Contemporary Mathematics
Volume 487, 2009

On the Construction of Galois Towers

Alp Bassa and Peter Beelen

ABSTRACT. In this paper we study an asymptotically optimal tame tower over the field with p^2 elements introduced by Garcia-Stichtenoth. This tower is related with a modular tower, for which explicit equations were given by Elkies. We use this relation to investigate its Galois closure. Along the way, we obtain information about the structure of the Galois closure of $X_0(p^n)$ over $X_0(p^r)$, for integers $1 < r < n$ and prime p and the Galois closure of other modular towers $(X_0(p^n))_n$.

1. Introduction

Using Goppa's construction of codes from curves over finite fields, Tsfasman–Vladut–Zink [13] constructed sequences of codes of increasing length with limit parameters above the Gilbert–Varshamov bound and hence better than those of all previously known such sequences. Their construction is mainly based on the existence of curves over a finite field of high genus with many rational points. This enhanced the interest in towers of curves over finite fields. Subsequently, other applications of such towers in coding theory and cryptography were discovered, for instance for the construction of hash functions, low discrepancy sequences etc.

A natural idea is to search for such sequences of curves, with some additional structure, which would reflect itself in some additional structure of the objects constructed from them. Stichtenoth [12] constructed for example sequences of self-dual and transitive codes attaining the Tsfasman–Vladut–Zink bound over finite fields with square cardinality. This was done by using a tower of function fields $E_0 \subseteq E_1 \subseteq E_2 \subseteq \ldots$, where all extensions E_n/E_0 are Galois.

Motivated by this, we study Galois closures of the modular towers $(X_0(p^n))_n$. In particular, we investigate the Galois closure of a tower $\mathcal{M}$ over $\mathbb{F}_{p^2}$ introduced by Garcia–Stichtenoth [3], which is recursively defined by

$$Y^2 = \frac{X^2+1}{2X}.$$

This tower corresponds to the modular tower $(X_0(2^n))_n$, for which explicit equation were given by Elkies [2]. Using this interpretation of $\mathcal{M}$ as a modular tower, we find the exact degrees of extensions in the Galois closure of it and study the Galois

1991 *Mathematics Subject Classification.* Primary:14H05, Secondary:11R32.
Key words and phrases. Function field, modular curve, Galois tower.

groups that appear. We show that the function fields of the Galois closure can be obtained as a compositum of three different embeddings of the function fields in the tower $\mathcal{M}$.

For more definitions and further details about (explicit) towers of algebraic function fields, we refer to [5].

2. Groups of Galois closure

In this section the field of definition is always assumed to be $\mathbb{C}$, the field of complex numbers. Let p be a prime number and $n > 1$ an integer. The following group is standard in the theory of modular curves:

$$\Gamma_0(p^n) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}) \,:\, c \equiv 0 \pmod{p^n} \right\}.$$

Associated to this group is the modular curve $X_0(p^n)$ which has been studied extensively in the literature, cf. [7, 8].

Let $0 < r < n$ be integers. The Galois closure of $X_0(p^n)$ over $X_0(p^r)$ has Galois group $\Gamma_0(p^r)/\Delta_r(p^n)$ with

$$\Delta_r(p^n) := \bigcap_{\sigma \in \Gamma_0(p^r)} \sigma \Gamma_0(p^n) \sigma^{-1}.$$

The group $\Delta_r(p^n)$ is the largest normal subgroup of $\Gamma_0(p^r)$ contained in $\Gamma_0(p^n)$, since if $H \trianglelefteq \Gamma_0(p^r)$ and $H \subset \Gamma_0(p^n)$, then $H \subset \bigcap_{\sigma \in \Gamma_0(p^r)} \sigma \Gamma_0(p^n) \sigma^{-1} = \Delta_r(p^n)$. The maximality of $\Delta_r(p^n)$ with respect to the above property will be used later.

The goal of this section is to compute the order of the groups $\Gamma_0(p^r)/\Delta_r(p^n)$ and to obtain information about its group structure. We start by describing the group $\Delta_r(p^n)$ in more detail.

PROPOSITION 2.1.

$$\Delta_r(p^n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(p^n) \,:\, p^{n-r} | a - d - bp^r \text{ and } p^{n-r} | 2bp^r \right\}$$

PROOF. We denote by H the group on the right-hand side of above equality. For an element

$$h = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

of $SL(2,\mathbb{Z})$ to be in H it needs to satisfy three things:
1) $p^n | c$,
2) $p^{n-r} | a - d - bp^r$ and
3) $p^{n-r} | 2bp^r$.

Clearly $H \subset \Gamma_0(p^n)$, so to prove the proposition it is enough to show that $H \trianglelefteq \Gamma_0(p^r)$ and that $\Delta_r(p^n) \subset H$, since then $\Delta_r(p^n) \supset H$ follows from the maximality of $\Delta_r(p^n)$.

First we prove that $H \trianglelefteq \Gamma_0(p^r)$. Conjugating an element $h \in H$ with a matrix

$$m = \begin{pmatrix} \alpha & \beta \\ \gamma p^r & \delta \end{pmatrix},$$

from $\Gamma_0(p^r)$ we find that

$$mhm^{-1} = \begin{pmatrix} -p^r\gamma(\alpha b + \beta d) + (\alpha a + \beta c)\delta & \alpha^2 b + \alpha\beta(d-a) - \beta^2 c \\ p^r\gamma(a-d)\delta - bp^{2r}\gamma^2 + c\delta^2 & p^r\gamma(\alpha b - \beta a) + (\alpha d - \beta c)\delta \end{pmatrix}.$$

We need to check that this an element of H. First we show that it is an element of $\Gamma_0(p^n)$. We have

$$p^r(a-d)\gamma\delta - bp^{2r}\gamma^2 + c\delta^2 \equiv bp^{2r}\gamma(\delta - \gamma) \equiv 0 \pmod{p^n}.$$

The first equality follows from properties 1) and 2) of h listed above. The last equality follows directly from property 3) of h if $p \neq 2$. If $p = 2$, then it only implies that 2^{n-1} divides bp^{2r}, but δ has to be odd if $p = 2$, implying that in this case 2 divides $\gamma(\delta - \gamma)$.

Using again that $a \equiv d + bp^r \pmod{p^{n-r}}$ and $c \equiv 0 \pmod{p^{n-r}}$, we see that the second condition for mhm^{-1} to be in H is equivalent to the statement

$$bp^r(p^r\beta(\alpha+\gamma) - \alpha(\alpha + 2\gamma - \delta)) \equiv 0 \pmod{p^{n-r}}.$$

From property 3) of h we see that this is satisfied if $p \neq 2$, while if $p = 2$, then $2^{n-r-1} | bp^r$ and $2 | \alpha(\alpha - \delta)$, since δ is odd if $p = 2$.

It remains to check that the third condition is satisfied, but this can easily be seen to hold as well. We conclude that $mhm^{-1} \in H$ and hence that $H \trianglelefteq \Gamma_0(p^r)$.

Now we wish to prove that $\Delta_r(p^n) \subset H$. In order to do this we introduce the element

$$A := \begin{pmatrix} 1 & 0 \\ p^r & 1 \end{pmatrix}.$$

Then for any $h \in \Gamma_0(p^n)$ we have that

$$AhA^{-1} = \begin{pmatrix} a - bp^r & b \\ c + p^r(a - d - bp^r) & d + bp^r \end{pmatrix},$$

which implies that if $AhA^{-1} \in \Gamma_0(p^n)$, then $p^{n-r} | a - d - bp^r$. Similarly, if $A^{-1}hA \in \Gamma_0(p^n)$, then $p^{n-r} | a - d + bp^r$. Therefore, if $h \in \Gamma_0(p^n) \cap A\Gamma_0(p^n)A^{-1} \cap A^{-1}\Gamma_0(p^n)A$, then $p^n | c$, $p^{n-r} | a - d - bp^r$ and $p^{n-r} | a - d + bp^r$, which is equivalent to conditions 1),2) and 3) above. In other words:

$$\Delta_r(p^n) \subset \left(\Gamma_0(p^n) \cap A\Gamma_0(p^n)A^{-1} \cap A^{-1}\Gamma_0(p^n)A \right) \subset H,$$

which concludes the proof. □

COROLLARY 2.2. *We have*

$$\Delta_r(p^n) = \Gamma_0(p^n) \cap A\Gamma_0(p^n)A^{-1} \cap A^{-1}\Gamma_0(p^n)A,$$

with

$$A := \begin{pmatrix} 1 & 0 \\ p^r & 1 \end{pmatrix}.$$

PROOF. In the above proposition we saw that

$$\Delta_r(p^n) \subset \left(\Gamma_0(p^n) \cap A\Gamma_0(p^n)A^{-1} \cap A^{-1}\Gamma_0(p^n)A \right) \subset H,$$

but we have also seen that $H \subset \Delta_r(p^n)$. □

The group $\Delta_r(p^n)$ has some further properties we wish to ascertain. For a group G, we denote by $[G, G]$ its commutator subgroup.

LEMMA 2.3. *Suppose that $n > r > 0$. We have*

$$[\Delta_r(p^n), \Delta_r(p^n)] \subset \Delta_r(p^{n+1})$$

and

$$g \in \Delta_r(p^n) \Rightarrow g^p \in \Delta_r(p^{n+1}).$$

As a consequence, the group $\Delta_r(p^n)/\Delta_r(p^{n+1})$ is an elementary abelian p-group.

PROOF. A direct calculation shows that $[\Delta_r(p^n), \Delta_r(p^n)] \subset \Gamma_0(p^{n+1})$. Also, since $\Delta_r(p^n) \trianglelefteq \Gamma_0(p^r)$, we find that for any $\sigma \in \Gamma_0(p^r)$ we have

$$\sigma[\Delta_r(p^n), \Delta_r(p^n)]\sigma^{-1} = [\sigma\Delta_r(p^n)\sigma^{-1}, \sigma\Delta_r(p^n)\sigma^{-1}] = [\Delta_r(p^n), \Delta_r(p^n)].$$

This implies that

$$[\Delta_r(p^n), \Delta_r(p^n)] = \bigcap_{\sigma\in\Gamma_0(p^r)} \sigma[\Delta_r(p^n), \Delta_r(p^n)]\sigma^{-1} \subset \Delta_r(p^{n+1}).$$

To prove the second item, we use that

$$\begin{pmatrix} a & b \\ cp^n & d \end{pmatrix}^k = \begin{pmatrix} a^k + \mathcal{O}(p^n) & b\frac{a^k-d^k}{a-d} + \mathcal{O}(p^n) \\ cp^n\frac{a^k-d^k}{a-d} + \mathcal{O}(p^{2n}) & d^k + \mathcal{O}(p^n) \end{pmatrix},$$

where $\mathcal{O}(p^m)$ denotes some number divisible by p^m. This can be showed directly using induction on k. If $k = p$, then $cp^n(a^p - d^p)/(a-d) \equiv cp^n(a-d)^{p-1} \bmod p^{n+1}$. Since $g \in \Delta_r(p^n)$ we have that $p^{n-r}|a - d - bp^r$, implying that $p|a - d$. Hence $g^p \in \Gamma_0(p^{n+1})$. By definition of $\Delta_r(p^n)$, we have that for any $\sigma \in \Gamma_0(p^r)$, the element $\sigma^{-1}g\sigma$ is in $\Gamma_0(p^n)$, implying that $(\sigma^{-1}g\sigma)^p = \sigma^{-1}g^p\sigma \in \Gamma_0(p^{n+1})$. This implies that $g^p \in \bigcap_{\sigma\in\Gamma_0(p^r)} \sigma\Gamma_0(p^{n+1})\sigma^{-1} = \Delta_r(p^{n+1})$.

The final statement of the lemma follows directly from the first two statements. □

3. The order of the group $\Delta_r(p^n)/\Gamma(p^n)$

The following congruence group is well-known:

$$\Gamma(p^n) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{p^n} \right\}.$$

It is the kernel of the reduction modulo p^n map: $\varphi : SL(2,\mathbb{Z}) \to SL(2,\mathbb{Z}/p^n\mathbb{Z})$ and one can show that this map is surjective ([**9**, section 1.6]). Also it is well known [**9**] that

$$\#SL(2,\mathbb{Z}/p^n\mathbb{Z}) = p^{3n} - p^{3n-2}. \tag{3.1}$$

Note that by Proposition 2.1 the group $\Gamma(p^n)$ is a (normal) subgroup of $\Delta_r(p^n)$. The goal of this section is to compute the cardinality of the group $\Delta_r(p^n)/\Gamma(p^n)$. We will start by giving several lemmas.

LEMMA 3.1. *We have that*

$$\Delta_r(p^n)/\Gamma(p^n) \cong \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in SL(2,\mathbb{Z}/p^n\mathbb{Z}) : p^{n-r}|a - d - bp^r \text{ and } p^{n-r}|2bp^r \right\}.$$

PROOF. This follows directly from Proposition 2.1 using the reduction modulo p^n map φ. □

LEMMA 3.2. *Let $n > r > 0$ be integers and suppose that p is an odd prime. Then we have that*

$$\#\Delta_r(p^n)/\Gamma(p^n) = \begin{cases} 2p^{r+n} & \text{if } n \le 2r, \\ 2p^{3r} & \text{else.} \end{cases}$$

PROOF. Using Lemma 3.1 and the assumption that p is odd, it is enough to count the number of triples $(a,b,d) \in (\mathbb{Z}/p^n\mathbb{Z})^3$ satisfying $p^n|ad-1$, $p^{n-r}|a-d$ and $p^{n-r}|bp^r$.

We claim that the number of $(a,d) \in (\mathbb{Z}/p^n\mathbb{Z})^2$ satisfying $p^n|ad-1$ and $p^{n-r}|a-d$ equals $2p^r$. From the conditions, it is clear that $p^{n-r}|a^2-1$, which implies that $a \equiv \pm 1 \pmod{p^{n-r}}$. This leaves exactly $2p^r$ possibilities for a. Given any a satisfying the last congruence, there exists exactly one $d \in \mathbb{Z}/p^n\mathbb{Z}$ such that $p^n|ad-1$ and by reducing modulo p^{n-r} we see that $d \equiv \pm 1 \equiv a$. This means that $p^{n-r}|a-d$ is satisfied for this d as well.

We claim that the number of $b \in \mathbb{Z}/p^n\mathbb{Z}$ such that $p^{n-r}|bp^r$ is equal to p^n if $n \le 2r$ and equal to p^{2r} if $n > 2r$. Indeed, if $n \le 2r$, the condition $p^{n-r}|bp^r$ is always satisfied, so that all b's in $\mathbb{Z}/p^n\mathbb{Z}$ are possible. If $n > 2r$, then the condition simplifies to $p^{n-2r}|b$, meaning that all p^{2r} multiples of p^{n-2r} in $\mathbb{Z}/p^n\mathbb{Z}$ are solutions.

Multiplying the number of possibilities for (a,d) with that for b, the lemma follows. □

LEMMA 3.3. *Let $n > r > 0$ be integers. Then we have that*

$$\#\Delta_r(2^n)/\Gamma(2^n) = \begin{cases} 2^{2r+1} & \text{if } n-r = 1, \\ 2^4 & \text{if } n = 3 \text{ and } r = 1, \\ 2^{2r+3} & \text{if } n-r = 2 \text{ and } r > 1, \\ 2^5 & \text{if } n = 4 \text{ and } r = 1, \\ 2^8 & \text{if } n = 5 \text{ and } r = 2, \\ 2^{2r+5} & \text{if } n-r = 3 \text{ and } r > 2, \\ 2^{n+r+2} & \text{if } n-r > 3 \text{ and } n \le 2r, \\ 2^{3r+3} & \text{if } n-r > 3 \text{ and } n > 2r. \end{cases}$$

PROOF. Using Lemma 3.1 it is enough to count the number of triples $(a,b,d) \in (\mathbb{Z}/2^n\mathbb{Z})^3$ satisfying
1) $2^n|ad-1$,
2) $2^{n-r}|a-d-b2^r$ and
3) $2^{n-r-1}|b2^r$.
Since $2^{n-r-1}|b2^r$, we see that $b2^r \equiv 0 \bmod 2^{n-r}$ or $b2^r \equiv 2^{n-r-1} \bmod 2^{n-r}$. Combining with 2), we see that $d \equiv a \bmod 2^{n-r}$ or $d \equiv a + 2^{n-r-1} \bmod 2^{n-r}$. Substituting in 1) gives that $a^2 \equiv 1 \bmod 2^{n-r}$ or $a^2 \equiv 1 + a2^{n-r-1} \bmod 2^{n-r}$. Since from 1), we can deduce that a is odd, the latter congruence simplifies to $a^2 \equiv 1 + 2^{n-r-1} \bmod 2^{n-r}$. We now distinguish several cases.

Case 1, $n-r = 1$. In this case all solutions are characterized by choosing $a \in \mathbb{Z}/2^n\mathbb{Z}$ to be odd, d its multiplicative inverse modulo 2^n and arbitrary $b \in \mathbb{Z}/2^n\mathbb{Z}$. Thus there are $2^{2n-1} = 2^{2r+1}$ possibilities.

Case 2, $n-r = 2$. We have seen that $a^2 \equiv 1 \bmod 4$ or $a^2 \equiv 3 \bmod 4$. The latter is not possible, so we deduce that $a^2 \equiv 1 \bmod 4$, which implies that $a \equiv d \bmod 4$ and $b2^r \equiv 0 \bmod 4$. All in all we get that we can choose $a \equiv \pm 1 \bmod 4$, $b2^r \equiv 0 \bmod 4$ and $d \equiv a^{-1} \bmod 2^n$. For $r = 1$ this gives 16 possibilities for (a,b,d) and for $r > 1$ exactly 2^{2r+3}.

Case 3, $n-r = 3$. First we get that $a^2 \equiv 1 \bmod 8$ or $a^2 \equiv 5 \bmod 8$, but the latter is again not possible, since $8|a^2-1$ for any odd number a. This means that $b2^r \equiv 0 \bmod 8$. Moreover, the condition that $a^2 \equiv 1 \bmod 8$ implies that $a \equiv \pm 1$ or $\pm 3 \bmod 8$. Counting similarly as above, we find that there are 32 possibilities for (a,b,d) if $r = 1$, 256 if $r = 2$ and 2^{2r+5} if $r > 2$.

Case 4, $n-r>3$. First we assume that $b2^r \equiv 0 \bmod 2^{n-r}$, which means that there are 2^{2r} possibilities for b if $n>2r$ and 2^n otherwise. Then we found that $a^2 \equiv 1 \bmod 2^{n-r}$, which implies that $a \equiv \pm 1$ or $\pm 1 + 2^{n-r-1} \bmod 2^{n-r}$, leaving $4 \cdot 2^r$ possibilities for a. Now we can choose d to be the multiplicative inverse of a modulo 2^n and a direct computation shows that $a \equiv d \bmod 2^{n-r}$. All in all we find 2^{n+r+2} possibilities if $n \leq 2r$ and 2^{3r+2} if $n>2r$, still assuming that $b2^r \equiv 0 \bmod 2^{n-r}$. Now assume that $b2^r \equiv 2^{n-r-1} \bmod 2^{n-r}$. This can only occur if $r \leq n-r-1$, or equivalently if $n>2r$ and then the number of possibilities for b is 2^{2r}. We saw that $a^2 \equiv 1+2^{n-r-1} \bmod 2^{n-r}$, implying that $a \equiv \pm 1 + 2^{n-r-2}$ or $\pm 1 - 2^{n-r-2} \bmod 2^{n-r}$. As before we choose d to be the inverse of a, but now we find that $d \equiv a + 2^{n-r-1} \bmod 2^{n-r}$, so that condition 2) is satisfied. Condition 3) is satisfied automatically. We find 2^{3r+2} possibilities if $n>2r$, but none if $n \leq 2r$. In total for case 4, we find 2^{n+r+2} possibilities for (a,b,d) if $n \leq 2r$ and 2^{3r+3} otherwise. □

4. Degrees and structure of Galois closure

Given $n>r>0$ and a prime p, we will now determine the degree of the Galois closure of $X_0(p^n)$ over $X_0(p^r)$. We quote the following well-known facts [**9**, section 1.6]: Let m be a positive integer. The degree of the covering $X(p^m) \to X(1)$ equals $p^{3m-2}(p^2-1)/2$, unless $p=2$ and $m=1$ in which case it equals 6. The degree of the extension $X_0(p^m) \to X(1)$ equals $(p+1)p^{m-1}$. As a consequence we see that the degree of $X(p^{m+1}) \to X(p^m)$ equals p^3 unless $p=2$ and $m=1$, in which case it equals 4. Also the degree of $X_0(p^{m+1}) \to X_0(p^m)$ equals p. This together with the previous results enables us to compute all degrees in the tower obtained by taking the Galois closure of $X_0(p^n)$ over $X_0(p^r)$ for running n and fixed r.

LEMMA 4.1. *Let $n>r>0$ be integers, p an odd prime and let $\tilde{X}_0^r(p^n)$ denote the Galois closure of $X_0(p^n)$ over $X_0(p^r)$. Then*

$$\deg(\tilde{X}_0^r(p^n) \to \tilde{X}_0^r(p^{n-1})) = \begin{cases} p(p-1)/2 & \text{if } n=r+1, \\ p^2 & \text{if } r+1<n\leq 2r, \\ p^3 & \text{if } n>2r. \end{cases}$$

For $n>r+1$, the covering $\tilde{X}_0^r(p^n) \to \tilde{X}_0^r(p^{n-1})$ is elementary abelian.

PROOF. From Lemma 3.2 we can calculate all degrees of the coverings $X(p^n) \to \tilde{X}_0^r(p^n)$. Indeed, since $-I \in \Delta_r(p^n)$ and $-I \notin \Gamma(p^n)$, the only thing we need to do is divide $\#\Delta_r(p^n)/\Gamma(p^n)$ by 2. Further, since $\deg(X_0(p^r) \to X(1)) = (p+1)p^{r-1}$ and $\deg(X(p^r) \to X(1)) = (p^2-1)p^{3r-2}/2$, we find that $\deg(X(p^r) \to X_0(p^r)) = (p-1)p^{2r-1}/2$. All in all we now know all degrees of the coverings $X(p^m) \to \tilde{X}_0^r(p^m)$ for $m \geq r$. Combined with the fact that $\deg(X(p^{m+1}) \to X(p^m)) = p^3$, the first part of the lemma follows. The second part follows directly from Lemma 2.3. □

LEMMA 4.2. *Let $n>r>0$ be integers and let $\tilde{X}_0^r(2^n)$ denote the Galois closure of $X_0(2^n)$ over $X_0(2^r)$. Then*

$$\deg(\tilde{X}_0^r(2^n) \to \tilde{X}_0^r(2^{n-1})) = \begin{cases} 2 & \text{if } n=r+1, \\ 2 & \text{if } n=r+2 \text{ and } r>1, \\ 2 & \text{if } n=r+3 \text{ and } r>2, \\ 4 & \text{if } n=r+2 \text{ and } r=1, \\ 4 & \text{if } n=r+3 \text{ and } r=1,2, \\ 4 & \text{if } n=r+4 \text{ and } r=1,2, \\ 4 & \text{if } r+4\leq n\leq 2r+1, \\ 8 & \text{if } n>2r+3 \text{ and } r=1, \\ 8 & \text{if } n>2r+2 \text{ and } r=2, \\ 8 & \text{if } n>2r+1 \text{ and } r>2. \end{cases}$$

PROOF. The proof is similar to that of the previous lemma, but now we use Lemma 3.3. □

LEMMA 4.3. *Let $n>r>0$ be integers and p a prime. The extension $X_0(p^n) \to X_0(p^r)$ is Galois if and only if*

(1) *$p=2$ and $n-r=1$,*
(2) *$p=2$, $r>1$ and $n-r=2$,*
(3) *$p=2$, $r>2$ and $n-r=3$,*
(4) *$p=3$ and $n-r=1$.*

In all of these cases the Galois group is cyclic.

PROOF. Since $\deg(X_0(p^n) \to X_0(p^r)) = p^{n-r}$, we can use Lemmas 4.1 and 4.2 to check when this degree is the same as $\deg(\tilde{X}_0^r(p^n) \to X_0(p^r))$. Assuming the covering $X_0(p^n) \to X_0(p^r)$ is Galois of order p^{n-r}, we also see that its Galois group is $\Gamma_0(p^r)/\Delta_r(p^n)$. However, the element $A \bmod \Delta_r(p^n)$, with A as in Corollary 2.2, has order p^{n-r}. □

5. Reduction mod ℓ.

Let p be a prime. Until now, we have assumed that all the modular curves we considered were defined over the field $\mathbb{C}$. However, it is well known that the curves $X_0(p^n)$ have a model defined over $\mathbb{Q}$ [**6**]. Denote by ζ_{p^n} a primitive p^n-th root of unity. The curve $X(p^n)$ has a model defined over $\mathbb{Q}(\zeta_{p^n})$ and the covering $X(p^n) \to X(1)$ is still Galois and has the same degree as when working over $\mathbb{C}$. Since the Galois closure of $X_0(p^n)$ over $X_0(p^r)$ is contained in $X(p^n)$, it also has a model defined over $\mathbb{Q}(\zeta_{p^n})$ and all degrees computed before are still correct when working over this field. These models have good reduction modulo a prime ℓ if $\ell \neq p$. The Galois covering $X(p^n) \to X_0(p^r)$ is not necessarily Galois after this reduction, but will be so when we consider it over a field containing a p^n-th root of unity. After having done so, the Galois group will be the same as before reducing and in particular its degree is the same. All group theoretic arguments used before are then still valid for the reductions, as long as the field of definition contains a p^n-th root of unity.

The following Lemmas will be useful:

LEMMA 5.1. *Let F be a function field over a perfect field K and let $f(T) \in F[T]$ be a separable irreducible polynomial over F. Let $\alpha \in \Omega$ be a root of $f(T)$ in some fixed algebraically closed field $\Omega \supset F$. Let K' be a separable algebraic*

extension of K. Suppose that there exists a place P of F, which splits completely in the extension $F(\alpha)/F$. Then the polynomial $f(T)$ is irreducible in $FK'[T]$ and $\mathcal{G}(f,F) \cong \mathcal{G}(f,FK')$ where $\mathcal{G}(f,F)$ and $\mathcal{G}(f,FK')$ denote the Galois group of f over F and FK', respectively.

PROOF. Since there exists a place P of F splitting completely in the extension $F(\alpha)/F$, the field K is algebraically closed in $F(\alpha)$. So the polynomial $f(T)$ is irreducible in $FK'[T]$ (cf. [**11**, Proposition III.6.6]). Denote by Z (respectively Z') the splitting field of $f(T)$ over F (respectively FK'). Let $\alpha_1, \ldots, \alpha_n$ be all conjugates of α over F. We have $Z = F(\alpha_1, \ldots, \alpha_n)$. Since $f(T)$ is irreducible in $FK'[T]$, the conjugates of α over FK' are also given by $\alpha_1, \ldots, \alpha_n$, and hence $Z' = FK'(\alpha_1, \ldots, \alpha_n) = ZK'$ and therefore

$$\mathcal{G}(f,FK') \cong \mathcal{G}(Z'/FK') \cong \mathcal{G}(Z/Z \cap FK').$$

Since the place P of F splits completely in the extension $F(\alpha)/F$, it will also split in the Galois closure Z/F. So the field K is algebraically closed in Z and hence $Z \cap FK' = F$. We obtain

$$\mathcal{G}(f,FK') \cong \mathcal{G}(Z/F) \cong \mathcal{G}(f,F).$$

□

By use of the primitive element theorem, we immediately get the following

LEMMA 5.2. *Let F be a function field over a perfect field K and let E be a finite separable extension of F. Let K' be a separable algebraic extension of K. Suppose that there exists a place P of F splitting completely in the extension E/F. Consider the constant field extensions FK' and EK' of F and E, respectively. Denote by $\mathcal{GC}(E/F)$ respectively $\mathcal{GC}(EK'/FK')$ the Galois closure of the extension E/F respectively EK'/FK'. Then*

$$\mathcal{GC}(EK'/FK') = \mathcal{GC}(E/F)K';$$

i.e., taking the Galois closure of such an extension commutes with extending the field of constants. Moreover the Galois groups of $\mathcal{GC}(EK'/FK')/FK'$ and $\mathcal{GC}(E/F)/F$ are isomorphic.

Denote by F_n the function field of the curve $X_0(p^n)$ reduced modulo a prime ℓ. Note that its constant field is $\mathbb{F}_\ell$. We would like to use Lemma 5.2 in order to gain information on $\mathcal{GC}(F_n/F_r)$. In order to do so, we need that the extension F_n/F_r contains a completely splitting place, but this is not true in general. It is well known however, that if we extend the constant field to $\mathbb{F}_{\ell^2}$, the tower $F_r \subset F_{r+1} \subset \cdots$ is asymptotically optimal. So if the constant field is $\mathbb{F}_{\ell^2}$, we can expect completely splitting places. The following lemma confirms this for a large class of cases.

LEMMA 5.3. *Suppose that ℓ and p are two primes such that $\ell \geq 13$ and $\ell \neq p$, and let $0 < r < n$ be two integers. The extension $F_n\mathbb{F}_{\ell^2}/F_r\mathbb{F}_{\ell^2}$ contains a completely splitting place.*

PROOF. Let $F_{-1}\mathbb{F}_{\ell^2}$ denote the function field arising by reducing the modular curve $X(1)$ modulo ℓ and then extending the constant field. The reason the function fields $F_n\mathbb{F}_{\ell^2}$ have many rational places is that the supersingular j-invariants in $F_{-1}\mathbb{F}_{\ell^2}$ are $\mathbb{F}_{\ell^2}$-rational and all places in $F_n\mathbb{F}_{\ell^2}$ lying above any of these j-invariants different from 0 and 1728 are $\mathbb{F}_{\ell^2}$-rational as well (see Lemma 5.3 in [**1**]). On the other hand, it is well known that the only branching in F_n/F_{-1} occurs at $j = 0$, $j = 1728$ and $j = \infty$.

In order to prove the lemma it is therefore enough to show that there exists a supersingular j-invariant different from 0 and 1728. Such a j-invariant always exists if $\ell \geq 13$ (see [**10**, section V.4]). □

6. Galois closure of a tame tower

Explicit equations for some of the towers considered above (and also for some other modular towers) were given by Elkies (see [**2**]). In particular let $p = 2$ and consider the tower

$$\ldots \to \ldots \to X_0(2^6) \to X_0(2^5) \to X_0(2^4).$$

Let ℓ be a prime such that $\ell \geq 13$. For $i \geq 0$ let M_i be the function field of the curve $X_0(2^{i+4})$, with the field of constants extended to $\mathbb{F}_{\ell^2}$. Hence we have a corresponding tower of function fields

$$\mathcal{M} = (M_0, M_1, M_2, \ldots)$$

over $\mathbb{F}_{\ell^2}$. This tower can be recursively defined as follows (see [**2**] and [**3**, Remark 5.9]): $M_0 = \mathbb{F}_{\ell^2}(x_0)$ is the rational function field and $M_n = M_{n-1}(x_n)$ where

$$x_n^2 = \frac{x_{n-1}^2 + 1}{2x_{n-1}}$$

for $n \geq 1$. This tower was studied in detail in [**3**]. It is an asymptotically optimal tower over $\mathbb{F}_{\ell^2}$. Following Section 5, we can use the group theoretical arguments considered before to obtain detailed information about the Galois closure of the tower $\mathcal{M}$. For $i \geq 0$ let G_i be the Galois closure of M_i over M_0 and consider the sequence of function fields $\mathcal{G} = (G_0, G_1, \ldots)$ called the Galois closure of the tower $\mathcal{M}$ over M_0. Let

$$\mathfrak{M} = \bigcup_{j=0}^{\infty} M_j \quad \text{and} \quad \mathfrak{G} = \bigcup_{j=0}^{\infty} G_j,$$

and let Ω be a fixed algebraically closed field containing $\mathfrak{M}$.

THEOREM 6.1. (1) *$\mathcal{G}$ is a tower over $\mathbb{F}_{\ell^2}$.*

(2) *The tower $\mathcal{G}$ is optimal; i.e., for the limit $\lambda(\mathcal{G})$ of $\mathcal{G}$ we have*

$$\lambda(\mathcal{G}) = \lambda(\mathcal{M}) = \ell - 1.$$

(3) *There exist two embeddings σ, τ of $\mathfrak{M}$ into Ω over M_0, such that*

$$G_i = M_i \cdot \sigma(M_i) \cdot \tau(M_i), \text{ for } i \geq 0,$$

and

$$\mathfrak{G} = \mathfrak{M} \cdot \sigma(\mathfrak{M}) \cdot \tau(\mathfrak{M}).$$

(4) *The extension M_3/M_0 (and more generally the extension M_{i+3}/M_i for $i \geq 0$) is a cyclic Galois extension of degree 8. In particular we have $G_3 = M_3$.*

(5) *We have*

$$[G_i : G_{i-1}] = \begin{cases} 2 & \text{if } 1 \leq i \leq 3, \\ 4 & \text{if } 3 < i \leq 5, \\ 8 & \text{if } 5 < i. \end{cases}$$

(6) *The G_i/G_{i-1} is an elementary abelian 2-extension for $i \geq 1$.*

PROOF. (1) Since there is a place of M_0 splitting completely in the tower $\mathcal{M}$, the result follows from [4, Prop. 2.1]
(2) See [4, Rem. 2.4].
(3) This follows directly from Corollary 2.2 by noting that the matrix

$$A = \begin{pmatrix} 1 & 0 \\ 2^4 & 1 \end{pmatrix}$$

is the same at every step.
(4) This follows from Lemma 4.3, with $p = 2, r = 4$.
(5) This is just a special case of Lemma 4.2.
(6) The Galois groups of the extension G_i/G_{i-1} is given by $\Delta_r(p^i)/\Delta_r(p^{i-1})$. So it follows from Lemma 2.3 that this extension is an elementary abelian 2-extension.

□

Next we will give some alternative generators and equations for the tower considered above. Let $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ be a tower of function fields over a field K, which is recursively defined by the polynomial $f(X, Y) \in K[X, Y]$; i.e., $F_0 = K(x_0)$ is the rational function field, and for every $n \geq 1$, we have $F_n = F_{n-1}(x_n)$ with $f(x_{n-1}, x_n) = 0$.

So in particular we have

$$F_n = F_0(x_1, x_2, \ldots, x_n)$$

for all $n \geq 1$. It turns out that for most of the interesting towers we in fact have

$$F_n = F_0(x_n).$$

The following Lemma gives an easy criterion for this to be the case.

LEMMA 6.2. *Let $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ be a tower of function fields over a field K recursively defined by $f(X, Y) \in K[X, Y]$. Suppose that there exists a place P of F_0 such that the place P is totally ramified in the extension F_n/F_0 and the unique place Q of F_n lying above P is unramified over $K(x_n)$. Then $F_n = F_0(x_n)$.*

PROOF. We have $F_0 \subseteq F_0(x_n) \subseteq F_n$. Since the place Q of F_n is unramified over $K(x_n)$, it will be unramified over $F_0(x_n)$. But since Q is totally ramified in the extension F_n/F_0, we have $F_0(x_n) = F_n$. □

Let ℓ be an odd prime and consider the tower $\mathcal{M} = (M_0, M_1, \ldots)$ over $\mathbb{F}_{\ell^2}$ above, which is recursively defined by

$$Y^2 = \frac{X^2 + 1}{2X}.$$

From the ramification in the tower $\mathcal{M}$ and Lemma 6.2 it follows that $M_n = M_0(x_n)$.

By Theorem 6.1 for $n \geq 0$ the extension M_{n+3}/M_n is a cyclic Galois extension of degree 8. It is hence natural to consider the tower $\mathcal{M}' = (M_0', M_1', M_2' \ldots)$ with $M_n' = M_{3n}$. This is in fact just an alternative way of defining the tower $\mathcal{M}$, where a step in this new description corresponds to 3 steps in the tower $\mathcal{M}$. For $n \geq 0$ let $x_n' = x_{3n}$. Clearly for $n \geq 1$ we then have $M_n' = M_0'(x_n') = M_{n-1}'(x_n')$. It can be verified that the minimal polynomial of x_n' over M_{n-1}' is given by

$$T^8 - T^4 - \frac{(x_{n-1}' - 1)^8}{128x_{n-1}'(x_{n-1}'^2 + 1)(x_{n-1}' + 1)^4} \in M_{n-1}'[T].$$

Letting $f(T) = T^8 - T^4$ we note that

$$\frac{(x_{n-1}' - 1)^8}{128x_{n-1}'(x_{n-1}'^2 + 1)(x_{n-1}' + 1)^4} = \frac{1}{16f\left(\frac{x_{n-1}'+1}{x_{n-1}'-1}\right)}.$$

It hence follows that the tower $\mathcal{M}' = (M_0', M_1', M_2', \ldots)$ can be recursively defined by

$$f(Y) = \frac{1}{16f\left(\frac{X+1}{X-1}\right)},$$

where $f(T) = T^8 - T^4$.

As mentioned before, the steps M_n'/M_{n-1}' are cyclic Galois extensions of degree 8. This can be seen explicitly. Define

$$\alpha_n = \frac{2x_n'}{x_{3n-2} + 1}.$$

Then $\alpha_n \in M_n'$ and it can be shown by an explicit calculation that

$$\alpha_n^8 = \frac{32x_{n-1}'^3}{(x_{n-1}'^2 + 1)(x_{n-1}' + 1)^4}. \tag{6.1}$$

Denote by P the place of M_0' that is the pole of function x_0', by Q a place of M_{n-1}' lying above P in the extension M_{n-1}'/M_0' and by R the place $Q \cap \mathbb{F}_{\ell^2}(x_{n-1}')$. From the ramification structure of the tower $\mathcal{M}$, it follows that R is the pole of the function x_{n-1}' and $e(Q|R) = 1$, see [3]. From this and equation (6.1) it then follows immediately that $M_n' = M_{n-1}'(\alpha_n)$.

We conclude by analyzing a property of the splitting locus of the tower $\mathcal{M}'$. For an odd prime number ℓ we define the Deuring polynomial

$$H(X) = \sum_{i=0}^{(\ell-1)/2} \binom{\frac{\ell-1}{2}}{i}^2 \cdot X^i \in \mathbb{F}_\ell[X].$$

The splitting locus of the tower $\mathcal{M}$ (and hence of $\mathcal{M}'$) is given by all $\alpha \in \bar{\mathbb{F}}_\ell$ such that $H(\alpha^4) = 0$, see [3]. By the recursive definition of the tower this means that if $H(\alpha^4) = 0$ and $\beta \in \bar{\mathbb{F}}_\ell$ satisfies $\beta^2 = (\alpha^2 + 1)/2\alpha$, then $H(\beta^4) = 0$. Considering the above description of the tower $\mathcal{M}'$, we then get the following property for the Deuring polynomial $H(X)$: let $\alpha \in \bar{\mathbb{F}}_\ell$ such that $H(\alpha^4) = 0$ and let $\beta \in \bar{\mathbb{F}}_\ell$ such that $f(\beta) = 1/(16 \cdot f(\frac{\alpha+1}{\alpha-1}))$. Then $H(\beta^4) = 0$.

References

[1] P. Beelen and I.I. Bouw, *Asymptotically good towers and differential equations*, Compositio Math. 141, pp. 1405–1424, 2005.
[2] N.D. Elkies, *Explicit modular towers*, in Proc. 35th Ann. Allerton Conf. on Communication, Control and Computing, Urbana, IL, 1997, pp. 23-32.
[3] A. Garcia, H. Stichtenoth and H. Rück, *On tame towers over finite fields*, J. Reine Angew. Math. 557, pp. 53–80, 2003.
[4] A. Garcia and H. Stichtenoth, *On the Galois closure of towers*, in Recent trends in coding theory and its applications, pp. 83–92, AMS/IP Stud. Adv. Math., 41, Amer. Math. Soc., 2007.
[5] A. Garcia and H. Stichtenoth (eds.), *Topics in geometry, coding theory and cryptography*, Algebr. Appl. 6, Springer-Verlag, 2007.
[6] J. Igusa, *Kroneckerian model of fields of elliptic modular functions*, Amer. J. Math. 81,, pp. 561–577, 1959.

[7] W. Maak, *Elliptische Modulfunktionen*, unter Benutzung einer Vorlesung von E. Hecke aus dem Jahre 1935, lecture notes, Göttingen Univ. 1955/56.
[8] B. Schoeneberg, *Elliptic Modular Functions*, Springer Verlag, 1974.
[9] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Iwanami Shoten Publishers and Princeton University Press, 1971.
[10] J.H. Silverman, *The arithmetic of elliptic curves*, Springer Verlag, 1986.
[11] H. Stichtenoth, *Algebraic function fields and codes*, Springer Verlag, 1993.
[12] H. Stichtenoth, *Transitive and self-dual codes attaining the Tsfasman–Vladut–Zink bound*, IEEE Trans. Inform. Theory 52, no. 5, pp. 2218–2224, 2006.
[13] M.A. Tsfasman, S.G. Vladut and T. Zink, *Modular curves, Shimura curves and Goppa codes, better than the Varshamov–Gilbert bound*, Math. Nachr. 109, pp. 21–28, 1982.

ECOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE, EPFL-SFB-IMB-CSAG, STATION 8, 1015, LAUSANNE, SWITZERLAND
E-mail address: alp.bassa@epfl.ch

DTU-MATHEMATICS, TECHNICAL UNIVERSITY OF DENMARK, MATEMATIKTORVET, BUILDING 303S, DK-2800, LYNGBY, DENMARK
E-mail address: p.beelen@mat.dtu.dk

Contemporary Mathematics
Volume 487, 2009

Codes defined by forms of degree 2 on quadric varieties in $\mathbb{P}^4(\mathbb{F}_q)$

Frédéric A. B. Edoukou

ABSTRACT. We study the functional codes of second order defined by G. Lachaud on $\mathcal{X} \subset \mathbb{P}^4(\mathbb{F}_q)$ a quadric of rank($\mathcal{X}$)=3,4,5. We give some bounds for the number of points of quadratic sections of $\mathcal{X}$, which are the best possible and show that codes defined on non-degenerate quadrics are better than those defined on degenerate quadrics. We also show the geometric structure of the minimum weight codewords and estimate the second weight of these codes. We also prove by using the theorem of Ax on the zeros of polynomials over a finite field that all the weights of the codewords of the codes $C_2(\mathcal{X})$ defined in any quadric in $\mathbb{P}^n(\mathbb{F}_q)$ are divisible by q. The paper ends with a conjecture on the number of points of two quadrics in $\mathbb{P}^n(\mathbb{F}_q)$ with no common hyperplane.

1. Introduction

We denote by $\mathbb{F}_q$ the field with q elements. Let $V = A^{n+1}(\mathbb{F}_q)$ be the affine space of dimension $n+1$ over $\mathbb{F}_q$ and $\mathbb{P}^n(\mathbb{F}_q) = \Pi_n$ the corresponding projective space. Then

$$\pi_n = \#\mathbb{P}^n(\mathbb{F}_q) = q^n + q^{n-1} + ... + 1.$$

We use the term forms of degree h to describe homogeneous polynomials f of degree h, and $Z(f)$ denotes the zeros of f in the projective space $\mathbb{P}^n(\mathbb{F}_q)$. Let $\mathcal{F}_h(V)$ be the vector space of forms of degree h in $V = \mathbb{A}^{n+1}(\mathbb{F}_q)$, $X \subset \mathbb{P}^n(\mathbb{F}_q)$ a variety and $|X|$ the number of rational points of X over $\mathbb{F}_q$. Let W_i be the set of points with homogeneous coordinates $(x_0 : ... : x_n) \in \mathbb{P}^n(\mathbb{F}_q)$ such that $x_j = 0$ for $j < i$ and $x_i \neq 0$. The family $\{W_i\}_{0 \leq i \leq n}$ is a partition of $\mathbb{P}^n(\mathbb{F}_q)$. The code $C_h(X)$ is the image of the linear map $c : \mathcal{F}_h(V) \longrightarrow \mathbb{F}_q^{|X|}$, defined by $c(f) = (c_x(f))_{x \in X}$, where $c_x(f) = f(x_0, ..., x_n)/{x_i}^h$ with $x = (x_0 : ... : x_n) \in W_i$. The length of $C_h(X)$ is equal to $|X|$. The dimension of $C_h(X)$ is equal to $\dim \mathcal{F}_h(V) - \dim \ker c$, where

$$\dim\ \mathcal{F}_h(V) = \binom{n+h}{h}. \tag{1.1}$$

The minimum distance of $C_h(X)$ is equal to the minimum over all non null polynomials f of $|X| - |X \cap Z(f)|$.

2000 *Mathematics Subject Classification.* Primary 05B25, 11T71, 14J29.
Key words and phrases. finite fields, functional codes, projective index, quadric varieties, regulus, weight.