Mordell-Weil lattices in characteristic 2
I: Construction and first properties

Noam D. Elkies

Introduction. In a famous 1967 paper [Š-T] Šafarevič and Tate constructed elliptic curves of arbitrarily large rank r over function fields of positive characteristic. The group of rational points of such a curve yields a lattice in Euclidean space of dimension r via the canonical Néron-Tate height. It seems natural to investigate the structure of this lattice, but curiously it was not until about 1990 that such lattices were examined in earnest. Shioda [Sh2] then found, as part of his analysis of the Néron-Severi groups of Fermat surfaces, a family of elliptic curves in characteristic $\equiv 5 \bmod 6$ similar to those of [Š-T] whose associated lattices produce sphere packings that improve on the previous density records for many r in the range $80 \leq r \lesssim 1000$. At about the same time I found three such families with similar sphere-packing properties for large r, one of which turned out to be identical with Shioda's. The other two families are in characteristic 2 and 3, and their lattices also recover previously known records in "small" dimensions $r \leq 32$ in addition to improving records for larger r. Further investigation revealed that these curves also provide fascinating examples and test cases for the arithmetic of elliptic curves over function fields.

This paper is the first of a series devoted to the characteristic-2 family. (Oesterlé had already reported on it briefly in [Oe].) We begin with a quick summary of lattices in Euclidean space and the associated sphere packings. We then introduce a family of hyperelliptic curves in characteristic 2, and use them to construct potentially constant elliptic curves of high rank analogous to those of [Š-T] in odd characteristic. By investigating the arithmetic of these curves we deduce lower bounds on the sphere-packing densities of their Mordell-Weil lattices and compare these to the records listed in [C-S]. Finally we interpret the equality condition on our lower bound in terms of a descent on the elliptic curve, and work out this descent explicitly enough to describe in some detail the 64-dimensional lattice which is the first one in our family to give a new record. Along the way we announce a few results whose proofs we defer to later papers of this series: some claims regarding isometries acting on our lattices, comparisons between these lattices in dimensions ≤ 32 and previously known lattices of the same dimensions, and most notably the rapid growth of $|Ш|$ for large r. With these exceptions, this paper is self-contained, in the sense that each new result asserted is proved, sometimes in more than one way.

Acknowledgements. John Conway and Neil Sloane's great treatise [C-S] introduced me to the sphere-packing problem; Michael Tsfasman's beautiful talk [Ts] on arithmetic constructions of lattices at the Journées Arithmétiques of 1989 gave the immediate impetus to look again at the Mordell-Weil lattices

of potentially constant curves, which I had idly considered some years earlier after reading [Š-T] but abandoned for lack of technical and computational tools; and Benedict Gross encouraged me to pursue these lattices further even when I found that the density bounds (see Thm. 1 below) were bad as $r \to \infty$. I would likely have never got my work on Mordell-Weil lattices off the ground without these three sources of inspiration. I am also grateful to Gross, as well as Tetsuji Shioda, for much valuable conversation and correspondence on these matters, and to J.-P. Serre for first writing me of Shioda's work and putting me in contact with him.

This work was made possible in part by funding from the Harvard Society of Fellows, the National Science Foundation, and the Packard Foundation.

Lattices and sphere packings. We very briefly review the ideas we need from [C-S, Ch.1]. We can take a *lattice* to be a finitely generated free abelian group $L \cong \mathbf{Z}^r$ equipped with a quadratic form $\|\cdot\| : L \to \mathbf{R}$ whose extension to $L \otimes \mathbf{R}$ is positive definite. This quadratic form identifies $L \otimes \mathbf{R}$ with r-dimensional Euclidean space $\mathbf{R}^r$ and L with a discrete co-compact subgroup of $\mathbf{R}^r$ whose covolume is the positive square root of the *discriminant* Δ of the bilinear form

$$\langle \cdot, \cdot \rangle : (v, v') \mapsto \frac{1}{2}(\|v + v'\| - \|v\| - \|v'\|) \tag{1}$$

on L associated to the quadratic form $\|\cdot\|$. The lattice (or the quadratic form) is said to be *integral* if $\langle v, v' \rangle \in \mathbf{Z}$ for all $v, v' \in L$, and *even* if $\|v\|$ is an even integer for all $v \in L$ (such L must be integral, by (1)).

The *packing radius* ρ of a lattice L is the radius of the largest open ball whose translates by L do not overlap, giving rise to a "sphere packing" (actually a packing of congruent balls) in $\mathbf{R}^r$. This radius is half the square root of the "minimal norm" (more properly, minimal nonzero norm) of L. The balls centered at the lattice vectors with this norm $N_{\min} = 4\rho^2$ are disjoint and tangent to the ball about the origin; thus the number of minimal vectors is called the *kissing number* of the lattice.

We adopt the following terminology from [C-S] for measuring the density of a (not necessarily lattice) packing of congruent balls of radius ρ in $\mathbf{R}^r$. The *center density* is the average number of balls per unit volume, which for a lattice packing is just $\Delta^{-1/2}$, the inverse of the covolume. To obtain the *packing density* we multiply this by the volume $V_r \rho^r$ of the balls being packed, where $V_r = \pi^{r/2}/\Gamma(r/2+1)$ is the volume of a unit ball in $\mathbf{R}^r$. We eliminate the factors of π by introducing the *normalized center density* δ, defined as the center density multiplied by ρ^r or equivalently the packing density divided by V_r, and (unlike the center density) invariant under scaling. For a lattice L as above we have

$$\delta = \delta(L) = \Delta^{-1/2}(N_{\min}/4)^{r/2}. \tag{2}$$

Thus a lower bound on $N_{\min}$ and an upper bound on Δ will guarantee a high density. For lattices in higher dimensions given by coordinates or matrices as in [C-S] it is easy to find Δ but often hard, and probably computationally intractable, to determine or even reasonably estimate $N_{\min}$. Curiously for the Mordell-Weil lattices that Shioda and we construct it is Δ that is hardest to evaluate, while the minimal norm can be even simpler to determine than the rank r !

A hyperelliptic curve. Fix a positive integer n, let $q = 2^n$, and let k be the finite field of q^2 elements. Then there exists a supersingular elliptic curve E_0/k with trace $-2q$, that is, with Frobenius endomorphism equal to multiplication by $-q$; indeed for n odd we can and will take E_0 to have Weierstrass form

$$E_0 : Y^2 + Y = X^3, \tag{3}$$

and for n even we take the quadratic twist

$$E_0 : Y^2 + Y = X^3 + a_6 \tag{4}$$

where $a_6 \in k$ is chosen so that its trace from k to the prime field $\mathbf{Z}/2\mathbf{Z}$ is 1. Let C/k be the hyperelliptic curve with affine model

$$C : u^2 + u = t^{q+1}. \tag{5}$$

This curve has genus $g = q/2$, its regular differentials being $P(t)\,dt$ with $P \in k[t]$ a polynomial of degree $< g$; the hyperelliptic involution of C is

$$\iota : (t, u) \mapsto (t, u + 1). \tag{6}$$

We then have:

Proposition 1. *The curve C has $q^2 + 2gq + 1 = 2q^2 + 1$ rational points over k, and its Jacobian* $\mathrm{Jac}(C)$ *is isogenous with E_0^g.*

Proof: To count rational points, note that $t \mapsto t^{q+1}$ is the norm map from k to its quadratic subfield; thus for all $t \in k$, the element t^{q+1} of that subfield can be written as $u^2 + u$ for some two distinct $u \in k$. Thus C has $2|k| = 2q^2$ finite k-rational points, to which we add the single point at infinity p_∞ to obtain $2q^2 + 1$ as claimed. Since this number is also $q^2 + 2gq + 1$, the maximum allowed by the Weil estimate, all the eigenvalues of the Frobenius endomorphism of $\mathrm{Jac}(C)$ are $-q$. Since the abelian variety E_0^g of dimension g also has all its eigenvalues of Frobenius equal $-q$, it follows from Tate's theorem [Ta2] that $\mathrm{Jac}(C)$ and E_0^g are isogenous. $\square$

Remarks: i) This Proposition can also be proved by noting that C is a quotient of the curve $u^q + u = t^{q+1}$, which is isomorphic to the Fermat curve F_{q+1}. Since it is known (again by counting points and applying the Weil estimate) that $\mathrm{Jac}(F_{q+1})$ is isogenous with a power of E_0, it follows that this must also be true for $\mathrm{Jac}(C)$. Still another approach is to exhibit, for generic $p : (t, u) = (t_0, u_0)$ on C, an explicit rational function on C whose divisor is $q(p) + (p^{q^2}) - (q+1)(p_\infty)$, namely the function

$$\sum_{m=0}^{n-1} (t_0^q t)^{2^m} + u + u_0^q, \tag{7}$$

which yields a direct, albeit ad-hoc, proof that the Frobenius map $p \mapsto p^{q^2}$ on C multiplies divisors of degree zero by $-q$ modulo linear equivalence.

ii) As is true for F_{q+1}, once $q > 2$ our curve has many more automorphisms than the $84(g-1)$ allowed for a curve of genus g in characteristic zero. Indeed, for each of the $2q^3 + 2q^2$ ways to choose $a, b, c \in k$ such that

$$a^{q+1} = 1, \;\; c^2 + c = b^{q+1} \tag{8}$$

we have an automorphism

$$(t, u) \mapsto (a(t+b), u + \sum_{m=0}^{n-1} (b^q t)^{2^m} + c) \tag{9}$$

of C. (This uses implicitly the identity $b^{q^2} = b$ for $b \in k$.) The normal subgroup of $2q^2$ automorphisms with $a = 1$ is an extraspecial 2-group 2_-^{1+2n} whose non-trivial central element is the hyperelliptic involution ι. Thus its representation on $T_l(\mathrm{Jac}(C)) \otimes \mathbf{Q}_l$ is the unique irreducible representation of dimension $2g = q$. Note that since the Frobenius endomorphism commutes with all these automorphisms we get by Schur's lemma an alternative proof of the fact that Frobenius acts on $\mathrm{Jac}(C)$ by some scalar multiplication. Van der Geer and van der Vlugt investigate in [G-V] a family of hyperelliptic curves in characteristic 2 which, like C, have genus 2^{n-1} and automorphisms by this extraspecial 2-group; much of our discussion of C/k will also apply with little change to these curves over the field of definition of their automorphism groups.

iii) For any factor f of $q+1$, the hyperelliptic curve $u^2 + u = t^f$ of genus $g' = (f-1)/2$ is a quotient of C and thus has Jacobian isogenous with $E_0^{g'}$. Thus such curves can also be used to produce Mordell-Weil lattices. In general the lattices obtained from these curves associated with proper factors of $q+1$ are not as good as those coming from C itself, but the factor $f = 13$ of $2^6 + 1 = 65$ turns out to yield a lattice homothetic with the Leech lattice of rank 24.

iv) Note that when $n = 1$ the "hyperelliptic" curve C becomes the supersingular elliptic curve E_0, and (9) gives its 24 automorphisms.

A potentially constant elliptic curve. Let L be the commutative group $\mathrm{Hom}_k(\mathrm{Jac}(C), E_0)$. Since $\mathrm{Jac}(C)$ is isogenous with E_0^g, this group has the same rank as $\mathrm{Hom}_k(E_0^g, E_0) = (\mathrm{End}_k(E_0))^g$. Now E_0 is supersingular, so its group of $\bar{k}$-endomorphisms has rank 4, and all these endomorphisms are defined over k because they commute with the Frobenius endomorphism (which is just the scalar $-q$). We conclude that the rank of $(\mathrm{End}_k(E_0))^g$, and thus also of $\mathrm{Hom}_k(\mathrm{Jac}(C), E_0)$, is

$$r = 4g = 2q = 2^{n+1}. \tag{10}$$

We next identify L with the k-rational maps $f : C \to E_0$ taking p_∞ to the origin $\mathbf{0}$ of E_0. The embedding of C into $\mathrm{Jac}(C)$ taking any $p \in C$ to the class of the divisor $(p) - (p_\infty)$ lets us restrict any homomorphism from

$\mathrm{Jac}(C)$ to E_0 to a map $f : C \to E_0$ with $f(p_\infty) = 0$. To go the other way we can use the group law on E_0 to extend any map $f : C \to E_0$ to a function $f_+ : \mathrm{Div}(C) \to E_0$, which must satisfy $f_+(D) = f_+(D')$ for any pair of linearly equivalent divisors D, D'; the restriction of f_+ to the degree-zero divisors then descends to a homomorphism $\mathrm{Jac}(C) \to E_0$ whose restriction to the embedding of C is $p \mapsto f(p) - f(p_\infty)$, and thus coincides with f if $f(p_\infty) = \mathbf{0}$. This concludes the construction, which also lets us identify pointwise addition and subtraction of maps $f : C \to E_0$ with the group operations on L.

In particular it follows that any $f : C \to E_0$ with $f(p_\infty) = \mathbf{0}$ must satisfy the identity

$$f(p) = -f(\iota(p)). \tag{11}$$

We may see this either by noting that the divisor $(p)+(\iota(p))$ is linearly equivalent to $2(p_\infty)$, or more concretely by noting that the map $f(p) + f(\iota(p)) : C \to E_0$ descends to $C/\langle\iota\rangle = \mathbf{P}^1$ and is thus constant (this is of course a special case of the proof of the fact $D \sim D' \Rightarrow f_+(D) = f_+(D')$ used earlier). Recalling that $-(x, y) = (x, y + 1)$ on E_0, this means that either f is the constant function $C \to \mathbf{0}$ or it is of the form

$$f(t, u) = (x(t), y(t) + u), \tag{12}$$

where x, y are rational functions satisfying

$$y^2 + y = x^3 + t^{q+1} + a_6 \tag{13}$$

with $a_6 = 0$ for n odd and a_6 as in (4) for n even. Conversely any pair (x, y) of rational functions satisfying (13) yields a rational map (12) that satisfies (11) and thus (since $\mathbf{0}$ is the unique fixed point of multiplication by -1 on E_0) takes p_∞ to $\mathbf{0}$.

We regard (13) as a Weierstrass model for an elliptic curve E over the global field $K = k(t)$. We then see that we have identified its Mordell-Weil group $E(K)$ with L, and thus recognized it as a free abelian group of rank r. (It is straightforward to check that the group laws of $E(K)$ and L are compatible with our identification.) Investigating further the arithmetic of this curve, we note that it has constant j-invariant 0, and thus is a potentially constant elliptic curve; indeed it becomes isomorphic with the constant curve E_0 under the quadratic extension $K(u) = k(C)$ of K. Moreover the curve has good reduction at all finite t, and additive bad reduction at $t = \infty$. The local reduction type at infinity may be determined by the change of coordinates $(x, y) = (t^{2z} x_1, t^{3z} y_1)$ where z is the smallest integer such that $6z > q$, obtaining

$$y_1^2 + t^{-3z} y_1 = x_1^3 + t^{q+1-6z} + t^{-6z} a_6 \tag{14}$$

with discriminant t^{-12z}. That this is a minimal model at infinity may be checked for instance by Tate's formulas [Ta3]. These formulas also tell us the local reduction type: if n is even then $q \equiv 4 \bmod 6$ and thus $q+1-6z = -1$, whence we find reduction type II, while if n is odd then $q \equiv 2 \bmod 6$, so $q+1-6z=-3$ and the reduction type is I_0^*. In the latter case we can describe each of the three nonidentity components of multiplicity one by $x_1 \equiv \xi t^{-1} \bmod t^{-2}$ or equivalently

$$x = \xi t^{(q+1)/3} + O(t^{(q-2)/3}) \tag{15}$$

at $t=\infty$, where ξ is one of the three cube roots of unity. In particular since $\boldsymbol{\mu}_3 \subset k$ we see that each of these components is defined over k and conclude that $c_\infty = 1+3 = 4$ in this case. Each nonidentity component (15) is represented by a point in the Mordell-Weil group $E(K)$, for instance the point $(x,y) = (\xi t^{(q+1)/3}, 0)$; thus the narrow Mordell-Weil group L_0, consisting of solutions of (13) which reduce on each fiber to points on its identity component, is of index 4 in L. [For even n every fiber of E has only one component and $L_0 = L$. For both even and odd n, points on the identity component of E are characterized by the condition that x_1 have no zero at infinity, or equivalently that x have a pole at $t=\infty$ of order greater than $(q+1)/3$; note that in every solution of (13) x must either satisfy (15) or have a pole of even order $> (q+1)/3$ at infinity, because every pole of y^2+y must have even order, while t^{q+1} has an odd-order pole at infinity.]

Heights and the Mordell-Weil lattice of E. The naïve height of a point $(x,y) \in L$ is the degree of x as a rational function of t. (We thus omit a factor of $\log|k|$ from both the naïve and the canonical height: in our setting, with positive global characteristic, that factor would achieve little but notational clutter. Of course both the naïve and the canonical heights of the zero point of L are zero in either normalization.) Recall that the canonical height can be characterized, following Tate, as the unique function $\hat{h} : L \to \mathbf{R}$ satisfying both the identity

$$\hat{h}(2P) = 4\hat{h}(P) \tag{16}$$

for all $P \in L$ and the condition that the difference between $\hat{h}$ and the naïve height is bounded. In our case we can determine $\hat{h}$ explicitly:

Proposition 2. *Let $P \in L$ be a nonzero point, with coordinates (x,y). Then the canonical height of P under the above normalization is* $\deg(x)$, *i.e. the canonical and naïve heights on $E(K)$ coincide. Furthermore*

$$\hat{h}(P) \geq \frac{q+1}{3} \tag{17}$$

for all nonzero $P \in L$, and $\hat{h}(P)$ is even unless n is odd and x satisfies (15) for some $\xi \in \boldsymbol{\mu}_3$, in which case $\hat{h}(P)$ is odd.

Proof: To identify the naïve and canonical heights we need only show that the naïve height already satisfies the identity (16). This we do by using the explicit addition law on E to compute that if P has coordinates (x,y) then $2P$ has coordinates

$$(x^4, y^4 + x^6 + x^3 + 1) \tag{18}$$

and noting that $\deg(x^4) = 4\deg(x)$. We have already used the fact that every pole of y^2+y has even order to show that x has a pole of order at least $(q+1)/3$ at infinity, from which the estimate (17) follows, and also that the order of this pole is either even or exactly equals $(q+1)/3$, the latter being possible only for odd n. To complete the determination of the parity of $\deg(x) = \hat{h}(P)$ note that any pole of $x^3 + t^{q+1} + a_6$, and thus also of x, at a finite $t \in \bar{k}$ must too have even order, and that the degree of x is its total number of poles counted with multiplicity. $\square$

Remarks: We can prove this Proposition, too, in several alternative ways. We could also obtain the formula for $\hat{h}$, following Néron [Né], as a sum of local contributions, using for instance the explicit formulas in [Si]; or, as in [Sh1, Sh2], using intersection theory, which also provides another interpretation of the estimate (17). Yet another route is to note that $\hat{h}(P)$ is half the canonical height of the map $f: C \to E_0$ associated to P when that map is regarded as a point on the constant elliptic curve $E_0/k(C)$ (this because the extension $k(C)/K$ has degree 2), and to show that this height is twice the degree of the rational map f, which again can be done either as in our proof above or following either of the alternative approaches. Each of these two approaches also yields a general proof of the fact that $\hat{h}(P)$ is even for all $P \in L_0$. Observe too that we can now give another proof that L is torsion-free: by (17) all nonzero $P \in L$ have positive canonical height.

The canonical height is a positive-definite form on L, giving it the structure of a lattice in $\mathbf{R}^r$, the *Mordell-Weil lattice* of E/K. We already have lower bounds on the minimal norms of L and L_0, and know for n odd that our bound $(q+1)/3$ on the minimal norm of L is attained by the points $(x,y) = (\xi t^{(q+1)/3}, 0)$. Even before estimating the discriminants of these lattices we can already describe them to some extent, finding a group of $48n(q^3+q^2)$ symmetries and, for odd n, comparing the sphere-packing densities of the lattices L_0, L.

The symmetries come from three sources: automorphisms of the hyperelliptic curve C, of the elliptic curve E_0, and of the ground field k. Thus an automorphism (9) of C yields the map

$$(x(t), y(t)) \mapsto \left(x(a(t+b)), y(a(t+b)) + \sum_{m=0}^{n-1} (b^q t)^{2^m} + c\right) \tag{19}$$

from L to itself which preserves the degree of x and thus the height. Likewise, given a, b, c in the 4-element field satisfying (8) with $n=1$ we have the isometry

$$(x(t), y(t)) \mapsto \left(a(x(t)+b), y(t) + b^2 x(t) + c\right) \tag{20}$$

of L, commuting with all the isometries (19). Finally let σ be the automorphism of K that fixes t and acts on k by $a \mapsto a^2$. When n is odd it is clear that σ induces an order-$2n$ isometry of L, because then the equation (13) defining E is defined over the 2-element prime field. When n is even we obtain instead the isometry

$$(x,y) \mapsto (\sigma(x), \sigma(y) + a_6) \tag{21}$$

of order $4n$ whose $(2n)$-th power is the isometry

$$-1 : (x,y) \mapsto (x, y+1) \tag{22}$$

of L (because we chose a_6 so that $\sum_{m=0}^{2n-1} \sigma^m(a_6) = 1$). Note that the groups (19,20) also contain this isometry, with $(a,b,c) = (1,0,1)$. Their normal subgroups of isometries with $a = 1$ generate the extraspecial 2-group $2_+^{1+2(n+1)}$ whose action on the 2^{n+1}-dimensional space $L \otimes \mathbf{R}$ must give its unique irreducible representation with nontrivial central character.

We have seen that L_0 has index 4 in L, and thus center density $1/4$ as large as that of L. On the other hand its minimal norm is at least $(q+4)/(q+1)$ times larger. Thus the normalized center density of L_0 is

$$\frac{1}{4}\left(\frac{q+4}{q+1}\right)^{r/2} = \frac{1}{4}\left(1 + \frac{3}{q+1}\right)^{q} \tag{23}$$

times that of L. The ratio (23) is ≥ 1 for all q, with equality only when $q=2$, and tends to $e^3/4 = 5.021\ldots$ as $q \to \infty$. Thus for $n > 1$ the lattice L_0 always yields a denser sphere packing than L, albeit by a bounded factor. The points in $L - L_0$ may still find use as "holes", i.e. vectors in $L_0 \otimes \mathbf{R}$ far from any point in L_0: a dense sphere packing of $\mathbf{R}^{r+1}$ might be obtained by stacking ("laminating") r-dimensional layers each consisting of L_0 or its translates by a suitable hole.

We next begin our investigation of the discriminant $\Delta(L)$ of L (a.k.a. the regulator of E/K) by computing the L-function $L(E/K, s)$. A comparison of local factors shows that this is the quotient of the L-functions of the constant curves $E_0/k(C)$ and E_0/K.[1] Thus since K is a rational function field the zeros of our L-function, regarded as a polynomial in $|k|^{-s}$, are the products of the inverses of the eigenvalues of Frobenius of E_0 and C, counted according to multiplicity. Since these eigenvalues all equal $-q$ we conclude that we have a zero of order $4g = r$ at q^{-2}, corresponding to $s = 1$, and no other zeros, so $L(E/K, s) = (q^{-2s} - q^{-2})^r$. (At least for n odd this could also be shown by regarding (13) as a "supersingular Delsarte surface" as Shioda does in odd characteristic [Sh2].)

But the conjecture of Birch and Swinnerton-Dyer, adapted by Artin and Tate to the function field case [Ta1], predicts that the rank of the Mordell-Weil group of an elliptic curve over a global field should equal the order of vanishing at $s=1$ of its L-function, and that the regulator of the curve should be the product of the leading term at $s = 1$ of that L-function with certain

[1] Indeed this method shows that for any elliptic curve over a global field F its L-function as a curve over a separable quadratic extension F' of F factors as the product of the L-functions over F of the original curve and its quadratic twist by F'/F.

arithmetic invariants of the curve. We have seen that for our curve E/K the order of vanishing equals the rank r as predicted. It then follows from Milne's theorem [Mi] that the rest of the conjecture is also true. The usual statement of the formula uses the definition of the canonical height that includes factors of $\log|k|$, but these powers conveniently cancel a factor $(\log|k|)^r$ introduced by differentiating the L-function r times at $s=1$. Using our earlier observation about the discriminant of the minimal model of E at infinity, and recalling that $E(K)$ has trivial torsion, we finally find

$$\Delta(L) = q^{2\lfloor q/6\rfloor}/(c_\infty |Ш|), \tag{24}$$

where $c_\infty = 1$ or 4 according as n is even or odd, and Ш is the Tate-Šafarevič group of E/K. Since $|Ш| \geq 1$ we thus have an upper bound on the discriminant.

Combining this with our estimates on $N_{\min}$ we conclude:

Theorem 1. *Both $|Ш|$ and $\Delta(L)$ are powers of 2. The narrow Mordell-Weil lattice L_0 of E/K has normalized center density*

$$\delta(L_0) \geq q^{-(q-4)/6}\left(\frac{q+2}{12}\right)^q \tag{25}$$

for n even, and

$$\delta(L_0) \geq \frac{1}{2} q^{-(q-2)/6}\left(\frac{q+4}{12}\right)^q \tag{26}$$

for n odd. Equality holds if and only if (13) has solutions in polynomials $x(t), y(t)$ with x of degree $2(\lfloor q/6\rfloor + 1)$ (in which case these solutions give the minimal vectors of L_0) and E/K has trivial Tate-Šafarevič group.

Proof: The product $q^{2\lfloor q/6\rfloor}/c_\infty$ of $|Ш|$ and $\Delta(L)$ is a power of 2. Furthermore $|Ш|$ is an integer, and the index-c_∞ sublattice L_0 of L is even so has integral discriminant. Since c_∞ is a power of 2, then, so are $|Ш|$ and $\Delta(L)$. We obtain the inequality on $\delta(L_0)$ by substituting into (2) the lower bound (17) on the minimal norm and the formula (24) for the discriminant, noting that for n odd the *narrow* Mordell-Weil lattice has minimal norm at least $(q+4)/3$ and index 4 in L. For equality to hold Ш must be trivial and the lower bound $2(\lfloor q/6\rfloor+1)$ on $N_{\min}$ must be attained. Since that lower bound on $\hat{h}\big((x,y)\big) = \deg(x)$ was the minimal order of the pole of x at $t=\infty$, that lower bound is attained precisely for those (x,y) such that x has a pole of that order at infinity and no other poles, i.e. x is a polynomial of that degree in t, in which case y must also be a polynomial. □ □

The lattice L_0 yields a sphere packing in dimension 2^{n+1} whose density equals the records listed in [C-S] for $n \leq 4$ and improves on those records for $5 \leq n \leq 9$. When $n=1$ the curves C, E_0 coincide so L is just the endomorphism ring of E_0, which is the ring of Hurwitz quaternions, homothetic as a lattice with the root lattice D_4 of normalized center density $1/8$; the narrow Mordell-Weil lattice L_0 consists of the inseparable endomorphisms, and is isometric with D_4, with deep holes at $L - L_0$. When $n = 2$ the Mordell-Weil lattice is isomorphic with the root lattice E_8 (with $\delta = 1/16$); this can be seen in several ways, for instance using Shioda's work on rational elliptic surfaces. When $n = 3$, I can show that L_0 is isomorphic with the Barnes-Wall lattice of dimension 16 and normalized center density 1/16, with some but not all its deep holes at $L - L_0$. When $n = 4$, I find that L has the same density $(9/8)^8$, indeed the same theta function, as Quebbemann's record lattice in dimension 32, but is not isomorphic with it; furthermore the scaled dual lattice

$$\{w \in L \otimes \mathbf{R} : \langle v, w \rangle \in 2\mathbf{Z} \text{ for all } v \in L\} \tag{27}$$

of L is a third nonisomorphic lattice with the same theta series.

For $n = 5, 6, \ldots, 11$ we find new lattices L_0 with the following parameters (we give the base-2 logarithm, rounded to two decimals, of the lower bound (25) or (26) on the normalized center density δ):

n	5	6	7	8	9	10	11
$r = 2^{n+1}$	64	128	256	512	1024	2048	4096
$\log_2 \delta \geq$	24.72	97.40	294.81	797.12	2012.25	4871.88	11439.76

These improve considerably on the previous records listed in [C-S]. (For $n = 5, 6, 7, 11$ these records are $\log_2(\delta) = 22,\ 88,\ 270.89$, and 11344; for $n = 8, 9, 10$ the previous record constructions do not work well in dimension exactly 2^{n+1}, but our δ's well exceed even the normalized densities of packings in somewhat higher dimensions listed in [C-S].) Note, however, that in any dimension r there exist lattices, not explicitly known for large r, with packing density at least 2^{1-r} (Minkowski-Hlawka, cf. [EOR]); for $n = 10, 11$ this amounts to normalized densities δ larger than those of our Mordell-Weil lattices. Once $n \geq 12$ the lower bounds (25,26) are worse than both the Minkowski-Hlawka bounds and the explicit lattices listed in [C-S]. We have shown that for $n \geq 9$ the Tate-Šafarevič group of E/K is nontrivial and used this to improve our bounds on $\delta(L)$, but even these new bounds (which increase those of Thm. 1 by factors of $2^6, 2^{20}, 2^{88}$ for $n = 9, 10, 11$) do not improve on Minkowski-Hlawka for $n = 10, 11$, nor on the explicit lattices for $n \geq 12$. Of course these Mordell-Weil lattices are still of interest for the arithmetic of the elliptic curves E.

The lattices constructed in [Sh2] are the Mordell-Weil lattices of the potentially constant curves $y^2 = x^3 + 1 + t^{p+1}$ over the field of p^2 elements where p is a prime power congruent to 5 mod 6; these have rank $2p - 2$, determinant $\leq p^{(p-5)/3}$ (with equality for prime p), and minimal norm $(p + 1)/3$. These are closely analogous to the Mordell-Weil lattices of the curves (13) and yield sphere packings only slightly worse (by a factor $< e^{1/6}$) in the few cases where the two constructions are directly comparable, i.e. produce lattices in the same dimension $2p-2 = 2^{n+1}$ — with the exception of $n=2, p=5$ where both lattices are isomorphic with E_8.

The ϕ-descent and the case $n = 5$. To compute $\Delta(L)$ from (24) we need to determine $|Ш|$. In general this promises to be a very difficult computation, requiring repeated 2-power descents on a supersingular curve in characteristic 2. But it is much simpler to test whether Ш is trivial, which we find to be the case for first few n. We begin with the inseparable 2-isogeny $\phi : E \to E$ defined by

$$\phi(x, y) = (x^2, y^2 + t^{q+1} + a_6). \tag{28}$$

This is inherited from the Frobenius isogeny $(x, y) \mapsto (x^2, y^2 + a_6)$ on E_0, and thus satisfies

$$\phi^2 = -2 \tag{29}$$

as may also be seen from the explicit formula (18) for multiplication by 2 on E. We now observe that since Ш is a 2-group,

$$|Ш| = 1 \iff |Ш_2| = 1 \iff |Ш_\phi| = 1, \tag{30}$$

where $Ш_2$ and $Ш_\phi$ are respectively the subgroups of Ш killed by 2 and ϕ. That is, Ш is trivial if and only if the Selmer group for ϕ, which a priori contains $L/\phi L$, is actually equal to $L/\phi L$. Now from (28) we have for all $P \in L$

$$\hat{h}(\phi(P)) = \deg x(\phi(P)) = \deg x(P)^2 = 2 \deg x(P) = 2\hat{h}(P). \tag{31}$$

Thus ϕ is a norm-doubling map of L, so in particular $L/\phi L$ is an elementary abelian 2-group of rank $r/2 = 2^n = q$, and Ш is trivial if and only if the Selmer group for ϕ has cardinality 2^q.

Fortunately we can describe the ϕ-descent almost completely:

Theorem 2. *Let k be a finite field of characteristic 2 and let K be the rational function field $K = k(t)$. Fix a polynomial $A_6(t)$ of odd degree d, and let E/K be the elliptic curve with Weierstrass model*

$$y^2 + y = x^3 + A_6. \tag{32}$$

Then E admits an isogeny

$$\phi : E \to E, \quad (x, y) \mapsto (x^2, y^2 + A_6) \tag{33}$$

with $\phi^2 = -2$, and the ϕ-descent map can be written as

$$\epsilon : E(K)/\phi E(K) \hookrightarrow K/K^2, \quad \mathbf{0} \mapsto 0,\ (x, y) \mapsto x \bmod K^2 \tag{34}$$

(with K and K^2 considered as additive groups). If v is a finite place of K then the local Selmer group of ϕ at v, i.e. the image $\epsilon(E(K_v)) \subset K_v/K_v^2$, consists of the classes with v-integral representatives. Every element of the Selmer group at $t = \infty$ has a representative x_0 of valuation $\geq -d/3$; furthermore, if this valuation equals $-d/3$ then $x_0^3/A_6 = 1$ at $t = \infty$, and if it is strictly between $-d/3$ and 0 then it is congruent to $-d \bmod 4$. Thus every nonzero element

of the global Selmer group for ϕ is has a unique representative x_0 which is an odd polynomial[2] *in t of degree $\leq d/3$ which is congruent to $d \bmod 4$ unless* $\deg(x_0) = d/3$ *and $x_0^3/A_6 = 1$ at $t = \infty$.*

Notes: We give this more general statement, allowing polynomials A_6 other than $t^{q+1}+a_6$, because we need it in subsequent papers (e.g. to realize the Leech lattice as a Mordell-Weil lattice) and the proof for $A_6 = t^{q+1}+a_6$ extends directly to arbitrary polynomials. We require that d be odd only for convenience: for any $A_3 \in K$, the change of coordinates $(x, y) \leftrightarrow (x, y + A_3)$ in (32) yields the equivalent Weierstrass form $y^2 + y = x^3 + A_6'$ where $A_6' = A_6 + A_3^2 + A_3$, and for any polynomial A_6 we can choose a polynomial A_3 such that A_6' has odd degree.

Since the squares in K are precisely the rational functions whose differential vanishes, we may identify K/K^2 with the exact differentials on the projective t-line. This gives us a useful alternative formulation of the ϕ-descent (34): $\epsilon(P)$ is the differential of $x(P)$. The local Selmer groups are then the regular exact differentials at finite places, and a subgroup of the exact differentials with a pole of degree at most $d/3 + 1$ at the place $t = \infty$.

Proof: That ϕ is an isogeny satisfying $\phi^2 = -2$ we verify as before by a direct computation. For nonzero points $P, Q \in E(K)$ with $P + Q \neq \mathbf{0}$ the addition formula gives

$$x(P + Q) = x(P) + x(Q) + m(P, Q)^2 \tag{35}$$

where $m(P, Q)$ is the slope of the line between P and Q (or of the tangent to E at P if $P = Q$). Thus the map $E(K) \to K/K^2$ taking $\mathbf{0}$ to 0 and nonzero P to the class of $x(P)$ is a group homomorphism. The kernel of this homomorphism contains $\phi E(K)$ since (32) exhibits $x(\phi(P))$ as a square; conversely if $(x, y) \in E(K)$ with $x = x_1^2$ we take $y_1 = y + x_1^3$ and find the point (x_1, y_1) on $E(K)$ with $\phi((x_1, y_1)) = (x, y)$. Thus the kernel of our homomorphism equals $\phi E(K)$ so ϵ is indeed a well-defined injection, so it gives the desired descent map. Note that this part holds for any field of characteristic 2 and any element A_6 of the field, so in particular we may use it for the localizations K_v of K.

Next let v be a finite place of K, and x_0 a v-integral element of K_v. We can then choose v-integral $x_1, y_1 \in K_v$ such that $x_1 \equiv x_0 \bmod K_v^2$ and $y_1^2 + y_1 \equiv x_1^3 + A_6 \bmod v$. Then

$$\eta := (x_1^3 + A_6) - (y_1^2 + y_1) \tag{36}$$

has positive v-valuation, and we can deform (x_1, y_1) to the K_v-integral point

$$(x_1, y_1 + \sum_{m=0}^{\infty} \eta^{2^m}) \tag{37}$$

[2] That is, a polynomial of the form $f(t) = tg(t^2)$ for some polynomial g; in characteristic 2 the usual characterization $f(-t) = -f(t)$ of odd polynomials fails.

of E whose image under ϵ is $x_0 \bmod K_v^2$, confirming that $x_0 + K_v^2$ is in the local Selmer group. Conversely let (x, y) be any point in $E(K_v)$. We may assume that x has a pole at v, else x itself is a v-integral representative of $x + K_v^2$. Since A_6 is regular at v, the pole of x must have even order, say $2z$, and then y has a pole of order $3z$ at v. Differentiating (32) we find that

$$\frac{dy}{dt} = x^2 \frac{dx}{dt} + \frac{dA_6}{dt}, \tag{38}$$

whence dx/dt vanishes at v to order at least $4z - (3z + 1) \geq 0$. Thus in this case too we see that x is v-integral modulo squares.

Finally let $v = v_\infty$ be the infinite place, and $P = (x, y)$ a nonzero point of $E(K_v)$. As in Prop. 2 we see that since A_6 has a pole at v_∞ of odd order d, but $y^2 + y$ cannot have a pole of odd order there, it follows that either x has valuation exactly $-d/3$ with $x^3/A_6 \equiv 1 \bmod v_\infty$ (in which case we're done), or a pole of even order $2z > d/3$. In the latter case, y has a pole of order $3z$, when by (38) the valuation of dx/dt at v_∞ is either $4z-d-1$ or (if $3z \geq q$) at least $z-1$. Thus in each case $\epsilon(P)$ lies in the subset of K_v/K_v^2 specified in the statement of Thm. 2. Since K is a function field of genus 0, any $x \in K$ has a decomposition into partial fractions which provides a representative of $x \bmod K^2$ whose pole at each place v has the same order as the best local representative of $x \bmod K_v^2$; thus we can identify the global Selmer group of ϕ with the odd polynomials whose class mod $K_{v_\infty}^2$ is in the local Selmer group at v_∞. □ □

We now return to our curves (13) over the field k of $q^2 = 2^{2n}$ elements:

Corollary. *For $n \leq 3$ equality holds in the estimates (25,26) of Thm. 1 on $\delta(L_0)$.*

Proof: In each case Thm. 2 gives a $(\mathbf{Z}/2)$-vector space of dimension $r/2 = 2^n$ containing the Selmer group, so $Ш_\phi$ and thus also $Ш$ is trivial, and we need only exhibit a polynomial solution of (13) whose x-coordinate has degree $2(\lfloor q/6 \rfloor + 1)$. Thus for $n = 1$ the Selmer group is contained in $\{at | a \in k\}$, a $(\mathbf{Z}/2)$-vector space of dimension 2, and $(x, y) = (t^2, t^3)$ is a minimal vector in L_0 of norm 2. For $n = 2$ we get the 4-dimensional space $\{at | a \in k\}$, and minimal vectors $(x, y) = (t^2 + t + b, t^3 + (b^8 + 1)t^2 + bt + c)$ with $b \in k$ of trace 1 and $c^2 + c = b^3 + a_6$. For $n = 3$ we find the space $\{at^3 + bt | a^4 = a, b \in k\}$ of dimension $2 + 6 = 8$, and a minimal vector $(x, y) = (t^4 + t^2 + t, t^6 + t^5 + t^4 + t^3)$. □

(By regarding these minimal vectors as certain maps (12) from the hyperelliptic curve C to E_0 we could obtain a less ad-hoc construction: for $n = 1$ we have $C = E_0$ and the point (t^2, t^3) becomes the 2-isogeny ϕ; and for $n = 2, 3$ we get quotient maps $C \to C/H \cong E_0$ where $H \subset 2_-^{1+2n}$ is a subgroup isomorphic to $(\mathbf{Z}/2)^{n-1}$ not containing the involution ι. For arbitrary n it turns out that such maps generate a subgroup of L homothetic to the Barnes-Wall lattice of dimension 2^{n+1}, a fact we shall demonstrate and exploit in subsequent papers.)

A closer analysis of the ϕ-descent at v_∞ allows us to show that equality holds in (25,26) for several higher n, at least through $n = 6$. We illustrate in detail the case $n=5$, which is the first case in which we obtain a lattice L_0 whose density exceeds the records of [C-S].

Proposition 3. *Let k be the field of $2^{10}=1024$ elements, let K be the rational function field $k(t)$, and let E be the elliptic curve $y^2+y=x^3+t^{33}$ over K. The Selmer group for the 2-isogeny $\phi: E \to E$ is contained in, and thus equal, to, the subspace of K/K^2 represented by the polynomials*

$$\{a_{11}t^{11}+a_9t^9+a_5t^5+a_9^4t^3+a_1t : a_3, a_5, a_9 \in k, a_{11}^4 = a_{11}\} \tag{39}$$

(NB this is an elementary abelian 2-group of rank $2+10+10+10=32$). The Tate-Šafarevič group of E/K is trivial. The narrow Mordell-Weil lattice L_0 has rank 64, discriminant $\Delta(L_0)=2^{52}$, minimal norm 12 and normalized center density $\delta(L_0)=2^{-26}3^{32}$. The points of the full Mordell-Weil lattice L not contained in L_0 are holes of norm 11; using these we can laminate L_0 to a periodic nonlattice sphere packing in $\mathbf{R}^{65}$ of normalized center density $3^{1/2}\delta(L_0)$.

Proof: We already know that L_0 has rank $2^6=64$. Once we identify the space (39) with the Selmer group, the triviality of Ш and the formula for the discriminant will follow from (30) and (24), recalling that $\Delta(L_0) = [L:L_0]^2\Delta(L) = 2^4\Delta(L)$. By Thm. 2 the Selmer group is contained in the space of odd polynomials of degree ≤ 11 in t whose t^{11} coefficient is either zero or a cube root of unity; furthermore for each cube root of unity ξ we have a point $(x,y)=(\xi t^{11},0)$ in $E(K)$ whose image under ϵ is ξt^{11}. Thus we can subtract $a_{11}t^{11}$ from (39) and consider only polynomials of degree ≤ 9, which by Thm. 2 must have degree 1, 5, or 9. In the degree 1 case there is nothing to prove. To handle the remaining two cases and thus complete the ϕ-descent at infinity we shall use the following

Lemma. *Let k be a perfect field of characteristic 2 and $(\eta_j)_{j=-\infty}^{d}$ any sequence of elements of k. Then*

$$\eta := \sum_{j=-\infty}^{d} \eta_j t^j \in k((t^{-1})) \tag{40}$$

can be written as y^2+y for some $y \in k((t))$ if and only if $\eta_0 = y_0^2+y_0$ for some $y_0 \in k$, and, for each odd $j_0 > 0$,

$$\sum_{m=0}^{\infty} (\eta_{2^m j_0})^{2^{-m}} = 0. \tag{41}$$

(Note that this sum is finite for each j, and the fractional exponents make sense in k.)

Proof of Lemma: Simply write $y=\sum_{j=-\infty}^{-d/2} y_j t^j$ and compare (40) termwise with the power series

$$y^2+y = \sum_{j=-\infty}^{-d/2} y_j^2 t^{2j} + y_j t^j = \sum_{j=-\infty}^{d} (y_j + y_{j/2}^2) t^j \tag{42}$$

(where of course $y_j = 0$ if j exceeds $d/2$ or is not an integer). This uniquely determines y_j for $j < 0$ by induction on j (or by adapting the trick used in (37)); the condition $\eta_0 = y_0^2 + y_0$ comes from the constant coefficients; and eliminating the undetermined coefficients $y_{2^m j_0}$ yields (41).

Now by comparing degrees in (38) we see that if $\epsilon((x,y))$ has degree 5 (or degree 9) then x has a pole of degree 14 (resp. 12) at infinity. We expand x in a Laurent series at infinity and apply our Lemma to $x^3 + t^{33}$. In the first case we write $x = \sum_{j=-\infty}^{14} x_j t^j$ with $x_5, x_{14} \neq 0$ and $x_j = 0$ for odd $j > 5$; then by taking $j_0 = 31$ in the Lemma we find $x_3 x_{14}^2 = 0$, whence $x_3 = 0$. In the second case we have $x = \sum_{j=-\infty}^{12} x_j t^j$ with $x_9, x_{12} \neq 0$ and $x_{11} = 0$. Taking $j = 33, 31, 27$ in our Lemma we obtain

$$x_9 x_{12}^2 = 1, \quad x_7 x_{12}^2 = x_3 x_{12}^2 + x_7 x_{10}^2 + x_9^3 = 0, \tag{43}$$

from which $x_7 = 0$ and $x_3 = x_9^4$ as claimed.

We now know the rank and discriminant of L. The minimal norm is at least 12 by Thm. 1; to prove that it equals 12 we need only exhibit one point with that norm. By adapting the criterion (41) to polynomials we compute that the degree-12 polynomial

$$a^{-1}t^{12} + a^2 t^9 + a^5 t^6 + a^8 t^3 + c \tag{44}$$

is the x-coordinate of a polynomial solution of $y^2 + y = x^3 + t^{33}$ provided[3]

$$a^{495} + a^{231} + a^{99} + a^{33} + 1 = 0, \quad c^8 + c^2 = a^{88} + a^{-11}. \tag{45}$$

Finally let $P_0 = 0, P_1, P_2, P_3$ be representatives of L/L_0. Then the open balls of radius $(12/4)^{1/2} = \sqrt{3}$ in $\mathbf{R}^{64+1}$ centered at $L_0 \times \{0\}$ and $(L_0 + P_1) \times \{1\}$ are disjoint. We cannot extend this to a 65-dimensional lattice, because the next layer $(L_0 + 2P_1) \times \{2\} = L_0 \times \{2\}$ would be too close to $L_0 \times \{0\}$. Still we can use the remaining two holes P_2, P_3 to construct a periodic nonlattice packing of 65-dimensional balls of radius $\sqrt{3}$ centered at

$$\bigcup_{j=0}^{3} (L_0 + P_j) \times (4\mathbf{Z} + j) \tag{46}$$

since $4 > \sqrt{12}$, and the normalized center density of this packing is $\sqrt{3}$ times that of L_0. $\square$

In fact it is feasible to compute the kissing number of these packings of $\mathbf{R}^{64}$ and $\mathbf{R}^{65}$. Thus the kissing number of L_0 or L is the number of polynomials $(x(t), y(t))$ over k with x of degree 12 or 11 such that $y^2 + y = x^3 + t^{33}$. This is tantamount to a system of simultaneous equations in the coefficients of x, y,

[3]The condition on a means that a^{33}, the norm of a from k to its 32-element subfield, is one of the 15 nonzero elements of that subfield whose trace is 0.

whose solutions we (assisted by a computer) may enumerate by eliminating all but a few of the variables and solving for the rest by trying all values in k. We find that L and L_0 have kissing numbers $2^{13}3^3 7\cdot 11 = 17031168$ and $2^{11}3^4 7^2 11 = 89413632$ respectively, and the nonlattice packing (46) has kissing number

$$89413632 + \frac{2}{3}17031168 = 100767744 = 2^{11}3^2 7\cdot 11\cdot 71. \tag{47}$$

Thus our construction also yields new record kissing numbers in dimensions 64 and 65.

References

[C-S] Conway, J.H., Sloane, N.J.A.: *Sphere Packings, Lattices and Groups.* New York: Springer 1993.

[EOR] Elkies, N.D., Odlyzko, A.M., and Rush, J.A.: On the packing densities of superballs and other bodies. *Invent. Math.* **105** (1991), 613–639.

[G-V] van der Geer, G., and van der Vlugt, M.: Reed-Muller Codes and Supersingular Curves I. *Compositio Math.* **84** (1992), 333–367.

[Mi] Milne, J.: On a conjecture of Artin and Tate. *Annals of Math.* **102** (1975), 517–533.

[Né] Néron, A: Quasi-fonctions et hauteurs sur les variétés abéliennes. *Annals of Math.* **82** (1965), 249–331.

[Oe] Oesterlé, J.: Empilements de sphères. *Astérisque* **189-90** (1990), 375–398 [= Séminaire Bourbaki 6/90, exposé 727].

[Š-T] Šafarevič, I.R., Tate, J.T.: The rank of elliptic curves. *Soviet Math. Dokl.* **8** (1967), 917–920. [trans. J.W.S.Cassels from *Dokl. Akad. Nauk SSSR* **175** (1967) #4.]

[Sh1] Shioda, T.: On the Mordell-Weil lattices. *Comment. Math. Univ. St. Pauli* **39** (1990), 211–240.

[Sh2] Shioda, T.: Mordell-Weil lattices and sphere packings. *Amer. J. Math.* **113** (1991), 931–948.

[Si] Silverman, J.H.: Computing Heights on Elliptic Curves. *Math. of Computation* **51** #183 (July 1988), 339–358.

[Ta1] Tate, J.: On the conjecture of Birch and Swinnerton-Dyer and a geometric analog. *Sém. Bourbaki* **306** (1965–66).

[Ta2] Tate, J.: Endomorphisms of Abelian Varieties over Finite Fields. *Invent. Math.* **2** (1966), 134–144.

[Ta3] Tate, J.: Algorithm for determining the type of a singular fiber in an elliptic pencil, Lect. Notes in Math. 476 (*Modular Functions of One Variable IV*), 33–52 (1975).

[Ts] Tsfasman, M.A.: Global fields, codes and sphere packings. *Astérisque* **198-199-200** (1991; proceedings of Journées Arithmétiques 1989), 373–396.

Dept. of Mathematics
Harvard University
Cambridge, MA 02138 USA

November, 1993