Serdica J. Computing **1** (2007), 171–184

Serdica
Journal of Computing

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

ON THE CONSTRUCTION OF CODES FROM AN ASYMPTOTICALLY GOOD TOWER OVER $\mathbb{F}_8$

Caleb McKinley Shor

Abstract. In 2002, van der Geer and van der Vlugt gave explicit equations for an asymptotically good tower of curves over the field $\mathbb{F}_8$. In this paper, we will present a method for constructing Goppa codes from these curves as well as explicit constructions for the third level of the tower. The approach is to find an associated plane curve for each curve in the tower and then to use the algorithms of Haché and Le Brigand to find the corresponding Goppa codes.

1. Introduction. In [2] and [3], Garcia and Stichtenoth gave equations for infinite families of curves over finite fields of square cardinality that have many points relative to their genera. One can use these towers to find asymptotically good towers of error-correcting codes, which are families of codes of increasing length for which the sum of the relative distance and rate is bounded below by a positive constant. In order to construct the associated Goppa codes, one method is to calculate a basis for the Riemann-Roch space associated to a particular divisor. This is a difficult task because of the singularities involved in each level of the towers.

ACM Computing Classification System (1998): J.2.
Key words: asymptotically good tower, code construction, desingularization.

A number of people have worked towards creating codes from these towers. Codes from the first few levels can be found in [10], for instance. Work has also been done to find a basis of $\mathcal{L}(mQ)$ for every level in each tower, such as in [1] and [7].

Since [2] and [3], a number of families of curves with many points relative to their genera have been found over various base fields. In [9], van der Geer and van der Vlugt presented a tower over $\mathbb{F}_8$, which is the main focus of this paper. To each curve in this tower, we are able to associate a projective plane curve that has the same corresponding function field. Once we have the plane curve, we can use the algorithms of [5] to construct the corresponding codes.

The aim of this paper is to demonstrate code construction from the first few levels of the tower of van der Geer and van der Vlugt along with a method to create codes from any level. Throughout, we will follow the function field and coding theory notation of [8]. In particular, for a linear code C over $\mathbb{F}_q$, one is often interested in length n, the dimension k, and the minimum distance d. For such a code, there are q^k codewords, and one can decode up to $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors.

2. A tower over $\mathbb{F}_8$. The asymptotically good tower of van der Geer and van der Vlugt (from [9]) can be described as follows: Let C be the closure of the affine curve in $\mathbb{P}^1 \times \mathbb{P}^1$ over $\mathbb{F}_2$ given by

$$y^2 + y = x + 1 + 1/x,$$

and let

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

For C_i the normalization of D_i, we consider the tower $\mathcal{C} = (C_1, C_2, \ldots)$. For $F_0 = \mathbb{F}_2(x_0)$, the function field F_i associated to C_i is

$$F_i = F_{i-1}(x_i),$$

where

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

for $j = 0, \ldots, i-1$.

The tower $\mathcal{C}$ has the nice property that in each cover, the only points that are ramified have coordinates in $\mathbb{F}_4$[1]. van der Geer and van der Vlugt used this ramification behavior to calculate the genera for every level of the tower.

[1]There are singular points on the curve D_i for $i \geq 3$ which can split into multiple points in the normalization C_i, so we may not be able to uniquely identify a ramified point by its coordinates in $\mathbb{F}_4$.

They also found that the curve $\mathcal{C}$ has 14 $\mathbb{F}_8$-rational points. Twelve of these points have coordinates in $\mathbb{F}_8 - \{0,1\}$, and they split completely in every level of the tower, giving us $6 \cdot 2^n$ $\mathbb{F}_8$-rational points in the nth level of the tower.

Putting the formulas for the genus and number of points together, they showed that over $\mathbb{F}_8$, one has $\lambda(\mathcal{C}) = 3/2$. Thus, this tower will lead to a family of codes with

$$d/n + k/n \geq 1 - \frac{2}{3} = \frac{1}{3} \text{ as } i \to \infty.$$

Throughout this paper, when working with this tower, we will let ρ and α be extension elements of $\mathbb{F}_2$ with $\rho^2+\rho+1 = 0$ and $\alpha^3+\alpha^2+1 = 0$ (so $\mathbb{F}_4 \cong \mathbb{F}_2(\rho)$ and $\mathbb{F}_8 \cong \mathbb{F}_2(\alpha)$).

2.1. Creating codes. In order to create a code $\mathcal{C}_{\mathcal{L}}(C_i, \mathcal{P}, D)$, one needs to calculate a basis of the Riemann-Roch space associated to a divisor D and evaluate the basis elements of this space at points in the divisor $\mathcal{P}$. For notation, in this section, let $P_{a_0,\ldots,a_i}$ denote the point $(a_0, \ldots, a_i) \in C_i$.

There is a unique point $P_{\infty,\ldots,\infty} \in C_i$, and we will take our divisor D to be $D = nP_{\infty,\ldots,\infty}$[2]. The divisor $\mathcal{P}$ will consist of the $6 \cdot 2^i$ points with coordinates in $\mathbb{F}_8 - \{0,1\}$.

The first level of the curve is given by the equation

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

The principal divisors of x_0 and x_1 are $(x_0) = 2P_{0,\infty} - 2P_{\infty,\infty}$ and $(x_1) = P_{\rho,0} + P_{\rho^2,0} - P_{0,\infty} - P_{\infty,\infty}$. By Riemann-Roch, since the genus is 1, there is 1 gap number. We are missing a pole of order 1 at $P_{\infty,\infty}$, and we can generate all other pole orders with x_0 and x_1 (noting that x_0x_1 has a single pole of order 3 at $P_{\infty,\infty}$). Since we can calculate a basis for $\mathcal{L}(mP_{\infty,\infty})$ for any m, the final step is to evaluate these functions at the points in the support of $\mathcal{P}$, which are the 12 points with coordinates in $\mathbb{F}_8 - \{0,1\}$, to create the encoding matrix for the code.

For the second level, this method works. However, for the third level, for which the genus is 15, using monomials in x_0, x_1, x_2, x_3, we only obtain 14 functions in $\mathcal{L}(29P_{\infty,\infty,\infty,\infty})$ instead of the expected 15.

[2]For P a point of degree 1 (such as $P_{\infty,\ldots,\infty}$), by Riemann-Roch,

$$\dim \mathcal{L}(nP) \geq n + 1 - g,$$

with equality for $n > 2g - 2$. When $\dim \mathcal{L}(k-1)P = \dim \mathcal{L}(kP)$, k is called a *Weierstrass gap number*, and there are no functions f such that $(f)_\infty = kP$. Since $\dim \mathcal{L}((k-1)P) + 1 = \dim \mathcal{L}(kP)$ for $k > 2g - 1$, the set of gap numbers lies between 1 and $2g - 1$, and there are precisely g of them.

What goes wrong in the third level? We are working with the curves C_i which are the normalizations of the curves D_i. D_1 and D_2 are smooth, but D_3 is not. Roughly speaking, the presence of singular points causes the genus to drop, which means there are fewer Weierstrass gap numbers, so there are more functions in $\mathcal{L}(D)$. These additional functions in $\mathcal{L}(D)$ are rational functions.

Since our monomials have poles at $P_{\infty,\ldots,\infty}$, there are only a finite number of monomials that have a pole of order $\leq n$ at $P_{\infty,\ldots,\infty}$. Thus, one can find all monomials in $\mathcal{L}(nP_{\infty,\ldots,\infty})$ in a finite amount of time. Rational functions, on the other hand, are harder to get a hold of because there are pole cancellations.

It turns out that every asymptotically good tower that has been found to date has curves with singularities. Thus, the question arises: Given an asymptotically good tower, is there an algorithmic way to find a basis for $\mathcal{L}(nP)$ on each level of the tower? We will explore one method by writing the curves in this tower as plane curves.

3. Obtaining plane curves. Consider the function field F_n associated to the nth level of the tower. The goal of this section is to find a plane curve with associated function field F_n. Since there is a unique nonsingular curve associated to every function field, the code created from the normalization of the plane curve will be equivalent to the code created from the normalization of the nth level of the tower. The motivation for writing the curve as a plane curve comes from [5] in which algorithms are given to create a code from a plane curve.

One way to find the plane curve is to find a primitive element for F_n over F_0, i.e., an element $\alpha_n \in F_n$ such that $F_n \cong F_0(\alpha_n)$. With α_n and its associated minimal polynomial $f_n(y) \in F_0[y] = \mathbb{F}_2(x_0)[y]$ over F_0, we have a plane curve in variables x_0 and y given by $f_n(y) = 0$. We can then clear the denominators of any x_0 terms to wind up with an element $\phi_n(x_0, y) \in \mathbb{F}_2[x_0, y]$. With ϕ_n, one can use [5] to construct the associated Goppa code.

Theorem 1. *There exists $\phi_n(x, y) \in \mathbb{F}_2[x, y]$ such that*

$$F_n \cong F_0(x_n)/(\phi_n(x_0, x_n)).$$

In other words, x_n is a primitive element for F_n/F_0.

P r o o f. By induction on n.

For $n = 1$,

$$\begin{aligned} F_1 &= \mathbb{F}_2(x_0, x_1) \Big/ \left(x_1^2 + x_1 + x_0 + 1 + \frac{1}{x_0}\right) \\ &= \mathbb{F}_2(x_0, x_1)/(x_0 x_1^2 + x_0 x_1 + x_0^2 + x_0 + 1). \end{aligned}$$

So $\phi_1(x,y) = xy^2 + xy + x^2 + x + 1 \in \mathbb{F}_2[x,y]$. The statement is true for $n = 1$.

Now, suppose the statement is true for $n = k-1$. Then there is a polynomial $\phi_{k-1}(x,y) \in \mathbb{F}_2[x,y]$ such that

$$F_{k-1} \cong \mathbb{F}_2(x_0, x_{k-1})/(\phi_{k-1}(x_0, x_{k-1})).$$

We have the field isomorphism

$$\begin{array}{rccc} \pi & : & \mathbb{F}_2(x_0,\ldots,x_{k-1}) & \rightarrow & \mathbb{F}_2(x_1,\ldots,x_k) \\ & & x_i & \mapsto & x_{i+1}. \end{array}$$

Thus, since

$$\phi_{k-1}(x_0, x_{k-1}) = 0,$$

we also have

$$\phi_{k-1}(x_1, x_k) = 0.$$

Since

$$x_1^2 = x_1 + x_0 + 1 + \frac{1}{x_0}, \tag{1}$$

we can reduce all powers of x_1 to be elements of $\mathbb{F}_2(x_0) + x_1\mathbb{F}_2(x_0)$. Thus,

$$\phi_{k-1}(x_1, x_k) = f(x_0, x_k) + x_1 \cdot g(x_0, x_k),$$

for $f(x,y), g(x,y) \in \mathbb{F}_2(x,y)$. In particular,

$$x_1 = \frac{f(x_0, x_k)}{g(x_0, x_k)},$$

so $x_1 \in \mathbb{F}_2(x_0, x_k)$. Using (1) from above, we have

$$\begin{aligned} x_0 + 1 + \frac{1}{x_0} &= x_1^2 + x_1 \\ &= \left(\frac{f(x_0, x_k)}{g(x_0, x_k)}\right)^2 + \frac{f(x_0, x_k)}{g(x_0, x_k)}. \end{aligned}$$

Thus,

$$x_0 + 1 + \frac{1}{x_0} + \left(\frac{f(x_0, x_k)}{g(x_0, x_k)}\right)^2 + \frac{f(x_0, x_k)}{g(x_0, x_k)} = 0,$$

so we have a relation between x_0 and x_k. We clear denominators and let the resulting minimal polynomial be $\phi_k(x_0, x_k)$.

By induction,

$$\mathbb{F}_2(x_0, x_{k-1}) \cong F_{k-1} = \mathbb{F}_2(x_0, \ldots, x_{k-1}).$$

Since $\mathbb{F}_2(x_0, \ldots, x_{k-1})$ is isomorphic to $\mathbb{F}_2(x_1, \ldots, x_k)$, we have

$$\mathbb{F}_2(x_1, x_k) \cong \mathbb{F}_2(x_1, \ldots, x_k).$$

From above, $x_1 \in \mathbb{F}_2(x_0, x_k)$, so

$$\begin{aligned} \mathbb{F}_2(x_0, x_k) &\cong \mathbb{F}_2(x_0, x_1, x_k) \\ &\cong \mathbb{F}_2(x_0)(x_1, x_k) \\ &\cong \mathbb{F}_2(x_0)(x_1, \ldots, x_k) \text{ (by induction)} \\ &\cong F_k. \end{aligned}$$

Thus, we have found $\phi_k(x, y) \in \mathbb{F}_2[x, y]$ such that

$$F_k \cong \mathbb{F}_2(x_0, x_k)/(\phi_k(x_0, x_k)),$$

and so the claim is true for all positive integers n. □

For each n, we have a polynomial relation

$$\phi_n(x_0, x_n) = 0,$$

which defines a curve $D_n \subset \mathbb{P}^1(\overline{\mathbb{F}_2}) \times \mathbb{P}^1(\overline{\mathbb{F}_2})$. Removing finitely many points with $x_0 = \infty$ or $x_n = \infty$, we have an affine curve in $\overline{\mathbb{F}_2}^2$. In the projective closure, we add finitely many points to obtain a curve C_n, which is birationally equivalent to D_n and hence has an isomorphic function field.

Using the method described above, one can obtain equations for plane curves associated to any level of the tower. The first few levels of the tower are given by:

$$\begin{aligned} \phi_1(x, y) &= xy^2 + xy + x^2 + x + 1; \\ \phi_2(x, y) &= x^3y^4 + x^2y^4 + xy^4 + x^4 + x^3y + x^2y^2 + xy + 1; \\ \phi_3(x, y) &= x^7y^8 + x^6y^8 + x^5y^8 + x^6y^6 + x^7y^4 + x^6y^5 + x^5y^6 + x^3y^8 \\ &\quad + x^5y^5 + x^2y^8 + x^7y^2 + x^6y^3 + x^3y^6 + xy^8 + x^8 + x^7y \\ &\quad + x^5y^3 + x^4y^4 + x^3y^5 + x^2y^6 + x^2y^5 + x^4y^2 + x^3y^3 \\ &\quad + x^2y^3 + xy^4 + x^4 + xy^2 + xy + 1. \end{aligned}$$

Note that the equations get large quickly, with $^\circ(\phi_n) = 2^{n+1} - 1$.

4. Effective construction. In this section, we give the results of applying the algorithms from [5] to the absolutely irreducible projective plane curve $\mathcal{C}$ given by $\phi_3(X, Y, Z) = 0$, where

$$\begin{aligned}\phi_3(X,Y,Z) \;=\; & X^8Z^7 + X^7Y^8 + X^7Y^4Z^4 + X^7Y^2Z^6 + X^7YZ^7 + X^6Y^8Z \\ & + X^6Y^6Z^3 + X^6Y^5Z^4 + X^6Y^3Z^6 + X^5Y^8Z^2 + X^5Y^6Z^4 \\ & + X^5Y^5Z^5 + X^5Y^3Z^7 + X^4Y^4Z^7 + X^4Y^2Z^9 + X^4Z^{11} \\ & + X^3Y^8Z^4 + X^3Y^6Z^6 + X^3Y^5Z^7 + X^3Y^3Z^9 + X^2Y^8Z^5 \\ & + X^2Y^6Z^7 + X^2Y^5Z^8 + X^2Y^3Z^{10} + XY^8Z^6 + XY^4Z^{10} \\ & + XY^2Z^{12} + XYZ^{13} + Z^{15}.\end{aligned}$$

There are 20 singular points in the closure of $\mathbb{F}_2$ corresponding to the following points:

$P_1 = (1:0:0)$	$P_2 = (0:1:0)$	$P_3 = (\rho:1:1)$
$P_4 = (1:\rho:1)$	$P_5 = (\rho:0:1)$	$P_6 = (\alpha:\alpha^2:1)$
$P_7 = (\alpha:\alpha^3:1)$	$P_8 = (\alpha^3:\alpha:1)$	$P_9 = (\alpha^3:\alpha^5:1)$,

along with their conjugate points from the Galois action of $\mathbb{F}_4$ or $\mathbb{F}_8$ over $\mathbb{F}_2$ (denoted $P_3', P_4', P_5', P_6', P_6'', P_7', P_7'', P_8', P_8'', P_9'$, and P_9'').

By a sequence of blowing-ups, we compute the desingularization tree. For each singular point P_i, we denote the result of the jth blowing-up by $Q_{i,j}$. The resulting non-singular infinitely near points are given in Table 1.

The components of the adjunction divisor can be calculated from the desingularization tree. To simplify notation, let the $\mathbb{F}_2$-rational divisors $R_1, \ldots, R_8$

$P_1 : (y,z) = (0,0)$ $r = 7$	$\longrightarrow$	$Q_{1,1} : (y, z_1) = (0,0)$
$P_2 : (x,z) = (0,0)$ $r = 7$	$\longrightarrow$	$\begin{cases} Q_{2,1} : (x,z_1) = (0,\rho) \\ Q_{2,2} : (x,z_1) = (0,\rho^2) \\ Q_{2,4} : (x_1,z) = (0,0) \\ Q_{2,5} : (x,z_2) = (0,\rho) \\ Q_{2,6} : (x,z_2) = (0,\rho^2) \end{cases}$
$P_3 : (x,y) = (\rho,1)$ $r = 2$	$\longrightarrow$	$\begin{cases} Q_{3,2} : (x,y_2) = (\rho,1) \\ Q_{3,3} : (x,y_2) = (\rho,\rho^2) \end{cases}$
$P_4 : (x,y) = (1,\rho)$ $r = 2$	$\longrightarrow$	$\begin{cases} Q_{4,4} : (x,y_4) = (1,\rho) \\ Q_{4,5} : (x,y_4) = (1,\rho^2) \end{cases}$
$P_5 : (x,y) = (\rho,0)$ $r = 2$	$\longrightarrow$	$\begin{cases} Q_{5,2} : (x,y_2) = (\rho,1) \\ Q_{5,3} : (x,y_2) = (\rho,\rho^2) \end{cases}$
$P_6 : (x,y) = (\alpha,\alpha^2)$ $r = 2$	$\longrightarrow$	$\begin{cases} Q_{6,1} : (x,y_1) = (\alpha,\alpha) \\ Q_{6,2} : (x,y_1) = (\alpha,\alpha^3) \end{cases}$
$P_7 : (x,y) = (\alpha,\alpha^3)$ $r = 2$	$\longrightarrow$	$\begin{cases} Q_{7,1} : (x,y_1) = (\alpha,\alpha) \\ Q_{7,2} : (x,y_1) = (\alpha,\alpha^3) \end{cases}$
$P_8 : (x,y) = (\alpha^3,\alpha)$ $r = 2$	$\longrightarrow$	$\begin{cases} Q_{8,1} : (x,y_1) = (\alpha^3,\alpha^5) \\ Q_{8,2} : (x,y_1) = (\alpha^3,\alpha^6) \end{cases}$
$P_9 : (x,y) = (\alpha^3,\alpha^5)$ $r = 2$	$\longrightarrow$	$\begin{cases} Q_{9,1} : (x,y_1) = (\alpha^3,\alpha^5) \\ Q_{9,2} : (x,y_1) = (\alpha^3,\alpha^6) \end{cases}$

Table 1. Blow-ups of all singular points

be as follows:

$$\begin{aligned}
R_1 &= Q_{1,1}, \\
R_2 &= Q_{2,1} + Q_{2,2}, \\
R_3 &= Q_{2,4}, \\
R_4 &= Q_{2,5} + Q_{2,6}, \\
R_5 &= Q_{3,2} + Q_{3,3} + Q'_{3,2} + Q'_{3,3}, \\
R_6 &= Q_{4,4} + Q_{4,5} + Q'_{4,4} + Q'_{4,5}, \\
R_7 &= Q_{5,2} + Q_{5,3} + Q'_{5,2} + Q'_{5,3}, \\
R_8 &= Q_{6,1} + Q_{6,2} + Q'_{6,1} + Q'_{6,2} + Q''_{6,1} + Q''_{6,2} + Q_{7,1} + Q_{7,2} \\
&\quad + Q'_{7,1} + Q'_{7,2} + Q''_{7,1} + Q''_{7,2} + Q_{8,1} + Q_{8,2} + Q'_{8,1} + Q'_{8,2} \\
&\quad + Q''_{8,1} + Q''_{8,2} + Q_{9,1} + Q_{9,2} + Q'_{9,1} + Q'_{9,2} + Q''_{9,1} + Q''_{9,2}.
\end{aligned}$$

The adjunction divisor is then the degree-152 divisor

$$\mathcal{A} = 42R_1 + 6R_2 + 6R_3 + 18R_4 + 2R_5 + 4R_6 + 2R_7 + R_8.$$

Comparing the nonsingular model of $\mathcal{C}$ to the third level of the original tower, we find correspondences between points, given in Table 2[3].

Point on the plane curve model	Point on the third level of the tower
$Q_{1,1}$	$P_{\infty,\infty,\infty,\infty}$
$Q_{2,1}$ and $Q_{2,2}$	$P_{\rho,0,\infty,\infty}$ and $P_{\rho^2,0,\infty,\infty}$
$Q_{2,4}$	$P_{0,\infty,\infty,\infty}$
$Q_{2,5}$ and $Q_{2,6}$	$P_{1,\rho,0,\infty}$ and $P_{1,\rho^2,0,\infty}$

Table 2. Correspondence between plane curve and tower points

We will let $D = nR_1$ $(= nQ_{1,1})$. However, rather than dealing with an arbitrary value for n, it turns out that once we have calculated a basis for $\mathcal{L}(29R_1)$, we can use the functions in that basis to (multiplicatively) generate all functions with higher pole orders.

As for $\mathcal{P}$, we will take the points to be all of the points with affine coordinates in $\mathbb{F}_8 - \{0, 1\}$. There are 36 points of the form $(\alpha^i : \alpha^j : 1)$ on the curve. Twelve of these are singular points which split into the non-singular points in the support of R_8, and the other 24 are non-singular points. Let the divisor R_9 denote the sum of these 24 non-singular points. Thus, our divisor

$$\mathcal{P} = R_8 + R_9$$

consists of 48 points with coordinates in $\mathbb{F}_8$ (which correspond to the 48 points with coordinates in $\mathbb{F}_8 - \{0, 1\}$ in the third level of the tower).

With the parametrizations of X, Y, and Z at all of the points in the adjunction divisor $\mathcal{A}$ and the divisor D, we can begin to search for a form G_0 with

$$\begin{aligned}(G_0) &\geq \mathcal{A} + D \\ &= 71R_1 + 6R_2 + 6R_3 + 18R_4 + 2R_5 + 4R_6 + 2R_7 + R_8.\end{aligned}$$

[3]Aside from the given points in the table, all other points on the plane curve model have $Z = 1$, so we can use the X and Y coordinates of a point on the plane model to determine the x_0 and x_3 coordinates of the corresponding point in the tower. For instance, when $Z = 1$, the four points in R_5 have $(X, Y) = (\rho, 1)$ or $(\rho^2, 1)$, and these correspond to the four points $P_{\rho,1,\rho,1}$, $P_{\rho^2,1,\rho,1}$, $P_{\rho,1,\rho^2,1}$, and $P_{\rho^2,1,\rho^2,1}$.

Choosing forms that vanish at points in the support of $\mathcal{A}$, we obtain the form

$$G_0 = Y(Y+Z)(X+Z)^4Z^2(Y^3+Y^2Z+Y^3)(Y^3+YZ^2+Y^3),$$

so that

$$(G_0) = 72R_1 + 6R_2 + 6R_3 + 20R_4 + 2R_5 + 4R_6 + 2R_7 + R_8 + R_9,$$

and hence $(G_0) \geq \mathcal{A} + D$.

The next step is to search for all forms G of degree 14 so that $(G) \geq (G_0) - D$. We do this by finding the local parametrizations of the forms X, Y, and Z at all of the points in the support of G_0, from which one can get the local parametrizations of all monomials of degree 14. Then, one searches for linear combinations of these monomials that give the appropriate levels of vanishing. The result is a set of linearly independent forms $\{G_i : i = 1, \ldots, 15\}$ for which $\{G_i/G_0 : i = 1, \ldots, 15\}$ forms a basis for $\mathcal{L}(D)$. Note that while some of these functions may have the same pole order at $Q_{1,1}$, one can take linear combinations to obtain the 15 different pole orders.

To create the code, we evaluate the functions in $\mathcal{L}(D)$ at the points in the support of $\mathcal{P} = R_8 + R_9$. Since these points are all in the open set defined by $Z \neq 0$, by a change of coordinates, we can consider affine coordinates $x = X/Z$ and $y = Y/Z$. The basis elements for $\mathcal{L}(D)$, in affine coordinates, are given in Table 3.

Returning to the question of the missing function on the third level of the tower, it turns out that we were missing a function with a pole of order 21. This function, in coordinates (x_0, x_1, x_2, x_3), is

$$\frac{(x_0^7+1)x_3(x_3^3+1)}{(x_0+1)^4(x_3^7+1)}.$$

Note that even if we had found this function, the numerator and denominator vanish on points with coordinates in $\mathbb{F}_8 - \{0, 1\}$, so evaluating this function at these points requires more work.

For any function f in $\mathcal{L}(D)$ and any point P in $\mathcal{P}$, if $f(P) = \frac{0}{0}$, then we blow-up P and apply a monoidal transformation to f. After a finite sequence of blowing-ups and transformations, the either the numerator or denominator will cease to vanish. In fact, the denominator will cease to vanish because our functions only have poles at $Q_{1,1}$. Thus, we will get a meaningful result, so we can create our encoding matrix. The results of these function evaluations at certain points in $\mathcal{P}$ are in Table 4 and Table 5.

Order	Function
0	1
8	x
12	$\frac{y}{g_0}\left(\ (1+y^3)(x^2+x^3+x^6)+(y^3+y^7)(x+x^4+x^5)\ \right)$
14	$\frac{1}{g_0}\left(\begin{array}{c}(y^3+y^4+y^5+y^6)(1+x^2+x^4+x^6)\\ +x^3(1+y+y^2)+(x+x^5)(1+y^2+y^8)\end{array}\right)$
15	$\frac{y}{g_0}\left(\begin{array}{c}(y^3+y^4+y^5+y^6)(1+x^2+x^4+x^6)\\ +(x+x^5)(y+y^2+y^7)+x^3(1+y+y^2)\end{array}\right)$
16	x^2
20	$\frac{y}{g_0}\left(\ (y^3+y^7+x^7(1+y^3)+x^4(1+y^7)\ \right)$
21	$\frac{1}{g_0}\left(\ (1+x^7)y^2(1+y^3)\ \right)$
22	$\frac{x}{g_0}\left(\begin{array}{c}(y^3+y^5+y^6+y^8)(1+x^2+x^6+x^4)\\ +(1+y^2+y^4)(x+x^3+x^5)+x^4(1+y^8)\end{array}\right)$
23	$\frac{x}{g_0}\left(\ (1+y^3)(x+x^3+x^5)+(y^3+y^7)(1+x^2+x^4+x^6)\ \right)$
24	$\frac{1}{g_0}\left(\begin{array}{c}(y^3+y^4+y^5+y^6)(x^2+x^3+x^5+x^6)+1+x^8\\ +x^7(y+y^2)+x^4(1+y+y^2)+x(y^2+y^8)+x^5(y+y^8)\end{array}\right)$
26	$\frac{1}{g_0}\left(\begin{array}{c}1+(y^3+y^4+y^5+y^5)(x^3+x^5)+x+x^7\\ +(1+y^2+y^8)(1+x^2+x^4+x^6)+x^8y(1+y)\end{array}\right)$
27	$\frac{1}{g_0}\left(\begin{array}{c}(1+y^2+y^3+y^7+y^8)(x^2+x^3+x^5+x^6)+x(1+y^7)\\ +(x^3+x^5)(y+y^8)+x^4(1+y^4+y^5+y^6)+y^6\\ +x^8y(1+y+y^2)+x^7y^4(1+y+y^3)\end{array}\right)$
28	$\frac{xy}{g_0}\left(\ y^3+y^7+x^7(1+y^3)+x^4(1+y^7)\ \right)$
29	$\frac{1}{g_0}\left(\begin{array}{c}1+(y+y^3+y^4)(x^3+x^4+x^5)+x^4+y^7(x^3+x^5+x^7)\\ +(y^2+y^5+y^6)(x^2+x^6+x^7+x^8)+x(y^6+y^7)\\ +x^8(1+y^6)\end{array}\right)$

Table 3. Pole orders of basis elements for $\mathcal{L}(29Q_{1,1})$ with $x = X/Z$, $y = Y/Z$, and $g_0(x,y) = G_0(x,y,1) = (x+1)^4y(y^7+1)$

	$Q_{6,1}$	$Q_{6,2}$	$Q_{7,1}$	$Q_{7,2}$	$Q_{8,1}$	$Q_{8,2}$	$Q_{9,1}$	$Q_{9,2}$
f_0	1	1	1	1	1	1	1	1
f_8	α	α	α	α	α^3	α^3	α^3	α^3
f_{12}	α	0	α	0	α	α^4	α	α^4
f_{14}	α^3	0	α^3	0	α^4	0	α^4	0
f_{15}	α^2	α^4	α^5	α^3	1	α	α^5	α^4
f_{16}	α^2	α^2	α^2	α^2	α^6	α^6	α^6	α^6
f_{20}	α	α^2	α	α^2	α^5	0	α^5	0
f_{21}	1	α^5	α	α^6	α^2	α	α^6	α^5
f_{22}	α^5	0	α^5	0	α^6	1	α^6	1
f_{23}	α	α^5	1	α^4	α^2	α^4	α^5	1
f_{24}	α^5	α^4	α^5	α^4	α^6	0	α^6	0
f_{26}	0	α	0	α	α	α^6	α	α^6
f_{27}	α^2	α^6	0	α^3	α^4	α	α^2	1
f_{28}	α^2	α^3	α^2	α^3	α	0	α	0
f_{29}	0	α	α^3	1	α^4	1	α^4	α

Table 4. Basis elements of $\mathcal{L}(29Q_{1,1})$ evaluated at certain points in $\mathcal{P}$

In order to create a code with dimension $k > 15$, one can use the functions in $\mathcal{L}(29Q_{1,1})$ to (multiplicatively) generate functions with larger pole orders. (Note that we really can do this.) Given the function

$$f_l = f_{j_1} f_{j_2} \dots f_{j_n}$$

with $j_m \in I$ for $m = 1, 2, \dots, n$ (and $\sum j_m = l$), one can calculate $f_l(P)$ by

$$f_l(P) = f_{j_1}(P) f_{j_2}(P) \dots f_{j_n}(P).$$

Equivalently, to calculate the row in the encoding matrix corresponding to f_l, one can multiply coordinate-wise the rows corresponding to f_{j_1}, f_{j_2}, $\dots$, f_{j_n}. This will produce a code with the following parameters:

$$\begin{aligned} \text{length} &= 48 \\ \text{dimension} &= k \\ \text{distance} &\geq 34 - k. \end{aligned}$$

	(α,α)	(α,α^4)	(α,α^5)	(α,α^6)	(α^3,α^2)	(α^3,α^3)	(α^3,α^4)	(α^3,α^6)
f_0	1	1	1	1	1	1	1	1
f_8	α	α	α	α	α^3	α^3	α^3	α^3
f_{12}	0	α	0	α	α	α	α^4	α^4
f_{14}	α^5	α^2	α^5	α^2	1	1	α^5	α^5
f_{15}	0	α^4	1	1	α	α^6	0	α^6
f_{16}	α^2	α^2	α^2	α^2	α^6	α^6	α^6	α^6
f_{20}	α^2	α	α^2	α	α^5	α^5	0	0
f_{21}	α^4	α^2	α	α^4	α^3	α^4	α^4	α^6
f_{22}	α^6	1	α^6	1	α	α	α^5	α^5
f_{23}	α^6	α^6	α^2	α^4	α	1	α	α^6
f_{24}	α^4	α^5	α^4	α^5	α^6	α^6	0	0
f_{26}	1	α^5	1	α^5	α^3	α^3	1	1
f_{27}	α^5	1	α^3	α^2	α^5	α^5	0	α^6
f_{28}	α^3	α^2	α^3	α^2	α	α	0	0
f_{29}	α^2	1	1	α^6	0	α^2	0	1

Table 5. Basis elements of $\mathcal{L}(29Q_{1,1})$ evaluated at certain points in $\mathcal{P}$

Acknowledgments. I would like to thank Emma Previato for encouragement and many useful conversations. This work was supported by NSF grant DMS-0205643.

REFERENCES

[1] Aleshnikov I., V. Deolalikar, V. Kumar, H. Stichtenoth. Towards a basis for the space of regular functions in a tower of function fields meeting the Drinfeld-Vladuţ bound. In: Finite Fields and Applications (Eds D. Jungnickel, H. Neiderreiter) Springer, Berlin-Heidelberg, 2001.

[2] Garcia A., H. Stichtenoth. A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladuţ bound. *Inv. Math.* **121** (1995), 211–222.

[3] Garcia A., H. Stichtenoth. On the asymptotic behaviour of some towers of function fields over finite fields. *J. Number Theory* **61**, *147*, (1996), 248–273.

[4] Greuel G.-M., G. Pfister, H. Schönemann. *Singular* 2.0, A Computer Algebra System for Polynomial Computations. Centre for Computer Algebra, University of Kaiserslautern, 2001, `http://www.singular.uni-kl.de`.

[5] Haché G., D. Le Brigand. Effective construction of algebraic geometry codes. *IEEE Trans. Inform. Theory* **41**, *6* (1995), 1615–1628.

[6] Martin J. I. F., Ch. Lossen. A *Singular* 2.0 Library for Applications to Algebraic Geometry Codes. Centre for Computer Algebra, University of Kaiserslautern, 2001, `http://www.singular.uni-kl.de`.

[7] Shum K. W., I. Aleshnikov, P. V. Kumar, H. Stichtenoth, V. Deolalikar. A low-complexity algorithm for the construction of algebraic-geometric codes better than the Gilbert-Varshamov bound. *IEEE Trans. Inform. Theory* **47**, *6* (2001), 2225–2241.

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

[9] van der Geer G., M. van der Vlugt. An asymptotically good tower of curves over the field with eight elements. *Bull. London Math. Soc.* **34**, *3* (2002), 291–300.

[10] Voss C., T. Høholdt. An explicit construction of a sequence of codes attaining the Tsfasman-Vlăduţ-Zink bound. The first steps. *IEEE Trans. Inform. Theory* **43** (1997), 128–135.

Caleb McKinley Shor
Bates College Math Department
3, Andrews Road
Lewiston, ME 04240
e-mail: `cshor@bates.edu`

Received October 23, 2006
Final Accepted June 27, 2007