Codes from Surfaces with Small Picard Number[*]

John Little[†] and Hal Schenck[‡]

Abstract. Extending work of M. Zarzar, we evaluate the potential of Goppa-type evaluation codes constructed from linear systems on projective algebraic surfaces with small Picard number. Putting this condition on the Picard number provides some control over the numbers of irreducible components of curves on the surface and hence over the minimum distance of the codes. We find that such surfaces do not automatically produce good codes; the sectional genus of the surface also has a major influence. Using that additional invariant, we derive bounds on the minimum distance under the assumption that the hyperplane section class generates the Néron–Severi group. We also give several examples of codes from such surfaces with minimum distance better than the best known bounds in Grassl's tables.

Key words. error control code, algebraic surface, Picard number, evaluation code

AMS subject classifications. 94B27, 14F17

DOI. 10.1137/17M1128277

1. Introduction. A convenient reference for all of the coding theory concepts we will need is [12]. We first recall a general setup for defining error-correcting codes from algebraic varieties X defined over $\mathbb{F}_q$. The *evaluation*, or *functional code*, produced from a subset $\mathcal{S} = \{P_1, \ldots, P_n\}$ of the $\mathbb{F}_q$-rational points on X and an $\mathbb{F}_q$-vector space of functions $\mathcal{F}$ defined on $\mathcal{S}$ is defined as follows. The set of codewords is the image of the mapping

$$(1.1) \qquad ev_{\mathcal{S}} : \mathcal{F} \longrightarrow \mathbb{F}_q^n,$$
$$f \mapsto (f(P_1), \ldots, f(P_n)).$$

When $\mathcal{F}$ is the vector space of sections of a line bundle $\mathcal{O}_X(D)$ for some divisor D on X defined over $\mathbb{F}_q$, we will call the resulting evaluation code $C(\mathcal{S}, D, \mathbb{F}_q)$. Several general statements about the parameters $[n, k, d]$ of $C(\mathcal{S}, D, \mathbb{F}_q)$ follow from these definitions:

- n is $|\mathcal{S}|$.
- k is equal to the dimension of the space of functions obtained by restricting the elements of $\mathcal{F}$ to $\mathcal{S}$. (This equals $\dim \mathcal{F}$ unless there are nonzero elements of $\mathcal{F}$ vanishing on all of $\mathcal{S}$.)
- d is determined by the maximal number of zeroes of a section of $\mathcal{O}_X(D)$ at the points in $\mathcal{S}$.

[†]Department of Mathematics and Computer Science, College of the Holy Cross, Worcester, MA 01610 (jlittle@holycross.edu).

[‡]Department of Mathematics, Iowa State University, Ames, IA 50011 (hschenck@iastate.edu).

Hence the properties of these codes are closely tied to the algebraic geometry of the variety X and the divisor D. The well-known Goppa codes from algebraic curves are first examples. The survey [14] includes a discussion of previous work on codes obtained from various types of varieties by similar methods.

In [15], in the case when X is a toric surface, under the hypothesis that q is sufficiently large, we obtained upper and lower bounds on the minimum distance of toric surface codes by relating codewords of small weight to reducible sections of the line bundle $\mathcal{O}_X(D)$ and Minkowski summands of the polygon P_D defined by D. Our results were later extended and improved by Soprunov and Soprunova in [20].

In [27], Zarzar suggested that surfaces X in $\mathbb{P}^3$ with small Picard number over $\mathbb{F}_q$ might lead to good evaluation codes and provided a number of examples in support of this idea. Zarzar's approach in [27] is related to, but is in some sense orthogonal to, that of [15] and [20]; the idea is to impose conditions so that not too much factorization of sections can occur. The methods employed in [27] are specific to the case of surfaces in $\mathbb{P}^3$, and Voloch–Zarzar give an extension to surfaces in $\mathbb{P}^n$ in [26]. Couvreur used these ideas to produce some very good codes in [7].

Our goals in this paper are to refine and extend the results of [27] and [26], to report the results of some experimentation with this approach, and to indicate both situations where this approach succeeds in producing good codes and situations where it does not.

We will begin with some general observations about this class of codes in section 2. The definition of the Néron–Severi group and its role in bounding the minimum distance will be reviewed in section 3. In section 4, we focus on anticanonical rational surfaces: specifically, surfaces obtained by blowing up a small number of points in $\mathbb{P}^2$. Classical work of Swinnerton-Dyer [21] plays a key role here. We close with an example (in effect, a variation of a construction studied in [7]) in which our bounds are better than previous bounds from [4] and [8]. We obtain some codes better than the best known examples in Grassl's tables [10].

2. General coding-theoretic observations. All of the examples we consider will come from projective surfaces $X \subset \mathbb{P}^r$, $r \geq 3$, given by explicit sets of homogeneous polynomial equations. In this situation, when $D = sH$ is a positive integer multiple of a hyperplane section of the surface, it is possible to work with a more concrete version of the evaluation codes introduced above. Namely, we can take $\mathcal{S} = X(\mathbb{F}_q)$, the whole set of $\mathbb{F}_q$-rational points of X. We then choose a homogeneous coordinate vector for each point normalized so that the rightmost nonzero entry is 1; that is, there exists some ℓ, $0 \leq \ell \leq r$, such that

$$P = (x_0 : \cdots : x_\ell = 1 : 0 : \cdots : 0).$$

We write $\mathbb{F}_q[x_0, \ldots, x_r]_s$ for the vector space of homogeneous polynomials of degree s. Each $f \in \mathbb{F}_q[x_0, \ldots, x_r]_s$ has a well-defined value in $\mathbb{F}_q$ at the P as above.

Definition 2.1. *The evaluation code from $\mathcal{S} = X(\mathbb{F}_q)$ in this form and $\mathcal{F} = \mathbb{F}_q[x_0, \ldots, x_r]_s$ will be denoted $C(X, s, \mathbb{F}_q)$.*

Remark 2.2. The code defined this way will coincide with the algebraic geometry code constructed from $H^0(X, \mathcal{O}(s))$ when X is projectively normal; if that condition is not satisfied, the $C(X, s, \mathbb{F}_q)$ code may only give a subcode of the algebraic geometry code.

As in section 1.7 of [12], we will say that a linear code C with generator matrix G is *monomially equivalent* to a second code C' if there exists an $n \times n$ monomial matrix M such that $G' = GM$ is a generator matrix for C'. A monomial matrix has the form $M = DP$, where D is an invertible $n \times n$ diagonal matrix and P is a permutation matrix. Monomial equivalence is a natural equivalence relation to use to classify our codes because it preserves all the quantities of interest—n, k, d, and the number of codewords of each weight (the weight enumerator).

If X is projectively normal (see Remark 2.2 above), and $f \in k[x_0, \ldots, x_r]_s$ with $s \geq 1$ is fixed, then the global sections of $\mathcal{O}_X(sH)$ can be identified with the rational functions g/f for $g \in k[x_0, \ldots, x_r]_s$. If there exists such an f that vanishes at none of the points in $X(\mathbb{F}_q)$, then it is easy to see that the code $C(X(\mathbb{F}_q), sH, \mathbb{F}_q)$ described in the introduction is monomially equivalent to this one.

We will need a way to say, roughly speaking, that the $\mathbb{F}_q$-rational points on a variety over $\mathbb{F}_q$ determine the equations of X in all sufficiently low degrees. For instance, if X is a hypersurface of degree m, we will mean that there are no forms of degree $< m$ vanishing on $X(\mathbb{F}_q)$ and that in degree m the only forms vanishing on $X(\mathbb{F}_q)$ also vanish on X. We will require similar conditions in higher codimensions.

Definition 2.3. *A projective variety X over $\mathbb{F}_q$ is $\mathbb{F}_q$-general if the homogeneous ideal of X is generated in degrees $\leq m$ for some $m \geq 1$ and if, for all ℓ with $1 \leq \ell \leq m$, every homogeneous form of degree ℓ that vanishes on $X(\mathbb{F}_q)$ also vanishes on X.*

Example 2.4. An example of a variety that does not satisfy this definition is a conic X in $\mathbb{P}^2$ over $\mathbb{F}_q$ whose defining equation of degree $m = 2$ factors into two Frobenius-conjugate linear forms with coefficients in $\mathbb{F}_{q^2}$. Then $X(\mathbb{F}_q)$ consists of just the point of intersection of the two conjugate $\mathbb{F}_{q^2}$-lines, and the condition in Definition 2.3 fails for $\ell = 1$ and $\ell = 2$.

Varieties that are not $\mathbb{F}_q$-general are essentially of no use in our construction, so we will assume from now on that this $\mathbb{F}_q$-generality condition holds.

The code $C(X, 1, \mathbb{F}_q)$ plays a special role. Note that if $X \subset \mathbb{P}^r$, then $k = r + 1$, and using the standard basis $\{x_0, x_1, \ldots, x_r\}$ for $\mathbb{F}_q[x_0, \ldots, x_r]_1$, the columns of the standard generator matrix will consist of the normalized homogeneous coordinate vectors of points $P \in X(\mathbb{F}_q)$. This observation has some immediate consequences.

Proposition 2.5. *Let X and X' be varieties, both defined over $\mathbb{F}_q$.*
   (i) *If X and X' are projectively equivalent over $\mathbb{F}_q$, then the code $C(X, 1, \mathbb{F}_q)$ is monomially equivalent to $C(X', 1, \mathbb{F}_q)$.*
  (ii) *Assume also that both X and X' are $\mathbb{F}_q$-general. Then the converse also holds: if $C(X, 1, \mathbb{F}_q)$ is monomially equivalent to $C(X', 1, \mathbb{F}_q)$, then X and X' are projectively equivalent over $\mathbb{F}_q$.*

Proof. (i) If X and X' are projectively equivalent over $\mathbb{F}_q$, there is an invertible $(r + 1) \times (r + 1)$ matrix A over $\mathbb{F}_q$ defining a projective linear transformation $\phi_A(P) = AP$ on $\mathbb{P}^r$ such that $\phi_A(X) = X'$. By our hypotheses, ϕ_A also maps $X(\mathbb{F}_q)$ bijectively to $X'(\mathbb{F}_q)$. It follows that, after adjusting with an invertible diagonal matrix D to normalize the columns (the homogeneous coordinate vectors of the points in $X'(\mathbb{F}_q)$) to the form described above, the matrix $G' = (AG)D$ will be the standard generator matrix for $C(X', 1, \mathbb{F}_q)$. But AG is also

a generator matrix for $C(X, 1, \mathbb{F}_q)$ since A is invertible. Hence the two codes are monomially equivalent.

(ii) Conversely, suppose $C(X, 1, \mathbb{F}_q)$ and $C(X', 1, \mathbb{F}_q)$ are monomially equivalent. If we take the standard generator matrix G of the first code, this means that there exists an invertible diagonal matrix D and a permutation matrix P such that $G(DP)$ is a generator matrix for $C(X', 1, \mathbb{F}_q)$. The rows of this matrix correspond to some basis for the vector space of linear forms with coefficients in $\mathbb{F}_q$. So there is an invertible $(r+1) \times (r+1)$ matrix A over $\mathbb{F}_q$ such that $A(G(DP)) = (AG)(DP)$ is a generator matrix for $C(X', 1, \mathbb{F}_q)$ whose rows correspond to the basis $\{x_0, x_1, \ldots, x_r\}$. Multiplying by another invertible diagonal matrix D' on the right to normalize the columns if necessary, we will obtain the standard generator matrix of $C(X', 1, \mathbb{F}_q)$ in the form $(AG)(DPD')$. By an easy computation with matrices of these forms, the product DPD' can be rewritten in the form $D''P$ for another invertible diagonal matrix D''. So we have $G' = (AG)(D''P) = (AGD'')P$, and G' and AGD'' differ only by a permutation of the columns. So the columns of AGD'' are just the normalized forms of the images of the points in $X(\mathbb{F}_q)$ under ϕ_A. This shows $\phi_A(X(\mathbb{F}_q)) = X'(\mathbb{F}_q)$, and we claim that $\phi_A(X) = X'$ because of the assumption of $\mathbb{F}_q$-generality. This follows since if f is any homogeneous polynomial in the vanishing ideal of X, then $f \circ \phi_A^{-1}$ vanishes on $X'(\mathbb{F}_q)$ and hence on all of X'. Therefore X and X' are projectively equivalent over $\mathbb{F}_q$. ∎

3. Bounds in terms of the Picard number. From now on, we will consider only codes constructed from smooth, projective, absolutely irreducible surfaces X defined over $\mathbb{F}_q$. In addition, we will fix a particular embedding $X \hookrightarrow \mathbb{P}^r$ and work with particular polynomial equations for X. We will not repeat all of those hypotheses each time we refer to a surface X. The *Néron–Severi group* of X over $\mathbb{F}_q$, denoted by $\mathrm{NS}(X) = \mathrm{NS}_{\mathbb{F}_q}(X)$, is the group of $\mathbb{F}_q$-rational divisors on X modulo algebraic equivalence. This is a finitely generated abelian group with a free part isomorphic to $\mathbb{Z}^\rho$ for some $\rho \geq 1$. The rank $\rho = \rho(X)$ is known as the *Picard number* of X. We note that this is sometimes called the *arithmetic Picard number* to distinguish it from the *geometric Picard number* of the corresponding variety X over the algebraic closure of $\mathbb{F}_q$. In this article, the phrase "Picard number" with no modifier will always refer to the arithmetic Picard number. The relevance of the Picard number for coding theory is based on the following facts from [26] and [27].

Proposition 3.1 (see [26, Lemma 2.2]). *If* $\mathrm{NS}(X)$ *is generated by the class of an ample divisor* H *and* $[D] = [mH]$, *then the divisor of zeros of a nonzero element of* $L(D)$ *has at most* m *distinct* $\mathbb{F}_q$-*irreducible components.*

Proof. For the convenience of the reader, we reproduce the proof in [26]. Suppose $f \in L(D)$ is a nonzero rational function, and consider the decomposition

$$(f)_0 = a_1 D_1 + \cdots + a_\ell D_\ell,$$

where D_i are $\mathbb{F}_q$-irreducible and a_i are integers ≥ 1. Then since D_i is algebraically equivalent to $b_i H$ for some integer $b_i \geq 1$ over $\mathbb{F}_q$,

$$\ell H^2 \leq \sum_i a_i b_i H^2 = (f)_0 H = (f)_\infty H \leq m H^2.$$

This implies $\ell \leq m$. ∎

For surfaces in $\mathbb{P}^3$, [27] provides a somewhat sharper statement.

Proposition 3.2 (see [27, Lemma 2.1]). *Let X be a surface of degree a in $\mathbb{P}^3$, where a is not divisible by the characteristic of $\mathbb{F}_q$. If $\mathrm{NS}(X)$ is generated by the class of an effective divisor D (so the Picard number of X is 1) and Y is an absolutely irreducible surface of degree $1 \leq m < a$, then $X \cap Y$ is absolutely irreducible.*

In this case, $\mathrm{NS}(X)$ is generated by the class of a plane section, and the statement follows. Applying Proposition 3.1 and the Hasse–Weil–Serre bound, we have the following bound on $n - d_1$, where $d_1 = d(C(X, 1, \mathbb{F}_q))$.

Theorem 3.3. *Let H be an absolutely irreducible $\mathbb{F}_q$-hyperplane section of a surface X. Assume the class of H generates $\mathrm{NS}(X)$ over $\mathbb{F}_q$. Then*

$$(3.1) \qquad\qquad n - d_1 \leq 1 + q + \pi \lfloor 2\sqrt{q} \rfloor,$$

where π is the sectional genus of X (the arithmetic genus of the curves in the hyperplane section class).

Proof. If f is any linear form defined over $\mathbb{F}_q$, then the divisor $D = X \cap V(f)$ is linearly equivalent, hence algebraically equivalent, to H on X. Taking $m = 1$ in Proposition 3.1, D must also be irreducible over $\mathbb{F}_q$. Any codeword produced by evaluation of a linear form f where D is also absolutely irreducible will have at most $1 + q + \pi \lfloor 2\sqrt{q} \rfloor$ zero entries by the form of the Hasse–Weil–Serre bound for singular curves as in [2].

It remains to consider the case that D is irreducible over $\mathbb{F}_q$ but not absolutely irreducible. In this case, by Theorem 3.2 of [13] there is some $r \geq 2$ such that $D = D_1 \cup \cdots \cup D_r$ with all D_i absolutely irreducible and defined over $\mathbb{F}_{q^r}$. These absolutely irreducible components are permuted by the action of the cyclic group $\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$. By Lemma 2.8 and Proposition 3.8 of [13],

$$D(\mathbb{F}_q) = \mathrm{Sing}(D)(\mathbb{F}_q) = (D_1 \cap \cdots \cap D_r)(\mathbb{F}_q).$$

Hence for any pair $i \neq j$,

$$|D(\mathbb{F}_q)| \leq D_i \cdot D_j,$$

using the intersection form on X.

By the *adjunction formula* on X (see, for instance, [11, Proposition V.1.5]), we have

$$(3.2) \qquad\qquad 2\pi - 2 = (K_X + H) \cdot H,$$

where K_X is the canonical divisor class on X. On the other hand, the reducible divisor D has the same arithmetic genus as the irreducible curve H since D is linearly equivalent to H. Since $D = D_1 + \cdots + D_r$ as divisors on X, the bilinearity of the intersection form gives

$$(3.3) \qquad
\begin{aligned}
2\pi - 2 &= (K_X + D) \cdot D \\
&= \sum_{i=1}^{r} (K_X + D_i) \cdot D_i + 2 \sum_{i<j} D_i \cdot D_j \\
&= \sum_{i=1}^{r} (2p_a(D_i) - 2) + 2 \sum_{i<j} D_i \cdot D_j.
\end{aligned}$$

The D_i are irreducible over the algebraic closure of $\mathbb{F}_q$, so their arithmetic genus satisfies $p_a(D_i) \geq 0$. Hence for all i,

$$2p_a(D_i) - 2 = (K_X + D_i) \cdot D_i \geq -2.$$

Hence rearranging the last equality from (3.3), we see for all pairs $i \neq j$,

$$(3.4) \qquad D_i \cdot D_j \leq \frac{1}{r(r-1)}(2\pi - 2 + 2r) = \frac{1}{r(r-1)}(2\pi - 2) + \frac{2}{r-1}.$$

Comparing the Hasse–Weil–Serre upper bound and the bound from (3.4), since $r \geq 2$ and $\frac{2}{r-1} \leq 2$,

$$\frac{1}{r(r-1)}(2\pi - 2) < \pi \lfloor 2\sqrt{q} \rfloor$$

and

$$\frac{2}{r-1} < 1 + q$$

for all q. This shows that any curves in the class of H that are irreducible over $\mathbb{F}_q$, but not absolutely irreducible, have fewer $\mathbb{F}_q$-rational points than the Hasse–Weil–Serre upper bound for absolutely irreducible curves. ∎

Example 3.4. An example related to the proof of Theorem 3.3 comes from the elliptic quadric surfaces X in $\mathbb{P}^3$. The Picard number is $\rho(X) = 1$ in this case, and the Néron–Severi group is generated by the class of a smooth plane section (a plane conic). There are also tangent planes intersecting X in pairs of lines, but these lines are only defined over the quadratic extension of $\mathbb{F}_q$. Hence we have reducible divisors $D = D_1 + D_2$ in this class, with D_i lines over the algebraic closure of $\mathbb{F}_q$. The only $\mathbb{F}_q$-rational point on such a section is the point of tangency (where the two lines meet). The upper bound in (3.4) is achieved in this case. This is the situation described in Example 2.4.

We also consider the codes $C(X, s, \mathbb{F}_q)$ for $s > 1$ and set $d_s = d(C(X, s, \mathbb{F}_q))$. Our main observation here is that, at least when q is sufficiently large, the minimum distance of $C(X, s, \mathbb{F}_q)$ is, to some extent, controlled by the minimum distance of $C(X, 1, \mathbb{F}_q)$. The simplest statement here concerns $n - d_s$, the largest number of zeros in any nonzero codeword.

Theorem 3.5. *Under the hypotheses of Theorem 3.3, if q is sufficiently large, then*

$$n - d_s \leq s(n - d_1).$$

Proof. Consider the divisor $D = X \cap V(f)$ for f of degree s. We begin with the case when $D = X \cap V(f)$ has a decomposition $D = D_1 \cup \cdots \cup D_r$ into absolutely irreducible components defined over $\mathbb{F}_q$. By Corollary 3 of [3],

$$|D(\mathbb{F}_q) - (rq + 1)| \leq 2\pi_D \sqrt{q},$$

where π_D is the arithmetic genus (which depends only on s). We note that the curve D is absolutely connected because D is an ample divisor on X (see Corollary III.7.9 of [11]). Among the forms of degree s are those that factor over $\mathbb{F}_q$ into products of linear forms. By

arguments similar to those we used in [15], it is not difficult to see that when q is sufficiently large, the lower bound

$$sq + 1 - 2\pi_D\sqrt{q}$$

on $|D(\mathbb{F}_q)|$ for sections with s components is greater than the upper bound

$$rq + 1 + 2\pi_D\sqrt{q}$$

for sections with r components for all $r < s$. The maximum possible number of points on a reducible D with a decomposition of this form is attained for some D with $r = s$, and hence each D_i is a hyperplane section. Hence D has at most $s(n - d_1)$ $\mathbb{F}_q$-rational points, and the corresponding codewords have at most $s(n - d_1)$ zero entries.

It remains to consider the case where $D = X \cap V(f)$ has some $\mathbb{F}_q$-irreducible component that is not absolutely irreducible. But then the argument given in the proof of Theorem 3.3 shows that the largest possible number of $\mathbb{F}_q$-points on any such component can only decrease relative to the case where that $\mathbb{F}_q$-irreducible component is absolutely irreducible.

Hence when q is large enough, we will have $n - d_s \leq s(n - d_1)$. ∎

We will not address the problem of determining precise bounds on the q for which the conclusion of Theorem 3.5 holds in this article because this tends to depend on particular properties of the surface X and the divisor D. To conclude this section, we record an observation that may be of independent interest. It is possible to use these properties of evaluation codes to deduce properties of the surfaces they come from.

Corollary 3.6. *Let X be a smooth projective surface defined over $\mathbb{F}_q$ and assume that the bound given in (3.1) does not hold. Then the class of the hyperplane section H does not generate $\mathrm{NS}(X)$.*

Proof. If (3.1) does not hold, then some hyperplane section of X must be reducible, and the irreducible components give elements of $\mathrm{NS}(X)$ that are not in the subgroup generated by the class of H. ∎

In the situation of the corollary, if the components come from different algebraic equivalence classes, then in particular $\rho(X) > 1$.

4. Picard number 1 (or small) is not enough. A first obstacle to making use of these ideas is simply the problem of finding explicit surfaces with small Picard number.

4.1. Codes from smooth cubic surfaces in $\mathbb{P}^3$. The article [27] uses smooth cubic surfaces in $\mathbb{P}^3$ as a test case. In this subsection, we provide more details about these codes and show that an example from [27] is actually the best possible for codes from these surfaces in the situation considered there.

Over the algebraic closure of $\mathbb{F}_q$, a smooth cubic surface is obtained as the blow-up of $\mathbb{P}^2$ in six points in general position and always has 27 lines as in the classical situation over $\mathbb{C}$. Moreover, the orthogonal complement of the canonical class in the Picard group can be identified with the E_6 lattice, and the Weyl group of E_6 acts on the lines. However, the lines may only be defined over an extension of $\mathbb{F}_q$, and some cubics contain no $\mathbb{F}_q$-rational lines. The article [21] gives a classification of the possibilities according to the action of the Frobenius automorphism on the set of lines. That classification is based on the conjugacy class of the

Weyl group containing the Frobenius automorphism. According to Table 1 of [21], there are exactly five possible types of cubics with $\rho(X) = 1$; such an X contains no $\mathbb{F}_q$-rational lines or conics. The types are denoted as follows:

(4.1)

Class	Permutation type	$N_1 = |X(\mathbb{F}_q)|$	ord(η_j)
C_{10}	$\{3, 6^3, 6\}$	$q^2 - q + 1$	$2, 2, 3, 3, 6, 6$
C_{11}	$\{3^9\}$	$q^2 - 2q + 1$	$3, 3, 3, 3, 3, 3$
C_{12}	$\{3, 6^4\}$	$q^2 + 2q + 1$	$3, 3, 6, 6, 6, 6$
C_{13}	$\{3, 12^3\}$	$q^2 + 1$	$3, 3, 12, 12, 12, 12$
C_{14}	$\{9^3\}$	$q^2 + q + 1$	$9, 9, 9, 9, 9, 9$

The second column indicates how the 27 lines on the surface over the algebraic closure are permuted by the Frobenius automorphism of X. To give some idea of the intricacies here, we note that on C_{10} and C_{12} cubics, there is one orbit of length 3 consisting of three coplanar lines defined over $\mathbb{F}_{q^3}$; hence the plane containing them is defined over $\mathbb{F}_q$. The other 24 lines on a C_{10} or C_{12} are permuted in four orbits of size 6. But those orbits of length 6 have different structures. According to a discussion on page 59 of [21], on a C_{10} cubic, three of the orbits consist of three skew lines and their three transversals, but none of the orbits on a C_{12} has that form. On the other hand, one of the orbits on a C_{12} consists of two triangles in planes interchanged by the square of the Frobenius. (Those triangles split over $\mathbb{F}_{q^6}$.)

In the last column, the η_j give a description of the six nontrivial reciprocal roots of the factor in the denominator of the zeta function of X corresponding to the H^2 cohomology group: $\alpha_j = \eta_j q$, where η_j is a primitive ord(η_j)th root of unity. From the specific shape of the zeta function for smooth cubics in $\mathbb{P}^3$ (in particular, the fact that both factors corresponding to the H^1 and H^3 cohomology are trivial), knowing only the η_j allows us to compute $N_r = |X(\mathbb{F}_{q^r})|$ for all $r \geq 1$.

A recent paper by Rybakov and Trepalin [18] studies when cubic surfaces of these types exist over particular finite fields.

Experimental Results 4.1. *With a random search, we found cubic surfaces of each of these types over $\mathbb{F}_7$ and constructed the codes $C(X, k, \mathbb{F}_7)$ for $k = 1, 2$. The following list gives parameters for the corresponding codes for $k = 1$. The best possible d values are taken from* [10].

- C_{10}: *found* $[43, 4, 30]$, $[43, 4, 31]$ *(best possible d for $n = 43, k = 4$ is $d = 35$).*
- C_{11}: *found* $[36, 4, 23]$, $[36, 4, 24]$ *examples (best possible d is $28 \leq d \leq 29$).*
- C_{12}: *found* $[64, 4, 51]$ *(best possible d is $52 \leq d \leq 53$).*
- C_{13} *(very rare): found* $[50, 4, 37]$ *(best possible $d = 42$).*
- C_{14} *(rare): found* $[57, 4, 44]$ *(best possible $d = 47$).*

The frequent occurrence of the number $n - d = 13$ here can be explained as follows. Recall the Hasse–Weil–Serre bound: if X is a smooth curve of genus g over $\mathbb{F}_q$, then

$$|X(\mathbb{F}_q) - (1 + q)| \leq g \cdot \lfloor 2\sqrt{q} \rfloor.$$

Hence an upper bound on the number of $\mathbb{F}_7$-points on a smooth plane cubic is $1 + 7 + \lfloor 2\sqrt{7} \rfloor = 13$, and this bound is achieved, for instance, for the Weierstrass form cubic $y^2 z = x^3 + 3z^3$. Moreover, singular (but irreducible) plane sections all have either $q = 7$ ("split" node), $q + 1 =$

8 (cusp), or $q + 2 = 9$ ("nonsplit" node) $\mathbb{F}_7$-points. Note, however, that some of the C_{10} and C_{11} surfaces have no plane sections with 13 $\mathbb{F}_7$-points. Also observe that delving deeper into the structure of these codes, for instance by using Magma to compute the weight enumerators for a large collection of codes from cubics, reveals the striking feature of how variable they are. Even among codes with the same d, there will be many different nonequivalent codes. This is a reflection of Proposition 2.5, of course. The $C(X, 1, \mathbb{F}_q)$ codes effectively encode all the structure of X up to projective equivalence.

As Zarzar observed, among the cubics with Picard number 1, the C_{12} cubics are clearly the best for construction of codes. This also provides some confirmation of Zarzar's *ansatz* concerning the Picard number. Cubics with $\rho(X) > 1$ contain lines rational over $\mathbb{F}_q$ and hence have reducible plane sections with two or more irreducible rational components. The $C(X, 1, \mathbb{F}_q)$ codes will have $n - d > 13$, although n can also be as large as $q^2 + 7q + 1$.

Evaluating quadrics, Zarzar also reported a code $C(X, 2, \mathbb{F}_7)$ from a C_{12} cubic surface with parameters $[64, 10, 38]$. Here, following the pattern from Theorem 3.5, the minimum weight codewords come from reducible quadrics intersecting the cubic X in reducible curves with two components, both of which are smooth plane cubics with 13 $\mathbb{F}_7$-rational points. Moreover, the line of intersection of the two planes meets the cubic in three points rational over $\mathbb{F}_{q^3}$, so the resulting codewords have exactly $13 + 13 = 26$ zeros. By contrast, smooth intersections of a cubic and a quadric in $\mathbb{P}^3$ are curves of genus 4 with at most 24 $\mathbb{F}_7$-rational points, according to [24]. The Hasse–Weil–Serre upper bound $1 + 7 + 4 \cdot \lfloor 2\sqrt{7} \rfloor = 28$ is not achieved in this case.

A natural question to ask here is how well the codes from C_{12} cubics might do over other, larger fields. Based on a large amount of experimental data, we offer the following conjecture that bears on this question. We say an irreducible plane cubic curve is *optimal* over $\mathbb{F}_q$ if it contains the largest possible number of $\mathbb{F}_q$-rational points over all plane cubics. As above with $g = 4$, the Hasse–Weil–Serre bound is not always achieved when $g = 1$. But compared to the higher genus case, much more is known about when the bound is not reached. In particular, when $g = 1$ and the bound is not reached, there exist curves with $q + \lfloor 2\sqrt{q} \rfloor$ $\mathbb{F}_q$-rational points, that is, just one less than the bound. See [16].

Conjecture 4.2. *For all $q \geq 7$, C_{12} cubic surfaces over $\mathbb{F}_q$ always contain optimal cubic plane sections.*

It is possible to normalize the equations of C_{12} cubics using the description of the lines on these surfaces given in the paragraph after table (4.1) above. Up to projective equivalence in $\mathbb{P}^3$, we can put the triangle orbit in the plane $w = 0$, so the plane section $X \cap V(w)$ is defined by an equation of the form $L \cdot F(L) \cdot F^2(L)$, where L is a linear form in x, y, z with coefficients in $\mathbb{F}_{q^3}$. Letting M be a second linear form in x, y, z, w with coefficients in $\mathbb{F}_{q^2}$, any C_{12} cubic is projectively equivalent to one given by an equation of the form

$$(4.2) \qquad\qquad L \cdot F(L) \cdot F^2(L) = w \cdot M \cdot F(M).$$

This is a special case of the *Cayley–Salmon form* of the equation of a cubic surface studied in classical algebraic geometry; see [9]. The Frobenius orbit of the line defined by $L = M = 0$

consists of the six lines defined by

$$L = M = 0, \quad F(L) = F(M) = 0,$$
$$F^2(L) = M = 0, \quad L = F(M) = 0,$$
$$F(L) = M = 0, \quad F^2(L) = F(M) = 0.$$

The first, third, and fifth of these lie in the plane $M = 0$, and the second, fourth, and sixth lie in $F(M) = 0$, and those two triangles are interchanged by F.

Experimental Results 4.3. *By considering equations of the form* (4.2), *it is feasible, when* q *is small, to generate surfaces in every projective equivalence class over* $\mathbb{F}_q$ *by varying the coefficients in the linear forms L and M, then test all of them for existence of optimal hyperplane sections. Using this approach, we have verified the conjecture for $q \leq 9$. We have also done extensive random searches for all $q \leq 37$ that have produced no counterexamples. We hope to return to this conjecture in future work.*

Over $\mathbb{F}_7$, our results also show that there are sufficiently many optimal plane sections such that there always exist two in distinct planes whose line of intersection meets the cubic in no points rational over $\mathbb{F}_7$. Hence the $C(X, 2, \mathbb{F}_7)$ codes from C_{12} cubics always have the parameters $[64, 10, 38]$ found by Zarzar.

Since the best known code from [10] with $n = 64, k = 10$ over $\mathbb{F}_7$ has $d = 41$, we have another strong heuristic indication that *in addition to limiting the Picard number, the genus of the components of maximally reducible curves on X in the linear system giving the evaluation functions must also be controlled if the construction of this paper is to produce really good codes.* Similarly, if the conjecture above holds in general, we expect that (using the notation from Theorem 3.5) the $C(X, 2, \mathbb{F}_q)$ codes will always have $n - d_2 = 2(n - d_1)$, i.e., twice the optimal number of $\mathbb{F}_q$-rational points on a curve of genus 1.

4.2. Higher degree surfaces in $\mathbb{P}^3$. We briefly indicate some of the features of the construction of this paper that can prevent it from producing good codes from higher-degree surfaces. The main issue is that even if we can control the presence of reducible plane sections, if X is a smooth surface of degree m and H is a plane, then provided that $X \cap H$ is a smooth curve, it has genus $g = \frac{(m-1)(m-2)}{2}$. For q fixed, the Hasse–Weil–Serre upper bound on $|(X \cap H)(\mathbb{F}_q)|$ used to derive (3.1) grows like a constant times m^2, and the minimum distance of the resulting codes often seems to decrease too rapidly with m to produce codes better than the best known examples.

Experimental Results 4.4. *For any $m \geq 5$, consider the surface in $\mathbb{P}^3$ given by*

$$X_m = V(w^m + xy^{m-1} + yz^{m-1} + zx^{m-1}).$$

Our motivation for looking at surfaces of this form was that in [19] *Shioda proved that these have Picard number 1 over $\mathbb{C}$. On the other hand, for $m = 4$, this equation defines a K3 surface with geometric Picard number 20. Since these surfaces are defined over $\mathbb{Z}$, we can also consider their reductions* mod p *for any prime p and use them to construct codes, although the Picard numbers of the reduced surfaces may be larger than 1.*

Even in the case $m = 4$, there are q for which the surface X_4 contains no lines or conics defined over $\mathbb{F}_q$ and hence has no reducible plane sections. For instance, with $q = 11$ and $k = 1$, we obtain a code $C(X_4, 1, \mathbb{F}_{11})$ with parameters $[144, 4, 120]$. The minimum weight codewords come from smooth plane quartic curves ($g = 3$) with 24 points rational over $\mathbb{F}_{11}$. These are optimal for $g = 3$ according to [24]. The optimal number of $\mathbb{F}_{11}$-rational points on a curve with $g = 1$ is 18. Hence codes from a C_{12} cubic surface over $\mathbb{F}_{11}$ containing optimal cubic plane sections has the same $n = 144$ and $k = 4$, but $d = 144 - 18 = 126$.

The cases $m \geq 5$ are similar. For instance, the surface X_5 over $\mathbb{F}_9$ contains no $\mathbb{F}_9$-rational lines or conics. The $C(X_5, 1, \mathbb{F}_9)$ code has parameters $[91, 4, 71]$, and the nonzero words of minimum weight come from irreducible plane quintic curve sections. Although curves of genus $g = 6$ with as many as 32 $\mathbb{F}_9$-rational points are known according to [24], none of those are contained in this surface. But the best known and best possible d in this case is $d = 79$ according to [10].

Experimental Results 4.5. *In [25], van Luijk provides examples for the case not covered in Shioda's results, giving an explicit family of quartic $K3$ surfaces in $\mathbb{P}^3$ over $\mathbb{Q}$ with geometric Picard number 1. (Although such surfaces have long been known to exist, the fact that this example was only published in 2007 is a reflection of the difficulty of finding explicit examples.) Let*

$$
\begin{aligned}
f_1 &= x^3 - x^2y - x^2z + x^2w - xy^2 - xyz + 2xyw + xz^2 + 2xzw + y^3 + y^2z, \\
&\quad -y^2w + yz^2 + yzw - yw^2 + z^2w + zw^2 + 2w^3, \\
f_2 &= xy^2 + xyz - xz^2 - yz^2 + z^3, \\
g_1 &= z^2 + xy + yz, \\
g_2 &= z^2 + xy.
\end{aligned}
$$

Then for any homogeneous quartic h, the surface

$$
wf_1 + 2zf_2 - 3g_1g_2 + 6h = 0
$$

is a smooth $K3$ surface with Picard number 1 over $\mathbb{Q}$. Once again, if h has coefficients in $\mathbb{Z}$, we can look at reductions of such surfaces mod p and use them to construct codes.

We generated 50 such surfaces X randomly over $\mathbb{F}_7$. Of these, 38 were smooth, and those surfaces had a wide range of values of $|X(\mathbb{F}_7)|$—as small as 38 and as large as 69. The corresponding $C(X, 1, \mathbb{F}_7)$ codes for the surface with the maximal number of points had parameters $[69, 4, 52]$. We mention the following easy observation. Smooth plane curves of degree $m = 4$ have genus 3, and the largest possible number of $\mathbb{F}_7$-rational points is 20 by [24]. The same is true for any irreducible plane quartic. It follows that if any such surface yields a code with $n - d \geq 21$, then some plane section must be reducible. The irreducible components of such plane sections cannot give classes that are integer multiples of the hyperplane class in $\mathrm{NS}(X)$, so $[H]$ does not generate that group.

Discussion 4.6. We think these examples show that the larger sectional genera of quartic and quintic surfaces will tend to produce codes with smaller d than codes from cubic surfaces having the same n. Moreover, this tends to be true even when none of the irreducible plane sections of the surface are optimal curves of genus $g = \frac{(m-1)(m-2)}{2}$. On the other hand, some surfaces of higher degree may have many more $\mathbb{F}_q$-rational points than any cubic surface and

that might tend to overcome the effects of the greater sectional genus. So the situation is still rather subtle and we cannot say that higher degree surfaces are automatically bad in the construction of this paper.

5. Restricting $\rho(X)$ and the sectional genus. From the previous section, we see that to obtain good codes from an algebraic surface, in addition to restricting the Picard number, it is probably also necessary to restrict the sectional genus g of the surface. For small values of g, this puts some severe restrictions on the available classes of surfaces. The following results are very well known; the article [1] provides a convenient reference with arguments valid in characteristic $p > 0$. We use the notation from that paper, where $g(L)$ denotes the arithmetic genus of the curves in the linear system corresponding to an ample line bundle L.

Theorem 5.1 (see [1, Theorem 1.5]). *If X is a smooth surface over an algebraically closed field of characteristic $p > 0$ and L is an ample line bundle with $g(L) = 0$, then (up to isomorphism) (X, L) is one of the following:*
1. *$(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(r))$, $r = 1, 2$;*
2. *$(Q, \mathcal{O}_Q(1))$, where Q is a smooth quadric surface in $\mathbb{P}^3$; or*
3. *$(F_r, \mathcal{O}_{F_r}(E + sf))$, where $r \geq 1$, F_r is a Hirzebruch surface, E is a rational curve on F_r with $E^2 = -r$, $f^2 = 0$, $E \cdot f = 1$, and $s \geq r + 1$. The sections of the given line bundle embed the surface as a rational scroll of degree $\delta = 2s - r$ in $\mathbb{P}^{\delta+1}$.*

In other words, there are very few examples, and the codes from those surfaces are well-understood from the perspective of coding theory as projective Reed–Muller codes, codes from quadrics and scrolls, or toric surface codes.

The results of applying this construction to more general rational surfaces have been discussed in several works. In [8], Davis studied codes obtained from certain very explicit rational surfaces with an eye toward proving uniform bounds on the minimum distance. Let X be the blow-up of $\mathbb{P}^2$ at eight or fewer points, let E_0 be the class of the proper transform of a line, and for $i \geq 1$, let E_i be the exceptional curve over a blown up point. To obtain the minimum distance, [8] employs a strategy along the lines of [15]: find sections which have maximal possible factorization. The result is the following.

Theorem 5.2 (see [8]). *Let $T \subset \mathbb{P}^2(\mathbb{F}_q)$ be the "big torus," namely,*

$$T = \{(x_0 : x_1 : x_2) \in \mathbb{P}^2(\mathbb{F}_q) \mid x_0 x_1 x_2 \neq 0\}.$$

If $D = mE_0 - \sum m_i E_i$ is a nef divisor and $q \geq \max\{m + 2, 2m - \sum m_i\}$, then the minimum distance of the $C(T, D, \mathbb{F}_q)$ code satisfies

$$d \geq (q-1)^2 - m(q-1).$$

In [4], this bound is improved by 1, and Couvreur applies many of these ideas to produce some quite good codes in [7].

The case of sectional genus $g = 1$ seems to be favorable for these coding theory applications. But again there are actually very few examples, as we see from [1].

Theorem 5.3 (see [1, Theorem 1.8]). *If X is a smooth surface over an algebraically closed field of characteristic $p > 0$ and L is an ample line bundle with $g(L) = 1$, then (X, L) is either an elliptic scroll (that is, a ruled surface over an elliptic curve) or a Del Pezzo surface.*

Scrolls never seem to yield good results in our construction because $\rho(X) \geq 2$ and there are always hyperplane sections containing several fibers of the ruling. So we will concentrate on the Del Pezzo case.

5.1. The Del Pezzo quartic in $\mathbb{P}^4$. In this subsection, we start by considering a code obtained from a surface which is a blow-up of $\mathbb{P}^2$ at five general points. Over a finite field, these surfaces were classified by Rybakov in [17]. One reason to consider these surfaces is that the higher embedding dimension means that the dimension of the $C(X, 1, \mathbb{F}_q)$ codes will be larger.

Experimental Results 5.4. *With a random search, we found the following X, a Del Pezzo surface of degree 4 in $\mathbb{P}^4$, defined as*

$$\mathbf{V}(2x^2 - 2vy - 2xy - 2y^2 + 3vz - xz - 2yz - 2z^2 - 2xw + 2yw + 2zw + 3w^2,$$
$$- v^2 + 2vx - x^2 - vy - xy - vz + 2yz + 2z^2 - 3vw - 2xw + 2yw - 2zw - 2w^2).$$

It can be checked easily that
- *X is smooth,*
- *X has 57 $\mathbb{F}_7$-rational points, and*
- *X contains no $\mathbb{F}_7$-rational lines or conics.*

The corresponding $C(X, 1, \mathbb{F}_7)$ code has parameters $[57, 5, 44]$.

Since there are no $\mathbb{F}_7$-rational lines or conics contained in this surface, all the hyperplane sections by $\mathbb{F}_7$-rational planes are irreducible. As in the discussion of cubic surfaces, $n-d \leq 13$ for any such surface since the hyperplane sections of X are elliptic quartic curves in $\mathbb{P}^3$ ($g = 1$). There are optimal $g = 1$ curves that appear as hyperplane sections for this surface, so $d = 44$. By way of contrast, however, since X is a surface in $\mathbb{P}^4$, we have $k = 5$. The resulting code has parameters equal to the best known code in [10] for this n, k over $\mathbb{F}_7$.

5.2. Codes from other surfaces with sectional genus one. For a different sort of example related to the approach taken in [8] and [7], take cubics in $\mathbb{P}^2$ through three points defined over $\mathbb{F}_{q^3}$ in a general Frobenius orbit $\mathcal{P}_3 = \{P, F(P), F^2(P)\}$. We assume in particular that the points in $\mathcal{P}_3$ are *not collinear*. If we use the system of cubics in $\mathbb{P}^2$ containing $\mathcal{P}_3$ to map $\mathbb{P}^2$ into $\mathbb{P}^6$, we obtain a certain type of Del Pezzo surface X of degree 6 defined over $\mathbb{F}_q$. (These surfaces are discussed in general in [9].)

Proposition 5.5. *This surface X has Picard number $\rho(X) = 2$.*

Proof. We start by computing the zeta function of the surface X. Since X is $\mathbb{P}^2$ blown up in a Frobenius orbit of three points defined over $\mathbb{F}_{q^3}$, to count points over extensions of $\mathbb{F}_q$, we just look at the corresponding numbers of points on $\mathbb{P}^2$, and then add in the $\mathbb{F}_{q^r}$-rational points on three copies of $\mathbb{P}^1$ defined over $\mathbb{F}_{q^3}$ (other than the points we blew up). This gives

$$|X(\mathbb{F}_{q^r})| = \begin{cases} 1 + q^{2r} + q^r, & r \equiv 1, 2 \bmod 3, \\ 1 + q^{2r} + 4q^r, & r \equiv 0 \bmod 3. \end{cases}$$

This implies the zeta function of X equals the zeta function of $\mathbb{P}^2$ over $\mathbb{F}_q$, multiplied by $\frac{1}{1-q^3t^3}$. (This is a special case of Lemma 2.7 in [17].) Hence because of the form of the zeta

function described by the Weil conjectures (proved by Deligne), we have

$$Z(X,t) = \frac{1}{(1-t)P_2(t)(1-q^2t)},$$

where $P_2(t)$ (the factor corresponding to the H^2 cohomology) factors as

$$P_2(t) = (1-qt)\prod_{j=1}^{3}(1-\alpha_j t),$$

with $\alpha_j = q, e^{2\pi i/3}q, e^{4\pi i/3}q$.

By the results of Tate from [23], this is enough to imply that $\rho(X) = 2$. In [23], Tate conjectured that the Picard number of any smooth projective surface over $\mathbb{F}_q$ is equal to the multiplicity of q as a reciprocal root of the "H^2-factor" in the denominator of the zeta function. Although the equality remains conjectural in general, Tate also showed that the Picard number is bounded above by the number of reciprocal roots equal to q in all cases. The bound is 2 in this case, but we can also see two independent elements of NS(X) by considering the proper transforms on X of lines in $\mathbb{P}^2$, and of the conics through the three points in $\mathcal{P}_3$. We believe Tate's conjecture was probably known previously for this type of surface, but we were not able to find a convenient reference. In any case, the bound suffices for our purposes. ∎

Results from [7] show the $C(X, 1, \mathbb{F}_q)$ codes on these surfaces are already quite good. For completeness, we indicate the proof from this point of view.

Proposition 5.6 (see [7, Theorem 3.8], which is equivalent to this). *For all prime powers q, $C(X, 1, \mathbb{F}_q)$ is a $[q^2 + q + 1, 7, q^2 - q - 1]$ linear code over $\mathbb{F}_q$.*

Proof. The sections of X by hyperplanes in $\mathbb{P}^6$ are the images of cubics in the plane passing through $\mathcal{P}_3$. Since $\mathcal{P}_3$ is general, there are no $\mathbb{F}_q$-rational lines containing all three points in $\mathcal{P}_3$, but there is a 2-parameter family of $\mathbb{F}_q$-rational conics containing those points. Hence the cubics through $\mathcal{P}_3$ contain reducible cubics consisting of the union of an $\mathbb{F}_q$-rational conic through $\mathcal{P}_3$ and an arbitrary $\mathbb{F}_q$-rational line. Among the codewords of the $C(X, 1, \mathcal{P}_3)$ code, then, we will always find some coming from cubics that factor as an $\mathbb{F}_q$-rational conic containing $\mathcal{P}_3$ and an $\mathbb{F}_q$-rational line that intersects the conic in two conjugate points defined over $\mathbb{F}_{q^2}$. This gives codewords with $2(q+1) = 2q+2$ zeros. We claim that this is the largest possible number of zeros in any nonzero codeword, which yields $d = (q^2 + q + 1) - (2q + 2) = q^2 - q - 1$ as in the statement to be proved. The claim follows from a case-by-case analysis of the possible factorizations of a cubic C containing $\mathcal{P}_3$. If C is irreducible, the Hasse–Weil–Serre bound implies

$$|C(\mathbb{F}_q)| \leq 1 + q + \lfloor 2\sqrt{q} \rfloor \leq (1 + \sqrt{q})^2.$$

But $(1 + \sqrt{q})^2 < 2q + 2$ for all $q \geq 2$. If $C = Q \cup L$, where Q is a conic containing $\mathcal{P}_3$ and L is a line such that $Q \cap L$ consists of distinct $\mathbb{F}_q$-rational points, then $|(Q \cup L)(\mathbb{F}_q)| = (q+1) + (q+1) - 2 = 2q$. If the line L is tangent to Q, then $|(Q \cup L)(\mathbb{F}_q)| = (q+1) + (q+1) - 1 = 2q+1$. So such cubics give codewords containing $2q$ or $2q + 1$ zeros. Finally, there are no reducible cubics with three $\mathbb{F}_q$-rational line components in this linear system since if such a line contains

P, then it would have to contain the whole Frobenius orbit $\mathcal{P}_3$. But there are no such lines by our general position hypothesis for $\mathcal{P}_3$. Hence the minimum weight codewords will have $2q + 2$ zeros as claimed. ∎

For example, this yields codes with parameters as follows:
- $q = 7$: $[57, 7, 41]$.
- $q = 8$: $[73, 7, 55]$.
- $q = 9$: $[91, 7, 71]$.

All three of these equal the best known values for d for these n, k according to [10].

To conclude our discussion we will consider the $C(X, 2, \mathbb{F}_q)$ codes from these Del Pezzo surfaces.

Theorem 5.7. *Let $q > 5$. Then $C(X, 2, \mathbb{F}_q)$ is a $[q^2 + q + 1, 19, \leq q^2 - 3q - 1]$ code over $\mathbb{F}_q$. Moreover, $d = q^2 - 3q - 1$ for all prime powers $q > 36$.*

Proof. The dimension of the space of homogeneous polynomials of degree 2 on $\mathbb{P}^6$ is $\binom{6+2}{2} = \binom{8}{2}$. However, it is easy to check that the ideal of X is generated by 9 linearly independent quadrics. Hence $k = \dim_{\mathbb{F}_q} C(X, 2, \mathbb{F}_q) \leq \binom{8}{2} - 9 = 19$. The $\mathbb{F}_q$-rational points on X are in a general enough position to guarantee that Definition 2.3 is satisfied. Hence the dimension of the code is exactly $k = 19$.

To show that the minimum distance is bounded above by $q^2 - 3q - 1$, we claim first that there are codewords with precisely $4q + 2$ zeros. Sections of X by quadrics in $\mathbb{P}^6$ correspond to elements of the linear system of sextic curves in the plane with double points at the three points in $\mathcal{P}_3$. Among the elements of that linear system are reducible sextics of the form $(C_1 \cup L_1) \cup (C_2 \cup L_2)$, where the C_i are $\mathbb{F}_q$-conics through $\mathcal{P}_3$, the L_i are $\mathbb{F}_q$-lines, and for each i, $C_i \cap L_1$ and $C_i \cap L_2$ both consist of two Frobenius-conjugate points defined over $\mathbb{F}_{q^2}$. Note that there are $2q + 2$ $\mathbb{F}_q$-rational points on $C_i \cup L_i$ for each i. However, since C_1 and C_2 both pass through $\mathcal{P}_3$, their fourth point of intersection must be defined over $\mathbb{F}_q$. Moreover L_1 and L_2 also meet in an $\mathbb{F}_q$-rational point. Hence the union $(C_1 \cup L_1) \cup (C_2 \cup L_2)$ contains $(2q + 2) + (2q + 2) - 2 = 4q + 2$ $\mathbb{F}_q$-rational points. Evaluating a polynomial corresponding to one of these sextics gives a codeword of weight $q^2 + q + 1 - (4q + 2) = q^2 - 3q - 1$.

To conclude the proof, we need to show that if $q > 36$, no section of X by a quadric in $\mathbb{P}^6$ gives a curve with more than $4q + 2$ $\mathbb{F}_q$-rational points. Sextic curves in the plane with double points at the points of $\mathcal{P}_3$ have arithmetic genus $g = 7$. By Corollary 3.3 of [5], if $6 \leq \sqrt{q}$ (hence the prime power q satisfies $q > 36$), then a plane curve of $d = 6$ and genus $g = 7$ has at most

$$\frac{(2 \cdot 7 - 2) + (q + 2) \cdot 6}{2} = 3q + 12$$

$\mathbb{F}_q$-rational points. This result is based on the Stöhr–Voloch theorem (see [22]) and the fact that curves of small degree relative to q are automatically Frobenius-classical. We see $3q + 12 < 4q + 2$ for all $q > 11$, and hence in particular for all $q > 36$.

If Y is the union of an absolutely irreducible quintic with double points at the points of $\mathcal{P}_3$ and a line, then by [2], Y has at most $1 + q + 3\lfloor 2\sqrt{q} \rfloor + 1 + q = 2 + 2q + 6\lfloor 2\sqrt{q} \rfloor$ $\mathbb{F}_q$-rational points. This is $< 4q + 2$ for all $q > 36$.

If Y is the union of a quartic and a conic, then similarly Y can have at most $1 + q + 3\lfloor 2\sqrt{q} \rfloor + 1 + q = 2 + 2q + 3\lfloor 2\sqrt{q} \rfloor$ $\mathbb{F}_q$-rational points, and this is also $< 4q + 2$ for all $q > 9$.

If Y is the union of two irreducible cubics containing $\mathcal{P}_3$, then Y has at most $2 + 2q + 4\sqrt{q}$ $\mathbb{F}_q$-rational points. This is $< 4q + 2$ for all $q \geq 5$. If $Y = Z_1 \cup (C \cup L)$ where Z_1 is an irreducible cubic over $\mathbb{F}_q$ and $C \cup L$ is a cubic of the form considered in the second paragraph of this proof, then Y contains at most $1 + q + 2\sqrt{q} + 2q + 2 = 3 + 3q + 2\sqrt{q}$ $\mathbb{F}_q$-rational points. But $3 + 3q + 2\sqrt{q} < 2 + 4q$ for all $q > 5$. Finally, any $Y = (C_1 \cup L_1) \cup (C_2 \cup L_2)$ has at most $4q + 2$ $\mathbb{F}_q$-rational points as well since the arrangements considered in the previous paragraph have *smallest number of common points* defined over $\mathbb{F}_q$ in $(C_1 \cup L_1) \cap (C_2 \cup L_2)$. ∎

Experimental Results 5.8. *By* `Magma` *calculations we have verified that the equality* $d = q^2 - 3q - 1$ *also holds for* $q = 7$ *and* $q = 9$ *using particular choices of the Frobenius orbit* $\mathcal{P}_3 = \{P, F(P), F^2(P)\}$. *This yields a* $[57, 19, 27]$ *code over* $\mathbb{F}_7$ *and a* $[91, 19, 53]$ *code over* $\mathbb{F}_9$.

The code over $\mathbb{F}_7$ *improves on the best previously known* d *by 1. Grassl observed via another* `Magma` *calculation that this code is equivalent to a cyclic code, and the cyclic form has been added to the database* [10].

The code over $\mathbb{F}_9$ *improves the best previously known* $d = 51$ *by 2.*

On the other hand, for $q = 8$, *and again for a particular choice of Frobenius orbit, the parameters of the* $C(X, 2, \mathbb{F}_8)$ *code we tested were* $[73, 19, 37]$, *while* $8^2 - 3 \cdot 8 - 1 = 39$ *and the database* [10] *contains a* $[73, 19, 39]$ *code. The minimum weight codewords for our* $[73, 19, 37]$ *code come from absolutely irreducible plane sextics with nodes at the three points in* $\mathcal{P}_3$ *and no other singularities, and hence curves of geometric genus 7. The 36* $\mathbb{F}_8$*-rational points on these curves happen to improve on the largest number of* $\mathbb{F}_8$*-rational points for curves of genus 7 reported in the database* [24] *as of September* 2017.

In Theorem 3.12 of [7], Couvreur considers the linear system of all quintic curves in $\mathbb{P}^2$ passing through a Frobenius orbit $\mathcal{P}_3$ and constructs a $[q^2 + q + 1, 18, q^2 - 3q - 1]$ code. Our examples improve his by increasing the dimension by 1.

6. Concluding remarks.
Our work raises a number of questions:
1. Are there other surfaces where Theorems 3.3 and 3.5 apply to yield really good codes?
2. What happens for varieties of dimension ≥ 3?
3. Is Conjecture 4.2 true in general?

We hope to return to these in future work.

REFERENCES

[1] M. ANDREATTA AND E. BALLICO, *Classification of projective surfaces with small sectional genus: char* $p > 0$, Rend. Sem. Mat. Univ. Padova, 84 (1990), pp. 175–193.

[2] Y. AUBRY AND M. PERRET, *A Weil theorem for singular curves*, in Arithmetic, Geometry, and Coding Theory, R. Pellikaan, M. Perret, and S.G. Vladut, eds., de Gruyter, Berlin, 1996, pp. 1–7.

[3] Y. Aubry and M. Perret, *On the characteristic polynomials of the Frobenius endomorphism for projective curves over finite fields*, Finite Fields Appl., 10 (2004), pp. 412–431.

[4] E. Ballico, *Codes coming from a blowing up of the plane*, Afr. Mat., 24 (2013), pp. 93–96.

[5] H. Borges and M. Homma, *Points on singular Frobenius nonclassical curves*, Bull. Braz. Math. Soc. (N.S.), 48 (2017), pp. 93–101.

[6] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system.* I. *The user language*, J. Symbolic Comput., 24 (1997), pp. 235–265.

[7] A. Couvreur, *Construction of rational surfaces yielding good codes*, Finite Fields Appl., 17 (2011), pp. 424–441.

[8] J. Davis, *Algebraic geometric codes on anticanonical surfaces*, J. Pure Appl. Algebra, 215 (2011), pp. 496–510.

[9] I. Dolgachev, *Classical Algebraic Geometry*, Cambridge University Press, Cambridge, UK, 2012.

[10] M. Grassl, *Bounds on the Minimum Distance of Linear Codes and Quantum Codes*, http://www.codetables.de (accessed 2017-09-09).

[11] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, Berlin, Heidelberg, New York, 1977.

[12] W.C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, UK, 2003.

[13] G. Lachaud and R. Rolland, *On the number of points of algebraic sets over finite fields*, J. Pure Appl. Algebra, 219 (2015), pp. 5117–5136.

[14] J. Little, *Algebraic geometry codes from higher dimensional varieties*, in Advances in Algebraic Geometry Codes, E. Martinez-Moro, C. Munuera, and D. Ruano, eds., Ser. Coding Theory Cryptol. 5, World Sci. Publ., Hackensack, NJ, 2008, pp. 257–293.

[15] J. Little and H. Schenck, *Toric surface codes and Minkowski sums*, SIAM J. Discrete Math., 20 (2006), pp. 999–1014, https://doi.org/10.1137/050637054.

[16] A. Perucca, *Elliptic Curves over Finite Fields with Many Points*, http://antonellaperucca.net/perucca_maxpoints.pdf (accessed 2017-09-02).

[17] S. Rybakov, *The zeta function of conic bundles and of Del Pezzo surfaces of degree four over finite fields*, Russian Math. Surveys, 60 (2005), pp. 986–987.

[18] S. Rybakov and A. Trepalin, *Minimal cubic surfaces over finite fields*, Mat. Sb., 208 (2017), pp. 148–170 (in Russian); translation in Sb. Math., 208 (2017), pp. 1399–1419.

[19] T. Shioda, *On the Picard number of a complex projective variety*, Ann. Sci. École Norm. Sup. (4), 14 (1981), pp. 303–321.

[20] I. Soprunov and J. Soprunova, *Toric surface codes and Minkowski length of polygons*, SIAM J. Discrete Math., 23 (2009), pp. 384–400, https://doi.org/10.1137/080716554.

[21] H.P.F. Swinnerton-Dyer, *The zeta function of a cubic surface over a finite field*, Proc. Cambridge Philos. Soc., 63 (1967), pp. 55–71.

[22] K.O. Stöhr and J. Voloch, *Weierstrass points on curves over finite fields*, Proc. London Math. Soc., 52 (1986), pp. 1–19.

[23] J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, in Séminaire Bourbaki, Vol. 9, Exp. 306, Soc. Math. France, Paris, 1995, pp. 415–440.

[24] G. van der Geer, E. Howe, K. E. Lauter, and C. Ritzenthaler, *Table of Curves with Many Points*, http://www.manypoints.org, 2009 (accessed 2017-09-03).

[25] R. van Luijk, *K3 surfaces with Picard number one and infinitely many rational points*, Algebra Number Theory, 1 (2007), pp. 1–15.

[26] J. Voloch and M. Zarzar, *Algebraic geometric codes on surfaces*, in Arithmetic, Geometry, and Coding Theory, Sémin. Congr. 21, Soc. Math. France, Paris, 2010, pp. 211–216.

[27] M. Zarzar, *Error-correcting codes on low rank surfaces*, Finite Fields Appl., 13 (2007), pp. 727–737.