1997

The Nordstrom–Robinson Code is Algebraic-Geometric

Judy L. Walker

University of Nebraska - Lincoln, judy.walker@unl.edu

Follow this and additional works at: <https://digitalcommons.unl.edu/mathfacpub>

Part of the [Applied Mathematics Commons](#), and the [Mathematics Commons](#)

Walker, Judy L., "The Nordstrom–Robinson Code is Algebraic-Geometric" (1997). *Faculty Publications, Department of Mathematics*. 187.

<https://digitalcommons.unl.edu/mathfacpub/187>

This Article is brought to you for free and open access by the Mathematics, Department of at DigitalCommons@University of Nebraska - Lincoln. It has been accepted for inclusion in Faculty Publications, Department of Mathematics by an authorized administrator of DigitalCommons@University of Nebraska - Lincoln.

The Nordstrom–Robinson Code is Algebraic-Geometric

Judy L. Walker

Abstract—The techniques of algebraic geometry have been widely and successfully applied to the study of linear codes over finite fields since the early 1980's. Recently, there has been an increased interest in the study of linear codes over rings. In a previous paper [10], we combined these two approaches to coding theory by introducing and studying algebraic-geometric codes over rings. In this correspondence, we show that the Nordstrom–Robinson code is the image under the Gray mapping of an algebraic geometric code over $\mathbb{Z}/4\mathbb{Z}$.

Index Terms—Algebraic geometry, codes, Nordstrom–Robinson code.

I. INTRODUCTION

Algebraic-geometric codes over finite fields have been widely and successfully studied since their introduction by Goppa in 1977 [1]. The study of linear codes over rings gained new importance recently with the paper of Hammons, Kumar, Calderbank, Sloane, and Solé [2] which shows that certain nonlinear binary codes are actually the images of linear codes over $\mathbb{Z}/4\mathbb{Z}$ under the Gray map. In [10] and [11], we combined these two areas of coding theory by defining and studying algebraic-geometric codes over rings. It is now natural to ask whether or not the linear $\mathbb{Z}/4\mathbb{Z}$ codes in [2] can be constructed as algebraic-geometric codes.

In Section II below, we give an overview of those results of [2] which we need. Section III contains a summary of the relevant results of [10]. Section IV is the heart of the correspondence, and it is there where we prove our main result: The Nordstrom–Robinson code is the nonlinear image of an algebraic geometric code over $\mathbb{Z}/4\mathbb{Z}$.

II. KERDOCK AND PREPARATA CODES AND THE RESULTS OF HAMMONS ET AL.

The Kerdock and Preparata codes are two families of nonlinear binary codes which were discovered in 1972 and 1968, respectively. For each odd $m \geq 3$, there is a Kerdock code $\mathcal{K}_m$ and a Preparata code $\mathcal{P}_m$, each of length $n = 2^{m+1}$. The minimum distance of $\mathcal{K}_m$ is $2^m - 2^{(m-1)/2}$. It has 4^{m+1} codewords, which is more than any known linear code of the same length and minimum distance. $\mathcal{P}_m$ has $2^{(n-2m-2)}$ codewords and minimum distance 6. Again, $\mathcal{P}_m$ has more codewords than any known linear code with the same length and minimum distance. When $m = 3$, $\mathcal{K}_m$ and $\mathcal{P}_m$ coincide as a nonlinear binary code of length 16 called the Nordstrom–Robinson code. This code has more codewords than any possible linear code of the same length and minimum distance. In general, $\mathcal{K}_m$ and $\mathcal{P}_m$ are “formally dual,” which means that their weight distributions are MacWilliams transforms of each other. All of these properties make

Manuscript received September 27, 1996; revised February 10, 1997. The material in this correspondence is a portion of the author's Ph.D. dissertation, written under the direction of Prof. Nigel Boston at the University of Illinois. The material in this correspondence was presented in part at the ACGT-5, Luminy, France, June 1995.

The author is with the Department of Mathematics and Statistics, University of Nebraska, Lincoln, NE 68588-0323 USA.

Publisher Item Identifier: S 0018-9448(97)05018-9.

these codes very desirable and interesting. Until recently, however, their structure has been a mystery.

Definition 2.1: Let $\beta, \gamma: \mathbb{Z}/4\mathbb{Z} \rightarrow \mathbb{F}_2$ be the (nonlinear) maps given by

c	$\beta(c)$	$\gamma(c)$
0	0	0
1	0	1
2	1	1
3	1	0

The Gray map $\varphi: (\mathbb{Z}/4\mathbb{Z})^n \rightarrow (\mathbb{F}_2)^{2n}$ is given by

$$\varphi((c_1, \dots, c_n)) = (\beta(c_1), \dots, \beta(c_n), \gamma(c_1), \dots, \gamma(c_n)).$$

The Lee weight on codes over $\mathbb{Z}/4\mathbb{Z}$ is defined by setting $w_L(0) = 0$, $w_L(1) = w_L(3) = 1$, and $w_L(2) = 2$, and then defining $w_L((x_1, \dots, x_n))$ to be $w_L(x_1) + \dots + w_L(x_n)$. It is easy to see that if a vector $\mathbf{x}$ over $\mathbb{Z}/4\mathbb{Z}$ has Lee weight w , then the vector $\varphi(\mathbf{x})$ over $\mathbb{F}_2$ has Hamming weight w . Thus the Gray map is an isometry

$$((\mathbb{Z}/4\mathbb{Z})^n, \text{Lee weight}) \rightarrow (\mathbb{F}_2^{2n}, \text{Hamming weight}).$$

For each odd $m \geq 3$, Hammons et al. [2] exhibit linear $\mathbb{Z}/4\mathbb{Z}$ codes $\hat{\mathcal{K}}_m$ and $\hat{\mathcal{P}}_m$ of length 2^m such that

$$\varphi(\hat{\mathcal{K}}_m) = \mathcal{K}_m$$

and

$$\varphi(\hat{\mathcal{P}}_m) = (\text{a nonlinear code with the same parameters as}) \mathcal{P}_m.$$

We would like to know which, if any, of the codes $\hat{\mathcal{K}}_m$ and $\hat{\mathcal{P}}_m$ can be realized as algebraic-geometric $\mathbb{Z}/4\mathbb{Z}$ codes, a notion which we define now.

III. ALGEBRAIC-GEOMETRIC CODES OVER RINGS

We begin by recalling one version of the definition of algebraic-geometric codes over finite fields

Definition 3.1: Let X be a smooth, absolutely irreducible curve over the finite field $\mathbb{F}_q$. Let $\mathcal{P} = \{P_1, \dots, P_n\}$ be a set of n distinct $\mathbb{F}_q$ -rational points on X , and let G be a (Weil) divisor on X . For simplicity, assume that none of the P_i appears with nonzero coefficient in G . Denote by $\mathcal{L}(G)$ the vector space of functions associated to G

$$\mathcal{L}(G) = \{f \in \mathbb{F}_q(X) \mid \text{div}(f) + G \geq 0\} \cup \{0\}.$$

Then the algebraic-geometric code associated to X , $\mathcal{P}$, and G is given by

$$C_{\mathbb{F}_q}(X, \mathcal{P}, G) = \{(f(P_1), \dots, f(P_n)) \mid f \in \mathcal{L}(G)\}.$$

The idea behind the construction of algebraic-geometric codes over rings is to mimic Goppa's construction, while allowing a ring A to

take the place of the finite field $\mathbb{F}_q$. In this correspondence, we will only be concerned with $A = \mathbb{Z}/4\mathbb{Z}$, so we will restrict ourselves to that case. In fact, all of the results of this section hold for any local, Artinian, Gorenstein ring. In particular, the results hold for Galois rings; see [11].

By a curve X over $\mathbb{Z}/4\mathbb{Z}$, we will mean a connected scheme which is projective, smooth, and of relative dimension one over $\text{Spec}(\mathbb{Z}/4\mathbb{Z})$. Since X is projective, we may realize it as a subscheme of $\mathbb{P}_{\mathbb{Z}/4\mathbb{Z}}^t$ for some t . We may then describe X more concretely by saying it is defined by homogeneous polynomials $h_1, \dots, h_m$ in $t+1$ variables over $\mathbb{Z}/4\mathbb{Z}$ such that if we reduce these polynomials modulo 2, the resulting polynomials will define a smooth, connected curve X' contained in $\mathbb{P}_{\mathbb{F}_2}^t$. We will always assume that X' is absolutely irreducible. We define the genus of X to be the genus of X' .

The construction of an algebraic-geometric code over the finite field $\mathbb{F}_q$ requires a set of distinct $\mathbb{F}_q$ -rational points on the curve. Here, we will need a set of disjoint $\mathbb{Z}/4\mathbb{Z}$ points, i.e., solutions in $\mathbb{Z}/4\mathbb{Z}$ to the defining equations of X which, when reduced modulo 2, give distinct $\mathbb{F}_2$ -rational points on X' .

The notion of Weil divisors is inadequate for curves over $\mathbb{Z}/4\mathbb{Z}$, so we need to look elsewhere for something to play the role of the Weil divisor G in our construction. For curves over finite fields there is a one-to-one correspondence between linear equivalence classes of Weil divisors and linear equivalence classes of Cartier divisors, which we define below. First, we define rational and regular functions.

Definition 3.2: Let X be a curve over $\mathbb{Z}/4\mathbb{Z}$, with defining polynomials $h_1, \dots, h_m$. Let I be the ideal generated by these polynomials. A rational function g on X is an equivalence class of quotients g_1/g_2 , where g_1 and g_2 are homogeneous polynomials of the same degree, g_2 is not in the ideal generated by 2 and I , and the equivalence is given by

$$\frac{g_1}{g_2} \sim \frac{g'_1}{g'_2}$$

whenever

$$g_1 g'_2 - g'_1 g_2 \in I.$$

A rational function g is *regular* on the open subset U of X if for some expression $g = g_1/g_2$ of g , g_2 is never equal to 0 or 2 on U .

Definition 3.3: A Cartier divisor is an equivalence class of sets of pairs $\{(U_i, f_i)\}$, where $\{U_i\}$ is an open cover of X and each f_i is an invertible rational function on U_i , such that for each i and j , f_i/f_j is an invertible regular function on $U_i \cap U_j$; see [3] for details.

The correspondence in the finite field case between Weil divisors and Cartier divisors does not hold for curves over $\mathbb{Z}/4\mathbb{Z}$, and it turns out that Cartier divisors are much more useful and natural in our new setting. Consequently, the role of the Weil divisor G is now played by a Cartier divisor, which we will also denote as G . Since we are now working over the ring $\mathbb{Z}/4\mathbb{Z}$ instead of a field $\mathcal{L}(G)$ is no longer a vector space. Instead, it is a $\mathbb{Z}/4\mathbb{Z}$ -module of rational functions associated to G

$$\mathcal{L}(G) = \{\text{rational functions } h \text{ on } X \mid \text{for each } i,$$

$$f_i h \text{ is a regular function on } U_i\}.$$

Given a Cartier divisor $G = \{(U_i, f_i)\}$ on X , we can find an associated Weil divisor G' on X' as follows. The topologies on X and X' are the same, so the open cover $\{U_i\}$ of X is also an open cover of X' . Each invertible rational function f_i is a quotient of homogeneous polynomials of the same degree over $\mathbb{Z}/4\mathbb{Z}$, so reducing both the numerator and the denominator modulo 2 gives a quotient

of homogeneous polynomials of the same degree over $\mathbb{F}_2$. It is easy to see that this quotient is in fact a rational function on X' . This gives us a Cartier divisor on X' associated to G . Recalling that the linear equivalence classes of Cartier divisors on X' are in one-to-one correspondence with the linear equivalence classes of Weil divisors on X' , we let G' be the Weil divisor on X' corresponding to the Cartier divisor we just constructed. We will use the notation $G' = \phi^*(G)$ to denote the Weil divisor on X' associated to the Cartier divisor G on X .

In certain cases, the $\mathbb{Z}/4\mathbb{Z}$ module $\mathcal{L}(G)$ is free and we can find its rank using the following version of the well-known Riemann–Roch theorem [3].

Theorem 3.4 [10]: Let X be a curve over $\mathbb{Z}/4\mathbb{Z}$ and G a Cartier divisor on X . Let X' be the associated curve over $\mathbb{F}_2$ and $G' = \phi^*(G)$ the Weil divisor on X' associated to G . Define the degree of G to be $\deg G = \deg G'$ and the genus g of X to be the genus of X' . Assume that $\deg G > 2g - 2$. Then $\mathcal{L}(G)$ is a free $\mathbb{Z}/4\mathbb{Z}$ module of rank $\deg G + 1 - g$.

Suppose now that Z is a $\mathbb{Z}/4\mathbb{Z}$ point on X such that we can realize the Cartier divisor G as $G = \{(U_i, f_i)\}$ in such a way that for some i , $Z \in U_i$ and f_i is actually an invertible regular function on U_i . In this situation, we say that Z is *not in the support of* G . Notice that if Z is not in the support of G and $h \in \mathcal{L}(G)$, then in some open set U_i containing Z , we can write $h = g/f_i$ with g a regular function on U_i , and f_i an invertible regular function on U_i . In other words, h is a regular function on an open set containing Z and it makes sense to evaluate h at Z .

We are now ready to define algebraic-geometric codes over $\mathbb{Z}/4\mathbb{Z}$.

Definition 3.5: Let X be a curve over $\mathbb{Z}/4\mathbb{Z}$, $\mathcal{Z} = \{Z_1, \dots, Z_n\}$ a set of disjoint $\mathbb{Z}/4\mathbb{Z}$ points on X , and G a Cartier divisor on X . Assume that for each i , Z_i is not in the support of G . Then we define the algebraic-geometric code associated to X , $\mathcal{Z}$, and G to be

$$C_{\mathbb{Z}/4\mathbb{Z}}(X, \mathcal{Z}, G) = \{(h(Z_1), \dots, h(Z_n)) \mid h \in \mathcal{L}(G)\}.$$

These codes are defined more generally in [10], and their properties are explored there. We give here only those properties that will be needed in the remainder of this correspondence. First, we give the basic parameters.

Theorem 3.6: Let X be a curve over $\mathbb{Z}/4\mathbb{Z}$, G a Cartier divisor on X , and $\mathcal{Z} = \{Z_1, \dots, Z_n\}$ a set of disjoint $\mathbb{Z}/4\mathbb{Z}$ points on X . Let g denote the genus of X , and suppose $2g - 2 < \deg G < n$. Then

$$C = C_{\mathbb{Z}/4\mathbb{Z}}(X, \mathcal{Z}, G)$$

is a free code of length n , dimension $k = \deg G + 1 - g$, and minimum (Hamming) distance $d \geq n - \deg G$.

Remark 3.7: The reader may notice that the very important Lee distance is not mentioned in the above theorem. This is a point of current research for the author, and results in this vein will be published elsewhere.

Next, we would like to relate algebraic-geometric codes over $\mathbb{Z}/4\mathbb{Z}$ to algebraic-geometric codes over $\mathbb{F}_2$. Recall that if X is a curve over $\mathbb{Z}/4\mathbb{Z}$ then we can obtain a curve X' over $\mathbb{F}_2$ by reducing the defining polynomials of X modulo 2. Further, if $\mathcal{Z} = \{Z_1, \dots, Z_n\}$ is a set of disjoint $\mathbb{Z}/4\mathbb{Z}$ points on X , then we can reduce the coordinates of each Z_i modulo 2 to get a set $\mathcal{P} = \{P_1, \dots, P_n\}$ of distinct $\mathbb{F}_2$ -rational points on X' . Finally, recall that associated to a Cartier divisor G on X is a Weil divisor $G' = \phi^*(G)$ on X' . This means that given an algebraic-geometric code $C_{\mathbb{Z}/4\mathbb{Z}}(X, \mathcal{Z}, G)$ over $\mathbb{Z}/4\mathbb{Z}$, there is an associated algebraic-geometric code $C_{\mathbb{F}_2}(X', \mathcal{P}, G')$ over $\mathbb{F}_2$. The next theorem relates these two codes further.

Theorem 3.8: Let X , $\mathcal{Z}$, and G be as above. Let

$$\mathcal{P} = \{P_1, \dots, P_n\} \subset X'(\mathbb{F}_q)$$

be the set of closed points contained in $Z_1, \dots, Z_n$, and let G' be the Weil divisor on X' associated to the Cartier divisor G on X . Consider the codes $C = C_{\mathbb{Z}/4\mathbb{Z}}(X, \mathcal{Z}, G)$, $C' = C_{\mathbb{F}_2}(X', \mathcal{P}, G')$, and $\bar{C} = \pi(C)$, where $\pi: (\mathbb{Z}/4\mathbb{Z})^n \rightarrow \mathbb{F}_2^n$ denotes coordinatewise projection modulo 2. Then

$$\bar{C} = C'.$$

IV. MAIN RESULT

In Theorem 3.6, we made the assumption that $2g-2 < \deg G < n$, where g is the genus of X and $n = \#\mathcal{Z}$. In the field case, this restriction yields what Pellikaan, Shen, and van Wee [8] call *strongly algebraic-geometric* codes, and we will follow their lead by referring to $C_{\mathbb{Z}/4\mathbb{Z}}(X, \mathcal{Z}, G)$ as strongly algebraic-geometric if $2g-2 < \deg G < n$. The following result from their paper has an unfortunate implication for us.

Theorem 4.1 [8]: There exists a strongly algebraic-geometric code of length n over $\mathbb{F}_2$ if and only if $n \leq 8$.

Corollary 4.2: $\hat{\mathcal{K}}_m$ and $\hat{\mathcal{P}}_m$ are not strongly algebraic-geometric over $\mathbb{Z}/4\mathbb{Z}$ for $m > 3$.

Proof: By Theorem 3.8, the coordinate-wise linear projection of a strongly algebraic-geometric $\mathbb{Z}/4\mathbb{Z}$ code is a strongly algebraic-geometric code over $\mathbb{F}_2$ of the same length. Hence, by Theorem 4.1, a strongly algebraic-geometric code over $\mathbb{Z}/4\mathbb{Z}$ has length at most 8. Further, the image of such a code under the Gray map has length at most 16. Since the lengths of $\mathcal{K}_m$ and $\mathcal{P}_m$ are each 2^{m+1} , the result follows. $\square$

This means that only for $m = 3$ can $\hat{\mathcal{K}}_m$ or $\hat{\mathcal{P}}_m$ be a strongly algebraic-geometric $\mathbb{Z}/4\mathbb{Z}$ code. The Nordstrom–Robinson code $\hat{\mathcal{K}}_3 = \hat{\mathcal{P}}_3$ is the one remaining possibility. Hammons *et al.* show that the Nordstrom–Robinson code is $\varphi(C)$, where C is the so-called octacode. It is this code which we will show is strongly algebraic-geometric.

The computations in this section were done with the assistance of both Macaulay and Mathematica. Macaulay is a program for doing commutative algebra and algebraic geometry developed by Bayer and Stillman [9]. For information about Mathematica, see [12].

The octacode is a free linear code C over $\mathbb{Z}/4\mathbb{Z}$ of length 8 and dimension 4, with generator matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 2 & 3 & 1 \\ 0 & 0 & 1 & 0 & 3 & 3 & 3 & 2 \\ 0 & 0 & 0 & 1 & 2 & 3 & 1 & 1 \end{pmatrix}. \quad (4.1)$$

The coordinate-wise linear projection $\bar{C}$ of C is a binary code with generator matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \quad (4.2)$$

which is immediately recognizable as a generator matrix of the [8, 4, 4] extended Hamming code. By Theorem 3.8, if C is a strongly algebraic-geometric code over $\mathbb{Z}/4\mathbb{Z}$, then $\bar{C}$ is a strongly algebraic-geometric code over $\mathbb{F}_2$. Our first step will be to construct $\bar{C}$ as a binary strongly algebraic-geometric code.

The first thing we need to find is a smooth, absolutely irreducible curve X' defined over $\mathbb{F}_2$ with at least eight rational points. Any elliptic curve has at most five $\mathbb{F}_2$ -rational points by the Hasse–Weil bound. By definition a hyperelliptic curve admits a finite morphism of degree two to $\mathbb{P}^1$, so any such curve has at most six $\mathbb{F}_2$ -rational points. Since all curves of genus two are hyperelliptic, we now move on to genus three. The canonical embedding of a nonhyperelliptic

curve of genus three is a plane quartic, so the number of $\mathbb{F}_2$ -rational points is at most $\#\mathbb{P}^2(\mathbb{F}_2) = 7$. Hence the genus g of X must be at least four. On the other hand, since we must have a divisor G' on X' satisfying $2g-2 < \deg G' < 8$, g must be at most four. Thus we are looking for a nonhyperelliptic curve of genus four. Note that this forces $\deg G' = 7$.

By [3, Example IV.5.2.2], a smooth nonhyperelliptic curve of genus four over an algebraically closed field can be realized via its canonical embedding as a curve of degree six in $\mathbb{P}^3$. Further, this curve is the complete intersection of an irreducible quadric surface and an irreducible cubic surface. It is not difficult to see that this result in fact holds for any perfect field so the curve we seek must arise in this way.

Up to projective equivalence, there are three irreducible quadric surfaces over $\mathbb{F}_2$: $xw + yz = 0$, $x^2 + xy + y^2 + zw = 0$, and $x^2 + yz = 0$ [4]. The number of rational points on these surfaces are nine, five and seven, respectively, so the curve we are searching for can only lie on the first of these surfaces. An appropriate cubic surface was found using trial-and-error. The equations for the curve we use are

$$0 = xw + yz$$

$$0 = x^2w + x^2y + xy^2 + x^2z + xz^2 + y^2w + yw^2 + z^2w + zw^2.$$

Hereafter, we refer to the quadric and cubic above as $\mathcal{Q}$ and $\mathcal{F}$, respectively. It is easy to check that this curve is smooth (and hence absolutely irreducible) of genus four and has eight $\mathbb{F}_2$ -rational points.

Remark 4.3: For later reference, we would like to give an explicit proof that this curve is smooth. Milne [7, Proposition I.3.24(c)] gives a Jacobian criterion for smoothness of affine curves. Using Euler's equation, which states that a homogeneous polynomial $f(x_1, x_2, \dots, x_n)$ of degree m satisfies

$$\sum x_i(\partial f / \partial x_i) = mf(x_1, x_2, \dots, x_n)$$

one can give a Jacobian criterion for smoothness of projective curves. In particular, to show our curve is smooth, it is enough to show that all monomials of some fixed degree are in the ideal generated by $\mathcal{F}$, $\mathcal{Q}$, and the 2×2 minors of the Jacobian matrix

$$\begin{pmatrix} \frac{\partial \mathcal{Q}}{\partial x} & \frac{\partial \mathcal{Q}}{\partial y} & \frac{\partial \mathcal{Q}}{\partial z} & \frac{\partial \mathcal{Q}}{\partial w} \\ \frac{\partial \mathcal{F}}{\partial x} & \frac{\partial \mathcal{F}}{\partial y} & \frac{\partial \mathcal{F}}{\partial z} & \frac{\partial \mathcal{F}}{\partial w} \end{pmatrix}.$$

In fact, all monomials of degree six are in this ideal and thus our curve is smooth.

Our next task is to find a divisor G' of degree seven on the curve, preferably with support disjoint from the eight rational points. The simplest way to do this is to find a point of degree seven on the curve.

By definition a point of degree seven on X' is a point with residue field $\mathbb{F}_{128}$. Such points are in one-to-one correspondence with Galois orbits of the solutions $(x : y : z : w) \in \mathbb{P}_{\mathbb{F}_2}^3$ to the equations defining X' such that $\mathbb{F}_{128}$ is the smallest subfield of $\bar{\mathbb{F}}_2$ in which the solution $(x : y : z : w)$ can be written. Here the Galois action refers to the action of $\text{Gal}(\mathbb{F}_{128}/\mathbb{F}_2) \simeq \mathbb{Z}/7$. If we think of $\mathbb{F}_{128}$ as $\mathbb{F}_2[t]/(1+t+t^7)$, then this Galois group is generated by the Frobenius element $\tau_2: t \mapsto t^2$. This action extends naturally to an action on solutions $(x : y : z : w)$ via

$$\tau_2: (x : y : z : w) \mapsto (x^2 : y^2 : z^2 : w^2).$$

One can check that there are exactly twenty points of degree seven on our curve. One of them corresponds to the Galois orbit of

$$(1 : t^6 : 1 + t^2 + t^3 + t^5 + t^6 : t + t^3 + t^4).$$

We refer to this point of degree seven, and to the (Weil) divisor it represents, as G' . By the usual Riemann–Roch theorem, $\mathcal{L}(G')$ has dimension four.

Lemma 4.4: Each of the following triples represents three equivalent expressions for a rational function on the curve, and together with the constant function 1, they form a basis for $\mathcal{L}(G')$.

$$g_1 = \left(\frac{wx + wy + xy + y^2 + wz + xz}{wy + xy + y^2 + z^2}, \frac{wx + xy + y^2}{w^2 + x^2 + wy + y^2 + z^2}, \frac{wx^2 + w^2y + wxy + xy^2 + y^3 + w^2z + wxz}{w^3 + w^2y + wy^2 + y^3 + w^2z + wxz + wz^2} \right)$$

$$g_2 = \left(\frac{z^2}{wy + xy + y^2 + z^2}, \frac{wz + xz + z^2}{w^2 + x^2 + wy + y^2 + z^2}, \frac{wx^2 + w^2y + wxy + wy^2 + xy^2 + wz^2}{w^3 + w^2y + wy^2 + y^3 + w^2z + wxz + wz^2} \right)$$

$$g_3 = \left(\frac{wz}{wy + xy + y^2 + z^2}, \frac{w^2 + wx + wz}{w^2 + x^2 + wy + y^2 + z^2}, \frac{w^3 + wx^2 + wy^2 + xy^2 + wxz}{w^3 + w^2y + wy^2 + y^3 + w^2z + wxz + wz^2} \right).$$

Proof: For simplicity, write

$$g_i = \left(\frac{n_{i1}}{d_1}, \frac{n_{i2}}{d_2}, \frac{n_{i3}}{d_3} \right)$$

and let

$$R = \mathbb{F}_2[x, y, z, w]/(\mathcal{Q}, \mathcal{F}).$$

To show each triple g_i represents a rational function, it is enough to show that 1) each difference $n_{ij}d_k - n_{ik}d_j$ is 0 in R and 2) none of the denominators d_i are in the ideal of $\mathbb{F}_2[x, y, z, w]$ generated by $\mathcal{Q}$ and $\mathcal{F}$. The following equations verify 1):

$$\begin{aligned} n_{11}d_2 - n_{12}d_1 &= (x + y + z + w)\mathcal{F} + (xz + xw + w^2)\mathcal{Q} \\ n_{12}d_3 - n_{13}d_2 &= (xy + yw + zx + w^2)\mathcal{F} + (x^3 + x^2z \\ &\quad + xyz + y^2z + yw^2 + w^3)\mathcal{Q} \\ n_{21}d_2 - n_{22}d_1 &= z\mathcal{F} + xz\mathcal{Q} \\ n_{22}d_3 - n_{23}d_2 &= (xy + y^2 + xw + yw + w^2)\mathcal{F} \\ &\quad + (x^3 + x^2y + xy^2 + x^2z + y^2z \\ &\quad + x^2w + y^2w + xzw)\mathcal{Q} \\ n_{31}d_2 - n_{32}d_1 &= w\mathcal{F} + xw\mathcal{Q} \\ n_{32}d_3 - n_{33}d_2 &= (xy + y^2 + yw + zw)\mathcal{F} + (x^3 + x^2y \\ &\quad + x^2z + y^2w + yw^2 + zw^2 + w^3)\mathcal{Q}. \end{aligned}$$

2) is easily shown by checking that each d_i is nonzero at some point on the curve.

Now let I be the ideal in R generated by d_1, d_2 , and d_3 . A simple Macaulay calculation shows that I is an ideal of codimension three and degree seven. This means that the zeros of this ideal form a divisor of degree seven on X' . It is easy to check that the point G' is a zero of the ideal, so it must be the only zero since it has degree seven. Hence, each g_i is regular away from G' and we have $g_i \in \mathcal{L}(G')$, ($i = 1, 2, 3$). Since the set $\{1, g_1, g_2, g_3\}$ is a set of $4 = \dim \mathcal{L}(G')$ linearly independent functions contained in $\mathcal{L}(G')$, it must be a basis. $\square$

We give three equivalent representations of each rational function so we can easily evaluate them at all of the $\mathbb{F}_2$ -rational points on the curve. In fact, to evaluate one of the rational functions at a rational point P on the curve, choose a representative which has nonzero denominator at P . Since the representatives are equivalent, it does

not matter which one (with nonzero denominator) is chosen. Notice that all three representatives are necessary, as only d_1 is nonzero at the point $(1 : 0 : 1 : 0)$ of X' , only d_2 is nonzero at the point $(1 : 0 : 0 : 0)$ of X' , and only d_3 is nonzero at the point $(1 : 1 : 0 : 1)$ of X' .

Remark 4.5: Because we will want to generalize this construction to a construction over $\mathbb{Z}/4\mathbb{Z}$, we would like to express G' as a Cartier divisor. Since the set of denominators $\{d_1, d_2, d_3\}$ of the representatives for the rational functions g_1, g_2 , and g_3 in Theorem 4.4 generate the maximal ideal of $R = \mathbb{F}_2[x, y, z, w]/(\mathcal{Q}, \mathcal{F})$ corresponding to G' , one of the d_i must be a local parameter in some neighborhood U_0 of G' ; set s to be this d_i . Let $U_1 = X' \setminus G'$. Then $\{(U_0, s), (U_1, 1)\}$ is a Cartier divisor which represents G' .

Theorem 4.6: The binary $[8, 4, 4]$ extended Hamming code is strongly algebraic-geometric.

Proof: Let X' and G' be as above, and let $\mathcal{P} = X'(\mathbb{F}_2) =$

$$\{(1 : 0 : 0 : 0), (0 : 1 : 0 : 0), (0 : 0 : 1 : 0), (0 : 0 : 0 : 1), (1 : 0 : 1 : 0), (1 : 1 : 0 : 0), (0 : 0 : 1 : 1), (0 : 1 : 0 : 1)\}.$$

Using the basis of $\mathcal{L}(G')$ as given in Lemma 4.4, we find that $C_{\mathbb{F}_2}(X', \mathcal{P}, G')$ has generator matrix (4.2). $\square$

Our next task is to “lift” this construction to a construction of the octacode as a strongly algebraic geometric code over $\mathbb{Z}/4\mathbb{Z}$. We first need some lemmas.

Lemma 4.7: If $\hat{\mathcal{Q}}$ and $\hat{\mathcal{F}}$ represent homogeneous quadric and cubic polynomials in $(\mathbb{Z}/4\mathbb{Z})[x, y, z, w]$ such that

$$\begin{aligned} \hat{\mathcal{Q}} &\equiv \mathcal{Q}(\text{mod } 2) \\ \hat{\mathcal{F}} &\equiv \mathcal{F}(\text{mod } 2) \end{aligned}$$

then the subscheme X of $\mathbb{P}_{\mathbb{Z}/4\mathbb{Z}}^3$ defined by the equations $\hat{\mathcal{Q}} = 0$, $\hat{\mathcal{F}} = 0$ is a curve over $\text{Spec } \mathbb{Z}/4\mathbb{Z}$ with X' (as defined above) as its associated curve over $\mathbb{F}_2$.

Proof: Let J be the ideal of $(\mathbb{Z}/4\mathbb{Z})[x, y, z, w]$ generated by $\hat{\mathcal{F}}, \hat{\mathcal{Q}}$, and the 2×2 minors of the Jacobian matrix

$$\begin{pmatrix} \frac{\partial \hat{\mathcal{Q}}}{\partial x} & \frac{\partial \hat{\mathcal{Q}}}{\partial y} & \frac{\partial \hat{\mathcal{Q}}}{\partial z} & \frac{\partial \hat{\mathcal{Q}}}{\partial w} \\ \frac{\partial \hat{\mathcal{F}}}{\partial x} & \frac{\partial \hat{\mathcal{F}}}{\partial y} & \frac{\partial \hat{\mathcal{F}}}{\partial z} & \frac{\partial \hat{\mathcal{F}}}{\partial w} \end{pmatrix}.$$

As before, X is smooth if J contains all monomials of some given degree. By Remark 4.3, $J + (2)$ contains all monomials of degree six. Hence, $J + (2)$ is locally the unit ideal. By Nakayama’s lemma [6], J itself is locally the unit ideal, and so the result follows. $\square$

Lemma 4.8: Let X be a curve over $\mathbb{Z}/4\mathbb{Z}$ as described in Lemma 4.7, and let G' be the divisor on X' defined above. Let

$$g_i = (n_{i1}/d_1, n_{i2}/d_2, n_{i3}/d_3), \quad i = 1, 2, 3$$

be as in Lemma 4.4 so that $\{1, g_1, g_2, g_3\}$ is a basis for $\mathcal{L}(G')$. Suppose we can find triples $\hat{g}_i$ for $i = 1, 2, 3$ such that

$$\hat{g}_i = (\hat{n}_{i1}/\hat{d}_1, \hat{n}_{i2}/\hat{d}_2, \hat{n}_{i3}/\hat{d}_3), \quad i = 1, 2, 3$$

are rational functions on X and $\hat{n}_{ij} \equiv n_{ij}(\text{mod } 2)$, $\hat{d}_j \equiv d_j(\text{mod } 2)$. Then there is a Cartier divisor G on X such that $\phi^*G = G'$ and $\{1, \hat{g}_1, \hat{g}_2, \hat{g}_3\}$ is a basis of $\mathcal{L}(G)$.

Proof: By Remark 4.5, G' is a Cartier divisor on X' of the form $\{(U_0, s), (U_1, 1)\}$ where $s = d_i$ for some $i \in \{1, 2, 3\}$. Since the underlying topologies of X and X' are the same, we can regard U_0 and U_1 as open sets on X . Further, by Nakayama’s lemma, $\hat{s} = \hat{d}_i$ (same i) is a local parameter for some “lift” G of G' . The Cartier divisor $\{(U_0, \hat{s}), (U_1, 1)\}$ represents G , and it is easy to check that $\phi^*(G) = G'$. By Theorem 3.4, $\mathcal{L}(G)$ is a free $\mathbb{Z}/4\mathbb{Z}$ module of rank

$$\begin{aligned}
\hat{g}_1 &= \left(\frac{wx + 3wy + xy + y^2 + 3wz + xz}{\hat{d}_1}, \frac{wx + xy + y^2 + 2yz}{\hat{d}_2}, \frac{wx^2 + w^2y + wxy + 2wy^2 + xy^2 + 3y^3 + w^2z + wxz + 2xyz + 2yz^2}{\hat{d}_3} \right) \\
\hat{g}_2 &= \left(\frac{2xy + 2yz + z^2}{\hat{d}_1}, \frac{2wy + 3wz + 3xz + 3z^2}{\hat{d}_2}, \frac{wx^2 + 3w^2y + wxy + 3wy^2 + xy^2 + 2wyz + 2xyz + 2y^2z + 3wz^2 + 2yz^2}{\hat{d}_3} \right) \\
\hat{g}_3 &= \left(\frac{2wy + 2xy + wz + 2xz}{\hat{d}_1}, \frac{w^2 + wx + wz}{\hat{d}_2}, \frac{w^3 + wx^2 + wy^2 + xy^2 + wxz}{\hat{d}_3} \right)
\end{aligned} \tag{4.3}$$

$4 = \dim_{\mathbb{F}_2} \mathcal{L}(G')$. Another application of Nakayama's lemma shows that the elements $1, \hat{g}_1, \hat{g}_2, \hat{g}_3$ of $\mathcal{L}(G)$ form a basis. $\square$

Consequently, if we find any system of lifts $X, \hat{g}_1, \hat{g}_2, \hat{g}_3$ as above, by simply evaluating 1 along with the rational functions $\hat{g}_i$ at a set of disjoint $\mathbb{Z}/4\mathbb{Z}$ points lying over the points of $\mathcal{P}$, we get an explicit construction of a strongly algebraic-geometric code C whose linear projection is the binary $[8, 4, 4]$ extended Hamming code. Finding a system so that C is the octacode amounts to solving a system of 313 linear equations in 402 unknowns. Luckily, the equations are consistent and we can use a simple C program to solve them. We summarize the results in the following theorem.

Theorem 4.9: The octacode is a strongly algebraic-geometric code over $\mathbb{Z}/4\mathbb{Z}$. More precisely, let X be the projective scheme over $\mathbb{Z}/4\mathbb{Z}$ defined by the equations

$$\begin{aligned}
0 &= wx + yz \\
0 &= 2w^2x + wx^2 + 3w^2y + 2wxy + 3x^2y + 3wy^2 \\
&\quad + 3xy^2 + 3w^2z + x^2z + 2wyz + 3wz^2 + xz^2.
\end{aligned}$$

Then

- 1) X is a curve over $\text{Spec } \mathbb{Z}/4\mathbb{Z}$.
- 2) There is a Cartier divisor G on X so that $\mathcal{L}(G)$ is a free $\mathbb{Z}/4\mathbb{Z}$ module of rank 4 with minimal generating set consisting of the constant function 1, along with the rational functions as shown in (4.3) at the top of this page, where

$$\begin{aligned}
\hat{d}_1 &= 2x^2 + 3wy + xy + y^2 + 2wz + 2yz + z^2 \\
\hat{d}_2 &= w^2 + 2wx + x^2 + wy + 2xy + y^2 + 2yz + 3z^2 \\
\hat{d}_3 &= w^3 + 2w^2x + 2wx^2 + 3w^2y + 2wxy + 3wy^2 \\
&\quad + 2xy^2 + 3y^3 + w^2z + 3wxz + 2x^2z + 2y^2z \\
&\quad + wz^2 + 2xz^2 + 2yz^2.
\end{aligned}$$

- 3) Let $\mathcal{Z}$ be the subset of the $\mathbb{Z}/4\mathbb{Z}$ points on X represented in coordinate form as

$$\begin{aligned}
&\{(1 : 0 : 0 : 0), (0 : 1 : 0 : 0), (0 : 0 : 1 : 0), (0 : 0 : 0 : 1), \\
&(1 : 0 : 3 : 0), (1 : 3 : 0 : 0), (0 : 0 : 1 : 3), (0 : 1 : 0 : 3)\}.
\end{aligned}$$

Then the algebraic-geometric $\mathbb{Z}/4\mathbb{Z}$ code $C_{\mathbb{Z}/4\mathbb{Z}}(X, \mathcal{Z}, G)$ is the octacode.

Proof: 1) follows from Lemma 4.7. To show 2), we must first show that for each i , the three expressions for $\hat{g}_i$ do indeed represent the same rational function on X . As before, write

$$\hat{g}_i = (\hat{n}_{i1}/\hat{d}_1, \hat{n}_{i2}/\hat{d}_2, \hat{n}_{i3}/\hat{d}_3).$$

Let $\hat{\mathcal{F}}$ be the cubic in the statement of the theorem and $\hat{\mathcal{Q}}$ the quadric. Then the following equations (which are "lifts" of the equations in

the proof of Lemma 4.4) hold:

$$\begin{aligned}
\hat{n}_{11}\hat{d}_2 - \hat{n}_{12}\hat{d}_1 &= (w + x + 3y + 3z)\hat{\mathcal{F}} \\
&\quad + (3w^2 + 3wx + 2x^2 + 2wy \\
&\quad + 2xy + 2y^2 + xz + 2yz + 2z^2)\hat{\mathcal{Q}} \\
\hat{n}_{12}\hat{d}_3 - \hat{n}_{13}\hat{d}_2 &= (w^2 + 2wx + wy + xy + 2y^2 + 3wz)\hat{\mathcal{F}} \\
&\quad + (3w^3 + 2wx^2 + 3x^3 + 3w^2y + 2wxy \\
&\quad + 2wy^2 + 2xy^2 + 2y^3 + 2w^2z + 3x^2z \\
&\quad + 3wyz + 3xyz + 3y^2z + 2wz^2 \\
&\quad + 2xz^2 + 2z^3)\hat{\mathcal{Q}} \\
\hat{n}_{21}\hat{d}_2 - \hat{n}_{22}\hat{d}_1 &= (2x + 2y + z)\hat{\mathcal{F}} + (2x^2 + 2xy \\
&\quad + 2y^2 + xz + 2yz + 2z^2)\hat{\mathcal{Q}} \\
\hat{n}_{22}\hat{d}_3 - \hat{n}_{23}\hat{d}_2 &= (w^2 + wx + 3wy + xy + y^2 \\
&\quad + 2xz + 2z^2)\hat{\mathcal{F}} + (2w^3 + wx^2 \\
&\quad + 3x^3 + 2w^2y + x^2y + wy^2 + xy^2 \\
&\quad + 2y^3 + 2w^2z + 3wxz + 3x^2z \\
&\quad + 2xyz + 3y^2z + 2wz^2)\hat{\mathcal{Q}} \\
\hat{n}_{31}\hat{d}_2 - \hat{n}_{32}\hat{d}_1 &= (w + 2x + 2y + 2z)\hat{\mathcal{F}} \\
&\quad + (2w^2 + wx + 2wy)\hat{\mathcal{Q}} \\
\hat{n}_{32}\hat{d}_3 - \hat{n}_{33}\hat{d}_2 &= (2w^2 + wy + xy + y^2 + 3wz \\
&\quad + 2yz)\hat{\mathcal{F}} + (w^3 + 3x^3 + w^2y \\
&\quad + x^2y + wy^2 + 3w^2z + x^2z + 2xz^2)\hat{\mathcal{Q}}
\end{aligned}$$

and it is again easy to check that none of the $\hat{d}_i$, $i = 1, 2, 3$, are in the ideal generated by $\hat{\mathcal{F}}$ and $\hat{\mathcal{Q}}$. 2) now follows directly from Lemma 4.8. For 3), simply evaluate the basis of rational functions at the $\mathbb{Z}/4\mathbb{Z}$ points of $\mathcal{Z}$ to get the generator matrix (4.1). $\square$

ACKNOWLEDGMENT

The author wishes to thank the referees for their useful comments.

REFERENCES

- [1] V. D. Goppa, "Codes associated with divisors," *Probl. Pered. Inform.*, vol. 13, pp. 33–39, 1977. (English translation in *Probl. Inform. Transm.*, vol. 13, pp. 22–27, 1977.)
- [2] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The $\mathbb{Z}_4$ -linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Trans. Inform. Theory*, vol. 40, pp. 301–319, Mar. 1994.
- [3] R. Hartshorne, *Algebraic Geometry*. New York: Springer-Verlag, 1977.
- [4] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*. Oxford, U.K.: Clarendon, 1979.
- [5] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1993.
- [6] H. Matsumura, *Commutative Ring Theory*. Cambridge, U.K.: Cambridge Univ. Press, 1990.

- [7] J. S. Milne, *Étale Cohomology*. Princeton, NJ: Princeton Univ. Press, 1980.
- [8] R. Pellikaan, B.-Z. Shen, and G. J. M. van Wee, “Which linear codes are algebraic-geometric?,” *IEEE Trans. Inform. Theory*, vol. 37, pp. 583–602, 1991.
- [9] M. Stillman, M. Stillman, and D. Bayer, *Macaulay User Manual*, 1989.
- [10] J. L. Walker, “Algebraic geometric codes over rings,” submitted for publication.
- [11] ———, “Algebraic geometric codes over rings,” Ph.D. dissertation, University of Illinois, Urbana, IL, 1996.
- [12] S. Wolfram, *Mathematica: A System for Doing Mathematics*. Reading, MA: Addison-Wesley, 1991.