Bull. London Math. Soc. 34 (2002) 291–300 © 2002 London Mathematical Society
DOI: 10.1112/S0024609302001017

AN ASYMPTOTICALLY GOOD TOWER OF CURVES OVER THE FIELD WITH EIGHT ELEMENTS

GERARD VAN DER GEER AND MARCEL VAN DER VLUGT

Abstract

An explicit, asymptotically good, tower of curves over the field with eight elements is constructed. The genus and the number of rational points are calculated explicitly.

Introduction

In this note we construct an explicit, asymptotically good, tower of curves over the field $\mathbf{F}_8$. For a curve C, defined over a finite field $\mathbf{F}_q$ of cardinality q, we denote by $\#C(\mathbf{F}_q)$ the number of $\mathbf{F}_q$-rational points on C. Furthermore, we denote by $N_q(g)$ (as usual) the function

$$N_q(g) = \max\{\#C(\mathbf{F}_q) : C/\mathbf{F}_q,\ g(C) = g\},$$

where C runs through the set of smooth absolutely irreducible projective curves of genus g defined over $\mathbf{F}_q$. Drinfeld and Vladuts showed in [1] the inequality

$$\limsup_{g\to\infty} \frac{N_q(g)}{g} \leqslant \sqrt{q} - 1, \qquad (1)$$

and Ihara constructed in [6], for q a square, a sequence of modular curves that attains the upper bound in (1).

It then came as a surprise when in 1995 Garcia and Stichtenoth constructed in [3], for q a square, a tower of Artin–Schreier covers

$$\ldots \longrightarrow C_i \longrightarrow C_{i-1} \longrightarrow \ldots \longrightarrow C_1 \longrightarrow C_0,$$

which is defined over $\mathbf{F}_q$ and is given by a simple recursive equation such that

$$\lim_{i\to\infty} g(C_i) = \infty \quad \text{and} \quad \lim_{i\to\infty} \frac{\#C_i(\mathbf{F}_q)}{g(C_i)} = \sqrt{q} - 1.$$

An infinite tower $C_\bullet$ of covers of curves over $\mathbf{F}_q$:

$$\ldots \longrightarrow C_i \longrightarrow C_{i-1} \longrightarrow \ldots \longrightarrow C_1 \longrightarrow C_0,$$

with $g(C_i) > 1$ for some $i \geqslant 0$, is called an *asymptotically good tower* if

$$\ell(C_\bullet) = \lim_{i\to\infty} \frac{\#C_i(\mathbf{F}_q)}{g(C_i)} > 0.$$

Note that in [4] it is shown that this limit exists for towers having at least one index i with $g(C_i) > 1$.

Apart from having an evident charm of their own, asymptotically good towers are important for coding theory, since such towers enable the construction of long

Received 20 March 2001; revised 30 May 2001.

2000 *Mathematics Subject Classification* 11R58, 11G20, 14Hxx.

error-correcting codes over $\mathbf{F}_q$ that can correct a fixed percentage of errors per codeword, and have a positive transmission rate. However, for this application it is essential that the curves be in explicit form.

For q not a square, the results are much less complete. It is not known how good the Drinfeld–Vladuts upper bound (1) is for that case. For q not a square, asymptotically good towers of curves are mainly obtained by class field theory; see for example [**7**]. These constructions are not explicit. In 1985 Zink, using certain Shimura surfaces, constructed in [**8**] a tower $C_\bullet$ of curves defined over $\mathbf{F}_{p^3}$, for p a prime, with limit

$$\ell(C_\bullet) \geqslant \frac{2(p^2-1)}{p+2}, \tag{2}$$

but that construction is far from explicit. In [**5**] there is an explicit asymptotically good tower of Kummer covers over $\mathbf{F}_{q=p^m}$ for $m \geqslant 2$, with limit

$$\ell(C_\bullet) \geqslant \frac{2}{q-2}.$$

Here, we present an explicit tower $C_\bullet$ of Artin–Schreier curves defined over $\mathbf{F}_8$ and given by a simple recursive equation with limit

$$\ell(C_\bullet) = 3/2.$$

One should compare this with (2). It remains an interesting problem to see whether our explicit tower is related to that of Zink; see the remarks made by Elkies at the end of [**2**]. Another interesting problem is to extend our construction to other fields of odd degree over the prime field.

We give explicit formulas for the genus and number of rational points for the curves C_i in our tower. The ramification behaviour turns out to be rather subtle, with alternating ramification and non-ramification.

1. *The basic equation*

In our search for curves over finite fields with many points, we came across a curve defined over $\mathbf{F}_8$ with a remarkable property. The curve of genus 1 given by the affine equation

$$x_1^2 + x_1 = x_0 + 1 + 1/x_0$$

has fourteen $\mathbf{F}_8$-rational points, and attains the Hasse–Weil bound for $\mathbf{F}_8$. To each $x_0 \in \mathbf{F}_8 - \mathbf{F}_2$, there correspond two solutions $x_1 \in \mathbf{F}_8 - \mathbf{F}_2$; and if x_0 runs through $\mathbf{F}_8 - \mathbf{F}_2$, then so does x_1. This implies that the system of equations

$$x_{i+1}^2 + x_{i+1} = x_i + 1 + 1/x_i, \qquad i = 0, 1, 2, \ldots,$$

has sequences of solutions $(x_0, x_1, x_2, \ldots)$ for every $x_0 \in \mathbf{F}_8 - \mathbf{F}_2$.

Consider, in $\mathbb{P}^1 \times \mathbb{P}^1$ over the field $\mathbf{F}_2$, the closure of the affine curve given by the equation

$$x_1^2 + x_1 = x_0 + 1 + 1/x_0.$$

This defines a smooth projective curve C of genus 1, together with two morphisms $b_1 : C \to \mathbb{P}^1$, $(x_0, x_1) \mapsto x_0$, and $e_1 : C \to \mathbb{P}^1$, $(x_0, x_1) \mapsto x_1$, of degree 2. The curve C possesses two points that are rational over $\mathbf{F}_2$, eight points rational over $\mathbf{F}_4$, and fourteen points rational over $\mathbf{F}_8$. The correspondence C in $\mathbb{P}^1 \times \mathbb{P}^1$ preserves the points of $\mathbb{P}^1(\mathbf{F}_8) - \mathbb{P}^1(\mathbf{F}_2)$, and (surprisingly) also those of $\mathbb{P}^1(\mathbf{F}_4)$.

We consider the following infinite tower $C_\bullet$ of smooth projective curves defined over $\mathbf{F}_2$:

$$\longrightarrow C_i \xrightarrow{\pi_i} C_{i-1} \xrightarrow{\pi_{i-1}} \dots \xrightarrow{\pi_2} C_1 \xrightarrow{\pi_1} C_0 = \mathbb{P}^1,$$

where we take an affine coordinate x_0 on C_0, and where the cover $C_i \to C_{i-1}$ is given by the affine equation

$$x_i^2 + x_i = x_{i-1} + 1 + \frac{1}{x_{i-1}}, \quad \text{for } i \geqslant 1. \tag{3}$$

Equivalently, we can describe the curve C_i as the normalization of the curve D_i defined by

$$D_i = \{(p_0, p_1, \dots, p_i) \in \mathbb{P}^1 \times \dots \times \mathbb{P}^1 : (p_j, p_{j+1}) \in C, \text{ for } j = 0, \dots, i-1)\}.$$

This shows that for $i \geqslant 1$, C_i admits two maps, $b_i : C_i \longrightarrow C_{i-1}$ and $e_i : C_i \longrightarrow C_{i-1}$, given (on the model D_i) by $(p_0, \dots, p_i) \mapsto (p_0, \dots, p_{i-1})$ and $(p_0, \dots, p_i) \mapsto (p_1, \dots, p_i)$, respectively. The curve C_i is then the normalization of the fibre product

$$C_{i-1} \times_{C_{i-2}} C_{i-1}$$

via the maps b_{i-1} and e_{i-1}.

We now work over the algebraic closure $\mathbf{F}$ of $\mathbf{F}_2$, and consider geometric points of $C_i \otimes \mathbf{F}$. It will turn out that ramification in C_i/C_{i-1} can occur only at points P that map to a point of D_i with coordinates in $\mathbb{P}^1(\mathbf{F}_4)$. We therefore introduce the following notation for such points. By $P = P(a_0, a_1, \dots, a_i)$ with $a_j \in \mathbb{P}^1(\mathbf{F}_4)$, we denote a point on C_i such that $x_j(P) = a_j$ for $0 \leqslant j \leqslant i$. That is, the point $(a_0, \dots, a_i)$ is the image point in D_i, and will be called the *index sequence* of the point. Note that because of the normalization, a point $P(a_0, \dots, a_i)$ of C_i is not necessarily uniquely determined by its index sequence $(a_0, \dots, a_i)$ on D_i.

We shall write ρ for a primitive element of $\mathbf{F}_4$. Note that in an index sequence $(a_0, a_1, \dots, a_i)$ of a point P, we have

∞		∞
0		∞
1	is followed by	ρ or ρ^2
ρ		0 or 1
ρ^2		0 or 1.

Sometimes we shall write $(a_0, \dots, a_i, \infty^j)$ for a point $(a_0, \dots, a_i, \underbrace{\infty, \dots, \infty}_{j\times})$.

2. *The principal part of the x_i*

The main problem in finding the limit $\ell(C_\bullet)$ of our tower lies in the determination of the genus $g(C_i)$. In order to compute it, we have to find the ramification divisor of C_{i+1} over C_i. Since we are dealing with Artin–Schreier equations, we can restrict ourselves to the points that are poles of the function $f_i = x_i + 1 + 1/x_i$. The contribution to the ramification is determined by the orders $\mathrm{ord}_P(f_i^*)$ for the poles P on C_i of the Artin–Schreier reduction f_i^* of the function f_i.

LEMMA 2.1. *The zeros of x_i on C_i are of the form $P(a_0, a_1, \dots, a_i)$, with $a_i = 0$, $a_{i-j} \in \mathbf{F}_4 - \mathbf{F}_2$ for $j \geqslant 1$ odd, and $a_{i-j} = 1$ for $j \geqslant 2$ even. The poles of x_i are of the form $P(b_0, b_1, \dots, b_j, \infty^{i-j})$, with $0 \leqslant j \leqslant i-1$ and $(b_0, \dots, b_j)$ an index sequence of a zero of x_j or of the form $P(\infty^{i+1})$.*

Proof. We use induction on i. The lemma is true for x_0. From the equation

$$x_i^2 + x_i = \frac{x_{i-1}^2 + x_{i-1} + 1}{x_{i-1}} = f_{i-1}$$

it follows that we have equality of divisors on C_i:

$$(f_{i-1}) = (x_i) + (x_i + 1) = (x_i)_0 + (x_i)_1 - 2(x_i)_\infty.$$

So the poles of x_i lie above the poles of f_{i-1}, and the points P on C_i with $x_i(P) \in \mathbf{F}_2$ lie above the zeros of f_{i-1}. Moreover, we have

$$\begin{aligned}(f_{i-1}) &= (x_{i-1} + \rho) + (x_{i-1} + \rho^2) - (x_{i-1}) \\ &= (x_{i-1})_\rho + (x_{i-1})_{\rho^2} - (x_{i-1})_0 - (x_{i-1})_\infty,\end{aligned}$$

which implies that the poles of f_{i-1} are the zeros and poles of x_{i-1}, while the zeros of f_{i-1} are the points P on C_{i-1} with $x_{i-1}(P) \in \mathbf{F}_4 - \mathbf{F}_2$. Hence the poles of x_i are the points on C_i above the zeros and the poles of x_{i-1} on C_{i-1}, whereas the zeros of x_i lie above the points P on C_{i-1} with $x_{i-1}(P) \in \mathbf{F}_4 - \mathbf{F}_2$. So we obtain the index sequence of a pole of x_i by adding ∞ to a zero or pole of x_{i-1}, and we obtain the index sequence of a zero of x_i by adding a zero to an index sequence that ends with an element of $\mathbf{F}_4 - \mathbf{F}_2$, and in which 1 and elements of $\{\rho, \rho^2\}$ alternate. □

In the discussion that follows, we shall develop rational functions on C_i as a power series in a local parameter at a given point P; that is, we consider the function as an element of the quotient field of the completion of the local ring of P. Often, we are interested only in the principal part, and we ignore elements that are regular, that is, elements of (the completion of) the local ring. By the notation

$$f = g + O(P),$$

we mean that $f - g$ is regular at P, that is, is an element of O_P or of $\hat{O}_P$.

Consider now a sequence of points $P_0 \in C_0, P_1 \in C_1, \ldots, P_i \in C_i$, with $\pi_\ell(P_\ell) = P_{\ell-1}$ for $\ell = 1, \ldots, i$, and with the property that 1 and ρ or ρ^2 alternate in the index sequence $(a_0, \ldots, a_i)$ of P_i.

We shall first assume that $a_0 = 1$. Then the function $t = x_0 + 1$ provides a local parameter at P_0 on C_0, and the pull-back (under the maps π_ℓ) of this function (again denoted by t) is still a local parameter at the points P_j on C_j for $j \leqslant i$.

In the completion of the local ring $\hat{O}_{P_j} \cong \mathbf{F}[[t]]$, the function x_j can be written as a power series in t:

$$x_j = a_j + m_j(t),$$

where $m_j(t) \in \mathbf{F}[[t]]$ has $\mathrm{ord}_t(m_j) \geqslant 1$.

Lemma 2.2. *In the quotient field $\mathbf{F}((t))$ of the formal power series ring $\hat{O}_{P_j} \cong \mathbf{F}[[t]]$, the function $m_j(t)$ satisfies, for $0 \leqslant j \leqslant i$, the relations*

$$\frac{1}{m_j} = \begin{cases} \dfrac{a_{j-1}}{m_{j-1}} + O(P_j), & \text{for } j \geqslant 2 \text{ even,} \\[2ex] \dfrac{1}{m_{j-1}^2} + \dfrac{1}{m_{j-1}} + O(P_j), & \text{for } j \text{ odd.} \end{cases}$$

Proof. We start with $m_0(t) = t$. For even $j \geqslant 2$, we have $a_{j-1} \in \{\rho, \rho^2\}$ and $a_j = 1$, since we assumed that $a_0 = 1$.

From the relation

$$x_j^2 + x_j = x_{j-1} + 1 + 1/x_{j-1},$$

we obtain

$$\begin{aligned} m_j^2 + m_j &= a_{j-1} + m_{j-1} + 1 + 1/(a_{j-1} + m_{j-1}) \\ &= a_{j-1} + m_{j-1} + 1 + (1/a_{j-1}) \sum_{n=0}^{\infty} (m_{j-1}/a_{j-1})^n \\ &= a_{j-1}^2 m_{j-1} + m_{j-1}^2 + \text{higher powers of } m_{j-1}. \end{aligned}$$

This implies that m_j is the product of $a_{j-1}^2 m_{j-1}$ with a 1-unit u in m_{j-1}, that is, a unit of the form $u = 1 + r$ with $r \in (m_{j-1})$. So we get

$$\frac{1}{m_j} = \frac{a_{j-1}}{m_{j-1}} \cdot u = \frac{a_{j-1}}{m_{j-1}} + O(P_j).$$

For j odd, we have $a_j \in \{\rho, \rho^2\}$ and $a_{j-1} = 1$. In the same way as for j even, we obtain

$$a_j^2 + m_j^2 + a_j + m_j = 1 + m_{j-1} + 1 + \frac{1}{1 + m_{j-1}} = 1 + \sum_{n=2}^{\infty} m_{j-1}^n;$$

that is, $m_j^2 + m_j = \sum_{n=2}^{\infty} m_{j-1}^n$, so that we have

$$m_j = m_{j-1}^2 + m_{j-1}^3 + \text{higher powers of } m_{j-1}.$$

This means that

$$\begin{aligned} \frac{1}{m_j} &= \frac{1}{m_{j-1}^2} + \frac{1}{m_{j-1}} + \text{higher powers of } m_{j-1} \\ &= \frac{1}{m_{j-1}^2} + \frac{1}{m_{j-1}} + O(P_j). \end{aligned}$$

This completes the proof of the lemma. □

We denote the principal part of $1/m_j$ by F_j. We can now deduce the following corollary.

COROLLARY 2.3. *The principal part F_j of $1/m_j$ satisfies:*

$$F_j = \begin{cases} F_{j-1}^2 + F_{j-1}, & \textit{for } j \textit{ odd}, \\ a_{j-1} \cdot F_{j-1}, & \textit{for } j \geqslant 2 \textit{ even}. \end{cases}$$

Furthermore, F_j is a 2-linearized polynomial in $1/t$ of the form

$$F_j = \frac{b_k}{t^{2^k}} + \frac{b_{k-1}}{t^{2^{k-1}}} + \ldots + \frac{b_0}{t},$$

where $k = [(j+1)/2]$, the coefficients b_ℓ are in $\mathbf{F}_4$, and $b_k \neq 0$.

Proof. The relations for F_j follow at once from Lemma 2.2. We have $F_0 = 1/t$ and $F_1 = 1/t^2 + 1/t$, from which the formula for F_j follows by induction. □

For an index sequence $(a_0, a_1, \ldots, a_i)$ where $a_0 \in \{\rho, \rho^2\}$, we have a similar result.

3. *The ramification behaviour*

Now we study the ramification behaviour at a point $P_i = P(a_0, \ldots, a_{i-1}, a_i = 0)$ which is a zero of x_i on C_i for $i \geqslant 2$. We assume that $a_0 = 1$. Then $a_{\mathrm{odd}} \in \{\rho, \rho^2\}$, and i is even. At a point P_i where $a_0 \in \{\rho, \rho^2\}$, the ramification behaviour is similar.

Since we are working with Artin–Schreier covers, we introduce here the standard notation $\wp(f) = f^2 + f$ for an element f in one of our function fields.

Lemma 3.1. *A linear combination $\sum_{j=2,\,\mathrm{even}}^{i} B_{j,i}F_j$ with coefficients $B_{j,i} \in \mathbf{F}_4$ can be written as*

$$\sum_{j=2,\,\mathrm{even}}^{i} B_{j,i}F_j = \wp\left(\sum_{j=0,\,\mathrm{even}}^{i-2} B_{j,i-2}F_j \right) + B_i^* F_0 \tag{4}$$

with

$$B_i^* = \wp\left(\sum_{j=2,\,\mathrm{even}}^{i} B_{j,i}a_{j-1} \right) \tag{5}$$

and

$$B_{j,i-2} = \left(B_i^* + \wp\left(\sum_{k=2,\,\mathrm{even}}^{j} B_{k,i}a_{k-1} \right) \right) a_{j+1}^2 + \wp(B_{j+2,i}). \tag{6}$$

Proof. Using Corollary 2.3, we find, for even $j \geqslant 2$,

$$B_{j,i}F_j = B_{j,i}a_{j-1}F_{j-1} = B_{j,i}a_{j-1}\wp(F_{j-2}) = \wp(B_{j,i}^2 a_{j-1}^2 F_{j-2}) + \wp(B_{j,i}a_{j-1})F_{j-2};$$

that is

$$B_{j,i}F_j = \wp(B_{j,i}^2 a_{j-1}^2 F_{j-2}) + \wp(B_{j,i}a_{j-1})F_{j-2}. \tag{7}$$

Applying (7) to the second term in the right-hand side of (7), we obtain

$$\wp(B_{j,i}a_{j-1})F_{j-2} = \wp\big((\wp(B_{j,i}a_{j-1})a_{j-3}^2 F_{j-4}\big) + \wp(B_{j,i}a_{j-1})F_{j-4},$$

where we use $a_{\mathrm{odd}}^2 + a_{\mathrm{odd}} = 1$. Continuing in this way, we find an expression for $B_{j,i}F_j$ as

$$\wp(\text{linear combination of } F_{j-2}, \ldots, F_0\ ) + \wp(B_{j,i}a_{j-1})F_0.$$

Adding these relations for all terms in $\sum_{j=2,\,\mathrm{even}}^{i} B_{j,i}F_j$, we find (4) with coefficients satisfying the equations (5) and (6). □

Note that all the coefficients are in $\mathbf{F}_4$, and that B_i^* is in $\mathbf{F}_2$.

The cover C_{i+1}/C_i is given by the equation

$$x_{i+1}^2 + x_{i+1} = x_i + 1 + 1/x_i.$$

At a point P_i with index sequence $(1, a_1, \ldots, a_{i-1}, 0)$, we have the relation

$$x_{i+1}^2 + x_{i+1} = \frac{1}{m_i} + O(P_i) = F_i + O(P_i). \tag{8}$$

Therefore, the principal part of $x_{i+1}^2 + x_{i+1}$ at P_i is F_i. According to Lemma 3.1, we have

$$F_i = \wp\left(\sum_{j=0,\,\mathrm{even}}^{i-2} B_{j,i-2}F_j \right) + B_i^* F_0$$

with $B_i^* = a_{i-1}^2 + a_{i-1} = 1$ and $B_{j,i-2} = a_{j+1}^2$ for even $j = 0, 2, \ldots, i-2$.

By the substitution

$$X_{i+1} = \sum_{j=0}^{i-2} B_{j,i-2}F_j + x_{i+1},$$

we can reduce equation (8) to

$$X_{i+1}^2 + X_{i+1} = B_i^* F_0 + O(P_i) = F_0 + O(P_i), \tag{9}$$

with $F_0 = 1/t$.

Corollary 3.2. *The point $P_i = P(a_0 = 1, a_1, \ldots, a_i = 0)$ is totally ramified in C_{i+1}/C_i, and the contribution of P_i to the ramification divisor of C_{i+1}/C_i is* 2. *At the pole $P_{i+1} = P_i(\infty)$ of x_{i+1}, we have*

$$\mathrm{ord}_{P_{i+1}}(x_{i+1}) = -2^{[(i+1)/2]}.$$

As the next step, we consider the behaviour of the pole $P_{i+1} = P_i(\infty)$ of the function $f_{i+1} = x_{i+1} + 1 + 1/x_{i+1}$ in the cover C_{i+2}/C_{i+1}. At P_{i+1}, the equation of C_{i+2}/C_{i+1} is

$$\begin{aligned} x_{i+2}^2 + x_{i+2} &= x_{i+1} + O(P_{i+1}) \\ &= \sum_{j=0,\,\mathrm{even}}^{i-2} B_{j,i-2}F_j + X_{i+1} + O(P_{i+1}). \end{aligned} \tag{10}$$

If we apply Lemma 3.1 to the linear combination $\sum_{j=2,\,\mathrm{even}}^{i-2} B_{j,i-2}F_j$, the right-hand side of (10) becomes

$$\wp\left(\sum_{j=0,\,\mathrm{even}}^{i-4} B_{j,i-4}F_j \right) + B_{i-2}^* F_0 + B_{0,i-2}F_0 + X_{i+1} + O(P_{i+1}). \tag{11}$$

Then, by using (9), that is, by substituting $F_0 = X_{i+1}^2 + X_{i+1} + O(P_{i+1})$, expression (11) is converted to

$$\wp\left(\sum_{j=0,\,\mathrm{even}}^{i-4} B_{j,i-4}F_j \right) + \wp(B_{i-2}^* X_{i+1}) + \wp(B_{0,i-2}^2 X_{i+1}) + (B_{0,i-2}^2 + B_{0,i-2} + 1)X_{i+1} + O(P_{i+1})$$

with $B_{0,i-2}^2 + B_{0,i-2} + 1 = a_1^2 + a_1 + 1 = 0$. Hence the equation of C_{i+2}/C_{i+1} at P_{i+1} is of the form

$$x_{i+2}^2 + x_{i+2} = \wp\left(\sum_{j=0}^{i-4} B_{j,i-4}F_j \right) + \wp\big((B_{i-2}^* + B_{0,i-2}^2)X_{i+1}\big) + O(P_{i+1}). \tag{12}$$

Corollary 3.3. *The pole P_{i+1} of f_{i+1} is unramified in the cover C_{i+2}/C_{i+1}, and at a point $P_{i+2} = P_{i+1}(\infty)$ above P_{i+1}, we have*

$$\mathrm{ord}_{P_{i+2}}(x_{i+2}) = -2^{[(i+1)/2]-1}.$$

Note that (12) implies that

$$x_{i+2} + \left(\sum_{j=0,\,\mathrm{even}}^{i-4} B_{j,i-4}F_j \right) + (B_{i-2}^* + B_{0,i-2}^2)X_{i+1}$$

is integral at the point P_{i+2}.

To analyse the situation at P_{i+2}, we start with the equation of C_{i+3}/C_{i+2} at this point:

$$\begin{aligned} x_{i+3}^2 + x_{i+3} &= x_{i+2} + O(P_{i+2}) \\ &= \left(\sum_{j=0,\,\mathrm{even}}^{i-4} B_{j,\,i-4} F_j \right) + (B_{i-2}^* + B_{0,\,i-2}^2) X_{i+1} + O(P_{i+2}). \end{aligned} \tag{13}$$

Using Lemma 3.1 and equation (9), the right-hand side of equation (13) is of the form

$$\begin{aligned} \wp\left(\sum_{j=0,\,\mathrm{even}}^{i-6} B_{j,\,i-6} F_j \right) &+ \wp\big((B_{i-4}^* + B_{0,\,i-4}^2) X_{i+1}\big) \\ &+ \big(\wp(B_{0,\,i-4}) + B_{i-2}^* + B_{0,\,i-2}^2\big) X_{i+1} + O(P_{i+2}). \end{aligned} \tag{14}$$

Since equation (6) implies that $\wp(B_{0,\,i-4}) = B_{i-2}^*$, the coefficient of X_{i+1} in (14) is $B_{0,\,i-2}^2 = a_1^2$. So the right-hand side of (13) has the form

$$\wp(\gamma) + B_{0,\,i-2}^2 X_{i+1} + O(P_{i+2})$$

for some $\gamma \in \mathbf{F}(C_{i+2})$. If we set

$$X_{i+3} = \sum_{j=0,\,\mathrm{even}}^{i-6} B_{j,\,i-6} F_j + (B_{i-4}^* + B_{0,\,i-4}^2) X_{i+1},$$

the equation of C_{i+3}/C_{i+2} becomes

$$X_{i+3}^2 + X_{i+3} = B_{0,\,i-2}^2 X_{i+1} + O(P_{i+2}). \tag{15}$$

COROLLARY 3.4. *The point P_{i+2} is totally ramified in the cover C_{i+3}/C_{i+2}, and the contribution to the ramification divisor is* 2. *At $P_{i+3} = P_{i+2}(\infty)$ above P_{i+2}, we have*

$$\mathrm{ord}_{P_{i+3}}(x_{i+3}) = -2^{[(i+1)/2]-1}.$$

If we continue along these lines we obtain the following formulas.

FORMULA 3.5. For t even and $2 \leqslant t \leqslant i$, the equation of C_{i+t}/C_{i+t-1} at a point P_{i+t-1} is

$$\begin{aligned} x_{i+t}^2 + x_{i+t} = \wp\left(\sum_{j=0,\,\mathrm{even}}^{i-2t} B_{j,\,i-2t} F_j \right) &+ \wp\big((B_{i-2t+2}^* + B_{0,\,i-2t+2}^2) X_{i+1}\big) \\ + \sum_{k=1}^{t/2-1} \wp\big((B_{2k-2,\,i-2t+4k} B_{2k-2,\,i-2}^2) X_{i+2k+1}\big) &+ O(P_{i+t-1}). \end{aligned}$$

FORMULA 3.6. For t odd and $3 \leqslant t \leqslant i-1$, the equation of C_{i+t}/C_{i+t-1} at a point P_{i+t-1} is

$$\begin{aligned} x_{i+t}^2 + x_{i+t} = \wp\left(\sum_{j=0,\,\mathrm{even}}^{i-2t} B_{j,\,i-2t} F_j \right) &+ \wp\big((B_{i-2t+2}^* + B_{0,\,i-2t+2}^2) X_{i+1}\big) \\ + \sum_{k=1}^{(t-3)/2} \wp\big((B_{2k-2,\,i-2t+4k} B_{2k-2,\,i-2}^2) X_{i+2k+1}\big) &+ B_{t-3,\,i-2}^2 X_{i+t-2} + O(P_{i+t-1}). \end{aligned}$$

REMARK 3.7. The function X_{i+2k+1} with $k \geqslant 1$ satisfies an equation of the form

$$X_{i+2k+1}^2 + X_{i+2k+1} = B_{2k-2,\,i-2}^2 X_{i+2k-1} + O(P_{i+2k}).$$

We also find that

$$\mathrm{ord}_{P_{i+t}}(x_{i+t}) = -2^{[(i+2)/2]-[t/2]}, \qquad \text{for } 2 \leqslant t \leqslant i.$$

Hence $\mathrm{ord}_{P_{2i}}(x_{2i}) = -1$, and this implies that from P_{2i} on, the extensions in the tower are totally ramified above P_{2i}, and their contribution to the ramification divisor is 2.

We summarize the preceding results in the following theorem.

THEOREM 3.8. *A pole $P_{i+j} = P(a_0, \ldots, a_{i-1}, 0, \infty^j)$ of x_{i+j} on C_{i+j} for $j \geqslant 1$ (or of $1/x_i$ on C_i for $j = 0$) with $a_0 = 1$, is*

(1) *totally ramified in C_{i+j+1}/C_{i+j} for j with $j = 0, 2, 4, \ldots, i-2$ or with $j \geqslant i$, and each of these contributes 2 to the ramification divisor;*

(2) *unramified in C_{i+j+1}/C_{i+j} for $j = 1, 3, 5, \ldots, i-1$.*

For a pole that has an index sequence starting with $a_0 \in \{\rho, \rho^2\}$, there is the following similar result.

THEOREM 3.9. *A pole $P_{i+j} = P(a_0, \ldots, a_{i-1}, 0, \infty^j)$ of the function x_{i+j} on C_{i+j} for $j \geqslant 1$ with $a_0 \in \{\rho, \rho^2\}$ (or of $1/x_i$ on C_i for $j = 0$) is*

(1) *totally ramified in C_{i+j+1}/C_{i+j} for all j with $j = 0, 2, 4, \ldots, i-3$, and for all j with $j \geqslant i-1$, with contribution 2 to the ramification divisor;*

(2) *unramified in C_{i+j+1}/C_{i+j} for $j = 1, 3, 5, \ldots, i-2$.*

REMARK 3.10. We always have the totally ramified points $P(\infty, \infty, \ldots, \infty)$ and also $P(0, \infty, \infty, \ldots, \infty)$, which contribute 2 to the ramification divisor.

4. *The genus and the number of points in the tower*

In order to compute the genus of our curve C_i, we have to count the number of points on the curve C_i that contribute to the ramification divisor. We find, using Theorems 3.8 and 3.9 and Remark 3.10, that the following theorem holds.

THEOREM 4.1. *Let n_i be the number of points on C_i which are totally ramified in C_{i+1}/C_i. Then*

$$n_i = \begin{cases} ([(i+2)/4]+2)2^{i/2}, & \text{for } i \text{ even}, \\ ([i/4]+2)2^{(i+1)/2}, & \text{for } i \text{ odd}. \end{cases}$$

Now it is not difficult to determine the genus $g(C_i)$ of C_i. From the Hurwitz formula, it follows that

$$g(C_i) = 1 + \sum_{j=1}^{i-1} 2^{i-j-1} n_j. \tag{16}$$

If we combine (16) with Theorem 4.1, we get the next theorem.

THEOREM 4.2. *The genus $g(C_i)$ of C_i satisfies*

$$g(C_i) = 2^{i+2} + 1 - \begin{cases} (i+10)2^{(i/2)-1}, & \textit{for } i \textit{ even,} \\ (i+2[i/4]+15)2^{(i-3)/2}, & \textit{for } i \textit{ odd.} \end{cases}$$

Now we count the number $\#C_i(\mathbf{F}_8)$ of $\mathbf{F}_8$-rational points on C_i.

THEOREM 4.3. *For $i \geqslant 1$, we have $\#C_i(\mathbf{F}_8) = 6 \cdot 2^i + 2$.*

Proof. Let α be a primitive element of $\mathbf{F}_8$ that satisfies $\alpha^3 + \alpha + 1 = 0$. For $x \in \mathbf{F}_8 - \mathbf{F}_2$, we find that

$$\left\{x + \frac{1}{x} + 1 : x \in \mathbf{F}_8 - \mathbf{F}_2\right\} = \{\alpha, \alpha^2, \alpha^4\},$$

but also that

$$\{y^2 + y : y \in \mathbf{F}_8 - \mathbf{F}_2\} = \{\alpha, \alpha^2, \alpha^4\}.$$

This means that a point $x \in \mathbb{P}^1(\mathbf{F}_8)$ with $x \notin \mathbb{P}^1(\mathbf{F}_2)$ splits completely in the tower. This yields $6 \cdot 2^i$ rational points over $\mathbf{F}_8$ on C_i. Besides these, we have two totally ramified points $P(0, \infty, \ldots, \infty)$ and $P(\infty, \ldots, \infty)$ defined over $\mathbf{F}_2$. □

Combining this with the formula for the genus, we obtain the following theorem.

THEOREM 4.4. *The tower of curves $C_\bullet$ over $\mathbf{F}_8$ is asymptotically good, with limit*

$$\lim_{i\to\infty} \frac{\#C_i(\mathbf{F}_8)}{g(C_i)} = \frac{3}{2}.$$

References

1. V. G. DRINFELD and S. G. VLADUTS, 'Number of points of an algebraic curve', *Funct. Anal. Applications* 17 (1983) 68–69.

2. N. ELKIES, 'Explicit modular towers', *Proc. Thirty-fifth Annual Allerton Conference on Communication, Control and Computing, 1997* (ed. T. Basar and A. Vardy, Univ. of Illinois at Urbana Champaign, 1998).

3. A. GARCIA and H. STICHTENOTH, 'A tower of Artin–Schreier extensions of function fields attaining the Drinfeld–Vladuts bound', *Invent. Math.* 121 (1995) 211–222.

4. A. GARCIA and H. STICHTENOTH, 'On the asymptotic behaviour of some towers of function fields over finite fields', *J. Number Theory* 61 (1996) 248–273.

5. A. GARCIA, H. STICHTENOTH and M. THOMAS, 'On towers and composita of towers of function fields over finite fields', *Finite Fields Appl.* 3 (1997) 257–274.

6. Y. IHARA, 'Some remarks on the number of points of algebraic curves over finite fields', *J. Fac. Sci. Tokyo*, Ser. Ia, 28 (1982) 721–724.

7. H. NIEDERREITER and C. XING, 'Global function fields with many rational places and their applications', *Contemp. Math.* 225 (1999) 87–111.

8. TH. ZINK, 'Degeneration of Shimura curves and a problem in coding theory', *Fundamentals of computation theory*, Lecture Notes in Comput. Sci. 199 (Springer, Berlin, 1985) 503–511.

Korteweg–de Vries Institut
Universiteit van Amsterdam
Plantage Muidergracht 24
1018 TV Amsterdam
The Netherlands

geer@science.uva.nl

Mathematisch Instituut
Universiteit Leiden
Niels Bohrweg 1
2333 CA Leiden
The Netherlands

vlugt@math.leidenuniv.nl