Asian J. Math.
Vol. 16, No. 1, pp. 089–102, March 2012

003

CODES FROM INFINITELY NEAR POINTS*

BRUCE M. BENNETT†, HING SUN LUK‡, AND STEPHEN S.-T. YAU§

Dedicated to Professor Fabrizio Catanese on the occasion of his 60th birthday

Abstract. We introduce a new class of nonlinear algebraic-geometry codes based on evaluation of functions on infinitely near points. Let X be an algebraic variety over the finite field $\boldsymbol{F}_q$. An *infinitely near point of order* μ is a point P on a variety X' obtained by μ iterated blowing-ups starting from X. Given such a point P and a function f on X, we give a definition of $f(P)$ which is nonlinear in f (unless $\mu = 0$). Given a set $\mathcal{S}$ of infinitely near points $\{P_1, \cdots, P_n\}$, we associate to f its set of values $(f(P_1), \cdots, f(P_n))$ in $\boldsymbol{F}_q^n$. Let V be a k dimensional vector space of functions on X. Evaluation of functions in V at the n points of $\mathcal{S}$ gives a map $V \to \boldsymbol{F}_q^n$, which we view as an (n, q^k, d) code when the map is injective. Here d is the largest integer such that a function in V is uniquely determined by its values on any $n - d + 1$ points of $\mathcal{S}$. These codes generalize the Reed-Solomon codes, but unlike the R-S codes they can be constructed to have arbitrarily large code length n. The first nontrivial case is where $X = \boldsymbol{A}^2_{\boldsymbol{F}_q}$, affine 2-space, and we study this case in detail.

Key words. Algebraic-geometry code, blowing up, infinitely near points.

AMS subject classifications. 94B27.

1. Introduction.

Let $\boldsymbol{F}_q$ denote the field with $q = p^e$ elements. An (n, q^k, d) code is an injective map $G : V \to \boldsymbol{F}_q^n$, where V is a finite set with $k = \log_q |V|$. If C is the image of G, d is the minimum, over all pairs of distinct elements c_1, c_2 of C, of the number of coordinates in which c_1 and c_2 differ. d is called the *minimum distance* of the code. The ratio k/n is called the *transmission rate* of the code, and $\delta = d/n$ is called the *relative minimum distance*. For codes which are optimal from the standpoint of both transmission efficiency and error correction, it is desirable to make k/n and δ as large as possible, and also to make n large. n, k and d (or n, k/n and δ) are called the *parameters* of the code. Frequently $V = \boldsymbol{F}_q^k$ and G is a linear map; the code is then called a *linear* $[n, k, d]$ code. Even if G is not linear, it may be that $V = \boldsymbol{F}_q^k$ in a natural way. For both linear and nonlinear codes, by a pigeonhole argument, n, k, and d are constrained by the inequality $k + d \leq n + 1$ (or $k/n + \delta \leq 1 + 1/n$), called the 'Singleton bound' [TV, p27].

The simplest examples of linear algebraic-geometry codes are the Reed-Solomon codes. Here V is the vector space of polynomials of degree $\leq k - 1$ in one variable (k chosen arbitrarily). Let $\mathcal{S} = \{P_1, \cdots, P_q\}$ be the set of points in $\boldsymbol{F}_q$, i.e., the points on the affine line $\boldsymbol{A}^1_{\boldsymbol{F}_q}$. We define $G : V \to \boldsymbol{F}_q^q$ by $f \mapsto (f(P_1), \cdots, f(P_q))$; this map is linear in f. Since a polynomial in one variable of degree $k - 1$ is determined by its values on any k points, we have $d = q - k + 1$, i.e., $k + d = q + 1$. The Reed-Solomon codes were generalized by Goppa [G]. For the Goppa codes the vector space V consists of the rational (meromorphic) functions on a given algebraic curve X over $\boldsymbol{F}_q$ which represent the complete linear system associated to a divisor D on X, i.e., $V = L(D)$ in

*Received May 19, 2010; accepted for publication February 25, 2011.

†Department of Mathematics, University of California, Irvine, CA 92697-3875, USA.

‡Department of Mathematics, The Chinese University of Hong Kong, Shatin, N.T. Hong Kong (hsluk@math.cuhk.edu.hk).

§Department of Mathematics, Tsinghua University, Beijing 100084, P. R. China. Current Address: Department of Mathematics, Statistics and Computer Science (M/C 249), University of Illinois at Chicago, 851 South Morgan Street, Chicago, IL 60607-7045, USA (yau@uic.edu).

the standard algebraic-geometry notation. $\mathcal{S}$ is usually taken to be the set of all $\boldsymbol{F}_q$-rational points of X not contained in the support of D. Thus $k = \dim(L(D))(= l(D)$ in the standard notation), and the code length n depends on the number of $\boldsymbol{F}_q$-rational points on X. It has been shown that there are families of curves with arbitrarily large n, and good curve parameters k/n and δ. Denoting by $n(C)$, $M(C)$ and $d(C)$ the length, size and minimium distance of a code C over $\mathbb{F}_q$, let $U_q = \{(q, R) \in \mathbb{R}^2 : \exists\{C_i\}_{i=1}^{\infty}$ with $n(C_i) \to \infty$ and $\delta = \lim_{i\to\infty} \frac{d(C_i)}{n(C_i)}, R = \lim_{i\to\infty} \frac{\log_q M(C_i)}{n(C_i)}\}$. It is shown in [TV, section 1.3.1] that there exists a continuous function $\alpha_q(\delta)$, $\delta \in [0, 1]$ such that $U_q = \{(\delta, R) \in \mathbb{R}^2 : 0 \le R \le \alpha_q(\delta), 0 \le \delta \le 1\}$. Let H_q be the normalized entropy function $H_q(\delta) := \delta \log_q(q-1) - \delta \log_q \delta - (1-\delta)\log_q(1-\delta)$. Then the Gilbert-Varshamov bound [TV, p.34] holds:

$$\alpha_q(\delta) \ge R_{GV}(q, \delta) := 1 - H_q(\delta), \text{ for all } \delta \in (0, \frac{q-1}{q}) \tag{1.1}$$

Let $N(X/\mathbb{F}_q)$ denote the number of $\boldsymbol{F}_q$-rational points of an algebraic curve X. By the Hasse-Weil bound, $N(X/\mathbb{F}_q) \le q + 1 + 2g(X)\sqrt{q}$, where $g(X)$ is the genus of the curve X, one considers for any prime power q and any integer $g \ge 0$,

$$N_q(g) := \max_{g(X)=g} N(X/\mathbb{F}_q) \tag{1.2}$$

$$A(g) := \limsup_{g\to\infty} \frac{N_q(g)}{g} \tag{1.3}$$

Goppa's construction of algebraic-geometry codes gives [TV, corollary 3.4.2]

$$\alpha_q(\delta) \ge R_G(q, \delta) := 1 - \delta - \frac{1}{A(q)}, \text{ for all } \delta \in [0, 1] \tag{1.4}$$

When q is a square prime power, $A(q) = \sqrt{q} - 1$ [TVZ] and the Tsfasman-Vladut-Zink bound holds:

$$\alpha_q(\delta) \ge R_{TVZ}(q, \delta) := 1 - \delta - \frac{1}{\sqrt{q}-1}, \text{ for all } \delta \in [0, 1] \tag{1.5}$$

Recently, Xing [X] gave a beautiful new method of finding nonlinear algebraic-geometry codes over $\mathbb{F}_q$, using sections of line bundles as well as the sections' derivatives. Xing's codes improve the bounds (1.4) and (1.5). Indeed, for prime power q,

$$\alpha_q(\delta) \ge R_X(q, \delta) := 1 - \delta - \frac{1}{A(q)} + \sum_{i=2}^{\infty} \log_q\big(1 + \frac{q-1}{q^{2i}}\big), \text{ for all } \delta \in (0, 1) \tag{1.6}$$

and for square prime power q,

$$\alpha_q(\delta) \ge 1 - \delta - \frac{1}{\sqrt{q}-1} + \sum_{i=2}^{\infty} \log_q\big(1 + \frac{q-1}{q^{2i}}\big), \text{ for all } \delta \in (0, 1) \tag{1.7}$$

Xing's nonlinear codes unfortunately are nonconstructive. Nonlinear generalization of Goppa codes was also studied by Elkies [E1] using rational functions on curves. His codes in [E1] improve on Goppa's in a range of parameters that includes all the

Goppa codes that improve on Gilbert-Varshamov. More recently Elkies [E2] applied Xings' technique to his codes of [E1]. His new codes of [E2] have parameters that improve on Xing's, replacing the sum $\sum_{i=2}^{\infty} \log_q \left(1 + \frac{q-1}{q^{2i}}\right) = \frac{1}{\log q}\left(q^{-3} - q^{-4} + O(q^{-5})\right)$ in (1.7) by $\log_q(1 + \frac{1}{q^3}) = \frac{1}{\log q}(q^{-3} + O(q^{-6}))$ when q is a square prime power.

As pointed out by Elkies [E2], these nonlinear codes, unlike Goppa codes, are still very far from any practical use. In order to get codes with good parameters and large n, we are led back to the original idea of the Reed-Solomon codes, but now we remedy the severe restriction on n ($n = q$) by evaluating functions not just on points of X, but on *infinitely near points*. An infinitely near point is a point on a variety X' obtained from X by a sequence of blowing-ups (see §2 below). Since the number of infinitely near points is unlimited (if we allow sufficiently many iterated blowing-ups), we can now achieve large code lengths n at will. The problem is to find pairs $(\mathcal{S}, V)$ where $\mathcal{S}$ is a set of infinitely near points and V is a set of functions on X, so that d and k are jointly maximized. There is the initial question how to define the evaluation of functions at infinitely near points; the obvious definitions yield an uninteresting result (the values are zero). However there is a geometrically natural definition which permits explicit computation, but which is nonlinear. While this nonlinearity complicates the analysis, it leads to a clear presentation of the central issue in calculating d, namely, the calculation of the rank of a family of multivariable generalizations of Vandermonde matrices. The exact form of these matrices depends on the choice of V and $\mathcal{S}$, and the relevant results consist in showing that a judicious choice of pairs $(V, \mathcal{S})$ produces matrices of computably large rank. We illustrate our techniques by an example (Section 4) of a modified code which can be viewed as a linear approximation of our nonlinear code. The parameters of the new linear code are obtained in Theorem 4.3. In addition to being simple and explicit, the new linear code is self-orthogonal (Theorem 4.4). In Remark 4.5, the code is compared to algebraic geometry codes on curves and is shown to have a strong advantage in terms of the difference between n and the lower bound of $k + d$.

We would like to thank Hao Chen and the referee for their very helpful remarks.

2. Blowing up. Let X be an algebraic variety over a field $\boldsymbol{F}$. X is covered by Zariski open affine sets $\{X_i\}$; each X_i is associated to a ring of functions A_i which is a finitely generated $\boldsymbol{F}$-algebra. The points of X_i correspond to the maximal ideals M of A_i such that $A_i/M = \boldsymbol{F}$. (In other words, for the purpose of this study, we consider only the "$\boldsymbol{F}$-rational points" of the variety.) Let Y be a subvariety of X, defined on X_i by the ideal J_i in A_i. The "blowing up (or monoidal transform) of X with center Y" is a variety X' with a morphism $\pi : X' \to X$, such that π is an isomorphism outside $\pi^{-1}(Y)$ and $\pi^{-1}(Y)$ is the projectivized normal cone of Y in X. In particular if the ideal J is locally principal, i.e., if Y is a divisor on X, then π is an isomorphism (everywhere), since in this case the normal cone is a line bundle, which when projectivized reduces to Y itself. If Y is a point $\{y\}$, then X' is sometimes called a "quadratic transform", then $\pi^{-1}(y)$ is the projectivized tangent cone of X at y. Thus if X is nonsingular at y and $\pi : X' \to X$ is the quadratic transform of X with center $\{y\}$, then $\pi^{-1}(y)$ is $\boldsymbol{P}_F^{m-1}$ (projective $m-1$-space over F) where $\dim X = m$.

The construction of X' is local on X, so to describe it we may assume that X is affine with ring A. Then X' is covered by affine open sets X'_g where g ranges over all the elements of J. The affine ring A'_g of X'_g is $A[J/g]$, the A-subalgebra of the ring of fractions of A generated by all h/g, h in J. If g_1 and g_2 are in J,

then ${X'}_{g_1} \cap {X'}_{g_2} = {X'}_{g_1 g_2}$, and the inclusion ${X'}_{g_1 g_2} \subset {X'}_{g_1}$ corresponds to the canonical homomorphism $A[J/g_1 g_2] \leftarrow A[J/g_1]$. It follows that if $g_1, \cdots, g_m$ are a set of generators for J, then $X' = {X'}_{g_1} \cup {X'}_{g_2} \cup \cdots \cup {X'}_{g_m}$. The morphism $\pi|_{{X'}_g} : {X'}_g \to X$ corresponds to the canonical ring homomorphism $A[J/g] \leftarrow A$. Hence $\pi^{-1}(Y) \cap {X'}_g$ is defined by the ideal $JA[J/g]$, which is just the principal ideal $(g)A[J/g]$. Thus, $\pi^{-1}(Y)$ is the divisor on X' which is defined on ${X'}_g$ by $g = 0$; it is called the "exceptional divisor", denoted by E. Let E_g denote $E \cap {X'}_g$. Then the E_g are affine varieties which cover E, and the affine ring of E_g is $A[J/g]/(g)$.

For any f in A, let $\nu_J(f)$ be the highest power of J which contains f, so that $\nu_J(f) \geq 0$. Let $g_1, \cdots, g_m$ be a minimal set of generators of J; in particular $\nu_J(g_i) = 1$. We describe the affine ring $A[J/g_1]/(g_1)$ of E_{g_1}. For f in A, $f/g_1^{\nu_J(f)}$ is in $A[J/g_1]$; let $\overline{f/g_1^{\nu_J(f)}}$ be its image modulo (g_1). $A[J/g_1]/(g_1)$ is the graded A/J-algebra whose homogeneous piece of degree ν, denoted $(A[J/g_1]/(g_1))_\nu$, is the A/J-module generated by all $\overline{f/g_1^\nu}$, with $\nu_J(f) = \nu$, and with relations as follows: Let $f_1, \cdots, f_s$ be in A with $\nu_l = \nu_J(f_l), l = 1, \cdots, s$. Let $a_1, \cdots, a_s$ in A be given, with $\overline{a_l}$ the image of a_l modulo J. Then

$$\overline{a_1}\overline{f_1/g_1^{\nu_1}} + \cdots + \overline{a_s}\overline{f_s/g_1^{\nu_s}} = 0$$

in $\big(A[J/g_1]/(g_1)\big)_\nu$ iff

$$\nu_J(a_1 f_1 + \cdots + a_s f_s) > \nu.$$

It is equivalent to describe E as the projective variety over Y whose homogeneous coordinate ring is

$$Gr_J(A) = \oplus_{\nu \geq 0} J^\nu / J^{\nu+1}$$

and E_{g_i} is the affine piece of this projective variety where $\mathrm{In}_J(g_i) \neq 0$ (where $In_J(g_i)$ is the 'J-adic initial form' of g_i, i.e., g_i (modulo J^2)); it is homogeneous of degree 1 in the graded algebra. The statement that the g_i generate J is equivalent to saying that these $In_J(g_i)$ generate the graded algebra; i.e., that the E_{g_i} cover E.

Let $X' \to X$ be the blowing up of X with center Y. Suppose Z is a subvariety of X. We will define the strict transform Z' of Z in X' as follows. Suppose X is a variety with affine ring A, and $Z \subset X$ is a subvariety with ring $B = A/I$, where I is the ideal defining Z in X. The blowing up Z' of Z with center $Y \cap Z$ can be viewed as a subvariety of X' (the blowing up of X with center Y) called the *strict transform* of Z in X'; it is the closure in X' of $\pi^{-1}(Z - Z \cap Y)$ where $\pi : X' \to X$. The ideal which defines Z' in X' may be described explicitly as follows. Let g be an element of J; for simplicity we use the same notation g for its image in $B = A/I$. Then we have affine pieces ${X'}_g$ of X' and ${Z'}_g$ of Z', with affine rings ${A'}_g = A[J/g]$ and ${B'}_g = B[JB/g]$ respectively. Let ${I'}_g$ be the ideal in ${A'}_g$ defined by

$${I'}_g = \{f/g^{\nu_J(f)} | f \in I\};$$

$f/g^{\nu_J(f)}$ is called the *strict transform* of f in ${A'}_g$, and ${I'}_g$ is called the strict transform of I in ${A'}_g$. ${I'}_g$ is the ideal of ${Z'}_g$ in ${X'}_g$, i.e., ${B'}_g = {A'}_g/{I'}_g$. If $I = (f)A$ is a principal ideal, then ${I'}_g$ is the principal ideal $(f/g^{\nu_J(f)}){A'}_g$.

As an example we consider the case $X = \boldsymbol{A}_F^m$, affine m-space over a field F. The affine ring A of X is then $F[x_1, \cdots, x_m]$. Let Y be the origin of X, so that the ideal of Y is $J = (x_1, \cdots, x_m)F[x_1, \cdots, x_m]$. X', the blowing up of the origin

in X, is covered by the affine pieces $X'_{x_1}, \cdots, X'_{x_m}$. The affine ring of X'_{x_1}, for example, is $A'_{x_1} = F[x_1, \cdots, x_m][J/x_1] = F[x_1, x_2/x_1, \cdots, x_m/x_1]$. Letting $x'_i = x_i/x_1$ for $i \geq 2$, we may write $A_{x_1} = F[x_1, x'_2, \cdots, x'_m]$, and the map $\pi : X'_{x_1} \to X$ corresponds to the inclusion $F[x_1, x'_2, \cdots, x'_m] \supset F[x_1, \cdots, x_m]$; this inclusion holds since $x_1 x'_i = x_i$. The exceptional divisor is defined by $x_1 = 0$ on X'_{x_1}, i.e., $E_{x_1} : x_1 = 0$, so the affine ring of E_{x_1} may be identified with $F[x_2/x_1, \cdots, x_m/x_1]$, i.e., with $F[x'_2, \cdots, x'_m]$. Thus E is the $(m-1)$-dimensional projective space $\boldsymbol{P}_F^{m-1}$ with homogeneous coordinate ring $F[x_1, \cdots, x_m]$, and E_{x_i} is the affine piece of $\boldsymbol{P}_F^{m-1}$ where the homogeneous coordinate $x_i \neq 0$. Suppose $Z : f = 0$ is a hypersurface in $X = \boldsymbol{A}_F^m$ where $f = f(x_1, \cdots, x_m)$, and suppose the origin y is in Z. Let Z' denote the blowing up of y in Z. Then Z' is a hypersurface $f' = 0$ in X'. On Z'_{x_1} the affine ring B_{x_1} is a quotient of the affine ring A_{x_1} of X'_{x_1} by the ideal generated by the strict transform f' of f. $f' = f/x_1^{\nu_J(f)}$, viewed as a polynomial in $x_1, x'_2, \cdots, x'_m$. For instance if $m = 3$ and $f = x_1 x_2^2 + x_3^5$, then $\nu_J(f) = 3$ and $f'(x_1, x'_2, x'_3) = x'^2_2 + x_1^2 x'^5_3$. The exceptional fibre Z' is the double hyperplane $x'^2_2 = 0$ in $\boldsymbol{P}_F^{m-1}$.

3. Evaluation of functions at infinitely near points and explicit construction of codes. Let X be a variety, and let $X = X^{(0)}, X' = X^{(1)}, X^{(2)}, \cdots, X^{(\mu)}$ be a sequence of blowing-ups starting with X. This means the for each $k = 0, \cdots, \mu - 1$, there is a subvariety $Y^{(k)} \subset X^{(k)}$ such that $X^{(k+1)}$ is the blowing up of $X^{(k)}$ with center $Y^{(k)}$. Let $P \in X^{(\mu)}$. Let f be a function on X; for this discussion we may assume that X is affine with ring A, and that f is in A, i.e., assume f is a regular algebraic function on X. We want to define '$f(P)$'. Let $\psi^{(k)} : A \to B^{(k)}$ be the canonical map, where $B^{(k)}$ is the ring of regular algebraic functions on $X^{(k)}$. $\psi^{(k)}$ is the map on rings of functions corresponding to the composite of the canonical maps $X \leftarrow X' = X^{(1)} \leftarrow \cdots \leftarrow X^{(k-1)} \leftarrow X^{(k)}$. Thus we can simply define '$f(P)$' to be $\psi^{(u)}(f)(P)$. However this definition is uninteresting. For if $\psi^{(k)}(f)$ is in the ideal of $Y^{(k)}$ in $X^{(k)}$ for any $k < \mu$, then $\psi^{(\mu)}(f)(P) = 0$. And if f is not in the ideal of any of the $Y^{(k)}$, then $\psi^{(\mu)}(f)(P) = f(Q)$, where Q in X is the image of P under the composite of the canonical maps $X \leftarrow X = X^{(1)} \leftarrow X^{(2)} \leftarrow \cdots \leftarrow X^{(\mu)}$. Thus, this naive definition for '$f(P)$' gives no new information. We give a more informative definition below.

For the present work we will restrict our attention to the important special case of a sequence of quadratic transforms, i.e., the case where each center $Y^{(k)}$ is a point in $X^{(k)}$. For consistency of notation we will denote by $P^{(\mu)}$ the point P in $X^{(\mu)}$ where we want to evaluate f. We are going to evaluate f at $P^{(k)}$ by induction on k. In fact beginning with f we define a sequence of functions $f^{(k)}$ on $X^{(k)}$, $k = 0, \cdots, \mu$, and then we take $f^{(\mu)}(P^{(\mu)})$.

Definition 3.1.
(i) $f^{(0)} = f$.
(ii) If $f^{(k-1)}$ is defined, let

$$f^{(k)} = \left(f^{(k-1)} - f^{(k-1)}(P^{(k-1)})\right)',$$

where the prime ($'$) denotes strict transform with respect to the ideal $J^{(k-1)}$ of $P^{(k-1)}$, in the ring of an affine subset of $X^{(k)}$ which contains $P^{(k)}$.

To explain this, let $A^{(k)}$ be the ring of an affine subset U of $X^{(k)}$ which contains $P^{(k)}$, and let $J^{(k-1)}$ be the (maximal) ideal of $P^{(k-1)}$ in $A^{(k-1)}$. Then, as in §2, $A^{(k)} = A^{(k-1)}[g/t^{\nu_{J^{(k-1)}}(g)} | g \in J^{(k-1)}]$, where $t \in J^{(k-1)}$ is such that $J^{(k-1)}A^{(k)} =$

$(t)A^{(k)}$. Note that $f^{(k-1)} - f^{(k-1)}(P^{(k-1)})$ is in $J^{(k-1)}$ since it vanishes at $P^{(k-1)}$. Thus

$$\big(f^{(k-1)} - f^{(k-1)}(P^{(k-1)}\big)' = \big(f^{(k-1)} - f^{(k-1)}(P^{(k-1)})\big)/t^{\nu}$$

where $\nu = \nu_{J^{(k-1)}}\big(f^{(k-1)} - f^{(k-1)}(P^{(k-1)})\big)$ is > 0.

We will study the consequences of this definition in the case where $X = \boldsymbol{A}_F^m$. We begin with an example which illustrates the procedure in Definition 3.1.

EXAMPLE 3.2. We consider $X^{(0)} = \boldsymbol{A}_F^2$ with coordinate ring $A^{(0)} = F[t, z]$. Let $P^{(0)}$ be (0,0); the ideal $J^{(0)}$ of $P^{(0)}$ in $A^{(0)}$ is $(t, z)F[t, z]$. The blowing up $X^{(1)}$ of $X^{(0)}$ with center (0,0) is covered by two affine sets $X_t^{(1)}$ and $X_z^{(1)}$, which are isomorphic to $\boldsymbol{A}_F^2$ with coordinate rings $F[t, z/t]$ and $F[t/z, z]$ respectively. Let $P^{(1)}$ be the point in $X_t^{(1)}$ with coordinates $t = 0$, $z/t = 1$, and for convenience let $z' = z/t$. Note that the condition $t = 0$ means $P^{(1)}$ lies in the exceptional fibre of $X_t^{(1)}$ over $X^{(0)}$. The ideal of $P^{(1)}$ is $(t, z' - 1)F[t, z']$. Let $X^{(2)}$ be the blowing up of $X_t^{(1)}$ with center $P^{(1)}$. It is covered by two affine pieces $X_t^{(2)}$ and $X_{z'-1}^{(2)}$, whose coordinate rings are $F[t, (z' - 1)/t]$ and $F[t/(z' - 1), (z' - 1)]$ respectively. Let $P^{(2)}$ be the point in $X_t^{(2)}$ with coordinates $t = 0$, $(z' - 1)/t = 2$; $P^{(2)}$ lies in the exceptional fibre of $X_t^{(2)}$ over $X_t^{(1)}$. Let $f = f^{(0)} = zt^2 + t^3 + z^4$.

We calculate $f^{(k)}(P^{(k)}), k = 0, 1, 2$. We have $f^{(0)}(P^{(0)}) = 0$, so $f^{(1)} = f^{(0)}/t^3$ since $\nu_{J^{(0)}}(f^{(0)}) = 3$. Thus, in the t, z' coordinate system on $X_t^{(1)}$, we may write $f^{(1)} = z' + 1 + tz'^4$, so that $f^{(1)}(P^{(1)}) = 2$. Hence $f^{(1)} - 2 = (z' - 1) + t((z' - 1) + 1)^4$, i.e.,

$$f^{(1)} - 2 = (z' - 1) + t + 4t(z' - 1) + 6t(z' - 1)^2 + 4t(z' - 1)^3 + t(z' - 1)^4.$$

Therefore $\nu_{J^{(1)}}(f^{(1)} - 2) = 1$, so $f^{(2)} = (f^{(1)} - 2)/t$, i.e.,

$$f^{(2)} = (z' - 1)/t + 1 + 4t((z' - 1)/t) + 6t^2((z' - 1)/t)^2 + 4t^3((z' - 1)/t)^3 + t^4((z' - 1)/t)^4$$

Hence $f^{(2)}(P^{(2)}) = f^{(2)}(t = 0, (z' - 1)/t = 2) = 3$.

As the example above suggests, for the purpose of simplifying the above calculation it is convenient to have a coordinate system which simplifies the representation of the successive $P^{(k)}$'s. The following result assures that this can be done in a particularly nice way.

PROPOSITION 3.3. *Let $X^{(0)} = \boldsymbol{A}_F^m$, and let $X^{(0)}, X^{(1)}, \cdots, X^{(\mu)}$ be a sequence of quadratic transforms, where $X^{(k+1)}$ is obtained by blowing up given points $P^{(k)}$ in $X^{(k)}, k = 0, \cdots, \mu - 1$. Then there exists a coordinate system $t\ \widetilde{z}_1, \widetilde{z}_2 \cdots, \widetilde{z}_{m-1}$ on $\boldsymbol{A}_F^m$ with the property: The point $P^{(k)}$ is the origin in the affine piece of $X^{(k)}$ with coordinate functions t, $\widetilde{z}_1/t^k, \cdots, \widetilde{z}_{m-1}/t^k$, i.e., $P^{(k)} : t = 0$, $\widetilde{z}_1/t^k = 0, \cdots, \widetilde{z}_{m-1}/t^k = 0$.*

Unfortunately, the values $f^{(k)}(P^{(k)})$, $k = 0, \cdots, \mu$, depend on the affine pieces we choose successively on each $X^{(0)}, \cdots, X^{(k)}$. For the construction of our codes, we need to keep track of the affine sets covering each $X^{(k)}$ and their respective coordinate rings. We do so in order to evaluate f at all points on the exceptional divisor of each quadratic transform. Continuing with Example 3.3, we explain a scheme for coordinatizing all infinitely near points for $\mu = 2$, in which we replace $X^{(2)}$ by a larger variety $\mathcal{X}^{(2)}$.

EXAMPLE 3.2 (CONTINUED). We have $X^{(1)} = X_t^{(1)} \cup X_z^{(1)}$ where $X_t^{(1)}$ and $X_z^{(1)}$ are isomorphic to $\boldsymbol{A}_F^2$ with coordinate rings $F[t, z/t]$ and $F[t/z, z]$ respectively. Then the exceptional divisor $E^{(1)} = E_t^{(1)} \cup E_z^{(1)}$, where $E_t^{(1)} = E^{(1)} \cap X_t^{(1)}$ and $E_z^{(1)} = E^{(1)} \cap X_z^{(1)}$. $E_t^{(1)}$ consists of the points $P_\ell^{(1)}$, for all $\ell \in F$, with coordinates $t = 0$, $z' = \ell$. The ideal of $P_\ell^{(1)}$ is $(t, z' - \ell)F[t, z']$. Let $t' = \frac{t}{z}$. $E_z^{(1)}$ consists of the points $P_{\ell^*}^{(1)}$, for all $\ell^* \in F^* = F \setminus \{0\}$, now with coordinates $t' = \frac{1}{\ell^*}$, $z = 0$, and the point $P_\infty^{(1)}$ with coordinates $t' = 0$, $z = 0$. The corresponding ideals are $(t' - \ell', z)F[t', z]$, $\ell' = \frac{1}{\ell^*}$ for $P_{\ell^*}^{(1)}$ and $\ell' = 0$ for $P_\infty^{(1)}$.

Let $\mathcal{X}^{(2)}$ be the variety obtained by blowing up $X^{(1)}$ at each point of $E^{(1)}$. The exceptional divisor $E_\ell^{(2)}$ over $P_\ell^{(1)}$, $\ell \in F$, can be given in terms of the coordinates $(t, z' - \ell)$ in two ways as above. Namely, $E_\ell^{(2)}$ consists of the points with coordinates $t = 0$, $\frac{z'-\ell}{t} = m$, $m \in F$, and the points with coordinates $\frac{t}{z'-\ell} = m_1$, $z' - \ell = 0$, $m_1 \in F$, where, for $m^* \in F^*$, $t = 0$, $\frac{z'-\ell}{t} = m^*$ describe the same point as $\frac{t}{z'-\ell} = \frac{1}{m^*}$, $z' - \ell = 0$.

Similarly, $E_{\ell^*}^{(2)}$, $\ell^* \in F^*$, and the exceptional divisor $E_\infty^{(2)}$ over $P_\infty^{(1)}$ can be given in terms of the coordinates $(t' - \ell', z), \ell' = \frac{1}{\ell^*}$ for $P_{\ell^*}^{(1)}$ and $\ell' = 0$ for $P_\infty^{(1)}$. Thus, points on these exceptional divisors are given by $\frac{t'-\ell'}{z} = m'$, $z = 0$, $m' \in F$, or $t' - \ell' = 0, \frac{z}{t'-\ell'} = m'_1, m'_1 \in F$, where m' and m'_1 in F^* describe the same point if $m'm'_1 = 1$. We summarize the situation as follows:

$$
\begin{array}{l}
E^{(1)} = \{P_0^{(1)}, P_{\ell^*}^{(1)}, P_\infty^{(1)}\} \quad \ell^* \in F^* = F \setminus \{0\} \\
E^{(1)} = \{P_0^{(1)}, P_{\ell^*}^{(1)}\}, \text{ where } P_0^{(1)}, P_{\ell^*}^{(1)} \text{ are given by } t = 0, z' = 0, \ell^* \\
E^{(1)} = \{P_{\ell^*}^{(1)}, P_\infty^{(1)}\}, \text{ where } P_{\ell^*}^{(1)}, P_\infty^{(1)} \text{ are given by } t' = \frac{1}{\ell^*}, 0, z = 0 \\
E_0^{(2)} = \{P_{00}^{(2)}, P_{0m^*}^{(2)}, P_{0\infty}^{(2)}\} \quad m^* \in F \setminus \{0\} \\
E_{\ell^*}^{(2)} = \{P_{\ell^*0}^{(2)}, P_{\ell^*m^*}^{(2)}, P_{\ell^*\infty}^{(2)}\} \quad \ell^*, m^* \in F \setminus \{0\} \\
E_\infty^{(2)} = \{P_{\infty 0}^{(2)}, P_{\infty m^*}^{(2)}, P_{\infty\infty}^{(2)}\} \quad m^* \in F \setminus \{0\}
\end{array}
$$

The four sets of points

$$
\begin{array}{llll}
P_{00}^{(2)} P_{0m^*}^{(2)} & P_{0m^*}^{(2)} P_{0\infty}^{(2)} & P_{\ell^*0}^{(2)} P_{\ell^*m^*}^{(2)} & P_{\ell^*m^*}^{(2)} P_{\ell^*m^*}^{(2)} \\
P_{\ell^*0}^{(2)} P_{\ell^*m^*}^{(2)} & P_{\ell^*m^*}^{(2)} P_{\ell^*m^*}^{(2)} & P_{\infty 0}^{(2)} P_{\infty m^*}^{(2)} & P_{\infty m^*}^{(2)} P_{\infty\infty}^{(2)}
\end{array}
$$

are respectively given by

$$
\begin{array}{llll}
t = 0, \frac{z'-\ell}{t} = m & \frac{t}{z'-\ell} = m_1, z' - \ell = 0 & \frac{t'-\ell'}{z} = m', z = 0 & t' - \ell' = 0, \frac{z}{t'-\ell'} = m'_1 \\
(\ell, m \in F) & (\ell, m_1 \in F) & (\ell', m' \in F) & (\ell', m'_1 \in F)
\end{array}
$$

For simplicity, we consider polynomials $f \in A^{(0)} = F[t, z]$ with only terms of degrees 3 and 4. Thus

$$
f(t, z) = \sum_{i+j=3} a_{ij} t^i z^j + \sum_{\alpha+\beta=4} a_{\alpha\beta} t^\alpha z^\beta \tag{0}
$$

We write $f^{(0)} = f$. Then $f^{(0)}(P^{(0)}) = 0$ with $\nu_{J^{(0)}}(f^{(0)}) = 3$

The strict transform $f^{(1)} \in F[t, z']$ is given by

$$
f^{(1)}(t, z') = \frac{f^{(0)}}{t^3} = \sum_{i+j=3} a_{ij} z'^j + \sum_{\alpha+\beta=4} a_{\alpha\beta} t z'^\beta \tag{1}_t
$$

Evaluating at $t = 0, z' = \ell$, we may define

$(1)_{t,P_\ell^{(1)}}$ $$f^{(1)}(P_\ell^{(1)}) = a_{30} + a_{21}\ell + a_{12}\ell^2 + a_{03}\ell^3$$

On the other hand, the strict transform $f^{(1)} \in F[t', z]$ is given by

$(1)_z$ $$f^{(1)}(t', z) = \frac{f^{(0)}}{z^3} = \sum_{i+j=3} a_{ij} t'^i + \sum_{\alpha+\beta=4} a_{\alpha\beta} t'^\alpha z$$

Evaluating at $t' - 0, z = 0$, we may define

$(1)_{z,P_\infty^{(1)}}$ $$f^{(1)}(P_\infty^{(1)}) = a_{03}.$$

But, for $\ell^* \in F^*$, the value of $f^{(1)}(t', z)$ at $t' = \frac{1}{\ell^*}, z = 0$ is equal to $a_{03} + \frac{a_{12}}{\ell^*} + \frac{a_{21}}{\ell^{*2}} + \frac{a_{30}}{\ell^{*3}} = \frac{1}{\ell^{*3}} f^{(1)}(P_{\ell^*}^{(1)})$, which does not agree with $(1)_{t,P_{\ell^*}^{(1)}}$. By abuse of notation, we use the same symbol $f^{(1)}$ for both strict transforms, but we shall state the coordinates explicitly as in $(1)_t$ and $(1)_z$, so that no confusion would arise. To compute $f^{(2)}$, we consider $(1)_t$ and observe that

$$\begin{aligned}
&f^{(1)}(t, z') - f^{(1)}(0, \ell) \\
&= \sum_{i+j=3} a_{ij}(z'^j - \ell^j) + \sum_{\alpha+\beta=4} a_{\alpha\beta} t z'^\beta \\
&= \sum a_{ij}\big(\big((z' - \ell) + \ell\big)^j - \ell^j\big) + \sum a_{\alpha\beta} t\big((z' + \ell) + \ell\big)^\beta \\
&= \sum_{i+j=3} a_{ij} \sum_{k=1}^{j} \binom{j}{k} (z' - \ell)^k \ell^{j-k} + \sum_{\alpha+\beta=4} a_{\alpha\beta} t \sum_{\gamma=0}^{\beta} \binom{\beta}{\gamma} (z' - \ell)^\gamma \ell^{\beta-\gamma} \\
(2)_{t,z'-\ell} \quad &= \sum_{k-1}^{3} \Big(\sum_{j=k}^{3} a_{3-j,j} \binom{j}{k} \ell^{j-k} \Big) (z' - \ell)^k + \sum_{\gamma=0}^{4} \Big(\sum_{\beta=\gamma}^{4} a_{4-\beta,\beta} \binom{\beta}{\gamma} \ell^{\beta-\gamma} \Big) t (z' - \ell)^\gamma
\end{aligned}$$

Note the $\nu_{J^{(1)}}(f^{(1)}(t, z') - f^{(1)}(0, \ell)) = 1$ at $P_\ell^{(1)}$ if and only if

$(*)_\ell$ $$a_{21} + 2a_{12}\ell + 3a_{03}\ell^2 \neq 0 \quad \text{or} \quad a_{40} + a_{31}\ell + a_{22}\ell^2 + a_{13}\ell^3 + a_{04}\ell^4 \neq 0$$

Under the assumption that $\nu_{J^{(1)}}(f^{(1)}(t, z') - f^{(1)}(0, \ell)) = 1$, the strict transform of $f^{(2)} \in F[t, \frac{z'-\ell}{t}]$ is given by

$$\begin{aligned}
f^{(2)}(t, \frac{z' - \ell}{t}) &= \frac{f^{(1)}(t, z') - f^{(1)}(0, \ell)}{t} \\
&= \sum_{k=1}^{3} \left(\sum_{j=k}^{3} a_{3-j,j} \binom{j}{k} \ell^{j-k} \right) t^{k-1} \big(\frac{z' - \ell}{t}\big)^k \\
&\quad + \sum_{\gamma=0}^{4} \Big(\sum_{\beta=\gamma}^{4} a_{4-\beta,\beta} \binom{\beta}{\gamma} \ell^{\beta-\gamma} \Big) t^\gamma \big(\frac{z' - \ell}{t}\big)^\gamma
\end{aligned}$$

$(2)_{t,\frac{z'-\ell}{t}}$

Evaluating at $t = 0$, $\frac{z'-\ell}{t} = m$, we may define

$(2)_{t,\frac{z'-\ell}{t},P_{\ell m}^{(2)}}$ $f^{(2)}(P_{\ell m}^{(2)}) = (a_{21} + 2a_{12}\ell + 3a_{03}\ell^2)m + (a_{40} + a_{31}\ell + a_{22}\ell^2 + a_{13}\ell^3 + a_{04}\ell^4)$

On the other hand, the strict transform $f^{(2)} \in F[\frac{t}{z'-\ell}, z'-\ell]$ is given by

$$\begin{aligned} f^{(2)}(\frac{t}{z'-\ell}, z'-\ell) &= \frac{f^{(1)}(t,z') - f^{(1)}(0,\ell)}{z'-\ell} \\ &= \sum_{k=1}^{3} \big(\sum_{j=k}^{3} a_{3-j,j} \binom{j}{k} \ell^{j-k} \big) (z'-\ell)^{k-1} \\ &\quad + \sum_{\gamma=0}^{4} \big(\sum_{\beta=\gamma}^{4} a_{4-\beta,\beta} \binom{\beta}{\gamma} \ell^{\beta-\gamma} \big) \big(\frac{t}{z'-\ell} \big) (z'-\ell)^{\gamma} \end{aligned} \tag{2}_{\frac{t}{z'-\ell}, z'-\ell}$$

Evaluating at $\frac{t}{z'-\ell} = 0, z'-\ell = 0$, we may define for all $\ell \in F$

$$f^{(2)}(P^{(2)}_{\ell\infty}) = a_{21} + 2a_{12}\ell + 3a_{03}\ell^2 \tag{2}_{\frac{t}{z'-\ell}, z'-\ell, P^{(2)}_{\ell\infty}}$$

Again, for $m^* \in F^*$, the value of $f^{(2)}(\frac{t}{z'-\ell}, z'-\ell)$ at $\frac{t}{z'-\ell} = \frac{1}{m^*}$, $z'-\ell = 0$ is equal to $(a_{21} + 2a_{12}\ell + 3a_{03}\ell^2) + \frac{(a_{40}+a_{31}\ell+a_{22}\ell^2+a_{13}\ell^3+a_{04}\ell^4)}{m^*} = \frac{1}{m^*} f^{(2)}(P^{(2)}_{\ell m^*})$, which does not agree with $(2)_{t, \frac{z'-\ell}{t}, P^{(2)}_{\ell m^*}}$.

If we now consider $(1)_z$, then we observe that

$$\begin{aligned} & f^{(1)}(t',z) - f^{(1)}(\ell',0) \\ =& \sum_{i+j=3} a_{ij}({t'}^i - {\ell'}^i) + \sum_{\alpha+\beta=4} a_{\alpha\beta} {t'}^{\alpha} z \\ =& \sum_{k=1}^{3} \big(\sum_{i=k}^{3} a_{i,3-i} \binom{i}{k} \ell'^{i-k} \big) (t'-\ell')^k \\ & + \sum_{\gamma=0}^{4} \big(\sum_{\alpha=\gamma}^{4} a_{\alpha,4-\alpha} \binom{\alpha}{\gamma} \ell'^{\alpha-\gamma} \big) (t'-\ell')^{\gamma} z \end{aligned} \tag{2}_{t'-\ell', z}$$

Note that $\nu_{J^{(1)}}(f^{(1)}(t',z) - f^{(1)}(\ell',0)) = 1$ if and only if

$$3a_{30}{\ell'}^2 + 2a_{21}\ell' + a_{12} \neq 0 \ \text{ or } \ a_{40}{\ell'}^4 + a_{31}{\ell'}^3 + a_{22}{\ell'}^2 + a_{13}\ell' + a_{04} \neq 0 \tag{\#}_{\ell'}$$

For $\ell^* \in F$, $(\#)_{\frac{1}{\ell^*}}$ only partially matches with $(*)_{\ell^*}$. Namely

$$\frac{a_{40}}{{\ell^*}^4} + \frac{a_{31}}{{\ell^*}^3} + \frac{a_{22}}{{\ell^*}^2} + \frac{a_{13}}{\ell^*} + a_{04} \neq 0 \text{ iff } a_{40} + a_{31}\ell^* + a_{22}{\ell^*}^2 + a_{13}{\ell^*}^3 + a_{04}{\ell^*}^4 \neq 0.$$

Assuming $\nu_{J^{(1)}}(f^{(1)}(t',z) - f^{(1)}(\ell',0)) = 1$, we have $f^{(2)} \in F[\frac{t'-\ell'}{z}, z]$ given by

$$\begin{aligned} & f^{(2)}\big(\frac{t'-\ell'}{z}, z\big) \\ =& \sum_{k=1}^{3} \big(\sum_{i=k}^{3} a_{i,3-i} \binom{i}{k} \ell'^{i-k} \big) \big(\frac{t'-\ell'}{z} \big)^k z^{k-1} \\ & + \sum_{\gamma=0}^{4} \big(\sum_{\alpha=\gamma}^{4} a_{\alpha,4-\alpha} \binom{\alpha}{\gamma} \ell'^{\alpha-\gamma} \big) \big(\frac{t'-\ell'}{z} \big)^{\gamma} z^{\gamma} \end{aligned} \tag{2}_{\frac{t'-\ell'}{z}, z}$$

Evaluating at $\frac{t'-\ell'}{z} = m', z = 0$, we may define for all $m' \in F$

$(2)_{\frac{t'-\ell}{z}, z, P^{(2)}_{\infty m'}}$ $\qquad f^{(2)}(P^{(2)}_{\infty m'}) = a_{12}m' + a_{04}$

Under the same assumption, $f^{(2)} \in F[t'-\ell', \frac{z}{t'-\ell'}]$ is given by

$$\begin{aligned} & f^{(2)}(t'-\ell', \frac{z}{t'-\ell'}) \\ =& \sum_{k=1}^{3} \Big(\sum_{i=k}^{3} a_{i,3-i} \binom{i}{k} \ell'^{j-k} \Big) (t'-\ell')^{k-1} \\ & + \sum_{\gamma=0}^{4} \Big(\sum_{\alpha=\gamma}^{4} a_{\alpha,4-\alpha} \binom{\alpha}{\gamma} \ell'^{\alpha-\gamma} \Big) (t'-\ell')^{\gamma} (\frac{z}{t'-\ell'}) \end{aligned}$$

$(2)_{t'-\ell', \frac{z}{t'-\ell'}}$

Evaluating at $t' - \ell = 0, \frac{z}{t'-\ell'} = 0$, we may define

$(2)_{t'-\ell', \frac{z}{t'-\ell'}, P^{(2)}_{\infty\infty}}$ $\qquad f^{(2)}(P^{(2)}_{\infty,\infty}) = a_{12}$

To summarize, the values of the various $f^{(2)}$ are related but not identical. Under the assumptions $(*)_\ell$ and $(\#)_{\ell'}$, we specify, in $(2)_{t, \frac{z'-\ell}{t}, P^{(2)}_{\ell m}}$, $(2)_{\frac{t}{z'-\ell}, z'-\ell, P^{(2)}_{\ell\infty}}$, $(2)_{\frac{t'-\ell}{z}, z, P^{(2)}_{\infty m'}}$ and $(2)_{t'-\ell', \frac{z}{t'-\ell'}, P^{(2)}_{\infty\infty}}$, values of $f^{(2)}$ at all points of $\mathscr{X}^{(2)}$. In general, $\nu_{J^{(1)}}(f^{(1)} - f^{(1)}(P^{(1)}))$ varies as $P^{(1)}$ varies in $E^{(1)}$. Still, we may apply the same procedure to specify values of $f^{(2)}$. Then we assign to each f the codeword $(f^{(1)}(P^{(1)}_\ell), f^{(1)}(P^{(1)}_\infty), f^{(2)}(P^{(2)}_{\ell m}), f^{(2)}(P^{(\ell)}_{\ell\infty}), f^{(2)}(P^{(2)}_{\infty m}), f^{(2)}(P^{(2)}_{\infty\infty}))$, for all $\ell, m \in F$. It would be interesting to find combinatorial relations among the $\nu_{J^{(1)}}$ at various points and among the forms of the strict transforms. Apparently there are too many cases to consider, but we need to know the number of specified values of $f^{(1)}$ and $f^{(2)}$ required to determined f, in order to compute the minimal distance of the resulting code.

Different codes can be constructed using a larger space of polynomials and a correspondingly longer sequence of blowing-ups. Since the combinatorics is involved, we illustrate the techniques by an example of a modified code based on the form of strict transforms in the next section.

4. Linear "approximation" of nonlinear codes. Write the finite field with q elements as $F = \{\ell_1, \cdots, \ell_q\}$, where we assume $q \geq 5$. Let V be the vector space of polynomials given by $V = \{f \in F[t,z] : f = \sum_{i+j=3} a_{ij} t^i z^j + \sum_{\alpha+\beta=4} a_{\alpha\beta} t^\alpha z^\beta\}$.

Consider the code $V \xrightarrow{w} F^n$, $n = q + q^2$, defined by

$$f \mapsto w_f = (c_1, \cdots, c_q, c_{11}, \cdots, c_{1q}, \cdots, c_{q1}, \cdots, c_{qq}),$$

where

$$c_i = a_{30} + a_{21}\ell_i + a_{12}\ell_i^2 + a_{03}\ell_i^3 \tag{4.1}$$

and

$$c_{jk} = (a_{30} + a_{21}\ell_j + a_{12}\ell_j^2 + a_{03}\ell_j^3)\ell_k + (a_{40} + a_{31}\ell_j + a_{22}\ell_j^2 + a_{13}\ell_j^3 + a_{04}\ell_j^4) \tag{4.2}$$

If we write

$$d_j = a_{40} + a_{31}\ell_j + a_{22}\ell_j^2 + a_{13}\ell_j^3 + a_{04}\ell_j^4 \tag{4.3}$$

then

$$c_{jk} = c_j\ell_k + d_j \tag{4.4}$$

The components of the codewords are suggested by the forms of $(1)_{t,P_\ell^{(1)}}$ and $(2)_{t,\frac{z'-\ell}{t},P_{\ell m}^{(2)}}$ in section 3. We treat all ℓ_i equally, ignoring assumptions $(*)_\ell$, $(\#)_{\ell'}$. Also we modify $(2)_{t,\frac{z'-\ell}{t},P_{\ell m}^{(2)}}$ so that $a_{30}, a_{21}, a_{12}, a_{03}$ appear in the same way as in $(1)_{t,P_\ell^{(1)}}$.

We give a lower bound of the minimum distance of this code. For convenience, we put the components of the codeword w_f in q columns, as follows:

$$\begin{array}{cccc} c_{11} & \cdots & c_{q1} & \\ \vdots & & \vdots & \\ \vdots & & \vdots & \\ c_{1q} & \cdots & c_{qq} & q \geq 5 \\ c_1 & & c_q & \\ \uparrow & & \uparrow & \\ \text{column } 1 & & \text{column } q & \end{array} \tag{4.5}$$

LEMMA 4.4. *If 2 entries are known in each of some 5 columns in (4.5), then all the coefficients of f can be determined.*

Proof. Suppose 2 entries are known in column i. There are two cases:

Case 1: c_i and $c_{ij} = c_i\ell_j + d_i$ are known. Then we know c_i and $d_i = c_{ij} - c_i\ell_j$.
Case 2: $c_{ij} = c_i\ell_j + d_i, c_{ik} = c_i\ell_k + d_i (j \neq k)$ are known. Then we know c_i and d_i, since $\begin{vmatrix} \ell_j & 1 \\ \ell_k & 1 \end{vmatrix} \neq 0$.

Then, by the hypothesis of the lemma, we know $5c_i$'s and $5d_j$'s. Any 4 of the $5c_i$'s determine $a_{30}, a_{21}, a_{12}, a_{03}$ by (4.1) in view of the 4×4 Vandermonde determinant. Similarly, the $5d_j$'s determined $a_{40}, a_{31}, a_{22}, a_{13}, a_{04}$ by (4.3). □

LEMMA 4.5. *Any $5q + 1$ entries in (4.5) determine f.*

Proof. Consider any N entries in (4.5). Count the number of entries in each column. Arrange these numbers in order, say $n_1 \leq n_2 \leq \cdots \leq n_q$. The "closest" case for which the hypothesis of Lemma 4.1 fails is:

$$n_1 = 1, \cdots, n_{q-4} = 1, n_{q-3} = q + 1, \cdots, n_q = q + 1$$

In this case, $N = n_1 + \cdots + n_q = (q - 4) + 4(q + 1) = 5q$. One more entry will realize the hypothesis of Lemma 4.1. □

THEOREM 4.6. *The minimum distance d of the code w satisfies $d \geq q^2 - 4q$. The other parameters of the code are $n = q^2 + q$ and $k = 9$. Furthermore, $\frac{q^2-4q+9}{q^2+q} \leq \frac{k}{n} + \frac{d}{n} \leq \frac{q^2+q+1}{q^2+q}$.*

Proof. The code length n is clearly q^2+q. For any distinct $f, g \in V$, w_f and w_g agree in at most $5q$ components. Hence $d(w_f, w_g) \geq n - 5q = q^2 - 4q$. This proves the bound $d \geq q^2 - 4q$. Since $q \geq 5$ implies $q^2 - 4q > 0$, $d(w_f, w_g) > 0$ for all $f \neq g$ in V. Hence $V \xrightarrow{w} F^n$ is injective. Then $k = \dim_F V = 9$. It follows that $\frac{k}{n} + \frac{d}{n} \geq \frac{q^2-4q+9}{q^2+q}$. Since w is a linear code, $\frac{k}{n} + \frac{d}{n} \leq \frac{q^2+q+1}{q^2+q}$ by the Singleton bound. □

THEOREM 4.7. *For $q > 7$, the code w is self-orthogonal, that is, $w \subset w^{\perp}$*

Proof. We first write down a basis for the code w. Then it suffices to check self-orthogonality on the basis. Recall that the polynomials we use are $f = \sum_{i+j=3} a_{ij} t^i z^j + \sum_{\alpha+\beta=4} a_{\alpha\beta} t^\alpha z^\beta$. Let u_j $(0 \leq j \leq 3)$, v_β $(0 \leq \beta \leq 4)$ be the words corresponding to the monomials $t^{3-j} z^j$ and $t^{4-\beta} z^\beta$ respectively. These words form a basis of w. Written explicitly by (4.1) and (4.2),

$$u_j = (\ell_1^j, \cdots, \ell_q^j, \ell_1^j \ell_1, \cdots, \ell_1^j \ell_q, \cdots, \ell_q^j \ell_1, \cdots, \ell_q^j \ell_q) \tag{4.6}$$

$$v_\beta = (0, \cdots, 0, \ell_1^\beta, \cdots, \ell_q^\beta, \cdots, \ell_1^\beta, \cdots, \ell_q^\beta) \tag{4.7}$$

where $F = \{\ell_1, \cdots, \ell_q\}$. Then for $0 \leq i, j \leq 3$ and $0 \leq \alpha, \beta \leq 4$,

$$u_i \cdot u_j = \sum_{k=1}^{q} \ell_k^i \ell_k^j + \sum_{k,m=1}^{q} (\ell_k^i \ell_m)(\ell_k^j \ell_m) = (\sum_{k=1}^{q} \ell_k^{i+j})(1 + \sum_{m=1}^{q} \ell_m^2) \tag{4.8}$$

$$u_j \cdot v_\beta = \sum_{k,m=1}^{q} (\ell_k^j \ell_m)(\ell_k^\beta) = (\sum_{k=1}^{q} \ell_k^{j+\beta})(\sum_{m=1}^{q} \ell_m) \tag{4.9}$$

$$v_\alpha \cdot v_\beta = \sum_{k,m=1}^{q} \ell_k^\alpha \ell_k^\beta = q(\sum_{k=1}^{q} \ell_k^{\alpha+\beta}) \tag{4.10}$$

Recall the trick that for any nonzero y in F, $\sum_{x \in F} x^n = \sum_{x \in F} (xy)^n$, hence $(\sum_{x \in F} x^n)(1 - y^n) = 0$, which implies that $\sum_{x \in F} x^n = 0$ for any positive integer n not divisible by $q-1$, in particular for $n < q-1$. In (4.8), since $i + j \leq 6$, all $u_i \cdot v_j$ vanish for $q > 7$. Together with the vanishing of the inner products in (4.9) and (4.10), the theorem is proved. □

REMARK 4.8. It is interesting to compare the code w with algebraic geometry codes on curves. In order to get an algebraic geometry code with our length $n = q^2+q$, one needs this number of F_q rational points on a curve over F_q. By the Hasse-Weil bound, the number of rational points on a curve of genus g is at most $q + 1 + 2g\sqrt{q}$. Hence one needs a curve of genus $g \geq \frac{1}{2}(q^{\frac{3}{2}} - q^{-\frac{1}{2}})$. Then the lower bound of $k + d$ for the resulting algebraic geometry code is $n + 1 - g$. Hence the difference between n and the lower bound of $k + d$ is $g - 1 \geq \frac{1}{2}(q^{\frac{3}{2}} - q^{-\frac{1}{2}}) - 1$. By theorem 4.3, the lower bound of $k + d$ for our code is $q^2 - 4q + 9$. Hence the difference between n and the lower bound of $k + d$ for our code is $(q^2 + q) - (q^2 - 4q + 9) < 5q$, which is much less than $\frac{1}{2} q^{\frac{3}{2}}$. In this sense, our construction is better.

The code w is a linearised version of codes from infinitely near points. We can increase k and n of w by taking polynomials of higher degrees and more variables. These modified codes can be constructed simply and explicitly.

REFERENCES

[C] H. Chen, *Codes on Garcia-Stichtenoth curves with true distance greater than Feng-Rao distance*, IEEE Trans. Inform. Theory, 45 (1999), pp. 706–709.

[CYY] M. H. Chiu, S. S. T. Yau and Y. Yu, *$\mathbb{Z}_q$-cyclic codes and quadratic residue codes*, Adv. in Appl. Math., 25 (2000), pp. 12–33.

[E1] N. D. Elkies, *Excellent nonlinear codes from modular curves*, Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing, pp. 200–208, ACM, New York, 2001.

[E2] N. D. Elkies, *Still better nonlinear codes from modular curves*, arXiv: math NT/0308046 v1, 5 Aug 2003.

[G] V. D. Goppa, *Codes on algebraic curves*, Soviet Math. Dokl., 24 (1981), pp. 170–172.

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

[TV] M. A. Tsfasman and S. G. Vladut, *Algebraic-Geometric Codes*, Kluwer, Dordrecht, 1991.

[TVZ] 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 (1982), pp. 21–28.

[X] C. Xing, *Nonliear codes from algebraic curves improving the Tsfasman-Vladut-Zink bound*, IEEE Transactions on Information Theory, 49:7 (2003), pp. 1653–1657.

[XC] C. Xing and H. Chen, *Improvements on parameters of one-point AG codes from Hermitian curves*, IEEE Trans. Inform. Theory, 48 (2002), pp. 535–537.