Remarks on codes from modular curves: MAPLE applications*

David Joyner and Salahoddin Shokranian

July 20, 1999

Contents

*Appeared in **Coding Theory and Cryptography: From the Geheimschreiber and Enigma to Quantum Theory**, (ed. D. Joyner), Springer-Verlag, 2000. Minor revisions made 3-23-2004.

1 Introduction

Suppose that V is a smooth projective variety over a finite field k. An important problem in arithmetical algebraic geometry is the calculation of the number of k-rational points of V, $|V(k)|$. The work of Goppa and others have shown its importance in geometric coding theory as well. We refer to this problem as the **counting problem**. In most cases it is very hard to find an explicit formula for the number of points of a variety over a finite field.

When the variety is a "Shimura variety" defined by certain group theoretical conditions (see §2 below), methods from non-abelian harmonic analysis on groups can be used to find an explicit solution for the counting problem. The Arthur-Selberg trace formula [S], provides one such method. Using the Arthur-Selberg trace formula, an explicit formula for the counting problem has been found for Shimura varieties, thanks primarily to the work of Langlands and Kottwitz ([Lan1], [K1]) [1]. Though it may be surprising and indeed very interesting that the trace formula allows one (with sufficient skill and expertise) to relate, when V is a Shimura variety, the geometric numbers $|V(\mathbb{F}_q)|$ to orbital integrals from harmonic analysis ([Lab], for example), or to a linear combination of coefficients of automorphic forms ([Gel], for example), or even to representation-theoretic data ([Cas2], for example), these formulas do not yet seem to be helping the coding theorist in any practical way that we know of.

However, another type of application of the trace formula is very useful. Moreno [M] first applied the trace formula in the context of Goppa codes to obtaining a new proof of a famous result of M. Tsfasman , S. Vladut, T. Zink, and Y. Ihara. (Actually, Moreno used a formula for the trace of the Hecke operators acting on the space of modular forms of weight 2, but this can be proven as a consequence of the Arthur-Selberg trace formula, [DL], §II.6.) This will be discussed below. We are going to restrict our attention in this paper to the interplay between Goppa codes of modular curves and the counting problem, and give some examples using MAPLE, where the programs using for the calculation is written in MAPLE by the first named author. In coding theory, curves with many rational points over

[1] For some introductions to this highly technical work of Langlands and Kottwitz, the reader is referred to Labesse [Lab], Clozel [Cl], and Casselman [Cas2].

finite fields are being used for construction of codes with some good specific characteristics. We discuss the Goppa codes, first from an abstract general perspective then turning to concrete examples associated to modular curves. We will try to explain these extremely technical ideas using a special case at a level to a typical graduate student with some background in modular forms, number theory, group theory, and algebraic geometry. For an approach similar in spirit, though from a more classical perspective, see the book of C. Moreno [M].

2 Shimura curves

In this section we study arithmetic subgroups, arithmetical quotients, and their rational compactifications. Ihara first introduced Shimura curves, a rational compactification of $\Gamma\backslash\mathbb{H}$ where Γ is a particular discrete subgroup, from a classical perspective. We shall recall them from both the classical and group-theoretical point of view. The latter perspective generalizes to higher dimensional Shimura varieties [Del].

2.1 Arithmetic subgroups

We assume that $G = SL(2)$ is the group of 2×2 matrices with entries from an algebraically closed field Ω. In particular the group of R-points of $SL(2)$ for a subring $R \subseteq \Omega$, with unit element 1 is defined by

$$SL(2, R) = \{g \in M(2, R) \mid \det(g) = 1\},$$

where $M(2, R)$ is the space of 2×2 matrices with entries from R. We now define congruence subgroups in $SL(2, \mathbb{Z})$. Let $SL(2, \mathbb{Z})$ be the subgroup of $SL(2, \mathbb{R})$ with integral matrices. Consider a natural number N, and let

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL(2, \mathbb{Z}) \mid \begin{array}{c} a, d \equiv 1 (\mathrm{mod}\, N) \\ b, c \equiv 0 (\mathrm{mod}\, N) \end{array} \right\},$$

We note that the subgroup $\Gamma(N)$ is a discrete subgroup of $SL(2, \mathbb{R})$, which is called the *principal congruence subgroup of level* N. Any subgroup of $SL(2, \mathbb{Z})$ that contains the principal congruence subgroup is called a *congruence subgroup*.

In general an *arithmetic subgroup* of $SL(2, \mathbb{R})$ is any discrete subgroup Γ that is commensurable with $SL(2, \mathbb{Z})$, where *commensurability* means that

the intersection $\Gamma \cap SL(2,\mathbb{Z})$ is of finite index in both Γ and $SL(2,\mathbb{Z})$. The group $\Gamma(N)$ has the property of being commensurable with $SL(2,\mathbb{Z})$.

2.2 Riemann surfaces as algebraic curves

Let us recall that the space $\mathbb{H} = \{z \in \mathbb{C} \mid Im(z) > 0\}$ is called *the Poincaré upper half plane*. This space plays fundamental rôle in the definition of the modular curves. Note that the group $SL(2,\mathbb{R})$ acts on $\mathbb{H}$ by

$$g \cdot z = (az+b)(cz+d)^{-1} = \frac{az+b}{cz+d},$$

where $z \in \mathbb{H}$, $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL(2,\mathbb{R})$.

We emphasize that the action of $SL(2,\mathbb{R})$ on $\mathbb{H}$ is *transitive*, i.e., for any two points $w_1, w_2 \in \mathbb{H}$ there is an element $g \in SL(2,\mathbb{R})$ such that $w_2 = g \cdot w_1$. This can easily be proved. We also emphasize that there are subgroups of $SL(2,\mathbb{R})$ for which the action is not transitive, among them the class of arithmetic subgroups are to be mentioned. For example, the group $SL(2,\mathbb{Z})$ does not act transitively on $\mathbb{H}$, and the set of orbits of the action of $SL(2,\mathbb{Z})$ on $\mathbb{H}$, and similarly any arithmetic subgroup, is infinite. We call the *arithmetic quotient* $\Gamma\backslash\mathbb{H}$ the set of orbits of the action of an arithmetic subgroup Γ on $\mathbb{H}$.

Example 1 *Take* Γ *to be the* Hecke subgroup $\Gamma_0(N)$ *defined by*

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL(2,\mathbb{Z}) \mid c \equiv 0 (\mathrm{mod}\, N) \right\},$$

for a natural number N*. This is a congruence subgroup and* $Y_0(N) = \Gamma_0(N)\backslash\mathbb{H}$ *is an arithmetic quotient. Such a quotient is not a compact subset, nor a bounded one, it is however a subset with finite measure (volume) under the non-Euclidean measure induced on the quotient from the group* $SL(2,\mathbb{R})$ *which is a locally compact group and induces the invariant volume element* $\frac{dx \wedge dy}{y^2}$*, where* x, y *are the real and the complex part of an element* $z \in \mathbb{H}$*.*

We now recall the basic ideas that turns an arithmetic quotient of the form $\Gamma\backslash\mathbb{H}$ into an algebraic curve. Let $\Gamma \subset SL(2,\mathbb{Q})$ be an arithmetic subgroup. The topological boundary of $\mathbb{H}$ is $\mathbb{R}$ and a point ∞. For the rational

compactification of $\mathbb{H}$ we do not need to consider all the boundaries $\mathbb{R}$ and $\{\infty\}$. In fact we need only to add to $\mathbb{H}$ the cusps of Γ (a **cusp** of Γ is a rational number (an element of $\mathbb{Q}$) that is fixed under the action of an element γ with the property that $|tr(\gamma)| = 2$). Any two cusps x_1, x_2 such that $\delta \cdot x_2 = x_1$ for an element $\delta \in \Gamma$ are called **equivalent**. Let $C(\Gamma)$ be the set of inequivalent cusps of Γ. Then $C(\Gamma)$ is finite. We add this set to $\mathbb{H}$ and form the space $\mathbb{H}^* = \mathbb{H} \cup C(\Gamma)$. This space will be equipped with certain topology such that a basis of the neighborhoods of the points of $\mathbb{H}^*$ is given by three type of open sets; if a point in $\mathbb{H}^*$ is lying in $\mathbb{H}$ then its neighborhoods consists of usual open discs in $\mathbb{H}$, if the point is ∞, i.e., the cusp ∞, then its neighborhoods are the set of all points lying above the line $Im(z) > \alpha$ for any real number α, if the point is a cusp different than ∞ which is a rational number, then the system of neighborhoods of this point are the union of the cusp and the interior of a circle in $\mathbb{H}$ tangent to the cusp. Under the topology whose system of open neighborhoods we just explained, $\mathbb{H}^*$ becomes a Hausdorff non-locally compact space. The quotient space $\Gamma\backslash\mathbb{H}^*$ with the quotient topology is a compact Hausdorff space. We refer to this compact quotient as the **rational compactification** of $\Gamma\backslash\mathbb{H}$. For a detailed discussion we refer the reader to [Shim].

When the arithmetic group is a congruence subgroup of $SL(2,\mathbb{Z})$ the resulting algebraic curve is called a **modular curve**. For example, the rational compactification of $Y(N) = \Gamma(N)\backslash\mathbb{H}$ is denoted by $X(N)$ and the compactification of $Y_0(N) = \Gamma_0(N)\backslash\mathbb{H}$ by $X_0(N)$.

Example 2 *Let $N = 1$. Then $\Gamma = \Gamma(1) = SL(2,\mathbb{Z})$. In this case $C(\Gamma) = \{\infty\}$, since all rational cusps are equivalent to the cusp ∞. So $\mathbb{H}^* = \mathbb{H} \cup \{\infty\}$, and $\Gamma\backslash\mathbb{H}^*$ will be identified by $\Gamma\backslash\mathbb{H} \cup \{\infty\}$. This may be seen as adding ∞ to the fundamental domain $\mathbb{F}_1 = \mathbb{F}$ of $SL(2,\mathbb{Z})$, that consists of all complex numbers in $z \in \mathbb{H}$ with $|z| \geq 1$ and $|Re(z)| \leq \frac{1}{2}$.*

The rational compactification of $\Gamma\backslash\mathbb{H}$ turns the space $\Gamma\backslash\mathbb{H}^*$ into a compact Riemann surface (cf. [Shim]) and so into an algebraic curve (cf. [Nara], or [SS]).

In general it is easiest to work with those arithmetic subgroups which are torsion free and we shall assume from this point on that the arithmetic subgroups we deal with have this property. For example $\Gamma(N)$ and $\Gamma_0(N)$ for $N \geq 3$ are torsion free.

2.3 An adelic view of arithmetic quotients

Consider the number field $\mathbb{Q}$, the field of rational numbers. Let $\mathbb{Q}_p$ be the completion of $\mathbb{Q}$ under the p-adic absolute value $|...|_p$, where $|a/b|_p = p^{-n}$ whenever a, b are integers and $a/b = p^n \prod_{\ell \neq p \text{ prime}} \ell^{e_\ell}$, $n, e_\ell \in \mathbb{Z}$. Recall that under the ordinary absolute value the completion of $\mathbb{Q}$ is $\mathbb{R}$. The ring of adeles of $\mathbb{Q}$ is the locally compact commutative ring $\mathbf{A}$ that is given by:

$$\mathbf{A} = \{(x_\infty, x_2, \cdots) \in \mathbb{R} \times \prod_p \mathbb{Q}_p \mid \text{ all but a finite number of } x_p \in \mathbb{Z}_p\},$$

where $\mathbb{Z}_p$ is the ring of integers of $\mathbb{Q}_p$ (as it is well known $\mathbb{Z}_p$ is a maximal compact open subring of $\mathbb{Q}_p$). An element of $\mathbf{A}$ is called an **adele**. If $\mathbf{A}_f$ denotes the set of adeles omitting the $\mathbb{R}$-component x_∞, then $\mathbf{A}_f$ is called the **ring of finite adeles** and we can write $\mathbf{A} = 3D\mathbb{R} \times \mathbf{A}_f$. Under the diagonal embedding $\mathbb{Q}$ is a discrete subgroup of $\mathbf{A}$.

We now consider the group $G = GL(2)$. For a choice of an open compact subgroup $K_f \subset G(\mathbf{A}_f)$, it is known that we can write the arithmetic quotient (which was originally attached to an arithmetic subgroup of $\Gamma \subset SL(2, \mathbb{Q})$) as the following quotient

$$Y(K_f) = G(\mathbb{Q}) \backslash [\mathbb{H} \times (G(\mathbf{A}_f)/K_f)] = \Gamma \backslash H, \tag{1}$$

where

$$\Gamma = G(\mathbb{Q}) \cap G(\mathbb{R}) K_f. \tag{2}$$

Thus our arithmetic subgroup Γ is completely determined by K_f. From now on we assume K_f has been chosen so that Γ is torsion free.

Definition 3 *Let $G = GL(2)$. To G is associated the Shimura variety $Sh(G)$ as follows. Let $N \geq 3$ be a natural number. Let $\Gamma(N)$ be the congruence subgroup of level N of $SL(2, \mathbb{Z})$, and $K = SO(2, \mathbb{R})$ the orthogonal group of 2×2 real matrices A with determinant 1 satisfying ${}^tAA = I_2$. Then*

$$Y(N) = \Gamma(N) \backslash \mathbb{H} \cong \Gamma(N) \backslash G(\mathbb{R}) / K.$$

We call this the modular space of level N. *Let*

$$K_f(N) = \{g \in G(\prod_p \mathbb{Z}_p) \mid g \equiv I_2 (\mathrm{mod}\, N)\}$$

be the **open compact subgroup of** $G(\mathbf{A}_f)$ **of level** N. *Then the modular space of level* N *can be written as:*

$$Y(N) \cong G(\mathbb{Q})\backslash G(\mathbf{A})/KK_f(N) = G(\mathbb{Q})\backslash[\mathbb{H} \times (G(\mathbf{A}_f)/K_f(N))].$$

Thus

$$X(K_f(N)) \cong Y(N).$$

Taking the projective limit over $K_f(N)$ *by letting* N *gets large (which means* $K_f(N)$ *gets small), we see that* $\lim_N Y(N) = G(\mathbb{Q})\backslash[\mathbb{H} \times G(\mathbf{A}_f)]$. *Then the (complex points of the)* **Shimura curve** $Sh(G)$ *associated to* $G = SL(2)$ *is defined by*

$$Sh(G)(\mathbb{C}) = G(\mathbb{Q})\backslash[\mathbb{H} \times G(\mathbf{A}_f)]. \tag{3}$$

Many mathematicians have addressed the natural questions

- What field are the curves $X(N)$, $X_0(N)$ defined over?
- How can they be described explicitly using algebraic equations?

Regarding the first question, by the general theory of Shimura varieties we know that for each reductive group G defined over $\mathbb{Q}$ satisfying the axioms of §2.1.1 in [Del], there is an algebraic number field $E = E_G$ over which a Shimura variety $Sh(G)$ is defined [Del]. In fact, the Shimura curves $X(N)$ and $X_0(N)$ are regular schemes proper over $\mathbb{Z}[1/N]$ (more precisely over $Spec(\mathbb{Z}[1/N])$) [2].

Regarding the second question, it is possible to find a **modular polynomial** $H_N(x, y)$ of degree

$$\mu(N) = N \prod_{p|N}(1 + \frac{1}{p})$$

for which $H_N(x, y) = 0$ describes (an affine patch of) $X_0(N)$. Let

$$G_k(q) = 2\,\zeta(k) + 2\,\frac{(2\,i\pi)^k}{(k-1)!}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n,$$

[2] This result was essentially first proved by Igusa [Ig] (from the classical perspective). See also [TV], Theorem 4.1.48, [Cas1] for an interesting discussion of what happens at the "bad primes", and Deligne's paper in the same volume as [Cas1].

where $q = e^{2\pi iz}$, $z \in \mathbb{H}$, $\sigma_r(n) = \sum_{d|n} d^r$, and let

$$\Delta(q) = 60^3 G_4(q)^3 - 27 \cdot 140^2 G_6(q)^2 = q \prod_{n=1}^{\infty} (1-q^n)^{24}.$$

Define the **j-invariant** by

$$j(q) = 1728 \cdot 60^3 G_4(q)^3 / \Delta(q) = q^{-1} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \dots .$$

(More details on Δ and j can be found for example in [Shim].) The key property satisfied by H_N is $H_N(j(q), j(q^N)) = 0$. It is interesting to note in passing that when N is such that the genus of $X_0(N)$ equals 0 (i.e., $N \in \{1, 3, 4, 5, 6, 7, 8, 9, 12, 13, 16, 18, 25\}$ [Kn]) then this implies that $(x, y) = (j(q), j(q^N))$ parameterizes $X_0(N)$. In general, comparing q-coefficients allows one to use a computer algebra system such as MAPLE to compute H_N for relatively small values of N. However, even for $N = 11$, some of the coefficients can involve one hundred digits or more. The cases $N = 2, 3$ are given in Elkies [E], for example. The paper by P. Cohen [Co] determines the asymptotic size of the largest coefficient of H_N (normalized to have leading coefficient equal to 1). She shows that the largest coefficient grows like $N^{c\mu(N)}$, where $c > 0$ is a constant. More practical equations for (some of) the $X_0(N)$ are given in T. Hibino and N. Murabayashi [HM], M. Shimura [ShimM], J. Rovira [R], G. Frey and M. Müller [FM], Birch [B], and the table in §2.5 below.

For deeper study of Shimura varieties and the theory of canonical models we refer the reader to [Del], [Lan2], and [Shim].

2.4 Hecke operators and arithmetic on $X_0(N)$

In this section we recall some well-known though relatively deep results on $X_0(N)(\mathbb{F}_p)$, where p is a prime not dividing N. These shall be used in the discussion of the Tsfasman, Vladut, Zink, and Ihara result later.

First, some notation: let $S_2(\Gamma_0(N))$ denote the space of holomorphic automorphic forms of weight 2 on $\Gamma_0(N)\backslash H$. Let $T_p : S_2(\Gamma_0(N)) \to S_2(\Gamma_0(N))$ denote the **Hecke operator** defined by

$$T_p f(z) = f(pz) + \sum_{i=0}^{p-1} f(\frac{z+i}{p}), \qquad z \in H.$$

Define T_{p^k} inductively by

$$T_{p^k} = T_{p^{k-1}} T_p - p T_{p^{k-2}}, \quad T_1 = 1,$$

and define the modified Hecke operators U_{p^k} by

$$U_{p^k} = T_{p^k} - p T_{p^{k-2}}, \quad U_p = T_p,$$

for $k \geq 2$. The Hecke operators may be extended to the positive integers by demanding that they be multiplicative.

Theorem 4 *("Congruence relation" of Eichler-Shimura [M], §5.6.7) Let $q = p^k$, $k > 0$ an integer. If p is a prime not dividing N then*

$$|X_0(N)(\mathbb{F}_q)| = q + 1 - a_q,$$

where

$$a_q = Tr(U_q).$$

Example 5 *One may try to compute the trace of the Hecke operators T_p acting on the space of holomorphic cusp forms of weight 2, $S_2(\Gamma_0(N))$, by using either the Eichler-Shimura trace formula, which we give below (see Theorem 6), or by using some easier but ad hoc ideas going back to Hecke which work in special cases. One simple idea is to note that $S_2(\Gamma_0(N))$ is spanned by simultaneous eigenforms of the Hecke operators (see for example, Proposition 51 in chapter III of [Ko]). In this case, it is known that the Fourier coefficient a_p, p prime not dividing N, of a normalized (to have leading coefficient $a_1 = 1$) eigenform is the eigenvalue of T_p (see for example, Proposition 40 in chapter III of [Ko]). If $S_2(\Gamma_0(N))$ is one-dimensional then any element in that space $f(z)$ is such an eigenform.*

The modular curve $X_0(11)$ is of genus 1, so there is (up to a non-zero constant factor) only one holomorphic cusp form of weight 2 in $S_2(\Gamma_0(11))$ (see Theorem 8 below). There is a well-known construction of this form (see [O2] or [Gel], Example 5.1), which we recall below. As we noted above, the p-th coefficient a_p (p a prime distinct from 11) of its Fourier expansion is known to satisfy $a_p = Tr(T_p)$. These will be computed using MAPLE.

Let $q = e^{2\pi i z}$, $z \in \mathbb{H}$, and consider **Dedekind's η-function**:

$$\eta(z) = e^{2\pi i z/24} \prod_{n=1}^{\infty} (1 - q^n).$$

Then

$$f(z) = \eta(z)^2\eta(11z)^2 q \prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2,$$

is an element of $S_2(\Gamma_0(11))$ [3]. *MAPLE gives*

$$\begin{gathered} f(z) = q - 2\,q^2 - q^3 + 2\,q^4 + q^5 + 2\,q^6 - 2\,q^7 - 2\,q^9 - 2\,q^{10} \\ +q^{11} - 2\,q^{12} + 4\,q^{13} + 4\,q^{14} - q^{15} - 4\,q^{16} - 2\,q^{17} + 4\,q^{18} + 2\,q^{20} \\ +2\,q^{21} - 2\,q^{22} - q^{23} - 4\,q^{25} - 8\,q^{26} + 5\,q^{27} - 4\,q^{28}... \end{gathered}$$

For example, the above expansion tells us that $Tr(T_3) = Tr(U_3) = -1$. *The curve* $X_0(11)$ *is of genus 1 and is isogenous to the elliptic curve* E *with Weierstrass model* $y^2 + y = x^3 - x^2$. *Over the field with* $p = 3$ *elements, there are* $|X_0(11)(\mathbb{F}_3)| = p + 1 - Tr(T_p) = 5$ *points in* $E(\mathbb{F}_3)$, *including* ∞*:*

$$E(\mathbb{F}_3) = \{[0,0],[0,2],[1,0],[1,2],\infty\}.$$

For a representation-theoretic discussion of this example, see [Gel], §14.

For an example of an explicit element of $S_2(\Gamma_0(32))$, *see Koblitz [Ko], chapter II §5 and (3.40) in chapter III. For a remarkable theorem which illustrates how far this* η*-function construction can be extended, see Morris' theorem in §2.2 of [R].*

To estimate a_{p^k}, one may appeal to an explicit expression for $Tr(T_{p^k})$ known as the "Eichler-Selberg trace formula", which we discuss next.

2.5 Eichler-Selberg trace formula

In this subsection, we recall the version of the trace formula for the Hecke operators due to Duflo-Labesse [DL], §6.

Let k be an even positive integer and let Γ be a congruence subgroup as in (2). Let S denote a complete set of representatives of $G(\mathbb{Q})$-conjugacy classes of $\mathbb{R}$-elliptic elements in Γ ($\mathbb{R}$-elliptic elements are those that are conjugate to

[3] In fact, if we write $f(z) = \sum_{n=1}^{\infty} a_n q^n$ then

$$\zeta_E(s) = (1-p^{-s})^{-1} \prod_{p \neq 11} (1 - a_p p^{-s} + p^{1-2s})^{-1},$$

is the global Hasse-Weil zeta function of the elliptic curve E of conductor 11 with Weierstass model $y^2 + y = x^3 - x^2$ [Gel], page 252.

an element of $SO(2,\mathbb{R})$, the orthogonal group). For $\gamma \in S$, let $w(\gamma)$ denote the cardinality of the centralizer of γ in Γ. If $r(\theta) = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix}$ then let $\theta_\gamma \in (0, 2\pi)$ denote the element for which $\gamma = r(\theta_\gamma)$. Let τ_m denote the image in $G(\mathbb{A}_f)$ of the set of matrices in $GL(2, \mathbb{A}_f)$ having coefficients in $\hat{\mathbb{Z}} = \prod_{p<\infty} \mathbb{Z}_p$ and determinant in $m\hat{\mathbb{Z}}$. Consider the subspace $S_k(\Gamma) \subset L^2(\Gamma\backslash H)$ formed by functions satisfying

- $f(\gamma z) = (cz+d)^k f(z)$, for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, $x \in H$,
- f is a holomorphic cusp form.

This is the space of holomorphic cusp forms of weight k on $\mathbb{H}$.

Let

$$\epsilon(\sqrt{m}) = \begin{cases} 1, & m \text{ is a square,} \\ 0, & \text{otherwise.} \end{cases}$$

and let

$$\delta_{i,j} = \begin{cases} 1, & i = j, \\ 0, & \text{otherwise.} \end{cases} .$$

Theorem 6 *("Eichler-Selberg trace formula") Let $k > 0$ be an even integer and $m > 0$ an integer. The trace of T_m acting on $S_k(\Gamma)$ is given by*

$$Tr(T_m) = \delta_{2,k} \sum_{d|m} b + \epsilon(\sqrt{m})(\tfrac{k-1}{12} m^{(k-2)/2} - \tfrac{1}{2} m^{(k-1)/2}) \\ - \sum_{\gamma \in S \cap \tau_m} w(\gamma)^{-1} m^{(k-2)/2} \frac{\sin((k-1)\theta_\gamma)}{\sin(\theta_\gamma)} - \sum_{d|m,\ d^2<m} b^{k-1}.$$

Remark 7 *Let $k = 2$, $m = p^2$, $\Gamma = \Gamma_0(N)$ and $N \to \infty$ in the above formula. It is possible to show that the Eichler-Selberg trace formula implies*

$$Tr(T_{p^2}) = g(X_0(N)) + O(1), \tag{4}$$

as $N \to \infty$. The proof of this estimate (see [M], chapter 5, or [LvdG], § V.4) uses the explicit formula given below for $g(X_0(N)) = \dim(S_2(\Gamma_0(N))$, which we shall also make use of later.

Theorem 8 *("Hurwitz-Zeuthen formula" [Shim]) [4] The genus of $X_0(N)$ is given by*

$$g(X_0(N)) = \dim(S_2(\Gamma_0(N)) = 1 + \frac{1}{12}\mu(N) - \frac{1}{4}\mu_2(N) - \frac{1}{3}\mu_3(N) - \mu_\infty(N),$$

[4] The genus formula for $X_0(N)$ given in [Shim] and [Kn] both contain a (typographical?) error. The problem is in the μ_2 term, which should contain a Legendre symbol $(\frac{-4}{n})$ instead of $(\frac{-1}{n})$. See for example [Ei] for a correct generalization.

where

$$\mu(N) = [SL(2,\mathbb{Z})/\Gamma_0(N)] = N\prod_{p|N}(1+\frac{1}{p}),$$

$$\mu_2(N) = \begin{cases} \prod_{p|N \text{ prime}}(1+(\frac{-4}{p})), & gcd(4,N)=1, \\ 0, & 4|N, \end{cases}$$

$$\mu_3(N) = \begin{cases} \prod_{p|N \text{ prime}}(1+(\frac{-3}{p})), & gcd(2,N)=1 \text{ and } gcd(9,N)\neq 9, \\ 0, & 2|N \text{ or } 9|N, \end{cases}$$

and

$$\mu_\infty(N) = \sum_{d|N}\phi(gcd(d,N/d)),$$

where ϕ is Euler's totient function and $(\frac{\cdot}{p})$ is Legendre's symbol.

The estimate (4) and the Eichler-Shimura congruence relation imply

$$|X_0(N)(\mathbb{F}_{p^2})| = p^2+1-Tr(T_{p^2}-pI) = p^2+1-Tr(T_{p^2})+p\dim(S_2(\Gamma_0(N))$$
$$= p^2+1-(g(X_0(N))+O(1)))+pg(X_0(N)) = (p-1)g(X_0(N))+O(1),$$

as $N\to\infty$.

2.6 The curves $X_0(N)$ of genus 1

It is known (see for example [Kn]) that a modular curve of level N, $X_0(N)$, is of genus 1 if and only if

$$N \in \{11,14,15,17,19,20,21,24,32,36,49\}.$$

In these cases, $X_0(N)$ is birational to an elliptic curve E having Weierstrass model of the form

$$y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6,$$

with a_1,a_2,a_3,a_4,a_6. If E is of above form then the **discriminant** is given by

$$\Delta = -b_2^2b_8-8b_4^3-27b_6^2+9b_2b_4b_6,$$

where

$$b_2 = a_1^2+4a_2, \qquad b_4 = 2a_4+a_1a_3, \qquad b_6 = a_3^2+4a_6,$$

$$b_8 = a_1^2 a_6 + 2a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2.$$

The conductor [5] N of E and its discriminant Δ have the same prime factors. Furthermore, $N|\Delta$ ([Kn], [Gel]).

Some examples, which we shall use later, are collected in the following table.

level	discriminant	Weierstrass model	reference
11	-11	$y^2 + y = x^3 - x^2$	[BK], table 1, p. 82
14	-28	$y^2 + xy - y = x^3$	p. 391, table 12.1 of [Kn]
15	15	$y^2 + 7\,xy + 2\,y = x^3 + 4\,x^2 + x$	p. 65, table 3.2 of [Kn]
17	17	$y^2 + 3\,xy = x^3 + x$	p. 65, table 3.2 of [Kn]
19	-19	$y^2 + y = x^3 + x^2 + x$	[BK], table 1, p. 82
20	80	$y^2 = x^3 + x^2 - x$	p. 391, table 12.1 of [Kn]
21	-63	$y^2 + xy = x^3 + x$	p. 391, table 12.1 of [Kn]
24	-48	$y^2 = x^3 - x^2 + x$	p. 391, table 12.1 of [Kn]
27	-27	$y^2 + y = x^3$	p. 391, table 12.1 of [Kn]
32	64	$y^2 = x^3 - x$	p. 391, table 12.1 of [Kn]
36		(see below)	§4.3 in [R]
49		(see below)	§4.3 in [R]

When $N = 36$, §4.3 in Rovira [R] gives $y^2 = x^4 - 4x^3 - 6x^2 - 4x + 1$, which is a hyperelliptic equation but not in Weierstrass form. To put it in Weierstrass form, we use the Maple **algcurve** package [6]. This produces a cubic equation in which the coefficient of x^3 is not one. Using the change-of-variable $y \longmapsto 2y$ (which maps the curve $X_0(36)$ to an isogenous one), we obtain the Weierstrass form $y^2 = x^3 + 64$, provided $p \neq 2$. This has conductor $\Delta = -1769472$.

When $N = 49$, §4.3 in Rovira [R] gives $y^2 = x^4 - 2x^3 - 9x^2 + 10x - 3$, which is a hyperelliptic equation but not in Weierstrass form. As in the previous case, we use the Maple **algcurve** package, which produces a cubic equation in which the coefficient of x^3 is not one. Again, the change-of-variable $y \longmapsto 2y$ (which maps the curve $X_0(49)$ to an isogenous one), yields the Weierstrass form $y^2 = x^3 - 35x - 98$, provided $p \neq 2$. This has conductor $\Delta = -1404298$.

[5] The conductor is defined in Ogg [O1], but see also [Gel], §I.2, or [Kn], P. 390.

[6] More precisely, we use the **WeierstrassForm** command written by Mark van Hoeij.

3 Codes

To have an idea of how the points of a curve over finite fields are used in the coding theory we first recall the definition of a code.

Let A be a finite set, which we regard as an alphabet. Let A^n be the n-fold Cartesian product of A by itself. In A^n we define the **Hamming metric** $d(x, y)$ by:

$$d(x, y) = d((x_1, \cdots, x_n), (y_1, \cdots, y_n)) := |\{i \mid x_i \neq y_i\}|.$$

We now assume that A^n is equipped with the Hamming metric. Then by definition a subset $C \subseteq A^n$ is called an $|A|$**-ary code**. An important case arises when we let A to be a finite field. Suppose that $q = p^m$ and $\mathbb{F}_q$ is a finite field with q elements. In this case we may put $A = \mathbb{F}_q$ and $y = (0, \cdots, 0)$. Then the **weight** of x is the Hamming length $||x|| = d(x, 0) = |\{i \mid x_i \neq 0\}|$. In particular a subset C of $\mathbb{F}_q^n$ is a code, and to it is associated two basic parameters: $k = \log_q |C|$, the **number of information bits** and $d = min\{||x - y|| \mid x, y \in C, y \neq 0\}$ the **minimum distance**. (A code with minimum distance d can correct $[\frac{d-1}{2}]$ errors.) Let

$$R = R(C) = \frac{k}{n},$$

which measures the information rate of the code, and

$$\delta = \delta(C) = \frac{d}{n},$$

which measures the error correcting ability of the code.

3.1 Basics on linear codes

If the code $C \subset \mathbb{F}_q^n$ is a vector space over $\mathbb{F}_q$ then we call C a **linear code**. The **parameters** of a linear code C are

- the **length** n,
- the **dimension** $k = \dim_{\mathbb{F}_q}(C)$,
- the minimum distance d.

Such a code is called an (n, k, d)**-code**. Let Σ_q denote the set of all $(\delta, R) \in [0,1]^2$ such that there exists a sequence C_i, $i = 1, 2, ...$, of (n_i, k_i, d_i)-codes for which $\lim_{i\to\infty} \delta_i = \delta$ and $\lim_{i\to\infty} R_i = R$.

The following theorem describes information-theoretical limits on how "good" a linear code can be.

Theorem 9 *(Manin [SS], chapter 1) There exists a continuous decreasing function*

$$\alpha_q : [0,1] \to [0,1],$$

such that

- α_q *is strictly decreasing on* $[0, \frac{q-1}{q}]$,
- $\alpha_q(0) = 1$,
- *if* $\frac{q-1}{q} \leq x \leq 1$ *then* $\alpha_q(x) = 0$,
- $\Sigma_q = \{(\delta, R) \in [0,1]^2 \mid 0 \leq R \leq \alpha_q(\delta)\}$.

Not a single value of $\alpha_q(x)$ is known for $0 < x < \frac{q-1}{q}$! It is not known whether or not the maximum value of the bound, $R = \alpha_q(\delta)$ is attained by a sequence of linear codes. It is not known whether or not $\alpha_q(x)$ is differentiable for $0 < x < \frac{q-1}{q}$, nor is it known if $\alpha_q(x)$ is convex on $0 < x < \frac{q-1}{q}$. However, the following estimate is known.

Theorem 10 *(Gilbert-Varshamov [MS], [SS] chapter 1) We have*

$$\alpha_q(x) \geq 1 - x\log_q(q-1) - x\log_q(x) - (1-x)\log_q(1-x).$$

In other words, for each fixed $\epsilon > 0$*, there exists an* (n, k, d)*-code* C *(which may depend on* ϵ*) with*

$$R(C)+\delta(C) \geq 1-\delta(C)\log_q(\frac{q-1}{q})-\delta(C)\log_q(\delta(C))-(1-\delta(C))\log_q(1-\delta(C))-\epsilon.$$

The curve $(\delta, 1 - \delta\log_q(\frac{q-1}{q}) - \delta\log_q(\delta) - (1-\delta)\log_q(1-\delta)))$ is called the **Gilbert-Varshamov curve**. This theorem says nothing about constructing codes satisfying this property! Nor was it known, until the work of Tsfasman, Valdut, Zink and Ihara, how to do so.

3.2 Some basics on Goppa codes

We begin with Goppa's basic idea boiled down to its most basic form. Let R denote a commutative ring with unit and let $m_1, m_2, ..., m_n$ denote a finite number of maximal ideals such that for each $1 \leq i \leq n$, we have $R/m_i \cong \mathbb{F}_q$. Define $\gamma : R \to \mathbb{F}_q^n$ by

$$\gamma(x) = (x + m_1, x + m_2, ..., x + m_n), \qquad x \in R.$$

Of course, in this level of generality, one cannot say much about this map. However, when R is associated to the coordinate functions of a curve defined over $\mathbb{F}_q$ then one can often use the machinery of algebraic geometry to obtain good estimates on the parameters (n, k, d) of the code associated to γ.

Let V be an irreducible smooth projective algebraic variety defined over the finite field $\mathbf{F}_q$. Let $\mathbf{F}_q(V)$ denote the field of rational functions on V. Let $\mathcal{P}(V)$ denote the set of prime divisors of V, which we may identify with the closed irreducible subvarieties of $V(\overline{\mathbf{F}_p})$ of codimension 1. For each $P \in \mathcal{P}(V)$, there is a valuation map $ord_P : \mathbf{F}_q(V) \to \mathbf{Z}$ (see Hartshorne [Ha], §II.6, page 130). Let $\mathcal{D}(V)$ denote the group of divisors of V, the free abelian group generated by $\mathcal{P}(V)$.

If $A = \sum_P a_P P, B = \sum_P b_P P \in \mathcal{D}(V)$ are divisors then we say $A \leq B$ if and only if $a_P \leq b_P$ for all $P \in \mathcal{P}(V)$. If $f \in \mathbf{F}_q(V)$ is a non-zero function then let

$$(f) = \sum_{P \in \mathcal{P}(V)} ord_P(f) P,$$

where $ord_P(f)$ is the order of the zero (pole) at P (as above). This is well-defined (since the above sum is finite by Lemma 6.1 in [Ha], §II.6, page 131). For $B \in \mathcal{D}(V)$, define $\mathcal{L}(B)$ to be the vector space

$$\mathcal{L}(B) = \{0\} \cup \{f \in \mathbf{F}_q(V) \mid f \neq 0, (f) \geq -B\}.$$

Pick n different points $P_1, P_2, ..., P_n$ in $V(\mathbf{F}_q)$ and choose a divisor $A = \sum_{P \in \mathcal{P}(V)} a_P P \in \mathcal{D}(V)$ disjoint from these points. Quite often, one does *not* want A to be rational. The **Goppa code** associated to $(V(\mathbf{F}_q), A)$ is the linear code $G = G(A, \{P_i\}, V)$ defined to be the subspace of $\mathbf{F}_q^n$ which is the image of the map

$$\gamma : \mathcal{L}(A) \to \mathbf{F}_q^n, \tag{5}$$

defined by $\gamma(f) = (f(P_1), ..., f(P_n))$. (In the case of curves, this code is called the **dual Goppa code** or **Goppa function code** in [P]. Goppa gave another geometric construction of codes using differentials for which we refer the reader to [P] or [TV].)

To specify a Goppa code, one must

- choose a smooth variety V over $\mathbf{F}_q$,
- pick rational points $P_1, P_2, ..., P_n$ of V,
- choose a divisor A disjoint from the P_i's,
- determine a basis for $\mathcal{L}(A)$,
- compute the matrix for γ.

3.3 Some estimates on Goppa codes

Let g be the genus of a curve $V = C$ and let $G = G(A, P, C)$ denote the Goppa code as constructed above. If G has parameters (n, k, d) and if we then the following lemma is a consequence of the Riemann-Roch theorem.

Lemma 11 *Assume G is as above and A satisfies $2g - 2 < deg(A) < n$. Then $k = dim(G) = deg(A) - g + 1$ and $d \geq n - deg(A)$.*

Consequently, $k + d \geq n - g + 1$. Because of Singleton's inequality[7], we have

- if $g = 0$ then G is an MDS code,
- if $g = 1$ then $n \leq k + d \leq n + 1$.

The previous lemma also implies the following lower bound.

Proposition 12 *([SS] §3.1, or [TV]) With G as in the previous lemma, we have $\delta + R = \frac{d}{n} + \frac{k}{n} \geq 1 - \frac{g-1}{n}$.*

[7]It is known that $n \geq d + k - 1$ for any linear (n, k, d)-code (this is the **Singleton inequality**), with equality if and only if the code is a so-called **MDS code** (MDS=minimum distance separable).

Theorem 8 above is an explicit formula for the genus of the modular curve $X_0(N)$. It may be instructive to plug this formula into the estimate in Proposition 12 to see what we get. The formula for the genus g_N of $X_0(N)$ is relatively complicated, but simplifies greatly when N is a prime number which is congruent to 1 modulo 12, say $N = 1 + 12m$, in which case $g_N = m - 1$. For example, $g_{13} = 0$. In particular, we have the following

Corollary 13 *Let $C = X_0(N)$, where N is a prime number which is congruent to 1 modulo 12 and which has the property that C is smooth over $\mathbb{F}_q$. Then the parameters (n, k, d) of a Goppa code associated to C must satisfy*

$$\frac{d}{n} + \frac{k}{n} \geq 1 - \frac{\frac{N-1}{12} - 2}{n}.$$

Based on the above Proposition, if one considers a family of curves X_i with increasing genus g_i such that

$$\lim_{i \to \infty} \frac{|X_i(\mathbb{F}_q)|}{g_i} = \alpha \tag{6}$$

one can construct a family of codes C_i with $\delta(C_i) + R(C_i) \geq 1 - \frac{1}{\alpha}$. It is known that $\alpha \leq \sqrt{q} - 1$ (this is the so-called **Drinfeld-Vladut bound**, [TV], Theorem 2.3.22).

The following result says that the Drinfeld-Vladut bound can be attained in case $q = p^2$.

Theorem 14 *(Tsfasman, Valdut, Zink [TV], Theorem 4.1.52) Let g_N denote the genus of $X_0(N)$. If N runs over a set of primes different than p then the quotients $g_N/|X_0(N)(\mathbb{F}_{p^2})|$ associated to the modular curves $X_0(N)$ tend to the limit $\frac{1}{p-1}$.*

More generally, if $q = p^{2k}$, then there is a family of Drinfeld curves X_i over $\mathbb{F}_q$ yielding $\alpha = \sqrt{q} - 1$ ([TV], Theorem 4.2.38, discovered independently by Ihara [I] at about the same time). In other words, the Drinfeld-Vladut bound is attained in case $q = p^{2k}$.

As a corollary to the above theorem, if $p \geq 7$ then there exists a sequence of Goppa codes G_N over $\mathbb{F}_{p^2}$ associated to a sequence of modular curves $X_0(N)$ for which $(R(G_N), \delta(G_N))$ eventually (for suitable large N) lies above

the Gilbert-Varshamov bound in Theorem 10. This follows from comparing the Gilbert-Varshamov curve

$$(\delta, 1 - \delta \log_q(\frac{q-1}{q}) - \delta \log_q(\delta) - (1-\delta)\log_q(1-\delta)))$$

with the curve $(\delta, \frac{1}{\sqrt{q}-1})$, $q = p^2$.

4 Examples

Example 15 *Let C denote the elliptic curve of conductor 32 (and birational to $X_0(32)$) with Weierstrass form $y^2 = x^3 - x$. If p is a prime satisfying $p \equiv 3 (\mathrm{mod}\, 4)$ then*

$$|C(\mathbf{F}_p)| = p + 1$$

(Theorem 5, §18.4 in Ireland and Rosen [IR]). Let $C(\mathbf{F}_p) = \{P_0, P_1, P_2, ..., P_n\}$, where P_0 is the identity, and if $A = kP_0$, for some $k > 0$. The parameters of the corresponding code $G = G(A, P, C)$ satisfy $n = p$, $d + k \geq n$, since $g = 1$, by the above Proposition. In this case, G is not an MDS code. As we observed above, a Goppa code constructed from an elliptic curve satisfies either $d + k - 1 = n$ (i.e., is MDS) or else $d + k = n$. Thus in this case,

$$n = p, \qquad d + k = p.$$

Let C be an elliptic curve. This is a projective curve for which $C(\mathbf{F}_q)$ has the structure of an algebraic group. Let $P_0 \in C(\mathbf{F}_q)$ denote the identity. Let $P_1, P_2, ..., P_n$ denote *all* the other elements of $C(\mathbf{F}_q)$ and let $A = aP_0$, where $0 < a < n$ is an integer. The following result is an immediate corollary of the results in [Sh] (see also §5.2.2 in [TV] for weaker but closely related results).

Theorem 16 *(Shokrollahi) Let $C, P_0, P_1, ..., P_n, D, A$, be as above.*

- *If $a = 2$ and $C(\mathbf{F}_q) \cong C_2 \times C_2$ (where C_n denotes the cyclic group of order n) then the code $G(A, D)$ is a $[n, k, d]$-code (n is the length, k is the dimension, and d is the minimum distance) with*

$$d = n - k + 1, \quad \text{and} \quad k = a.$$

- *Assume* $gcd(n, a!) = 1$. *If* $a \neq 2$ *or* $C(\mathbf{F}_q)$ *is not isomorphic to the Klein four group* $C_2 \times C_2$ *then* $G(A, D)$ *is a* $[n, k, d]$*-code (*n *is the length,* k *is the dimension, and* d *is the minimum distance) with*

$$k = a$$

and weight enumerator polynomial (see for example [MS] for the definition)

$$W_G(x) = x^n + \sum_{i=0}^{a-1} \left(\begin{array}{c} n \\ i \end{array} \right) (q^{a-1} - 1)(x-1)^i + B_a(x-1)^a,$$

where

$$B_a = \frac{1}{n}(q-1)(\left(\begin{array}{c} n-1 \\ a \end{array} \right) + (-1)^a(n-1)).$$

4.1 Weight enumerators (aprés des Shokrollahi)

In the case where E is given by the level 19, discriminant -19 Weierstrass model

$$y^2 + y = x^3 + x^2 + x,$$

and $p = 13$, we have

$$E(\mathbf{F}_p) = \begin{array}{l} \{[0,0], [0,12], [1,6], [3,0], [3,12], [4,2], [4,10], [5,3], [5,9], \\ [8,3], [8,9], [9,0], [9,12], [11,4], [11,8], [12,3], [12,9], \infty\} \end{array}.$$

Write $E(\mathbf{F}_p) = \{P_0, P_1, ..., P_{17}\}$, where P_0 denotes the identity element of the group law for E, let $A = kP_0$, and let $D = P_1 + ... + P_{17}$. The hypotheses of the above theorem are satisfied when we take $n = 17$ and $2 \leq k = a < 17$. The above construction associates to this data a Goppa code $G = G(A, D, E)$ which is a 7-error correcting code of length $n = 17$ over $\mathbf{F}_{13}$. Some of the weight enumerator polynomials W_G and the number of errors these codes G can correct are given in the following table.

$a = k$	weight enumerator W_G	number of errors G corrects
2	$x^{17} + 96x^2 + 12x + 60$	7
3	$x^{17} + 384x^3 + 480x^2 + 744x + 588$	6
4	$x^{17} + 1296x^4 + 2976x^3 + 6144x^2 + 10932x + 7212$	6
5	$x^{17} + 3072x^5 + 13200x^4 + ... + 95676$	5
6	$x^{17} + 5664x^6 + 40272x^5 + ... + 1236972$	5
7	$x^{17} + 8064x^7 + 92064x^6 + ... + 16095036$	4
8	$x^{17} + 9096x^8 + 160608x^7 + ... + 209212116$	4
9	$x^{17} + 8064x^9 + 219144x^8 + ... + 2719785636$	3
10	$x^{17} + 5664x^{10} + 235080x^9 + ... + 35357186484$	3

These were computed using a computer implementation of Shokrollahi's formula in the software package MAPLE. The number of codewords of minimum weight $n - k$ is the coefficient of the second highest term in $W_G(x)$. For example, when $k = 3$ the number of codewords of minimum weight $n - k = 14$ is 384.

A smaller example using the same elliptic curve E as above: taking $p = 3$, we find that

$$E(\mathbf{F}_p) = \{[0, 0], [0, 2], [1, 0], [1, 2], [2, 1], \infty\}.$$

The hypotheses of the above theorem are satisfied when we take $n = 5$ and $2 \leq k = a < 5$. The weight enumerator when $a = 2$ is

$$W_G(x) = x^5 + 4x^2 + 2x + 2,$$

and there are 4 codewords of minimum weight 3 in the corresponding elliptic (Goppa) code. This is a 1-error correcting code of length 5 (over $\mathbf{F}_3$).

4.2 The generator matrix (aprés des Goppa)

The method used in Goppa's Fermat cubic code example of [G], pages 108-109, can be easily modified to yield analogous quantities for certain elliptic Goppa codes.

Example 17 *Let E denote the elliptic curve (of conductor $N = 11$) which we write in homogeneous coordinates as*

$$y^2z + yz^2 = x^3 - x^2z.$$

Let $\phi(x,y,z) = xy + yz + xz$, let F denote the projective curve defined by $\phi(x,y,z) = 0$, and let D denote the divisor obtained by intersecting E and F. By Bezout's theorem (see for example, [G], page 80), D is of degree 6. To find the matrix of the linear transformation γ in (5), we must specify a basis for $\mathcal{L}(D)$. As in [G] page 109, a basis for $\mathcal{L}(D)$ is provided by the functions in the set

$$\mathcal{B}_D = \{1, x^2/\phi(x,y,z), y^2/\phi(x,y,z), z^2/\phi(x,y,z), xy/\phi(x,y,z), yz/\phi(x,y,z)\}.$$

(This is due to the fact that dim $\mathcal{L}(D) = \deg(D) = 6$ and the functions $f \in \mathcal{B}_D$ "obviously" satisfy $(f) \geq -D$.) We have

$$E(\mathbf{F}_{11}) = \begin{array}{c}\{[0,0,1],[0,1,0],[0,1,1],[1,1,1],[1,3,2],[1,5,3],[1,8,3],\\ [1,8,6],[1,9,2],[1,9,8],[1,10,1],[1,10,10]\}\end{array},$$

which we write as P_1, P_2, ..., P_{10}. For comparison,

$$E(\mathbf{F}_{11}) \cap \mathbf{P}^2(\mathbf{F}_{11})_{z=1} = \begin{array}{c}\{[0,0],[0,1],[1,1],[1,10],[2,5],[4,9],\\ [4,10],[6,7],[6,10],[7,8],[10,1],\infty\},\end{array}$$

where $\mathbf{P}^2(\mathbf{F}_{11})_{z=1}$ denotes the affine patch of projective 2-space with $z = 1$. Consider the matrix

$$G = \begin{bmatrix} 0 & 4 & 1 & 6 & 8 & 8 & 1 & 10 & 10 \\ 1 & 4 & 3 & 10 & 6 & 10 & 4 & 10 & 10 \\ 1 & 4 & 9 & 10 & 2 & 10 & 9 & 10 & 10 \\ 0 & 4 & 5 & 4 & 9 & 6 & 9 & 1 & 1 \\ 1 & 4 & 4 & 1 & 10 & 1 & 6 & 1 & 10 \\ 0 & 4 & 3 & 7 & 4 & 5 & 8 & 10 & 1 \end{bmatrix}.$$

The first row of G gives the values of $x^2/\phi(x,y,z)$ at $\{P_i \mid 1 \leq i \leq 10,\ \phi(P_i) \neq 0\} = \{P_3, P_4, P_6, P_7, ..., P_{12}\}$ (in other words, we simply throw out all the rational prime divisors corresponding to a pole of ϕ). The other rows are obtained similarly from the other functions corresponding to the basis elements of $\mathcal{L}(D)$: $y^2/\phi(x,y,z)$, $z^2/\phi(x,y,z)$, $xy/\phi(x,y,z)$, $yz/\phi(x,y,z)$. Performing

Gauss reduction mod 11 puts this in canonical form:

$$G' = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 2 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 5 \\ 0 & 0 & 1 & 0 & 0 & 0 & 2 & 0 & 6 \\ 0 & 0 & 0 & 1 & 0 & 0 & 6 & 6 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 5 \end{bmatrix},$$

so this code has minimum distance 2*, hence is only* 1*-error detecting. The corresponding check matrix is*

$$H = \begin{bmatrix} -1 & -1 & -2 & -6 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & -6 & 0 & -2 & 0 & 1 & 0 \\ -2 & -5 & -6 & -2 & -2 & -5 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 6 & 6 & 5 & 1 & 0 & 6 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 5 & 0 & 1 & 0 \\ 5 & 2 & 1 & 5 & 5 & 2 & 0 & 0 & 1 \end{bmatrix}.$$

Example 18 *Let E denote the elliptic curve (of conductor $N = 19$) which we write in homogeneous coordinates as*

$$y^2z + yz^2 = x^3 + x^2z + xz^2$$

Let $\phi(x, y, z) = x^2 + y^2 + z^2$, let F denote the projective curve defined by $\phi(x, y, z) = 0$, and let D denote the divisor obtained by intersecting E and F. By Bezout's theorem, D is of degree 6*. As in the previous example, a basis for $\mathcal{L}(D)$ is provided by the functions in the set*

$$\mathcal{B}_D = \{1, x^2/\phi(x, y, z), y^2/\phi(x, y, z), z^2/\phi(x, y, z), xy/\phi(x, y, z), yz/\phi(x, y, z)\}.$$

(Again, this is due to the fact that dim $\mathcal{L}(D) = \deg(D) = 6$ and the functions $f \in \mathcal{B}_D$ "obviously" satisfy $(f) \geq -D$.) We have

$$E(\mathbf{F}_7) = \begin{array}{c} \{\ [0,0,1], [0,1,0], [0,1,6], [1,0,2], [1,0,4], \\ [1,3,4], [1,3,6], [1,5,2], [1,5,6]\ \} \end{array},$$

which we write as P_1, P_2, ..., P_9. *Consider the matrix*

$$G = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 2 & 2 & 4 & 4 \\ 1 & 0 & 1 & 4 & 2 & 2 & 1 & 4 & 1 \\ 0 & 0 & 0 & 0 & 0 & 3 & 3 & 5 & 5 \\ 0 & 0 & 6 & 0 & 0 & 5 & 4 & 3 & 2 \\ 0 & 0 & 0 & 2 & 4 & 4 & 6 & 2 & 6 \end{bmatrix}.$$

The first row of G *gives the values of* $x^2/\phi(x,y,z)$ *at* $\{P_i \mid 1 \leq i \leq 9\}$. *The other rows are obtained similarly from the other functions corresponding to the basis elements of* $\mathcal{L}(D)$: $y^2/\phi(x,y,z)$, $z^2/\phi(x,y,z)$, $xy/\phi(x,y,z)$, $yz/\phi(x,y,z)$. *Performing Gauss reduction mod 7 puts this in canonical form:*

$$G' = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 4 \\ 0 & 1 & 0 & 0 & 0 & 0 & 6 & 0 & 6 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 3 & 4 \\ 0 & 0 & 0 & 1 & 0 & 0 & 6 & 1 & 6 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 3 & 5 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 4 & 4 \end{bmatrix},$$

so this code also has minimum distance 3, *hence is only* 1*-error correcting. The corresponding check matrix is*

$$H = \begin{bmatrix} 0 & -6 & -1 & -6 & -1 & -1 & 1 & 0 & 0 \\ -4 & 0 & -3 & -1 & -3 & -4 & 0 & 1 & 0 \\ -4 & -6 & -4 & -6 & -5 & -4 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 6 & 1 & 6 & 6 & 1 & 0 & 0 \\ 3 & 0 & 4 & 6 & 4 & 3 & 0 & 1 & 0 \\ 3 & 1 & 3 & 1 & 2 & 3 & 0 & 0 & 1 \end{bmatrix}.$$

For an example of the generating matrix of one-point elliptic codes associated to $x^3 + y^3 = 1$ over $\mathbb{F}_4$ has been worked out in several places (for example, see Goppa's book mentioned above, or the books [SS], §3.3, [P], SS5.3, 5.4, 5.7, or [M], §5.7.3).

5 Concluding comments

We end this note by making some comments:

(1) The algebraic geometric relation between the number of points over a finite field for a variety is related to the Betti numbers. However, an equivalent notion of genus for higher dimensional varieties is the "arithmetic genus". Can one develop a relation between the number of points over finite fields of a variety andits arithmetic genus, useful in coding theory?

(2) Can one construct "good" codes associated to the higher dimensional Shimura varieties?

Acknowledgements The first-named author is very grateful to both Pablo Legarraga and Will Traves for very useful and informative discussions. The second author wishes to thank the hospitalities and the financial supports of the Max-Planck Institut für Mathematik (Bonn) while he was involved with this paper. We also thank Amin Shokrollahi for helpful suggestions.

References

[B] B. J. Birch, *Some calculations of modular relations*, in **Modular forms of one variable, I**, (W. Kuyk, ed.) Proc. Antwerp Conf. 1972, Springer Lecture Notes in Math., 320, Springer-Verlag, NY, 1973.

[BK] B. J. Birch and W. Kuyk (eds), **Modular forms of one variable, IV**, Proc. Antwerp Conf. 1972, Springer Lecture Notes in Math., 476, Springer-Verlag, NY, 1975.

[BBGLMS] J.-F. Boutot, L. Breen, P. Gŕardin, J. Giraud, J.-P. Labesse, J. S. Milne, C. Soulé, **Variétés de Shimura et fonctions** L Publications Mathématiques de l'Université Paris VII [Mathematical Publications of the University of Paris VII], 6. Universite de Paris VII, U.E.R. de Mathematiques, Paris, 1979.

[Cas1] W. Casselman. *On representations of* GL_2 *and the arithmetic of modular curves*, in **Modular functions of one variable, II** (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pp. 107–141. Lecture Notes in Math., Vol. 349, Springer, Berlin, 1973.

(**Correction to: "On representations of** GL_2 **and the arithmetic of modular curves"**, in **Modular functions of one variable, IV** (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pp. 148–149. Lecture Notes in Math., Vol. 476, Springer, Berlin, 1975.)

[Cas2] ——, *The Hasse-Weil ζ-function of some moduli varieties of dimension greater than one*, in **Automorphic forms, representations and L-functions** (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, pp. 141–163, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 1979.

[Cl] L. Clozel, *Nombre de points des variétés de Shimura sur un corps fini (d'aprés R. Kottwitz)*, Seminaire Bourbaki, Vol. 1992/93. Asterisque No. 216 (1993), Exp. No. 766, 4, 121–149.

[Co] P. Cohen, *On the coefficients of the transformation polynomials for the elliptic modular function*, Math. Proc. Cambridge Philos. Soc. 95 (1984), 389–402.

[Del] P. Deligne, *Variétés de Shimura*. In **Automorphic Forms, Representations and L-functions**, Proc. Sympos. Pure Math. 33, part 2, (1979), 247-290.

[DL] M. Duflo and J.-P. Labesse, *Sur la formule des traces de Selberg*, Ann. Sci. Ecole Norm. Sup. (4) 4 (1971), 193–284.

[Ei] M. Eichler, *The basis problem for modular forms and the traces of Hecke operators*, in **Modular functions of one variable, I** (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pp. 1–36. Lecture Notes in Math., Vol. 320, Springer, Berlin, 1973.

[E] N. Elkies, *Elliptic and modular curves over finite fields and related computational issues*, in **Computational perspectives on number theory**, (ed. D. Buell, J. Teitelbaum), AMS/IP Studies in Adv. Math., 7, 1998, 21–76.

[FM] G. Frey and M. Müller, *Arithmetic of modular curves and applications*, preprint, 1998, available at `http://www.exp-math.uni-essen.de/zahlentheorie/preprints/Index.html`

[Gel] S. Gelbart, *Elliptic curves and automorphic representations*, Advances in Math. 21 (1976), no. 3, 235–292.

[G] V. D. Goppa, **Geometry and codes**, Kluwer, 1988.

[Ha] R. Hartshorne, **Algebraic geometry**, Springer-Verlag, 1977.

[HM] T. Hibino and N. Murabayashi, *Modular equations of hyperelliptic $X_0(N)$ and an application*, Acta Arithmetica 82 (1997)279-291.

[Ig] J. Igusa, *On the transformation theory of elliptic functions*, Amer. J. Math. 81 (1959)436–452.

[I] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Univ. Tokyo, 28 (1981)721–724.

[IR] K. Ireland and M. Rosen, **A classical introduction to modern number theory**, Grad Texts 84, Springer, 1982.

[Kn] A. Knapp, **Elliptic curves**, Mathematical Notes, Princeton Univ. Press, 1992.

[Ko] N. Koblitz, **Introduction to elliptic curves and modular forms**, Grad. Texts 97, Springer, 1984.

[K1] R. Kottwitz, *Shimura varieties and λ-adic representations*, In **Automorphic Forms, Shimura Varieties, and L-functions, Vol. 1**, Academic Press (1990), 161-209.

[K2] R. Kottwitz, *Points on Shimura varieties over finite fields*, Journal of A. M. S. 5 (1992), 373-444.

[Lab] J.P. Labesse, *Exposé VI*, in [BBGLMS].

[Lan1] R.P. Langlands, *Shimura varieties and the Selberg trace formula*, Can. J. Math. Vol. XXIX, No. 5 (1977), 1292-1299.

[Lan2] R.P. Langlands, *On the zeta function of some simple Shimura varieties*, Can. J. Math. Vol. XXXI, No. 6 (1979), 1121-1216.

[LvdG] J. Lint and G. van der Geer, **Introduction to coding theory and algebraic geometry**, Birkhäuser, Boston, 1988.

[MS] F. MacWilliams and N. Sloane, **The theory of error-correcting codes**, North-Holland, 1977.

[M] C. Moreno, **Algebraic curves over finite fields: exponential sums and coding theory**, Cambrdge Univ. Press, 1994.

[Nara] R. Narasimhan, **Complex analysis of one variable**, Basel, 1985.

[O1] A. Ogg, *Elliptic curves with wild ramification*, Amer. J. Math. 89(1967)1-21.

[O2] A. Ogg, **Modular forms and Dirichlet series**, Benjamin, 1969 (see also his paper in **Modular functions of one variable, I** (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pp. 1–36. Lecture Notes in Math., Vol. 320, Springer, Berlin, 1973.)

[P] O. Pretzel, **Codes and algebraic curves**, Oxford Lecture Series, vol 9, Clarendon Press, Oxford, 1998.

[R] J. G. Rovira, *Equations of hyperelliptic modular curves*, Ann. Inst. Fourier, Grenoble 41 (1991)779-795.

[Shim] G. Shimura, **Introduction to the arithmetic theory of automorphic functions**, Iwanami Shoten and Princeton University Press, 1971.

[ShimM] M. Shimura, *Defining equations of modular curves*, Tokyo J. Math. 18 (1995)443-456.

[Sh] M. A. Shokrollahi, *Kapitel 9* of **Beitraege zur algebraischen Codierungs- und Komplexitaetstheorie mittels algebraischer Funkionenkoerper**, Bayreuther mathematische Schriften, volume 30, pp. 1-236, 1991.

[S] S. Shokranian, **The Selberg-Arthur trace formula**, Springer-Verlag, Lecture Note Series 1503, 1992.

[SS] S. Shokranian and M.A. Shokrollahi, **Coding theory and bilinear complexity**, Scientific Series of the International Bureau, KFA Jülich Vol. 21, 1994.

[TV] M. A. Tsfasman and S. G. Vladut, **Algebraic-geometric codes**, Mathematics and its Applications, Kluwer Academic Publishers, Dordrechet 1991.

David Joyner
Mathematics Department
U.S. Naval Academy

Annapolis, MD 21402
wdj@gwmail.usna.edu

Salahoddin Shokranian
Departamento de Matemática
Universidade de Brasília
70910-900 Brasília- DF.
Brasil
sash@Ipe.mat.unb.br

and

Max-Planck Institut für Matehamtik
Vivatsgasse 7
53111 Bonn- Germany