Functiones et Approximatio
XXXIX.2 (2008), 345–360

SEQUENCES OF JACOBIAN VARIETIES WITH TORSION DIVISORS OF QUADRATIC ORDER

Roger D. Patterson, Alfred J. van der Poorten, Hugh C. Williams

To Władysław Narkiewicz
on entering his seventies

Abstract: A fortuitous intersection of work on periodic continued fraction expansions in hyperelliptic function fields and the study of parametrized families of quadratic number fields with high class number leads us to discover sequences of hyperelliptic curves whose Jacobians contain torsion divisors of order g^2. These sequences generalize those earlier constructed by Flynn and by Leprévost.
Keywords: Torsion divisors, hyperelliptic curves, periodic continued fractions.

1. Introduction

Rather little is known about the rational torsion structure of abelian varieties of dimension greater than one. This is in stark contrast to the dimension one case. A theorem of Mazur completely classifies all possible torsion structures for elliptic curves over $\mathcal{Q}$, and Merel has established the uniform boundedness of torsion on elliptic curves over number fields. In the genus two case, that of Jacobians of hyperelliptic curves $Y^2 = f(X)$, with f a polynomial over $\mathcal{Q}$ of degree 5 or 6 and with distinct zeros, there are results of Flynn [5], Leprévost [8, 9, 11] and of Howe, Leprévost, Poonen [7] providing curves whose Jacobians have non-trivial torsion subgroups; the paper [7] deals solely with split Jacobians. Using similar techniques, Flynn [6], later extended by Leprévost [10, 12], noticed that there exist sequences of hyperelliptic curves whose Jacobians possess rational torsion divisors of order g^2, where g is the genus of the curve. Our remarks here generalize these sequences of curves and suggest there are no others.

Our main tool in this investigation is the continued fraction expansion over function fields (and number fields) developed in [14] and [16]. In particular, we examine certain hyperelliptic curves $\mathcal{C}_n$ given by

$$d^2Y^2 = AX^{2n} + BX^n + C^2 \,,$$

2000 Mathematics Subject Classification: Primary 11G30; Secondary 11G20, 14H40, 14H45.

where $d, A, B, C \in \mathcal{F}_q[X]$. For carefully selected values of A, B, C, d we are able to show that the period length of the continued fraction expansion of Y is linear in n. Furthermore, the regulator $R(Y)$ grows quadratically in n, and since the genus g of $\mathcal{C}_n$ is $O(n)$, we see that for these examples the Jacobian of $\mathcal{C}_n$ has a rational torsion divisor of order g^2. Our many attempts to find families of curves (or families of discriminants in the number field case), called *jeepers* in [15], for which the period length can be given explicitly and grows at the rate of $O(n^{1+\epsilon})$ for a fixed $\epsilon > 0$ have not yielded any examples. This suggests that there are no jeepers and this means that there do not exist hyperelliptic curves whose Jacobians possess rational torsion divisors of order g^3; we conjecture that this is the case.

2. Sequences of Curves with Torsion Divisors

We study sequences of curves

$$\mathcal{C}_g : \quad Y^2 = (f_1 + f_2 - f_3)^2 + 4f_1f_3 \tag{2.1}$$

where f_1, f_2, and f_3 denote polynomials defined over $\mathcal{Q}$ and of degree at most $g+1$ in X, with $X \nmid f_1$, $(X-1) \nmid f_3$ and such that Y^2 is squarefree of degree $2g+1$ or $2g+2$. Note that of course

$$Y^2 = (f_1 - f_2 + f_3)^2 + 4f_1f_2 = (f_1 + f_2 + f_3)^2 - 4f_2f_3 \,. \tag{2.2}$$

Specificially, let r, l, and m denote pairwise relatively prime polynomials independent of g, not vanishing at $X = 0$ nor $X = 1$, and each dividing Y^2. Because Y^2 is squarefree, it follows that also rlm is squarefree. Now set

$$f_1 = r(X-1)^{q+1-R} \,, \quad f_2 = m(X-1)^k X^{g+1-M} \,, \quad f_3 = lX^{g+1-L} \,,$$

where k, and L, R, and M, are nonnegative integers bounded as $g \to \infty$.

Now take the points $P_0 = (0, f_1(0))$ and $P_1 = (1, f_3(1))$, noting that both lie on $\mathcal{C}_g$. First, suppose that $\deg(Y^2) = 2g+1$, and consider the divisors $D_0 = P_0 - (\infty)$, $D_1 = P_1 - (\infty)$. Further, let $\varphi_1 = Y - (f_1 + f_2 - f_3)$. One sees that the support of the divisor (φ_1) is contained in D_0, D_1 and the zeros of rl. However, rl has order 2, hence the support of (φ_1^2) is contained in D_0 and D_1. Specifically, $(\varphi_1^2) = 2(g+1-L)D_0 + 2(g+1-R)D_1$.

Just so, let $\varphi_2 = Y - (f_1 + f_2 + f_3)$. Since ml also has order 2, we similarly find that $(\varphi_2^2) = 2\left(2(g+1) - (L+M)\right) D_0 + 2kD_1$. Hence we have

$$\begin{pmatrix} \varphi_1^2 \\ \varphi_2^2 \end{pmatrix} = \begin{pmatrix} g+1-L & g+1-R \\ 2(g+1)-(L+M) & k \end{pmatrix} \begin{pmatrix} 2D_0 \\ 2D_1 \end{pmatrix} \,.$$

Taking determinants, we see that there exists a divisor whose order divides

$$4\left(2(g+1)^2 - (g+1)(L+M+2R-k) + R(L+M) + kL\right) \,.$$

While this may not be the divisor's exact order, it is a straightforward matter to detail sufficiently many of its multiples to confirm its order is at least g^2.

Second, if $\deg(Y^2) = 2g+2$ we take $D_0 = P_0 - (\infty^+)$, $D_1 = P_1 - (\infty^+)$, $D_\infty = (\infty^- - \infty^+)$. The calculations carry through *mutatis mutandis*.

2.1. An example

In [6], Flynn gives an example of these sequences. In our notation,

$$f_1 = t(X-1)^g\ , \quad f_2 = X^{g-k}(X-1)^{k+1}\ , \quad f_3 = -X^{g+1}\ .$$

The multiples of D_1 are

$$\begin{aligned} &i(0,1) \quad + j(1,1) \quad + s\infty \ \text{ for } \ 0 \le i \le g,\ 0 \le j \le g-i\ ; \\ &i(0,-1) + j(1,-1) + s\infty \ \text{ for } \ 0 \le i \le g,\ 0 \le j \le i\ ; \\ &i(0,1) \quad + j(1,-1) + s\infty \ \text{ for } \ 1 \le i \le g,\ 1 \le j \le g-i-1\ ; \end{aligned}$$

and

$$i(0,-1) + j(1,-1) + s\infty \text{ for } 1 \le i \le g, 1 \le j \le i\ .$$

Here $s = g - i - j$.

It seems this argument works for r, l, m of any fixed order. However, the only functions whose divisors are of fixed order for all g are of order 2, which corresponds to r, l, and m indeed dividing Y^2.

3. Interlude on Continued Fraction Expansions

It turns out that saying more about the multiples of D_1 seems best done by way of continued fractions because certain multiples are, well, too complicated to give explicitly. The continued fraction expansion allows us to bypass this difficulty.

3.1. Units and torsion

By definition of the notion *unit*, a unit–say $u = a + b\sqrt{f}$–of the field $\mathcal{K}(X)[\sqrt{f(X)}]$ has trivial valuation at all finite places; that is, the support of the divisor (u) is contained in the infinite places. When $\deg(f)$ is even and the leading coefficient of f is a square, the infinite place $|\ |_\infty$ of $\mathcal{K}[X]$ splits into two infinite places, say ∞^+ and ∞^-, of $\mathcal{K}[X, \sqrt{f(X)}]$. Because (u) is the divisor of a function and thus has degree zero, we must have

$$(u) = m(\infty^+ - \infty^-)$$

for some positive integer m. Thus, $(\infty^+ - \infty^-)$ is a divisor in the Jacobian of $Y^2 = f(X)$ whose order divides m. The unit u is a *fundamental* unit precisely if the order of the divisor $(\infty^+ - \infty^-)$ is exactly m.

Moreover, a quadratic function field $\mathcal{K}(X)[\sqrt{f(X)}]$ contains a *nontrivial* unit u – thus, one with $b \neq 0$ – if and only if the continued fraction expansion of $\sqrt{f(X)}$ *is* periodic. Each step of the continued fraction expansion adds some multiple $d(\infty^+ - \infty^-)$ of $(\infty^+ - \infty^-)$, in fact where d is the degree of the partial quotient. The precise correspondence between the continued fraction expansion of $Y = \sqrt{f}$

and the addition of multiples of $(\infty^+ - \infty^-)$ is detailed by Tom Berry [3], thereby generalizing results of Adams and Razar [2]. Our remarks here imply that the *regulator* of the domain $\mathcal{K}[X, Y]$ is the degree of its fundamental unit, and this equals the torsion order of the divisor $(\infty^+ - \infty^-)$.

3.2. Continued fraction expansions

One best writes each line of the continued fraction expansion of Y as

$$\frac{Y + P_h}{Q_h} = a_h - \frac{(\overline{Y} + P_{h+1})}{Q_h} \tag{3.1}$$

where $\overline{Y}$ denotes the conjugate of Y. The terms $(Y + P_h)/Q_h$ on the left are called *complete quotients*; the a_h are the *partial quotients*.

3.3. ... and Mumford representations

Denote a typical zero of Q_h by ϑ_h. Then each $(\vartheta_h, -P_h(\vartheta_h))$ is a point on the curve $Y^2 = D$ considered defined over the algebraic closure $\overline{\mathcal{K}}$ of the base field. More, the formal sum of the points $(\vartheta_h, -P_h(\vartheta_h))$ as ϑ_h runs through the zeros of Q_h with multiplicity fixes a divisor on the Jacobian of the curve over $\mathcal{K}$. Our remarks above amount to the assertion that for each h this divisor is the appropriate multiple of the divisor at infinity. Incidentally, the pair $(Q_h, -P_h)$ is essentially the *Mumford representation* of that divisor.

3.4. Exceptional curves

We add that if the base field $\mathcal{K}$ is finite then the box principle guarantees that Y has a periodic continued fraction expansion, and thus that $\mathcal{K}[X, Y]$ has nontrivial units. If, however, $\mathcal{K}$ is infinite then periodicity is a rare happenstance and the existence of a nontrivial unit – equivalently, that the divisor at infinity be torsion – is *exceptional*.

3.5. Base fields of characteristic 2

Of course remarks about $Y^2 = D$ make no sense in characteristic 2. That's easily dealt with. First set $D = S^2 + 4R$ with polynomials S and R and next, in place of the curve $Y^2 - D = 0$ consider the curve $Z^2 - SZ - R = 0$. Then Z is well defined whenever D is, including in characteristic 2, and one may usefully study a continued fraction expansion with complete quotients $(Z + P'_h)/Q'_h$ obtained in effect by dividing the expansion of Y by 2, so that $P_h = S + 2P'_h$. The sequence of Mumford representations of the appropriate multiples of the divisor at infinity on (the Jacobian of) the curve $Z^2 - SZ - R = 0$ is now given by the pairs $(Q'_h, -P'_h)$.

Table 1.

h	$a_h(X)$	$Q_h(X)$
0	$4X^{10}+4X^8+X^4+4X^3+X+1$	1
1	$3X^5+X^3+X$	$X^3(X+1)(X+4)$
2	$2X+3$	$Q_2(X)$
3	$3X^2+3X+3$	$X^5(X+2)(X+3)(X+4)$
4	$3X^4+3X^2$	X^6
5	$3X^5+2X^4+3X^3+2X^2+3X+2$	$X^2(X+1)(X+2)(X+3)$
6	$2X^2+2$	$4X^8+X^2+1$
7	$3X^6+3X^5+3X^4+3X^3+3X^2+3X$	$X(X+2)(X+3)(X+4)$
8	$2X+3$	$Q_8(X)$
9	$3X$	$X^7(X+1)(X+4)$
10	$2X+2$	$Q_{10}(X)$
11	$3X^3+2X^2+3X+2$	$X^4(X+1)(X+2)(X+3)$
12	$3X^6+3X^4+2$	X^4
13	$2X$	$4X^9+4X^7+X^3+X+1$
14	$3X^7+X^5+X^3+3X+3$	$X(X+1)(X+4)$
15	$3X^8+3X^6+2X^2+3X$	X^2
16	$3X+2$	$X^6(X+1)(X+2)(X+3)$
17	$2X+2$	$Q_{17}(X)$
18	$3X^3+X$	$X^5(X+1)(X+4)$
19	$2X+3$	$Q_{19}(X)$
20	$3X^4+3X^3+3X^2+3X+3$	$X^3(X+2)(X+3)(X+4)$
21	$3X^2+3$	X^8
22	$3X^7+2X^6+3X^5+2X^4+3X^3+2X^2+3$	$(X+1)(X+2)(X+3)$

3.6. A sequence of curves in characteristic 5

Here is an example of a sequence of curves where the divisor at infinity is torsion of order $O(g^2)$ if the base field is $\mathcal{F}_5$. Consider the curves $\mathcal{C}_n$ defined by

$$\mathcal{C}_n : \quad Y^2 = \left(4(X^2+1)X^n + X^4 + 4X^3 + X + 1\right)^2 + (X^2+4)X^3 .$$

In this example the divisor at infinity is torsion of order g^2; if the base field does not contain $\mathcal{F}_5$ this will not be so.

The expansion for $n = 8$ over $\mathcal{F}_5$ is given in Table 1; Q_2, Q_8, Q_{10}, Q_{17}, and Q_{19} have been suppressed because they are too ugly to fit the table.

Line 22 is halfway in the expansion because of the symmetry under conjugation entailed by $(X+1)(X+2)(X+3)$ dividing Y^2 over $\mathcal{F}_5[X]$. The period lengths and regulators satisfy the values in Table 2.

Table 2.

$n \pmod 6$	$lp(Y)$	$R(Y)$
0	$2n-2$	$\frac{1}{3}(2n^2+2n+3)$
$2,4$	$6n-4$	$2n^2+2n+3$

4. Main Result

Our comments on the connection between torsion divisors on Jacobians of hyperelliptic curves and continued fraction expansions now allow us to state our main results; we do that in terms of the divisor at infinity rather than at 1. The relevant transformation if effected by

$$X = \frac{1}{1-x} \quad \text{and} \quad Y = \frac{y}{(1-x)^{2g+2}} \,, \tag{4.1}$$

and it transforms the curves (2.1) into

$$y^2 = (rx^n + mx^k - l)^2 + 4rlx^n \,.$$

The terms r, l, m are now rational fractions in x derived from the corresponding functions on X.

Taking the inverse transformation will generically yield functions f_1, f_2, f_3 of degree $g+1$. However, there are exceptions typified by the example

$$y^2 = \big((1-x)x^n - x^k + 1\big)^2 - 4(x-1)x^n \,.$$

Here the term $(1-x)x^n$ transforms into $(X-(X-1))(X-1)^n$. This is f_1 in the earlier notation. It has degree $n+k-1$, while the terms f_2, f_3 have degree $n+k$. Changing the term $(1-x)$ to $t(1-x)$, which does not affect divisibility, yields the example on page 347.

We say that a sequence of positive integers (s_n) is of *quadratic order* in n if $s_n = an^2 + bn + c$ for some $a, b, c \in \mathcal{Q}$.

Theorem 4.1 (Main Theorem). *For $n = 1, 2, \ldots$ set*

$$\mathcal{C}_n \;:\quad d^2Y^2 = \big(qrf^n + (mf^k - l)/q\big)^2 + 4lrf^n \tag{4.2}$$

where each term on the right is a nontrivial polynomial, specifically with f irreducible, r, l, and m squarefree, and d chosen to ensure that Y^2 be squarefree, and so that

$$(qr, ml) = 1 \,, \quad (f, qrml) = 1 \,, \quad (m, l) = 1 \,, \quad \text{and} \quad q \mid (mf^k - l) \,.$$

Then the divisor at infinity on the Jacobian of $\mathcal{C}_n$ is torsion of quadratic order in n.

Proof. As a complete proof of this result, using only elementary methods, is given for the rather more delicate number field case in pp. 205–212 of [16], we will give a very brief sketch of the proof here. (We say 'rather more delicate' because incidental nonintegral coefficients that would not disturb the function-theoretic expansion at all may dramatically alter the corresponding numerical expansion.) In [16], it is show by a very lengthy and intricate induction argument that in the continued fraction expansion of Y there exist certain complete quotients $(Y+P_{h_i})/Q_{h_i}$ (for $i = 1, 2, \dots$) satisfying some very technical conditions, the most important of which from our perspective is that the values of the h_i are essentially independent of the value of n. It is then shown that for any integer t

$$h_{2nt-1} = a_t n + b_t \ ,$$

where a_t and b_t are rational numbers whose values depend on t but are independent of values of n in fixed congruence classes. Finally, it is established that there exists some t such that if $j = h_{2nt-1}$, then $Q_j = 1$. For the curves under consideration this means that the period of the continued fraction expansion of Y must be linear in n. Furthermore, $R(Y) = O(n^2)$ and therefore the divisor at infinity on the Jacobian of $\mathcal{C}_n$ is torsion of quadratic order in n. ■

One notices that as $n \to \infty$ the curve $\mathcal{C}_n$ has genus $n \deg(f) + O(1)$. Our earlier remarks presumed $q = d = 1$. The extra 'frill' q has little influence on the divisors. The removal of square factors provided by d is essential in the present function field case because a change of conductor, say replacing Y by dY, might radically change the torsion group of the Jacobian of the curve.

4.1. Genesis of our results

Our result has several sources. One is a history of constructions of sequentially increasing complexity (in effect, inclusion of more and more frills) of sequences of quadratic number fields of discriminants (D_n) with *explicitly computable* fundamental unit, say (u_n), and regulator (thus the logarithm of u_n) of size at least $O((\log D_n)^2)$. Another is a question of Schinzel [20, 21] who asks for polynomials D say defined over $\mathcal{Z}$ so that the period length of the continued fraction expansion of $\sqrt{D(n)}$ is bounded for integers n. The answer nicely connects numerical expansions with those in function fields.

(i) D must have square leading coefficient and be of even degree, say $\deg(D) = 2g + 2$.
(ii) Set $Y^2 = D(X)$, The domain $\mathcal{Q}[X][Y]$ must be *exceptional* in that it contains a nontrivial unit; in effect, the numerical periods all come from "numberisation" of the function field period.
(iii) Some such unit must *specialize* (writing $X = n$) to a unit in the number field.

Loosely speaking, our result derives from the numerical results detailed in [16] in the spirit of Schinzel's theorems. That this is so is all the more clear on

constructing an exceptional unit in the function field by the argument sketched in [15]; for a history of the numerical constructions see Chapter II of [14].

When D is quadratic, thus the $g = 0$ case, the second of Schinzel's conditions is always satisfied so only the third numerical condition is required. That gives rise to additional families of quadratic discriminants (D_n) for which one may explicitly compute the fundamental unit. However, their regulator is only of size $O(\log D_n)$. A simple transformation shows that the sequence

$$Y^2 + X^g Y + Y = X^{2g+1} + X^{g+1}$$

given by Flynn [6] is a function field analogue with torsion divisor of linear order in the genus.

4.2. A stripped example

One can get the correct feel for the content of the Main Theorem by studying the example

$$Y^2 = (X^{g+1} + X^k - 1)^2 + 4X^{g+1}\,, \tag{4.3}$$

where all the frills have been removed.

Set $S_1 = X^{g+1} + X^k - 1$, $S_2 = X^{g+1} - X^k + 1$, and $S_3 = X^{g+1} + X^k + 1$. Then the continued fraction expansion of Y is

$$\begin{array}{rcll}
Y & = & S_3 & - \quad (\overline{Y} + S_3) \\
(Y + S_3)/-4X^k & = & \frac{1}{2}(X^{g+1-k} + 1) & - \quad (\overline{Y} + S_1)/-4X^k \\
(Y + S_1)/-X^{g+1-k} & = & -2X^k & - \quad (\overline{Y} + S_2)/-X^{g+1-k} \\
(Y + S_2)/-4X^{2k} & = & -\frac{1}{2}X^{g+1-2k} & - \quad (\overline{Y} + S_1)/-4X^{2k} \\
(Y + S_1)/-X^{g+1-2k} & = & -2X^{2k} & - \quad (\overline{Y} + S_2)/-X^{g+1-2k} \\
 & \vdots & & \\
(Y + S_1)/-X^j & = & -2(X^{n+j} + X^{k-j}) & - \quad (\overline{Y} + S_3)/-X^j \\
(Y + S_3)/4X^{k-j} & = & \frac{1}{2}(X^{n-k+j} + X^j) & - \quad (\overline{Y} + S_1)/4X^{k-j} \\
(Y + S_1)/X^{n+j-k} & = & 2X^{k-j} & - \quad (\overline{Y} + S_2)/X^{n+j-k} \\
 & \vdots & &
\end{array}$$

where $j = n - \lfloor n/k \rfloor k$. Hence the multiples of $(\infty^+ - \infty^-)$ are simply $i(0, \pm 1) + j(\infty^+ - \infty^-)$ for $0 \le i \le g$, $0 \le j \le g + 1 - i$.

Notice the similarity to Flynn's example on page 347. Indeed, this curve is that example other than that there $r = t(1 - X)$. One sees that the effect of r is, at best, to double the period length of the expansion of Y.

4.3. Redressing the example

Reintroducing nontrivial l and m has somewhat more drastic effects on the expansion. Each introduces a bounded number of partial quotients between pairs of steps in the simplified expansion above; those partial quotients are fairly readily expressed in terms of q, r, lm, and X.

However it is the sum of the degrees of the partial quotients that gives us the torsion order of the divisor at infinity. Fortunately it is plain that the degree added by the extra steps is no more than $O(g)$. That follows immediately from there being only a bounded number of new steps introduced between each pair of complete quotients above and from the period length of Y being linear in g.

Readers keen to see the nastiness of the extra intermediate divisors introduced by the parameters l and m will choose to compute the Q_h's suppressed in the example on page 349.

Our opening discussion back on page 347 suggested that D_1 could be of torsion order as great as $8g^2$ or so. Indeed, Leprévost has given an example where D_1 has order $4g^2$. However it is clear from the present example that the divisor at infinity cannot have order noticeably greater than $2g^2$. Indeed, it has order $2g^2$ because, as remarked, l, and m cannot introduce more than $O(g)$ extra multiples. The reason for this distinction is that the transformation (4.1) is a biregular morphism of the Jacobian but that it is not a group homomorphism.

4.4. A converse to the main result

The investigations in [14] do suggest a converse to the Main Theorem. In brief, consider $\mathcal{C}_n : F(X) = A^2 f^{2n} + Bf^n + C^2$ with f irreducible (simply thinking $f = X$ will do) and suppose that the divisor at infinity on the Jacobian of $\mathcal{C}_n$ is torsion of quadratic order $an^2 + bn + c$ in n. The question is whether the $\mathcal{C}_n$ must be given by (4.2) as in the Main Theorem. In different words: do q, r, l and m provide all the frills that can be added to the stripped example without destroying its exceptional behavior? We know that, at the least, additional conditions are required beyond those just now stated. Certainly, some multiple of the divisor at infinity must be given by a power of f (for some positive j some Q_h must be of the shape f^j). The numerical context from which our result arises means we must insist that the period length is *a priori* linear in n (in any case, we know no families of longer period for which we can in fact explicitly compute a fundamental unit). Given those extra conditions, counting arguments do allow a proof [16], p. 204 that the $\mathcal{C}_n$ are those of the Main Theorem if the base field $\mathcal{K} = \mathcal{F}_q$ is finite.

Of course over a finite base field we do not need the presumption that the divisor at infinity is torsion of quadratic order. We recall that quadratic irrationals over $\mathcal{F}_q(X)$ a priori have periodic continued fraction expansion because the box principle eventually guarantees that the expansion produces some Q_h in $\mathcal{F}_q^*$; then the period length is sh for some appropriate divisor s of $q - 1$. However, if the sequence (4.2) of the Main Theorem is periodic then it turns out that the first Q_h in $\mathcal{F}_q^*$ in fact is 1, so the period lengths are effectively independent of q. Given that, it may well be that no more than just a mildly ingenious additional remark is needed to establish the converse over infinite fields.

4.5. Torsion subgroups and torsion divisors

We speak only of multiples of the one fixed divisor and thus say little about the torsion subgroup. Indeed, it is easy to construct sequences of hyperelliptic curves whose Jacobians contain subgroups of order at least g^2. The sequence

$$\mathcal{C}_g \ : \quad Y^2 = (aX^{g+1} + b)^2 + 4acX^{g+1} \quad \text{where } b + c \neq 0 \tag{4.4}$$

is one such example. Here we also have

$$Y^2 = (aX^{g+1} + b + 2c)^2 - 4c(b + c) \ ,$$

so the divisor $(\infty^+ - \infty^-)$ is of order $g + 1$; from (4.4) we read that the divisor $(Y + aX^{g+1} + b)$ also has torsion order $g + 1$. Hence $\mathcal{Z}_{g+1} \times \mathcal{Z}_{g+1}$ is a factor of the torsion subgroup of the Jacobian of $\mathcal{C}_g$.

All the more, the Jacobian of

$$Y^2 = (X + 1)(X + 2) \cdots (X + 2g + 1)$$

clearly has $2g + 1$ independent Weierstrass points, hence 2^{2g} divides the order of its torsion subgroup[1].

Plainly, it is necessary firmly to distinguish the case of calculating the full torsion subgroup from calculating the cyclic subgroup by some fixed divisor.

4.6. A bound on the torsion order?

As remarked at page 348, it is exceptional for the continued fraction expansion of the square root of a polynomial defined over an infinite field to be periodic. Thus the function fields of the curves comprising the sequences of the Main Theorem are exceptional. Moreover, they are interesting in having relatively large regulators. Indeed, it is not known if there exist sequences whose regulators are larger than $O(g^2)$.

4.7. A diagonal generalization

One may choose to study a sequence of curves

$$Y^2 = a_{2g+2}X^{2g+2} + a_{2g+1}X^{2g+1} + \cdots + a_1X + a_0$$

where each a_i is a function which depends on g. It is known that one can construct such sequences with non-trivial torsion divisors, and typically the a_i turn out to be linear recurrence sequences rather than polynomials. This is the point of view established in Madden [13]. Taking a sequence of sequences each satisfying the conditions of the Main Theorem and selecting an appropriate diagonal retrieves those results.

[1] An analogue in the number field setting is the sequence of quadratic fields of discriminant $D_n = \prod_{i=1}^{n} p_i$ where p_i is the i-th prime. There 2^{n-1} divides the order of the ideal class group.

5. Results in Genus 1 and 2

Consideration of the curves constructed by the Main Theorem in genus 1 and 2 shows that many of the known parametrized families of curves with torsion divisors are instances of our sequences. This degeneralization is a converse of Flynn's construction [5] of infinite sequences from a particular curve.

The quartic model of an elliptic curve with a 5-torsion point is given by

$$Y^2 = (X^2 + 2(t-1)X + 4t)^2 + 32tX \ .$$

This is $\mathcal{C}_1$ from (4.2) with the selections

$$r = X + 2t \ , \quad m = -2 \ , \quad l = 4t \ , \quad k = q = 1 \ .$$

5.1. High torsion in genus 2

Many of the genus 2 curves with non-trivial torsion divisors given by Leprévost [8, 9, 11] are special cases of curves from the Main Theorem; indeed Leprévost finds his curves by specializing infinite families.

The simplest curves of genus 2 from the Main Theorem are

$$Y^2 = (rX^3 + sX^k - t)^2 + 4rtX^3 \quad \text{where } k = 1, 2 \text{ and } r, s, t \in \mathcal{Q} \tag{5.1}$$

and have torsion of order 9. This family seems to be a 3-parameter family, however the transformation $X \mapsto X/r$, $Y \mapsto Y/r^2$ transforms (r, l, m) into $(1, mr, lr^2)$; it is thus just a 2-parameter family.

Another simple family is

$$Y^2 = \big((X-t)X^2 + X - t\big)^2 + 4t(X-t)X^2$$

with torsion 13.

We are fortunate to have Poonen's algorithm [17] for determining the torsion subgroup of the Jacobian, now implemented in MAMGA for hyperelliptic curves of genus 2. This assists us in detailing two slightly more complicated examples, namely

$$Y^2 = \big((X+1)X^2 + (t-1)X^2 - (X+t)\big)^2 + 4(X+t)(X+1)X^2 \tag{5.2}$$

with a torsion subgroup of order 20 and

$$Y^2 = \big((X-t^2)X^2 + (X+1)X - t^3(t+1)\big)^2 + 4t^3(t+1)(X-t^2)X^2$$

with order 22 – the extravagant equations emphasize the the connection with (4.2).

In some cases, one can find subsets of the stated curves with extra 2-torsion. For example, the curve (5.2) with $t = 4$ is

$$Y^2 = (X^3 + 4X^2 + X - 2)^2 + 12(X+1)$$

and has a torsion divisor of order 40. This is the extreme example given by Elkies [4].

As further instance, the family

$$Y^2 = \big(t(X-1)X^2 + X^2 + 1\big)^2 - 4X^2$$

has a divisor of order 14. However, if we take the subfamily $t = s(s+1)$ with $s \geq 1$ we find that $\mathcal{Z}_2 \times \mathcal{Z}_{14}$ is a factor of the torsion subgroup. The extra torsion is easily explained. The function Y^2 has a factor $tX^2 + X - 1$; when $t = s(s+1)$ this factor splits as $(sX+1)((s+1)X-1)$. More, when $s = 4$ we find, via Poonen's algorithm, that the complete torsion subgroup is $\mathcal{Z}_2 \times \mathcal{Z}_{28}$.

These examples remind us that 2-torsion can be gained by finding specific curves with extra linear factors. Finding curves with additional odd torsion is not as straightforward. However, even for the simple curves in (5.1), taking $r = l = 3$ and $m = 8$ yields a curve with torsion order 27 instead of the expected order 9.

In theory, the Main Theorem should be able to yield curves which have larger torsion subgroups than Leprévost's examples. However, in practice finding functions over $\mathcal{Q}$ simultaneously satisfying the various division requirements is difficult, particularly in low genus. Unsurprisingly, over appropriate finite base fields, divisibility comes rather more easily.

5.2. Generalizing elliptic curves with 7-torsion

The Main Theorem deals with curves with points of fairly small torsion order. In contrast, the family

$$Y^2 = \big(X^2 + (t^2 - t - 1)X + t^2(t-1)\big)^2 + 4t^2(t-1)X \tag{5.3}$$

contains an elliptic curve with a 7-torsion point; but (5.3) is not a curve included in our result. Moreover, we can construct new more complicated sequences of curves with torsion divisors – as in Victor Flynn's approach. Indeed, to construct the unit of $\mathcal{Q}[X,Y]$, with Y given by (5.3), we notice that

$$\begin{aligned} Y^2 &= (X^2 + (t^2 - t - 1)X \ \ + t^2(t-1))^2 + 4t^2(t-1)X \\ &= (X^2 + (t^2 - t - 1)X \ \ - t^2(t-1))^2 + 4t^2(t-1)X(X + t(t-1)) \\ &= (X^2 + (t^2 - 3t + 1)X - t^2(t-1))^2 + \quad 4(t-1)X(X + t(t-1))^2 \end{aligned}$$

and then form the unit by sequentially multiplying the ideals associated to each of the lines above, equivalently by adding the relevant divisors.

Here, as throughout, we have $Y^2 = S^2 + 4R$ for several pairs of polynomials (S,R). That gives us several $\mathcal{K}[X,Y]$-ideals $\langle R, \frac{1}{2}(Y+S)\rangle_{\mathcal{K}[X]}$, presented as $\mathcal{K}[X]$-modules. Note that, exactly because R divides the norm $(Y+S)(\overline{Y}+S) = -Y^2 + S^2$, such a module indeed is a $\mathcal{K}[X,Y]$-ideal.

Set $\mathfrak{a} = \langle R, \frac{1}{2}(Y+S)\rangle$, and so on. One knows, in effect from formulas for composing quadratic forms, that two such ideals $\mathfrak{a}$ and $\mathfrak{a}'$ *multiply nicely*, thus

yielding an ideal that is not less reduced than the given ideals, precisely when $\gcd(R, R', (\overline{S} + S'))$ is large; one's preference is that $\gcd(R, R')$ divides $(\overline{S} + S')$.

Above we have $R = t^2(t-1)X$ and $R' = t^2(t-1)X(X + t(t-1)) = R(X + t(t-1))$. Thus, recall that here t is just some suitable rational, $\gcd(R, R') = X$ whilst $\frac{1}{2}(S + S') = X^2 + (t^2 - t - 1)X$ obviously is divisible by X. Similarly the multiplication $\mathfrak{a}\mathfrak{a}''$ is a nice one. Just so, noting $R'' = (t-1)X(X + t(t-1))^2$, we have

$$\gcd(R', R'') = X(X + t(t-1))$$

while

$$\frac{1}{2}(S' + S'') = X^2 + (t^2 - 2t)X - t^2(t-1) = (X - t)(X + t(t-1)) \; .$$

This provides a large enough common divisor, $(X + t(t-1))$, to make $\mathfrak{a}'\mathfrak{a}''$ a nice multiplication.

This sort of thing makes clear that our ability to choose S, S', and S'' above as we have is not just fortuitous but actually is an essential part of our ability explicitly to obtain a nontrivial unit. Mind you, for the example (5.3) the discussion above is overkill because the list of reduced ideals provided by the continued fraction expansion is short enough not to warrant a diversion via the non-reduced ideals $\mathfrak{a}'$ and $\mathfrak{a}''$.

Suppose, however, we replace X by X^{n+2} throughout and, having done that, we set t to be some polynomial in X. Now, already so that the multiplication $\mathfrak{a}\mathfrak{a}'$ be nice, we will want that $t^2(t-1)$ and $X^{n+2}(X^{n+2} + (t^2 - t - 1))$ have a substantial common factor. The conditions $t \mid X^{n+2}$ and $t \neq 1$ turn out to be necessary and sufficient for our needs and there then is no loss of generality in always taking $t = X$ as n varies through the nonnegative integers.

That leads to Y^2 having a square factor X^4. After removing it we turn to studying a straightforward generalization of the situation we considered above, namely the sequence of curves

$$\begin{aligned} Y^2 &= \left(X^{2n+2} + (X^2 - X - 1)\, X^n + (X - 1)\right)^2 + 4X^2(X-1)X^n \\ &= \left(X^{2n+2} + (X^2 - X - 1)\, X^n - (X - 1)\right)^2 + 4(X-1)X^{n+1}(X^{n+1} + X - 1) \\ &= \left(X^{2n+2} + (X^2 - 3X + 1)X^n - (X - 1)\right)^2 + 4(X-1)X^n(X^{n+1} + X - 1)^2 \; . \end{aligned} \tag{5.4}$$

Strategic multiplication of the corresponding three ideals $\mathfrak{b}_n$, $\mathfrak{b}'_n$, and $\mathfrak{b}''_n$ eventually produces a unit. One best commences by first computing $\mathfrak{b}_n\mathfrak{b}'_n$ and $\mathfrak{b}'_n\mathfrak{b}''_n$ and then multiplying those two products. The continued fraction expansion of Y has period length $12n$ and, a more important quantity, regulator $7n^2 + 9n + 3$; thus the corresponding Jacobian contains a divisor of order $7n^2 + 9n + 3$. For details see [14], §28. But we remarked above that the sequences of curves of the Main Theorem cannot have torsion greater than $2g^2$ or so at infinity. It follows that the sequence of curves given by (5.4) is distinct from those of our result.

In fact, each curve of the sequence (5.4) is distinct from any of the curves of (4.2) of the Main Theorem. We know this from studying the multiples of the divisor at infinity by way of the continued fraction expansion of Y. Specifically, one notices that the continued fraction expansion supplies complete quotients whose denominators are of the shape TX^j where T contains primes which split, that is which divide Y^2, whereas none of the curves of the Main Theorem supplies a complete quotient of that kind.

6. Concluding Remarks

One may attempt to repeat the methods of the preceding section to construct sequences of curves from other hyperelliptic curves with a torsion divisor. However, it seems that not all such curves permit an extension. For instance, the Schinzel conditions of page 351 seem to inhibit extension of elliptic curves with a torsion point of order 10 or 12 to an infinite sequence of curves with torsion of quadratic order in the genus.

We do not know any parametrized families of numerical quadratic discriminants D_n with regulator of order greater than $O((\log D_n)^2)$ and *a fortiori* no families of hyperelliptic curves $\mathcal{C}_g$ over an infinite field with torsion divisor greater than $O(g^2)$ as their genus g goes to infinity. Patterson's investigations [14] are such as to recommend a wager on there in fact not being any such examples.

On the other hand higher degree analogues have barely been studied. Exceptions include the work cited and generalized by Brigitte Adam [1], suggesting that sequence of curves $\mathcal{C}_n$ given by

$$Y^3 - qX^nY^2 - (X^k - 1)Y - qX^n = 0\,,$$

where the polynomial q divides $X^k - 1$, have Jacobians with torsion divisors of quadratic order. There are also several known instances of linear torsion [18, 19].

References

[1] Brigitte Adam, *Généralisation d'une famille de Shanks*, Acta. Arith. **84** (1998), no. 1, 43–58. MR **1613298** (**99d:**11115)

[2] William W. Adams and Michael J. Razar, *Multiples of points on elliptic curves and continued fractions*, Proc. London Math. Soc. (3) **41** (1980), no. 3, 481–498. MR **591651** (**82c:**14031)

[3] T. G. Berry, *Continued fractions in hyperelliptic function fields*, Coding theory, cryptography and related areas (Guanajuato, 1998), Springer, Berlin, (2000), pp. 29–41. MR **1749446** (**2001c:**14050)

[4] N. D. Elkies, *Simple genus 2 Jacobians with high order torsion points* **http://www.math.harvard.edu/ elkies/g2_tors.html**

[5] E. V. Flynn, *Large rational torsion on abelian varieties*, J. Number Theory **36** (1990), no. 3, 257–265. MR **1077707** (**92b:**11036)

[6] ———, *Sequences of rational torsions on abelian varieties*, Invent. Math. **106** (1991), no. 2, 433–442. MR **1128221** (**93b:**11075)

[7] Everett W. Howe and Franck Leprévost and Bjorn Poonen, *Large torsion subgroups of split Jacobians of curves of genus two or three*, Forum Math. **12** (2000), no. 3, 315–364. MR **1748483** (**2001e:**11071)

[8] Franck Leprévost, *Famille de courbes de genre 2 munies d'une classe de diviseurs rationnels d'ordre 13*, C. R. Acad. Sci. Paris Sér. I Math. **313** (1991), no. 7, 451–454. MR **1127938** (**93b:**14053)

[9] ———, *Familles de courbes de genre 2 mumies d'une classe de diviseurs rationnels d'ordre 15, 17, 19 ou 21*, C. R. Acad. Sci. Paris Sér. I Math. **313** (1991), no. 11, 771–774. MR **1139836** (**92m:**14036)

[10] ———, *Famille de courbes hyperellipitques de genre g munies d'une class de diviseurs rationnels d'ordre* $2g^2 + 4g + 1$, Séminaire de Théorie des Nombres, Paris, 1991–92. Progr. Math., vol. 116, Birkhäuser Boston, Boston, MA, 1993, pp. 107–119. MR **1300885** (**96a:**11057)

[11] ———, *Jacobiennes de certaines courbes de genre 2: torsion et simplicité*, J. Théor. Nombres Bordeaux **7** (1995), no. 1, 283–306. MR **1413580** (**98a:**11078)

[12] ———, *Sur certains sous-groupes de torsion de Jacobiennes de courbes hyperelliptiques de genre* $g \geq 1$, Manuscripta Math. **92** (1997), no. 1, 47–63. MR **1427667** (**98a:**11079)

[13] Daniel J. Madden, *Constructing families of long continued fractions* Pacific J. Math. **198** (2001), no. 1, 123–147. MR **1831975** (**2002b:**11014)

[14] Roger D. Patterson, *Creepers: Real quadratic fields with large class number*, Ph.D. thesis, Macquarie University, Sydney, 2003, Manuscript available at **http://arxiv.org/abs/math/0703519**

[15] Roger D. Patterson and Alfred J. van der Poorten, *Jeepers, creepers, ...*, High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, Fields Inst. Commun., vol. 41, Amer. Math. Soc., Providence, RI 2004, pp. 305–316. MR **2076255** (**2005g:**11208)

[16] Roger D. Patterson and Alfred J. van der Poorten and Hugh C. Williams, *Characterization of a generalized Shanks sequence*, Pacific J. Math. **230** (2007), no. 1, 185–215. MR **2318452**

[17] Bjorn Poonen, *Computing torsion points on curves*, Experiment. Math. **10** (2001), no. 3, 449–465. MR **1917430** (**2003k:**11104)

[18] Renate Scheidler, *Purely cubic complex function fields with short periods*, Publ. Math. Debrecen **54** (1999), no. 3-4, 497–511. MR **1694527** (**2000c:**11190)

[19] ———, *Purely cubic complex function fields with small units*, Acta. Arith. **95** (2000), no. 4, 289–304. MR **1785197** (**2001g:**11178)

[20] A. Schinzel, *On some problems of the arithmetical theory of continued fractions*, Acta. Arith. **6** (1960/1961), 393–413. MR **0125814** (23 #A3111)

[21] ———, *On some problems of the arithmetical theory of continued fractions. II*, Acta. Arith. **7** (1961/1962), 287–298. MR **0139566** (25 #2998)

Addresses: R.D. Patterson: Department of Mathematics and Statistics, University of Calgary, Calgary, AB, Canada, T2N 1N4; A.J. van der Poorten: ceNTRe for Number Theory Research, 1 Bimbil Pl., Killara, NSW 2071, Australia; H.C. Williams: Department of Mathematics and Statistics, University of Calgary, Calgary, AB, Canada, T2N 1N4

E-mail: rogerp@math.ucalgary.ca, alf@maths.usyd.edu.au, williams@math.ucalgary.ca

Received: 31 December 2007; **revised:** 20 October 2008