases}$$

remark (i). It suffices to show that all solutions of degree $\leq 6$ (over $F_2$) are given
by $2B+P_1+2P_2$. For the other solutions (14 in number by Bezout's theorem)
then only two possibilities remain to be divided into Galoits orbits: one of length
14 or two of length 7.

remark (ii). Since (3.2) contains no new point of $F_{16}$ over $F_4$ by prop.3.3, no
solution of degree 4 exists. Therefore we may solve $(x,y)$ over $F_{32}$ (solutions of
degree 1,5) and over $F_{64}$ (solutions of degree 1,2,3,6).

remark (iii). $z\neq 0$ for a solution $(x:y:z)$ of $(x,y)$, since $z=0 \Rightarrow y,z=0 \Rightarrow x,y,z=0$.

First suppose $y=0$, then by (iii)

$$(3.3) \quad \Rightarrow \quad (x+z)^2z=0 \quad \Rightarrow \quad x=z$$

or

$$(x:y:z) = (1:0:1) = P_2 \quad (2x)$$

For $y\neq 0$, say $y=1$, we have

$$(3.3) \quad \Leftrightarrow \quad x(x+1) = (z+1)^3z^{-1}$$

Note that $z\neq 0$ by (iii). For $x,z \in F_{32}$ or $x,z \in F_{64}$ satisfying the last equation
one verifies if $(x:1:z)$ is a point on $X$. This is straightforward and, using some
tricky reductions, can in fact be done by hand, leading to the solutions

$P_1 \; (1x) \; \text{and} \; B_1,B_2,\ldots,B_5 \; (2x)$

By remarks (ii) and (i) this proofs the lemma.
3.11 Lemma. The equation \( y(x+y+z) = 0 \) determines a divisor over \( \mathbb{F}_2 \), say \( L_y(x+y+z) \), on the curve \( X \). With the notation of 3.4 we have

\[
L_y(x+y+z) \sim P_1 + 2P_2 + P_{i1} + P_{i2} + \ldots + P_{i15}
\]

with the \( P_{ik}, k=1,2,\ldots,15 \), pairwise different.

**Proof.** We consider the contributions of the irreducible components (\( N \) as defined in 3.2)

\[
y = 0 \sum_{\mu \in N} (1:0:1:1) \sum_{P \in X(\mathbb{F}_8)}\]

since for \( P=(x:y:z) \in X(\mathbb{F}_8) : x+y+z = (x^9+y^9+z^9)^4 = 0 \) and \( \#X(\mathbb{F}_8) = 9 \). The statement follows at once. In particular \( P \in L_y(x+y+z) \Rightarrow P \in X(\mathbb{F}_64) \). See also convention 3.4.

To determine the minimum distance we use prop.1.11:

3.12 Remark. For a Goppa code \( C^*(D,G) \), with \( D,G \) divisors on a curve \( X \), the minimum distance equals the smallest \( d \) for which there is a relation in \( \text{Div}(X) \) of the form

\[
G + Q \sim K + P_{i1} + P_{i2} + \ldots + P_{id}
\]

with \( Q \geq 0 \), \( K \) as in def.1.1 and the \( P_{ik} \in D, k=1,2,\ldots,d \), pairwise different.

3.13. Proposition. Let \( d \) be the minimum distance of the code \( C=C^*(D,11B) \). Then \( d \leq 15 \).
Proof. With the previous proposition it suffices to give a relation

\[ 11B + Q \sim K + P_{11} + P_{12} + \ldots + P_{115} \]

We have

\[
\begin{align*}
6L & \sim K \quad \text{(rem.3.1)} \\
9B & \sim 5L \quad \text{(cor.3.8)} \\
2B + E & \sim 3L \quad E \geq 0 \quad \text{(lem.3.10)} \\
2L & \sim P_1 + 2P_2 + P_{11} + P_{12} + \ldots + P_{115} \quad \text{(lem.3.11)}
\end{align*}
\]

These yield the required relation with \( Q = E - P_1 - 2P_2 \geq 0 \) by lem. 3.10. and the \( P_{ik} \in D, k=1,2,\ldots,15 \), pairwise different by lem.3.11 \( \Box \).

3.14.Lemma. For the code \( C \) suppose a relation (3.4), with \( d \leq 14 \), exists. Then there is a relation

\[ 2B + Q + P' \sim L + P + P' \sim 3L \]

with \( Q, P' \geq 0 \), \( D \geq 0 \) and \( \deg(P') \geq 4 \).

Proof. We assume a relation of the following form

\[ 11B + Q \sim K + P \]

\( P = P_{11} + P_{12} + \ldots + P_{1d}, d \leq 14 \). Using \( 9B \sim 5L \) (cor.3.8) and \( K \sim 6L \) (rem.3.1) we obtain

\[ 2B + Q \sim L + P \]

Through \( P \) we may choose a curve of degree 4, thus obtaining a \( P \in \text{Div}_{\geq 0}(X) \) satisfying \( P + P \sim 4L \). Then
\[ 2B + Q + P^- \sim L + P + P^- \sim 5L \]

Since \( 2B + Q + P^- \geq 0 \) we conclude that there is also a curve of degree 5 through \( P^- \). \( \text{Deg}(P^-)=36-\text{deg}(P)\geq22 \), hence the two curves (of degree 4 and 5) have a component in common, say of degree \( m \).

Noting that \( 2B+Q \cap P = \emptyset \), we obtain a \( P^* \in \text{Div}_{\geq0}(X), P^* \not\subseteq P^- \), with

\[ 2B + Q + P^* \sim L + P + P^* \sim (5-m)L \]

\( (m=1) \) We find two curves (of degree 3 and 4) through \( P^* \). Since in this case \( \text{deg}(P^*)=27-\text{deg}(P)\geq13 \), Bezout implies that the two curves have a component in common. Case \( (m=1) \) thus reduces to \( (m\geq2) \)

\( (m=2) \) We obtain the required relation. Indeed \( \text{deg}(P^*)=18-\text{deg}(P)\geq4 \)

\( (m=3) \) We find \( 2B+Q^\sim 2L \), \( Q\geq0 \). A contradiction with lem.4.x.

\( (m=4) \) The curve of degree 5 intersects \( X \) at \( 2B+P+P^* \), but then \( \text{deg}(2B+P+P^*)=46\geq45 \), a contradiction \( \emptyset \).

3.15 Theorem. The code \( C \), defined in 3.6, is of type \([513,485,15]\).

Proof. With propositions 3.5 en 3.13 the code \( C \) is of type \([513,485,1\leq d\leq15]\). We now assume \( d<15 \)

Then the lemma applies and we have the equivalences

\[ 2B + Q + P' \sim L + P + P' \sim 3L \]

with \( Q,P\geq0 \), \( D\geq P\geq0 \) and \( \text{deg}(P')\geq4 \). \( P' \) can be chosen such that \( Q \cap P = \emptyset \). Since \( 2B \cap P = \emptyset \) also we conclude, by lemma 3.10, that the third degree curve through \( 2B + Q + P' \) and the second degree curve through \( P + P' \) have no common component. Bezout then gives \( \text{deg}(P')\leq6 \).

Consider

\[ 2L \sim P + P' \sim \sigma^{6}P + \sigma^{6}P' = P + \sigma^{6}P' \]
Since \( \deg(P) = 18 - \deg(P') \geq 12 \), the two curves through \( P + P' \) and \( P + \sigma^6P' \) are equal (even with both curves reducible and one component in common, three common points remain for the other components; both are lines and thus fully determined by these three points), hence \( \sigma^6P' = P' \). However, lemma 3.10 and \( \deg(P') \geq 4 \) imply that \( P' \) contains a point with coordinates of degree 7 or 14 (over \( F_2 \)), so \( \sigma^6P' \neq P' \), a contradiction. We conclude \( d = 15 \) \( \diamond \).