Fields Institute Communications
Volume **60**, 2011

The ℓ-Rank Structure of a Global Function Field

Lisa Berger
Mathematics Department
Stony Brook University
Stony Brook, NY 11794-3651, USA
lbrgr@math.sunysb.edu

Jing Long Hoelscher
Department of Mathematics, Statistics, and Computer Science
University of Illinois at Chicago
851 S. Morgan Street
Chicago, IL 60607-7045, USA
jlong@math.uic.edu

Yoonjin Lee
Department of Mathematics
Ewha Womans University
11-1 Daehyun-Dong
Seodaemun-Gu
Seoul 120-750, South Korea
yoonjinl@ewha.ac.kr

Jennifer Paulhus
Department of Mathematical Sciences
Villanova University
800 Lancaster Avenue
Villanova, PA 19085-1699, USA
jennifer.paulhus@villanova.edu

Renate Scheidler
Department of Mathematics and Statistics
University of Calgary
2500 University Drive NW
Calgary, AB T2N 3Z4, Canada
rscheidl@ucalgary.ca

2010 *Mathematics Subject Classification.* Primary 11R58; Secondary 11R65, 11Y40, 14Q05, 14H05.

The third author is the corresponding author and is supported by Priority Research Centers Program through the National Research Foundation of Korea (NRF), funded by the Ministry of Education, Science and Technology (2009-0093827).

The last author is supported by NSERC of Canada.

Abstract. For any prime ℓ, it is possible to construct global function fields whose Jacobians have high ℓ-rank by moving to a sufficiently large constant field extension. This was investigated in some detail by Bauer et al. in [2]. The two main results of [2] are an upper bound on the size of the field of definition of the ℓ-torsion $\mathcal{J}[\ell]$ of the Jacobian, and a lower bound on the increase in the base field size that guarantees a strict increase in ℓ-rank. Here, we provide improvements to both these results, and give examples which illustrate that our techniques have the potential to yield the correct ℓ-rank over any intermediate field of the field of definition of $\mathcal{J}[\ell]$, including base fields that might be too large to be handled directly by computer algebra packages.

1 Introduction

Let q be any prime power and ℓ a prime not dividing q. Then the Jacobian of any function field $\mathbb{K}/\mathbb{F}_q$ is a finite Abelian group that can have ℓ-rank as large as $2g$. However, Jacobians of large ℓ-rank, and even just positive ℓ-rank, tend to be rare. This statement was made precise by Achter [1], who gave for any r with $0 \le r \le 2g$ and any sufficiently general family of curves over $\mathbb{F}_q$ an explicit formula for the proportion of curves whose Jacobians have ℓ-rank r over $\mathbb{F}_q$. For example, if $q \equiv 1 \pmod{\ell}$, then an elliptic curve has ℓ-rank 0, 1, or 2 over $\mathbb{F}_q$ with approximate probabilities $1 - \ell/(\ell^2-1)$, $1/\ell$, and $1/\ell(\ell^2-1)$, respectively. Similar behaviour holds for curves of higher genus.

It is thus clear that algebraic function fields of high ℓ-rank require special construction. For genus 2 hyperelliptic curves $y^2 = f(x)$ with $f(x) \in \mathbb{F}_q[x]$ square-free and $\deg(f) = 5$, the 2-rank can simply be read from the factorization of $f(x)$ into irreducibles over $\mathbb{F}_q$ [12]. In fact, the 2-rank of a quadratic function field is generally well understood [18]. A number of constructions for hyperelliptic curves of high 3-rank were presented in [2]; see also Chapter 7 of [16] for a somewhat different approach to generating such fields via cubic extensions. In a sequence of papers, Pacelli et al. found infinite families of quadratic [10, 11] and higher degree [13, 14] function fields of large 3-rank, and more generally, n-rank.

In this paper, we focus our attention on a method that constructs arbitrary function fields of large ℓ-rank by enlarging the base field $\mathbb{F}_q$. This procedure was first presented in Section 5 of [2], where it was described in the context of hyperelliptic function fields, but it is applicable to any type of function field $\mathbb{K}/\mathbb{F}_q$ — and in fact, any Jacobian variety — and any prime $\ell \nmid q$. The technique has the advantage that one can start with a function field $\mathbb{K}$ of any genus g over a very small base field $\mathbb{F}_q$. It requires the computation of the L-polynomial of $\mathbb{K}$ over this small field $\mathbb{F}_q$, which can be accomplished with a computer algebra package such as Magma [4]. Using only the factorization modulo ℓ of the reciprocal polynomial $F(t) \equiv t^{2g}L(t^{-1}) \pmod{\ell}$ of this L-polynomial, it is possible to find an upper bound on the degree n_ℓ over $\mathbb{F}_q$ of the field of definition of the full ℓ-torsion of the Jacobian of $\mathbb{K}/\mathbb{F}_q$. This factorization also provides lower bounds on the minimal extension degree over any base field that guarantees an increase in ℓ-rank, as well as a lower bound on that ℓ-rank increase.

The results in this article represent a number of improvements to the work of [2, Section 5]. We provide a simpler means for finding good upper bounds on n_ℓ and analyze the possible ℓ-ranks over all intermediate base fields $\mathbb{F}_q \subset \mathbb{F}_{q^n} \subset \mathbb{F}_{q^{n_\ell}}$.

In many cases, our results make it possible to find all these intermediate ℓ-ranks, requiring the computation of the L-polynomial $L(t)$ of $\mathbb{K}$ over the base field $\mathbb{F}_q$ only. Sometimes, the ℓ-rank of the Jacobian over an intermediate field $\mathbb{F}_{q^n}$ for very small n may also be needed. Apart from these ingredients, our methods involve only basic algebra and linear algebra.

We begin with an overview of the techniques of [2] in Section 3 and describe our improvements in Sections 4, 5 and 7, illustrating them with a number of examples. In the process, we rediscover and improve on known results for curves of genus 1 and 2 in Section 6.

2 Background and notation

For introductory reading on algebraic function fields, the reader is encouraged to consult [15, 17]. Throughout this paper, q will denote a prime power, $\mathbb{F}_q$ a finite field of order q, $\overline{\mathbb{F}}_q$ an algebraic closure of $\mathbb{F}_q$, and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. Furthermore, $\mathbb{F}_q[x]$ and $\mathbb{F}_q(x)$ are the ring of polynomials and the field of rational functions, respectively, in the indeterminate x with coefficients in $\mathbb{F}_q$. For $F \in \mathbb{F}_q[x]$, $\deg(F)$ denotes the degree of F.

An *algebraic function field* $\mathbb{K}/\mathbb{F}_q$ (of one variable over $\mathbb{F}_q$) is a finite algebraic extension of $\mathbb{F}_q(x)$. If $[\mathbb{K} : \mathbb{F}_q(x)]$ denotes the degree of the extension $\mathbb{K}/\mathbb{F}_q(x)$, then $\mathbb{K} = \mathbb{F}_q(x, y)$ where y is the root of some polynomial $F(x, Y) \in \mathbb{F}_q[x][Y]$ that is monic with respect to Y, has degree $[\mathbb{K} : \mathbb{F}_q(x)]$ in Y, and is irreducible over $\mathbb{F}_q(x)$. We will always assume that $\mathbb{F}_q$ is the *(full) constant field* of $\mathbb{K}$; that is, $\mathbb{F}_q$ is algebraically closed in $\mathbb{K}$. Equivalently, the polynomial $F(x, Y)$ is absolutely irreducible, i.e. irreducible over $\overline{\mathbb{F}}_q$.

Recall that a *place* $\mathfrak{p}$ of $\mathbb{K}/\mathbb{F}_q$ is the unique (principal) maximal ideal of some discrete valuation ring $\mathcal{O} = \mathcal{O}_\mathfrak{p}$ of $\mathbb{K}$. We denote the set of places of $\mathbb{K}/\mathbb{F}_q$ by $\mathbb{P}_\mathbb{K}$. A *divisor* D of $\mathbb{K}/\mathbb{F}_q$ is a formal sum of places, i.e. $D = \sum_{\mathfrak{p}\in\mathbb{P}_\mathbb{K}} a_\mathfrak{p}\mathfrak{p}$ where $a_\mathfrak{p} = 0$ for all but finitely many $\mathfrak{p} \in \mathbb{P}_\mathbb{K}$. The *degree* of D is the integer $\deg(D) = \sum_{\mathfrak{p}\in\mathbb{P}_\mathbb{K}} a_\mathfrak{p}$. Clearly, the divisors form an infinite Abelian group, the *divisor group* $\mathcal{D}_\mathbb{K}(\mathbb{F}_q)$ of $\mathbb{K}/\mathbb{F}_q$, and the divisors of degree zero form a subgroup of $\mathcal{D}_\mathbb{K}(\mathbb{F}_q)$, the *degree zero divisor group* $\mathcal{D}^0_\mathbb{K}(\mathbb{F}_q)$. A divisor is *principal* if there exists a non-zero element $z \in \mathbb{K}$ such that $D = \sum_{\mathfrak{p}\in\mathbb{P}_\mathbb{K}} v_\mathfrak{p}(z)\mathfrak{p}$, where $v_\mathfrak{p}$ is the discrete valuation on $\mathbb{K}$ associated to the place $\mathfrak{p} \in \mathbb{P}_\mathbb{K}$. Since every principal divisor has degree zero, the set $\mathcal{P}_\mathbb{K}(\mathbb{F}_q)$ of principal divisors is a subgroup of $\mathcal{D}^0_\mathbb{K}(\mathbb{F}_q)$.

The quotient group $\mathrm{Jac}_\mathbb{K}(\mathbb{F}_q) = \mathcal{D}^0_\mathbb{K}(\mathbb{F}_q)/\mathcal{P}_\mathbb{K}(\mathbb{F}_q)$ is the *(degree zero) divisor class group* of $\mathbb{K}/\mathbb{F}_q$; it is a finite Abelian group. The notation "Jac" stems from the following fact. There exists a unique non-singular, projective, absolutely irreducible, algebraic curve C so that $\mathbb{K}/\mathbb{F}_q$ is the function field of C. Then $\mathrm{Jac}_\mathbb{K}(\mathbb{F}_q)$ is isomorphic to the group of $\mathbb{F}_q$-rational points on the *Jacobian variety* of C. Hence, $\mathrm{Jac}_\mathbb{K}(\mathbb{F}_q)$ is sometimes simply referred to as the Jacobian of $\mathbb{K}/\mathbb{F}_q$. We denote by g the *genus* of $\mathbb{K}/\mathbb{F}_q$, or equivalently, the genus of C.

When $\mathbb{K}/\mathbb{F}_q$ has genus $g = 1$ and the set $C(\mathbb{F}_q)$ of points on C with coordinates in $\mathbb{F}_q$ is non-empty, C is an *elliptic curve*. In this case $C(\mathbb{F}_q)$ is an abelian group, where the addition is defined geometrically via the "chord and tangent" addition law, described most easily via the property "any three collinear points on the curve sum to zero". With these conditions, $\mathrm{Jac}_\mathbb{K}(\mathbb{F}_q)$ is isomorphic to $C(\mathbb{F}_q)$. Indeed, as an algebraic variety, an elliptic curve is isomorphic to its Jacobian, while for curves of higher genus this is no longer the case.

The divisor group of $\mathbb{K}/\mathbb{F}_q$ is closely related to the *zeta function* of $\mathbb{K}/\mathbb{F}_q$, i.e. the function $\zeta(s) = \sum_{D \in \mathcal{D}_{\mathbb{K}}(\mathbb{F}_q)} q^{-s \deg(D)}$. Here, s is a complex variable. If we set $t = q^{-s}$, then for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$,

$$\zeta(s) = \sum_{D \in \mathcal{D}_{\mathbb{K}}(\mathbb{F}_q)} t^{\deg(D)} = \frac{L(t)}{(1-t)(1-qt)} \ ,$$

where $L(t) = a_0 + a_1 t + \cdots + a_{2g} t^{2g}$ is called the *L-polynomial* of $\mathbb{K}/\mathbb{F}_q$. It is a polynomial of degree $2g$ with integer coefficients satisfying $a_0 = 1$ and $q^{g-i} a_i = a_{2g-i}$ for $0 \le i \le g-1$. The reciprocals of the roots of $L(t)$ are algebraic integers of absolute value $\sqrt{q}$ — this is generally referred to as the *Riemann hypothesis for function fields*, although it was in fact proved by Weil — and we have $|\operatorname{Jac}_{\mathbb{K}}(\mathbb{F}_q)| = L(1)$. This implies the *Hasse-Weil bounds*

$$(\sqrt{q}-1)^{2g} \le |\operatorname{Jac}_{\mathbb{K}}(\mathbb{F}_q)| \le (\sqrt{q}+1)^{2g} \ ,$$

which show that $\operatorname{Jac}_{\mathbb{K}}(\mathbb{F}_q)$ is a very large group even for function fields of modest size. As a result, computing the structure of $\operatorname{Jac}_{\mathbb{K}}(\mathbb{F}_q)$, or even just its order, generally tends to be a difficult problem. For small function fields, however, it is possible to compute the zeta function, L-polynomial, and possibly even the Jacobian, using for example a computer algebra package such as Magma.

For any prime ℓ, we denote the *ℓ-rank* of $\operatorname{Jac}_{\mathbb{K}}(\mathbb{F}_q)$ by $\ell\text{-rank}(\operatorname{Jac}_{\mathbb{K}}(\mathbb{F}_q))$. It is the dimension of the $\mathbb{F}_\ell$-module $\operatorname{Jac}_{\mathbb{K}}(\mathbb{F}_q)/\ell \operatorname{Jac}_{\mathbb{K}}(\mathbb{F}_q)$, which is also the minimum number of generators of the ℓ-Sylow subgroup of $\operatorname{Jac}_{\mathbb{K}}(\mathbb{F}_q)$ when viewed as a finite Abelian group. An upper bound on the ℓ-rank of $\operatorname{Jac}_{\mathbb{K}}(\mathbb{F}_q)$ is $2g$ if $\ell \nmid q$ and g if $\ell \mid q$. Here, we will only consider the former case and henceforth exclude the scenario where ℓ is the characteristic of $\mathbb{F}_q$.

3 Increasing the ℓ-rank via enlarging the base field

For completeness, we provide an overview of the aforementioned method given in Section 5 of [2]; for details and proofs, the reader is referred to that source. We continue to let $\mathbb{K}/\mathbb{F}_q$ be an algebraic function field and $\operatorname{Jac}_{\mathbb{K}}(\mathbb{F}_q)$ its Jacobian. Consider the field $\overline{\mathbb{K}} = \mathbb{K}\overline{\mathbb{F}}_q$, the compositum of $\mathbb{K}$ and $\overline{\mathbb{F}}_q$. Then $\overline{\mathbb{K}}/\overline{\mathbb{F}}_q$ is an unramified function field extension of $\mathbb{K}/\mathbb{F}_q$ of the same genus as $\mathbb{K}/\mathbb{F}_q$. Since $\mathbb{F}_q$ is algebraically closed in $\mathbb{K}$, we see that if we write $\mathbb{K} = \mathbb{F}_q(x,y)$ with $y \in \mathbb{K}$, then $\overline{\mathbb{K}} = \overline{\mathbb{F}}_q(x,y)$ and $[\overline{\mathbb{K}} : \overline{\mathbb{F}}_q(x)] = [\mathbb{K} : \mathbb{F}_q(x)]$.

Similarly, for any $n \in \mathbb{N}$, set $\mathbb{K}_n = \mathbb{K}\mathbb{F}_{q^n} = \mathbb{F}_{q^n}(x,y) \subset \overline{\mathbb{K}}$; then $[\mathbb{K}_n : \mathbb{F}_{q^n}(x)] = [\mathbb{K} : \mathbb{F}_q(x)]$. If $L(t) = \prod_{i=1}^{2g}(1-\omega_i t)$ is the L-polynomial of $\mathbb{K}/\mathbb{F}_q$, with $\omega_i \in \mathbb{C}$ for $1 \le i \le 2g$, then the L-polynomial of $\mathbb{K}_n/\mathbb{F}_{q^n}$ is $\prod_{i=1}^{2g}(1-\omega_i^n t)$.

For brevity, set $\mathcal{J} = \operatorname{Jac}_{\overline{\mathbb{K}}}(\overline{\mathbb{F}}_q)$ and $\mathcal{J}_n = \operatorname{Jac}_{\mathbb{K}_n}(\mathbb{F}_{q^n})$. As before, let ℓ be any prime not dividing q, and denote the ℓ-torsion of $\mathcal{J}$ and $\mathcal{J}_n$ by $\mathcal{J}[\ell]$ and $\mathcal{J}_n[\ell]$, respectively. Then $\mathcal{J}_n[\ell] \subset \mathcal{J}_{kn}[\ell]$ for all $k \in \mathbb{N}$, and $\mathcal{J}[\ell] \cong (\mathbb{Z}/\ell)^{2g}$. In fact, there exists a smallest field $\mathbb{F}_{q^{n_\ell}}$ such that $\mathcal{J}[\ell] \subseteq \mathcal{J}_{n_\ell}[\ell]$; this field is the *field of rationality* or *field of definition* of $\mathcal{J}[\ell]$. It follows that $\mathcal{J}_{n_\ell}[\ell] \cong (\mathbb{Z}/\ell)^{2g}$, and hence $\ell\text{-rank}(\mathcal{J}_{n_\ell}) = 2g$ is maximal. The method in [2, Section 5] provided partial answers to the following questions:

1. What is the exact value of n_ℓ? Is it at least possible to find an upper bound b on n_ℓ?

2. For any $n \in \mathbb{N}$, is it possible to ascertain if ℓ-rank$(\mathcal{J}_n) > \ell$-rank$(\mathcal{J}_1)$? If yes, is it possible to find (lower bounds on) such a value of n as well as the increase from ℓ-rank$(\mathcal{J}_1)$ to ℓ-rank$(\mathcal{J}_n)$?

The upper bound b on n_ℓ given in [2] requires a potentially tedious search, which is eliminated by the results of this paper. Moreover, we extend the answer given in [2] to Question 2 above by considering a more general scenario. In particular, this will allow us to deduce ℓ-ranks over large base fields, which might be too big for computers to handle, from those over smaller base fields.

The Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ acts on the ℓ-torsion $\mathcal{J}[\ell]$ of $\mathcal{J}$, whence we obtain a representation $\rho_\ell : \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \to \mathrm{Aut}(J[\ell])$. This representation factors through $\mathrm{Gal}(\mathbb{F}_{q^{n_\ell}}/\mathbb{F}_q)$. For any choice of $\mathbb{F}_\ell$-basis of $\mathcal{J}[\ell]$, we thus obtain

$$\rho_\ell : \mathrm{Gal}(\mathbb{F}_{q^{n_\ell}}/\mathbb{F}_q) \hookrightarrow \mathrm{GL}_{2g}(\mathbb{F}_\ell) \ .$$

The Galois group $\mathrm{Gal}(\mathbb{F}_{q^{n_\ell}}/\mathbb{F}_q)$ above is generated by the restriction π_{q,n_ℓ} of the Frobenius automorphism π_q on $\overline{\mathbb{F}}_q$ to $\mathbb{F}_{q^{n_\ell}}$. This is the automorphism that sends every element in $\mathbb{F}_{q^{n_\ell}}$ to its q-th power. Thus, the image of π_{q,n_ℓ} under ρ_ℓ is a matrix $M_\ell \in \mathrm{GL}_{2g}(\mathbb{F}_\ell)$ of order n_ℓ. In order to determine $n_\ell = \mathrm{ord}(M_\ell)$, we define ρ_ℓ in terms of a basis for which M_ℓ is in *primary rational canonical form*.

The explanation of the primary rational canonical form requires a brief excursion into linear algebra. Let V be a vector space over some field K and ϕ a linear transformation on V. In our context, we will have $K = \mathbb{F}_\ell$, $V = \mathcal{J}_{n_\ell}[\ell] \cong \mathbb{F}_\ell^{2g}$, and $\phi = \pi_{q,n_\ell}$; note that since π_{q,n_ℓ} acts on the places of $\mathbb{K}_{n_\ell}/\mathbb{F}_{q^{n_\ell}}$, this action extends naturally to $\mathcal{J}_{n_\ell}$ and hence to $\mathcal{J}_{n_\ell}[\ell]$.

Recall that the *minimal polynomial* of ϕ is the unique monic polynomial $G_\phi(t) \in K[t]$ of minimal degree with $G_\phi(\phi) = 0$; it divides all other polynomials $F(t) \in K[t]$ with $F(\phi) = 0$, including the *characteristic polynomial* $F_\phi(t)$ of ϕ whose roots are the eigenvalues of ϕ with appropriate multiplicities. In fact, $F_\phi(t)$ and $G_\phi(t)$ have the same roots, but potentially with different multiplicities.

For any monic polynomial $F(t) = t^m + a_{m-1}t^{m-1} + \cdots + a_0 \in K[t]$, the *companion matrix* of $F(t)$ is the $m \times m$ matrix

$$A_F = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & & & & & & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \\ -a_0 & -a_1 & -a_2 & -a_3 & \cdots & -a_{m-2} & -a_{m-1} \end{pmatrix} .$$

Note that $F(t)$ is both the minimal and the characteristic polynomial of its own companion matrix A_F.

A subspace W of V is said to be *ϕ-cyclic* if it spanned by the vectors $\phi^i(v)$, $i \geq 0$, for some $v \in V$. Then W is ϕ-cyclic if and only if W has an ordered basis relative to which the matrix associated to the restriction $\phi|_W$ of ϕ to W is the companion matrix of the minimal polynomial of $\phi|_W$.

Finally, for any finite collection of square matrices $A_1, A_2, \ldots, A_r$, we denote by $\mathrm{diag}(A_1, A_2, \ldots, A_r)$ the matrix that has the sub-matrices $A_1, A_2, \ldots, A_r$ along its diagonal and zeros everywhere else; it is a square matrix whose size is the sum of the sizes of the A_i, $1 \leq i \leq r$. We make use of the following decomposition theorem:

Theorem 3.1 (Theorem 5.1 of [2], based on results of [8]) *Let $\phi : V \to V$ be a linear transformation on a vector space V over a field K. Then there exist distinct monic irreducible polynomials $P_1, P_2, \ldots, P_s \in K[t]$ with the following properties:*

1. *For each i with $1 \le i \le s$, there exist $k_i \in \mathbb{N}$ and ϕ-cyclic subspaces $V_{i1}, V_{i2}, \ldots, V_{ik_i}$ such that V is the direct sum of the V_{ij} $(1 \le i \le s, 1 \le j \le k_i)$.*
2. *For each i with $1 \le i \le s$ and each j with $1 \le j \le k_i$, the minimal polynomial of the restriction of ϕ to V_{ij} is of the form $P_i^{m_{ij}}$ where the integers m_{ij} satisfy $m_{i1} \ge m_{i2} \ge \cdots \ge m_{ik_i} \ge 1$. In particular, $\dim(V_{ij}) = m_{ij} \deg(P_i)$.*
3. *V has a basis relative to which the matrix of ϕ is of the form*

$$A_\phi = \operatorname{diag}(A_{P_1^{m_{11}}}, \ldots, A_{P_1^{m_{1k_1}}}, \ldots, A_{P_s^{m_{s1}}}, \ldots, A_{P_s^{m_{sk_s}}}) \ , \tag{3.1}$$

   where $A_{P_i^{m_{ij}}}$ is the companion matrix of $P_i^{m_{ij}}$ for $1 \le i \le s$ and $1 \le j \le k_i$.
4. *The minimal polynomial of ϕ is $G_\phi = P_1^{m_{11}} P_2^{m_{21}} \cdots P_s^{m_{s1}}$.*
5. *The characteristic polynomial of ϕ is $F_\phi = P_1^{m_1} P_2^{m_2} \cdots P_s^{m_s}$ where $m_i = \sum_{j=1}^{k_i} m_{ij}$ for $1 \le i \le s$.*

The polynomials $P_i^{m_{ij}}$ $(1 \le i \le s, 1 \le j \le k_i)$ are uniquely determined by V and ϕ and are called the *elementary divisors* of ϕ (or of any matrix representing ϕ). The matrix A_ϕ is said to be the *primary rational canonical form* of ϕ (or of any matrix representing ϕ).

If A_ϕ has finite order in $\mathrm{GL}_{\dim(V)}(K)$ — this is the case in our context — then

$$\operatorname{ord}(A_\phi) = \operatorname{lcm}\{\operatorname{ord}(A_{P_i^{m_{ij}}}) \mid 1 \le i \le s, 1 \le j \le k_i\} \ ,$$

which is easy to compute if $\dim(V)$ is not too large and each companion matrix has sufficiently small order. Thus, if we were able to obtain the elementary divisors of π_{q,n_ℓ}, then we could easily obtain $n_\ell = \operatorname{ord}(A_{\pi_{q,n_\ell}})$. Unfortunately, it is unclear how to obtain these elementary divisors. It is however possible to obtain the characteristic polynomial $F_{\pi_{q,n_\ell}}(t) \in \mathbb{F}_\ell[t]$ from the L-polynomial of $\mathbb{K}/\mathbb{F}_q$ via $F_{\pi_{q,n_\ell}}(t) \equiv t^{2g} L(t^{-1}) \pmod{\ell}$. In other words, if we compute the L-polynomial of $\mathbb{K}/\mathbb{F}_q$ — using Magma, for example — and factor its reciprocal modulo ℓ to obtain $F_{\pi_{q,n_\ell}}(t) = P_1^{m_1} P_2^{m_2} \cdots P_s^{m_s}$ with $P_1, P_2, \ldots, P_s \in \mathbb{F}_\ell[t]$ monic and irreducible, then we can construct all possible matrices $A_{\pi_{q,n_\ell}}$ as given in (3.1) (with $\phi = \pi_{q,n_\ell}$) for all $1 \le i \le s$ and $1 \le j \le m_i$. One of these is the primary rational canonical form of π_{q,n_ℓ}, and although it is unknown which candidate matrix is the correct one, the maximum of their orders is an upper bound on n_ℓ. Moreover, in the case when $F_{\pi_{q,n_\ell}}(t)$ is square-free, i.e. $m_i = 1$ for $1 \le i \le s$, we see that $A_{\pi_{q,n_\ell}} = \operatorname{diag}(A_{P_1}, A_{P_2}, \ldots, A_{P_s})$ is uniquely determined. This is actually the case for many curves, and particularly for most hyperelliptic curves; see the work of Chavdarov [5] and Kowalski [9, Section 6].

We now summarize the main results of [2, Section 5]. The first provides a partial answer to Question 1 above.

Proposition 3.2 (Theorem 5.2 of [2]) *Let $L(t)$ be the L-polynomial of a function field $\mathbb{K}/\mathbb{F}_q$ of genus g, and set $F(t) \equiv t^{2g} L(t^{-1}) \pmod{\ell}$, $F(t) \in \mathbb{F}_\ell[t]$. Let $F = P_1^{m_1} P_2^{m_2} \cdots P_s^{m_s}$ be the factorization of $F(t)$ into powers of distinct monic*

irreducibles $P_i(t) \in \mathbb{F}_\ell[t]$ and define a set $\mathcal{S}$ as follows:

$$\mathcal{S} = \left\{(P_i^{m_{ij}}) \mid 1 \le i \le s,\ 1 \le j \le k_i,\ m_{i1} \ge \cdots \ge m_{ik_i} \ge 1, \text{ and } \sum_{j=1}^{k_i} m_{ij} = m_i \text{ for } 1 \le i \le s\right\} .$$

For any tuple $\mathbf{P} = (P_i^{m_{ij}}) \in \mathcal{S}$, define the matrix

$$A_{\mathbf{P}} = \operatorname{diag}(A_{P_1^{m_{11}}}, \ldots, A_{P_1^{m_{1k_1}}} \ \ldots, A_{P_s^{m_{s1}}}, \ldots, A_{P_s^{m_{sk_s}}}) ,$$

where $A_{P_i^{m_j}}$ is the companion matrix of $P_i^{m_{ij}}$. Set

$$b = \max\{\operatorname{ord}(A_{\mathbf{P}}) \mid \mathbf{P} \in \mathcal{S}\} ,$$

and let $\mathbb{F}_{q^{n_\ell}}$ be the field of rationality of $\mathcal{J}[\ell]$. Then $n_\ell \le b$, with equality if $F(t)$ is square-free.

We will improve this result in Theorem 4.3 below; in particular, we will note that in order to determine the maximum of all the $\operatorname{ord}(A_{\mathbf{P}})$ with $\mathbf{P} \in \mathcal{S}$, it suffices to consider only the trivial partitions consisting of just one summand $m_{i1} = m_i$ $(1 \le i \le s)$.

The following appears as a short discussion on pp. 521-522 of [2]. It can be useful if a lower bound on the ℓ-rank of $\mathcal{J}_{\mathbb{K}}(\mathbb{F}_q)$ is a priori known; for example, if $\mathbb{K}$ was obtained via one of the special constructions referred to in Section 1. For any two polynomials $P(t), G(t) \in \mathbb{F}_\ell[t]$ with $P(t)$ irreducible, we let $v_P(G)$ denote the exact power of $P(t)$ that divides $G(t)$.

Proposition 3.3 *Let $L(t)$ be the L-polynomial of a function field $\mathbb{K}/\mathbb{F}_q$ of genus g, and set $F(t) \equiv t^{2g}L(t^{-1}) \pmod{\ell}$, $F(t) \in \mathbb{F}_\ell[t]$. Suppose that $\ell\text{-rank}(\mathcal{J}_{\mathbb{K}}(\mathbb{F}_q)) \ge r$. Then $(t-1)^r$ divides $F(t)$, and if $v_{t-1}(F) = r$, then $\ell\text{-rank}(\mathcal{J}_{\mathbb{K}}(\mathbb{F}_q)) = r$.*

If $\ell\text{-rank}(\mathcal{J}_{\mathbb{K}}(\mathbb{F}_q)) \ge r$, then each polynomial $P_i^{m_i}$ $(1 \le i \le s)$ is a product of at least r elementary divisors $P^{m_{ij}}$ of π_{q,n_ℓ}.

Finally, [2] provided the following partial answer to Question 2 above.

Proposition 3.4 (Theorem 5.6 of [2]) *Let $L(t)$ be the L-polynomial of a function field $\mathbb{K}/\mathbb{F}_q$ of genus g, and set $F(t) \equiv t^{2g}L(t^{-1}) \pmod{\ell}$, $F(t) \in \mathbb{F}_\ell[t]$. Suppose $F(t)$ has an irreducible factor $P(t) \in \mathbb{F}_\ell[t]$ different from $t-1$. Let $A_P \in \mathrm{GL}_{\deg(P)}(\mathbb{F}_\ell)$ be the companion matrix of P, and set $n = \operatorname{ord}(A_P)$. Then $\ell\text{-rank}(\mathcal{J}_n) \ge \ell\text{-rank}(\mathcal{J}_k) + \deg(P)$ for any proper divisor k of n.*

The next four sections contain new results and improvements on the propositions from [2] presented above. Specifically, Section 4 gives a more explicit expression for the bound b on n_ℓ of Proposition 3.2 that eliminates the need to compute the maximum of the orders of all the matrix candidates. Section 5 provides a simple upper bound on (and multiple of) b. Section 6 applies our results to curves of genus 1 and 2, and Section 7 adds to Proposition 3.3 and improves on Proposition 3.4.

4 An explicit expression for the bound b

In order to further investigate the bound b on the degree n_ℓ of the field of rationality of $\mathcal{J}[\ell]$ over $\mathbb{F}_q$, we require some additional linear algebra. Recall that

an *elementary Jordan matrix* over some field K is an $m \times m$ matrix of the form

$$J_{m,\lambda} = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda & 1 & \cdots & 0 & 0 \\ 0 & 0 & \lambda & \cdots & 0 & 0 \\ \vdots & \vdots & & \ddots & & \vdots \\ 0 & 0 & 0 & \cdots & \lambda & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda \end{pmatrix} . \tag{4.1}$$

Let $A \in \mathrm{GL}_m(K)$. Over an algebraic closure $\overline{K}$ of K, the elementary divisors of A are of the form $(t-\lambda_i)^{m_{ij}}$ with $\lambda_i \in \overline{K}$ and $1 \le i \le s, 1 \le j \le k_i$, and the *Jordan canonical form* of A (or of the linear transformation represented by A) is the matrix

$$J_A = \mathrm{diag}(J_{m_{ij},\lambda_i})_{1\le i\le s,\, 1\le j\le k_i} .$$

In particular, the companion matrix A_F of a polynomial $F(t) \in K[t]$ with roots $\lambda_1, \lambda_2, \ldots, \lambda_r \in \overline{K}$ of respective multiplicities $m_1, m_2, \ldots, m_r$ has Jordan canonical form $J_{A_F} = \mathrm{diag}(J_{m_1,\lambda_1}, \ldots, J_{m_r,\lambda_r})$.

We begin with two basic results on elementary Jordan matrices and companion matrices. As usual, for any real number R, let $\lceil R \rceil$ denote the ceiling of R, i.e. the smallest integer that is greater than or equal to R. Furthermore, for any $\gamma \in \overline{\mathbb{F}}_\ell^*$, let $\mathrm{ord}_\ell(\gamma)$ denote the order of γ in $\overline{\mathbb{F}}_\ell^*$; note that since $\gamma \in \mathbb{F}_{\ell^d}^*$ for some $d \in \mathbb{N}$, $\mathrm{ord}_\ell(\gamma)$ divides $\ell^d - 1$ and is hence finite and not divisible by ℓ.

Lemma 4.1 *Let ℓ be a prime and $\lambda \in \overline{\mathbb{F}}_\ell^*$. Then* $\mathrm{ord}(J_{m,\lambda}) = \ell^{\lceil \log_\ell(m) \rceil} \mathrm{ord}_\ell(\lambda)$.

Proof For brevity, set $n = \lceil \log_\ell(m) \rceil$. Then $\ell^{n-1} < m \le \ell^n$. Induction yields

$$J_{m,\lambda}^i = \begin{pmatrix} \lambda^i & \binom{i}{1}\lambda^{i-1} & \binom{i}{2}\lambda^{i-2} & \cdots & \binom{i}{i-1}\lambda & 1 & 0 & 0 & \cdots & 0 \\ 0 & \lambda^i & \binom{i}{1}\lambda^{i-1} & \cdots & \binom{i}{i-2}\lambda^2 & \binom{i}{i-1}\lambda & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & & & & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & \lambda^i \end{pmatrix}$$

for $i \in \mathbb{N}$. Note that for $i \ge m$, all the entries on and above the main diagonal of $J_{m,\lambda}^i$ have the form $\binom{i}{j}\lambda^{i-j}$ with $0 \le j \le m-1$.

Recall that the exact power of ℓ dividing a binomial coefficient $\binom{i}{j}$ is the number of carries that occur when j is added to $i-j$ in base ℓ. For $i = \ell^n$ and $1 < j < \ell^n$, at least one such carry occurs, so $\binom{\ell^n}{j} \equiv 0 \pmod{\ell}$. Since $\ell^n \ge m$, we have $J_{m,\lambda}^{\ell^n} = \lambda^{\ell^n} I_m$, where I_m is the $m \times m$ identity matrix.

Since $\mathrm{ord}_\ell(\lambda)$ is not divisible by ℓ, it follows that

$$\mathrm{ord}(J_{m,\lambda}^{\ell^n}) = \mathrm{ord}_\ell(\lambda^{\ell^n}) = \frac{\mathrm{ord}_\ell(\lambda)}{\gcd(\mathrm{ord}_\ell(\lambda), \ell^n)} = \mathrm{ord}_\ell(\lambda) .$$

On the other hand, $\mathrm{ord}(J_{m,\lambda}^{\ell^n}) = \mathrm{ord}(J_{m,\lambda})/\gcd(\ell^n, \mathrm{ord}(J_{m,\lambda}))$, so it suffices to show that $\ell^n \mid \mathrm{ord}(J_{m,\lambda})$ to complete the proof.

To that end, let r be the exact power of ℓ dividing $\mathrm{ord}(J_{m,\lambda})$, and write $\mathrm{ord}(J_{m,\lambda})/\ell^r = a\ell + b$ with $a \ge 0$ and $0 < b < \ell$. Then $\mathrm{ord}(J_{m,\lambda}) - \ell^r = a\ell^{r+1} + (b-1)\ell^r$ with $0 \le b \le \ell - 1$. Thus, adding ℓ^r to $\mathrm{ord}(J_{m,\lambda}) - \ell^r$ in base ℓ produces no carries, so $\binom{\mathrm{ord}(J_{m,\lambda})}{\ell^r} \not\equiv 0 \pmod{\ell}$. If $r < n$, then $1 \le \ell^r \le \ell^{n-1} \le m-1$, so this would result in a non-zero entry above the main diagonal of

$J_{m,\lambda}^{\mathrm{ord}(J_{m,\lambda})} = I_m$, a contradiction. Hence $r \geq n$. It follows that $\ell^n \mid \mathrm{ord}(J_{m,\lambda})$, and hence $\mathrm{ord}(J_{m,\lambda}) = \ell^n \,\mathrm{ord}_\ell(\lambda)$. □

Lemma 4.2 *Let ℓ be a prime, $P(t) \in \mathbb{F}_\ell[t]$ an irreducible polynomial, and A_P the companion matrix of P. Then $\mathrm{ord}(A_{P^m}) = \ell^{\lceil \log_\ell(m) \rceil} \,\mathrm{ord}(A_P)$ for all $m \in \mathbb{N}$.*

Proof Let $d = \deg(P)$. Then P decomposes into linear factors over $\mathbb{F}_{\ell^d}^*$, say

$$P(t) = (t - \lambda_1)(t - \lambda_2) \cdots (t - \lambda_d) \ ,$$

with $\lambda_1, \lambda_2, \ldots, \lambda_d \in \mathbb{F}_{\ell^d}^*$ distinct. The Jordan canonical forms of the companion matrices A_P and A_{P^m} are

$$\begin{aligned} J_{A_P} &= \mathrm{diag}(\lambda_1, \lambda_2, \ldots, \lambda_d) \ , \\ J_{A_{P^m}} &= \mathrm{diag}(J_{m,\lambda_1}, J_{m,\lambda_2}, \ldots, J_{m,\lambda_d}) \ , \end{aligned}$$

respectively. Since $\lambda_1, \lambda_2, \ldots, \lambda_d \in \mathbb{F}_{\ell^d}^*$ are Galois conjugates, they all have the same order in $\mathbb{F}_{\ell^d}^*$; call this order r. Thus, $\mathrm{ord}(J_{A_P}) = \mathrm{lcm}(\mathrm{ord}_\ell(\lambda_1), \ldots, \mathrm{ord}_\ell(\lambda_d)) = r$. Furthermore, by Lemma 4.1, $\mathrm{ord}(J_{m,\lambda_i}) = \ell^n \,\mathrm{ord}_\ell(\lambda_i) = \ell^n r$ for $1 \leq i \leq d$, where as before, $n = \lceil \log_\ell(m) \rceil$. Since similar matrices have the same order, we have

$$\begin{aligned} \mathrm{ord}(A_{P^m}) &= \mathrm{ord}(J_{A_{P^m}}) = \mathrm{lcm}(\mathrm{ord}(J_{m,\lambda_i}) | 1 \leq i \leq s) \\ &= \ell^n r = \ell^n \,\mathrm{ord}(J_{A_P}) = \ell^n \,\mathrm{ord}(A_P) \end{aligned}$$

as claimed. □

We can now give a simpler expression for the bound b of Proposition 3.2 that can be gleaned directly from the L-polynomial of $\mathbb{K}/\mathbb{F}_q$ and avoids computing $\mathrm{ord}(A_{\mathbf{P}})$ for the entire collection of $\mathbf{P} \in \mathcal{S}$. We also observe that b is in fact a multiple of n_ℓ.

Theorem 4.3 *With the notation of Proposition 3.2, we have*

$$n_\ell \mid b = \mathrm{ord}(A_F) = \ell^{\lceil \log_\ell(\max\{m_i | 1 \leq i \leq s\}) \rceil} \cdot \mathrm{lcm}\left(\mathrm{ord}(A_{P_i}) \mid 1 \leq i \leq s \right) \ ,$$

where A_F is the companion matrix of $F(t)$.

Proof Note that for any integers μ, ν, M, N with $\mu, \nu \geq 0$ and M, N not divisible by ℓ, we have $\mathrm{lcm}(\ell^\mu M, \ell^\nu N) = \ell^{\max\{\mu,\nu\}} \,\mathrm{lcm}(M, N)$.

Recall that $\mathrm{ord}(A_{P_i})$ is equal to the order of each of the roots of P_i in $\mathbb{F}_{\ell^{\deg(P_i)}}$ and is thus coprime to any power of ℓ. Let $\mathbf{P} = (P_i^{m_{ij}}) \in \mathcal{S}$. Then by Lemma 4.2,

$$\begin{aligned} \mathrm{ord}(A_{\mathbf{P}}) &= \mathrm{lcm}\left(\mathrm{ord}(A_{P_i^{m_{ij}}}) \right) = \mathrm{lcm}\left(\ell^{\lceil \log_\ell(m_{ij}) \rceil} \,\mathrm{ord}(A_{P_i}) \right) \\ &= \ell^{\max\{\lceil \log_\ell(m_{ij}) \rceil\}} \,\mathrm{lcm}\left(\mathrm{ord}(A_{P_i}) \right) = \ell^{\lceil \log_\ell(m_{i1}) \rceil} \,\mathrm{lcm}\left(\mathrm{ord}(A_{P_i}) \right) \ , \end{aligned}$$

where the last equality above follows from the fact that $m_{i1} \geq m_{i2} \geq \ldots m_{ik_i}$ for all i with $1 \leq i \leq s$. Hence, in order to find b, we need to maximize the above expression over all $\mathbf{P} \in \mathcal{S}$. Since $\mathrm{lcm}(\mathrm{ord}(A_{P_i}))$ is fixed for each $\mathbf{P} \in \mathcal{S}$, this amounts to finding for each i with $1 \leq i \leq s$ the maximum value m_{i1} for all partitions of m_i. Clearly, this maximum is attained for the one-term partition $m_i = m_{i1}$, in which case $\mathbf{P} = (P_i^{m_i})$ corresponds to $F(t)$.

It is also clear that $\mathrm{ord}(A_{\mathbf{P}})$ divides b for all $\mathbf{P} \in \mathcal{S}$; in particular, $n_\ell \mid b$. Finally, we note that the matrices A_F and $\mathrm{diag}(A_{P_1^{m_1}}, \ldots, A_{P_s^{m_s}})$ have the same Jordan canonical form, and hence the same order b. □

To illustrate the above bound, we revisit Example 5.5 of [2].

Example 4.4 Consider $q = 179$, the hyperelliptic function field $\mathbb{K} = \mathbb{F}_{179}(x, y)$ of genus 4 with

$$y^2 = x^9 + 151\,x^8 + 168\,x^7 + 10\,x^6 + 32\,x^5 + 141\,x^4 + 110\,x^3 + 35\,x^2 + 160\,x + 2 \ ,$$

and $\ell = 3$. With the aid of Magma, we found that the zeta function of $\mathbb{K}$ is $\zeta(t) = L(t)/(179\,t^2 - 180\,t + 1)$ with

$$\begin{aligned} L(t) = {} & 179^4\,t^8 - 17 \cdot 179^3\,t^7 + 315 \cdot 179^2\,t^6 - 3041 \cdot 179\,t^5 + 56275\,t^4 \\ & - 3041\,t^3 + 315\,t^2 - 17\,t + 1 \ . \end{aligned}$$

Reducing $t^8 L(t^{-1})$ modulo 3, we obtain $F(t) = t^8 + t^7 + t^5 + t^4 + 2\,t^3 + 2\,t + 1 \in \mathbb{F}_3[t]$. Over $\mathbb{F}_3$, $F(t)$ factors as $F = P_1 P_2 P_3^2 P_4$ where

$$P_1(t) = t + 1, \quad P_2(t) = t + 2, \quad P_3(t) = t^2 + 1, \quad P_4(t) = t^2 + t + 2$$

are all irreducible over $\mathbb{F}_3$. Using Proposition 3.2, it was necessary to compute the maximum of the orders of the two matrices

$$\operatorname{diag}(A_{P_1}, A_{P_2}, A_{P_3}, A_{P_3}, A_{P_4}) \quad \text{and} \quad \operatorname{diag}(A_{P_1}, A_{P_2}, A_{P_3^2}, A_{P_4}) \ .$$

Using Theorem 4.3, we simply compute $\lceil \log_3(2) \rceil = 1$, and $\operatorname{ord}(A_{P_1}) = 2$, $\operatorname{ord}(A_{P_2}) = 1$, $\operatorname{ord}(A_{P_3}) = 4$, $\operatorname{ord}(A_{P_4}) = 8$. Thus, n_3 is a divisor of $b = 3 \cdot \operatorname{lcm}(2, 1, 4, 8) = 24$. Alternatively, we could have computed $\operatorname{ord}(A_F) = 24$.

We state some simple special cases of Theorem 4.3:

Corollary 4.5 *Let $L(t)$ be the L-polynomial of a function field $\mathbb{K}/\mathbb{F}_q$ of genus g, and set $F(t) \equiv t^{2g} L(t^{-1}) \pmod{\ell}$, $F(t) \in \mathbb{F}_\ell[t]$. Let $b = \operatorname{ord}(A_F)$, where A_F is the companion matrix of F. Then the following hold:*

1. *If $F(t)$ splits into distinct irreducible factors in $\mathbb{F}_\ell[t]$, all of which have degrees dividing $d \in \mathbb{N}$, then*

$$n_\ell = b = \operatorname{lcm}(\operatorname{ord}_\ell(\alpha_i)) \mid \ell^d - 1 \ ,$$

   where the $\alpha_i \in \mathbb{F}_{\ell^d}$ run through all the roots of F.
2. *If $F(t)$ is a product of powers of linear factors in $\mathbb{F}_\ell[t]$, and the largest exponent of any such linear factor is $m > 1$, then*

$$n_\ell \mid b = \ell^{\lceil \log_\ell(m) \rceil} \operatorname{lcm}(\operatorname{ord}_\ell(\alpha_i)) \mid \ell^{\lceil \log_\ell(m) \rceil}(\ell - 1) \ ,$$

   where the $\alpha_i \in \mathbb{F}_{\ell^d}$ run through all the roots of F.

Proof Recall that $n_\ell = b$ if $F(t)$ is square-free by Proposition 3.2. The corollary now follows from Theorem 4.3 and the fact that for any irreducible polynomial $P \in \mathbb{F}_\ell[t]$ and any root α of $P(t)$, $\operatorname{ord}(A_P) = \operatorname{ord}_\ell(\alpha) \mid \ell^{\deg(P)} - 1$. □

5 A simple bound on $b = \operatorname{ord}(A_F)$

It is at times desirable to have a bound on n_l that does not require any matrix order computation. In order to present such a bound, we further investigate the irreducible factors of the L-polynomial.

Lemma 5.1 *Let $P(t) \in \mathbb{F}_\ell[t]$ be an irreducible polynomial, and suppose there exists $\alpha \in \overline{\mathbb{F}}_\ell$ such that $\alpha^2 \neq q$ and $P(\alpha) = P(q/\alpha) = 0$. Then the map $\psi : \overline{\mathbb{F}}_\ell \to \overline{\mathbb{F}}_\ell$ via $\psi(\gamma) = q/\gamma$ is a permutation of order 2 on the roots of $P(t)$, so $\deg(P)$ is even.*

Proof Let $d = \deg(P)$. Note that since $P(t)$ has at least two distinct roots α and q/α, we have $d \geq 2$.

The Frobenius on $\overline{\mathbb{F}}_\ell$ sends elements to their ℓ-th powers. Since this Frobenius acts transitively on the roots of $P(t)$, these roots are of the form $\alpha_i = \alpha^{\ell^i}$ for $0 \leq i \leq d-1$. Let $q/\alpha = \alpha^{\ell^j}$. Then $j \neq 0$ as otherwise $\alpha^2 = q$. Hence $1 \leq j \leq d-1$.

Now for all i with $0 \leq i \leq d-1$,

$$\psi(\alpha_i) = \frac{q}{\alpha_i} = \frac{q}{\alpha^{\ell^i}} = \left(\frac{q}{\alpha}\right)^{\ell^i} = (\alpha^{\ell^j})^{\ell^i} = \alpha^{\ell^{j+i}} = \alpha_{i+j \pmod d} \ ,$$

so ψ maps any root α_i of $P(t)$ to another root of $P(t)$. It follows that ψ is a permutation on the roots of $P(t)$ whose order divides 2. Moreover, since $0 < j < d$ implies $i \not\equiv i + j \pmod d$, the order of ψ is exactly 2. In particular, for $i = 0$, we obtain $\alpha_0 = \psi(\psi(\alpha_0)) = \alpha_{2j \pmod d}$, so $d \mid 2j$. Since $1 \leq j \leq d-1$, we see that $d = 2j$ is even. □

Corollary 5.2 *With the notation and assumptions of Lemma 5.1, if A_P is the companion matrix of P, then* $\operatorname{ord}(A_P)$ *divides* $(\ell^{\deg(P)/2} + 1)\operatorname{ord}_\ell(q)$.

Proof From the proof of Lemma 5.1, we see that $q/\alpha = \alpha^{\ell^j}$ with $2j = d = \deg(P)$. Thus, $\alpha^{\ell^j+1} = q$, and hence $\alpha^{(\ell^j+1)\operatorname{ord}_\ell(q)} = 1$. Since $\operatorname{ord}(A_P) = \operatorname{ord}_\ell(\alpha)$, the claim follows. □

Definition 5.3 *Let $P(t) \in \mathbb{F}_\ell[t]$ be monic and irreducible. Then $P(t)$ is said to be of*

- type 1 *if $P(t)$ is the minimal polynomial of a square root of q;*
- type 2 *if there exists $\alpha \in \overline{\mathbb{F}}_\ell$ such that $\alpha^2 \neq q$ and $P(\alpha) = P(q/\alpha) = 0$;*
- type 3 *otherwise.*

Proposition 5.4 *Let $G(t) \in \mathbb{F}_\ell[t]$ be a monic polynomial of even degree with $G(0) \neq 0$, such that for every root α of $G(t)$, q/α is also a root of $G(t)$. Then $G(t) = G_1(t)G_2(t)G_3(t)$ where*

- *$G_1(t)$ is a (possibly empty) product of powers of type 1 irreducibles; specifically:*
  - *if q is a square modulo ℓ, say $q = \alpha^2$ with $\alpha \in \overline{\mathbb{F}}_\ell^*$, then $G_1(t) = (t-\alpha)^{2j_-}(t+\alpha)^{2j_+}$ for some $j_+, j_- \geq 0$;*
  - *if q is a non-square modulo ℓ, then $G_1(t) = (t^2 - q)^j$ for some $j \geq 0$;*
- *G_2 is a (possibly empty) product of powers of type 2 irreducibles;*
- *G_3 is a (possibly empty) product of powers of polynomials of the form $P(t)Q(t)$ where $P(t)$ and $Q(t)$ are type 3 irreducibles of the same degree with disjoint root sets such that q/α is a root of $Q(t)$ whenever α is a root of $P(t)$.*

Proof For any root α of $G(t)$, let $P_\alpha(t)$ denote the minimal polynomial of α. Let $G_1(t)$ and $G_2(t)$ denote the product of all type 1 and type 2 irreducible factors of $G(t)$, respectively, and set $G_3(t) = G(t)/G_1(t)G_2(t)$. Then $G_3(t)$ consists of type 3 irreducible factors of $G(t)$ only. Moreover, every root α of $G_1(t)$ satisfies $\alpha = q/\alpha$, every root of $G_2(t)$ satisfies $\alpha \neq q/\alpha$ and $P_\alpha(t) = P_{q/\alpha}(t)$, and every root of $G_3(t)$ satisfies $\alpha \neq q/\alpha$ and $P_\alpha(t) \neq P_{q/\alpha}(t)$.

Let α be any root of $G_3(t)$, and set $d = \deg(P_\alpha)$. Then $\alpha_i = \alpha^{\ell^i}$, $0 \leq i \leq d-1$, are the roots of $P_\alpha(t)$; see the proof of Lemma 5.1. Therefore, $q/\alpha_i = (q/\alpha)^{\ell^i}$, $0 \leq i \leq d-1$, are all the roots of $P_{q/\alpha}(t)$, so $\deg(P_{q/\alpha}) = d$. Moreover, no α_i is

a root of $P_{q/\alpha}(t)$, otherwise $P_\alpha(t) = P_{\alpha_i}(t) = P_{q/\alpha}(t)$. Hence $G_3(t)$ is of the form described above.

Now $\deg(G_3)$ is even, and by Lemma 5.1, $\deg(G_2)$ is also even. Thus, $\deg(G_1)$ must be even. Every root of $G_1(t)$ is a square root of q. If q is a non-square modulo ℓ, then $P_\alpha(t) = t^2 - q$, so $G_1(t)$ is as specified above. If q is a square modulo ℓ, say $q = \alpha^2$ with $\alpha \in \mathbb{F}_{\ell^d}^*$, then $P_\alpha(t) = t \pm a$. Thus, $G_1(t) = (t-a)^{n_-}(t+a)^{n_+}$ with $n_-, n_+ \geq 0$. Then $n_- + n_+ = \deg(G_1)$ is even. Now

$$G_1(0) = \frac{G(0)}{G_2(0)G_3(0)} = q^{(\deg(G) - \deg(G_2) - \deg(G_3))/2} = q^{\deg(G_1)/2} = \alpha^{\deg(G_1)} \ .$$

On the other hand, $G_1(0) = (-\alpha)^{n_-}\alpha^{n_+} = (-1)^{n_-}\alpha^{n_- + n_+} = (-1)^{n_-}\alpha^{\deg(G_1)}$. It follows that n_- is even, and hence n_+ is also even. □

Note that it is easy, given the irreducible factors of $G(t)$, to determine which are of type 2, as any such factor $P(t) = t^d + a_{d-1}t^{d-1} + \cdots + a_1 t + a_0$ satisfies $a_0 = q^d$ and $a_i = a_{d-i}q^{d-i}$ for $1 \leq i \leq d/2 - 1$.

The above results lead to a bound on b, with b as given in Proposition 3.2 and Theorem 4.3, and hence on n_l, that can be read solely from the factorization of $F(t)$ over $\mathbb{F}_\ell$. Hence, one can avoid computing any matrix orders.

Theorem 5.5 *Let $L(t)$ be the L-polynomial of a function field $\mathbb{K}/\mathbb{F}_q$ of genus g, and set $F(t) \equiv t^{2g}L(t^{-1}) \pmod{\ell}$, $F(t) \in \mathbb{F}_\ell[t]$. Set $b = \operatorname{ord}(A_F)$, where A_F is the companion matrix of $F(t)$. For $i = 1, 2, 3$, put $l_i = 1$ whenever $F(t)$ has no type i irreducible factor; otherwise, put $l_i = \ell^{\lceil \log_\ell(m_i) \rceil} N_i$, where*

$$\begin{aligned}
m_i &= \max\{v_P(F) \mid P \text{ is a type } i \text{ irreducible factor of } F\} \quad (i = 1, 2, 3)\,, \\
N_1 &= \begin{cases}
\operatorname{ord}_\ell(\alpha) & \text{if } q = \alpha^2 \text{ is a square modulo } \ell \\
 & \text{and } v_{t+\alpha}(F) = 0, \\
\operatorname{ord}_\ell(-\alpha) & \text{if } q = \alpha^2 \text{ is a square modulo } \ell \\
 & \text{and } v_{t-\alpha}(F) = 0, \\
\max\{\operatorname{ord}_\ell(\alpha), \operatorname{ord}_\ell(-\alpha)\} & \text{if } q = \alpha^2 \text{ is a square modulo } \ell \\
 & \text{and } v_{t+\alpha}(F) \cdot v_{t-\alpha}(F) \neq 0, \\
2 \operatorname{ord}_\ell(q) & \text{if } q \text{ is a non-square modulo } \ell,
\end{cases} \\
N_2 &= \operatorname{ord}_\ell(q) \operatorname{lcm}(\ell^{\deg(P)/2} + 1 \mid P \text{ is a type 2 irreducible factor of } F)\,, \\
N_3 &= \operatorname{lcm}(\ell^{\deg(P)} - 1 \mid P \text{ is a type 3 irreducible factor of } F)\,.
\end{aligned}$$

Then b divides $\operatorname{lcm}(l_1, l_2, l_3)$.

Proof Assume $l_1, l_2, l_3 > 1$. From the proof of Theorem 4.3, we obtained $b = \operatorname{lcm}(\ell^{\lceil \log_\ell(v_P(F)) \rceil} \operatorname{ord}(A_P))$ where the lcm runs over all the irreducible factors P of F. Thus, $b = \operatorname{lcm}(b_1, b_2, b_3)$ where

$$b_i = \operatorname{lcm}(\ell^{\lceil \log_\ell(v_P(F)) \rceil} \operatorname{ord}(A_P) \mid P \text{ is a type } i \text{ irreducible factor of } F)$$

for $i = 1, 2, 3$. As before, the power of ℓ in the lcm is just the largest power of ℓ occurring in any term. Furthermore, for any irreducible polynomial $P(t)$ and any root α of $P(t)$, $\operatorname{ord}(A_P) = \operatorname{ord}_\ell(\alpha)$ divides $|\mathbb{F}_{\ell^{\deg(P)}}^*| = \ell^{\deg(P)} - 1$ if $P(t)$ is of type 3, and $\operatorname{ord}(A_P) \mid (\ell - 1)(\ell^{\deg(P)/2} + 1)$ if $P(t)$ is of type 2 by Corollary 5.2. It follows that $b_3 \mid l_3$ and $b_2 \mid l_2$.

We use Proposition 5.4 to analyze b_1. Suppose first that $q = \alpha^2$ is a square in $\mathbb{F}_\ell^*$. If $v_{t+\alpha}(F) = 0$, then the only type 1 irreducible factor of $F(t)$ is $P(t) = t - \alpha$ with companion matrix $A_P = (\alpha)$. So by Lemma 4.2, $b_1 = \ell^{\lceil \log_\ell(v_{t-\alpha}(F))\rceil} \operatorname{ord}_\ell(\alpha) = l_1$. If $v_{t+\alpha}(F) \neq 0$, then set $n_\alpha = \operatorname{ord}_\ell(\alpha)$, $n_{-\alpha} = \operatorname{ord}_\ell(-\alpha)$, and assume without loss of generality that $n_{-\alpha} \geq n_\alpha$. Then $n_{-\alpha} = n_\alpha$ or $n_{-\alpha} = 2n_\alpha$, so $\operatorname{lcm}(n_{-\alpha}, n_\alpha) = n_{-\alpha} = \max\{n_\alpha, n_{-\alpha}\}$. It follows again by Lemma 4.2 that

$$b_1 = \operatorname{lcm}(\ell^{\lceil \log_\ell(v_{t-\alpha}(F))\rceil} n_\alpha \,, \ell^{\lceil \log_\ell(v_{t+\alpha}(F))\rceil} n_{-\alpha}) = \ell^{m_1} \max\{n_\alpha, n_{-\alpha}\} = l_1 \ .$$

Finally, if q is a non-square modulo ℓ, then A_{t^2-q} has eigenvalues $\pm\sqrt{q}$, both of order $2\operatorname{ord}_\ell(q)$. Thus, again $b_1 = l_1$. □

Corollary 5.6 *With the notation of Theorem 5.5, b divides* $\operatorname{lcm}(l_1', l_2', l_3)$*, where for $i = 1, 2$, $l_i' = 1$ if $F(t)$ has no type i irreducible factors; else*

$$l_1' = \begin{cases} \ell^{\lceil \log_\ell(m_1)\rceil}(\ell - 1) & \text{if } q \text{ is a square modulo } \ell\,, \\ 2\,\ell^{\lceil \log_\ell(m_1)\rceil}(\ell - 1) & \text{if } q \text{ is a non-square modulo } \ell\,, \end{cases}$$

$$l_2' = \ell^{\lceil \log_\ell(m_2)\rceil}(\ell - 1)\ \operatorname{lcm}(\ell^{\deg(P)/2} + 1 \mid P \text{ is a type 2 irreducible factor of } F)\,.$$

Proof This follows from the simple fact that the order of every element in $\mathbb{F}_\ell^*$ divides $\ell - 1$. □

The bound on b in Theorem 5.5 can be sharp:

Example 5.7 We revisit Example 4.4. We have $\ell = 3$ and $q = 179 \equiv -1 \pmod 3$, so q is a non-square modulo ℓ that has order 2. $P_3(t) = t^2 + 1$ is the only type 1 factor of $F(t)$ and $k = v_{P_3}(F) = 2$. So $l_1 = l_1' = 2 \cdot 3 \cdot 2 = 12$. $P_4(t)$ is the only type 2 factor of $F(t)$, so $l_2 = l_2' = 2 \cdot (3^1 + 1) = 8$. Finally, $P_1(t) = t + 1$ and $P_2(t) = t + 2$ form a pair of type 3 factors, so $l_3 = 3 - 1 = 2$. Hence, $b \mid \operatorname{lcm}(12, 8, 2) = 24$, and in fact $b = 24$ from Example 4.4.

Once again, we state a simple special case:

Corollary 5.8 *Let $L(t)$ be the L-polynomial of a function field $\mathbb{K}/\mathbb{F}_q$ of genus g, and set $F(t) \equiv t^{2g} L(t^{-1}) \pmod \ell$, $F(t) \in \mathbb{F}_\ell[t]$. Suppose that $F(t)$ is irreducible over $\mathbb{F}_\ell$, and let A_F be the companion matrix of $F(t)$. Then*

$$\operatorname{ord}(A_F) \mid \operatorname{ord}_\ell(q)(\ell^g + 1) \mid (\ell - 1)(\ell^g + 1)\ .$$

Proof This follows immediately from Theorem 5.5 or Corollary 5.2, since $F(t)$ is a type 2 polynomial. □

6 Genus 1 and 2 curves

In the case of elliptic (i.e. genus 1) curves, it is well-known that $\operatorname{ord}_\ell(q) \mid n_\ell$, which gives a lower bound on n_ℓ. In fact, for $q \not\equiv 1 \pmod \ell$, the Balasubramanian-Koblitz Theorem [3] states that $\mathcal{J}[\ell] \subseteq \mathbb{F}_{q^n}$ if and only if $\operatorname{ord}_\ell(q) \mid n$. Proposition 6.1 below is a slightly more precise statement than Lemma 2.1 of [6].

Proposition 6.1 *Let $L(t)$ be the L-polynomial of an elliptic function field $\mathbb{K}/\mathbb{F}_q$, and set $F(t) = t^2 L(t^{-1}) \pmod \ell$, $F(t) \in \mathbb{F}_\ell[t]$. Let n_ℓ be the degree of the field of rationality of $\mathcal{J}[\ell]$ over $\mathbb{F}_q$. Then the following hold:*

1. *If $F(t) = (t - \alpha)(t - q/\alpha)$ splits into two distinct linear factors in $\mathbb{F}_\ell[t]$, then $n_\ell = \operatorname{ord}_\ell(\alpha) \mid \ell - 1$.*
2. *If $F(t)$ is irreducible in $\mathbb{F}_\ell[t]$, then $n_\ell \mid \ell^2 - 1$.*

3. *If $F(t) = (t-\alpha)^2$ is the square of a linear factor in $\mathbb{F}_\ell[t]$, then $n_\ell \mid \ell \operatorname{ord}_\ell(\alpha) \mid \ell(\ell-1)$. This can only occur if q is a square modulo ℓ.*

Proof This is immediate from Corollaries 4.5 and 5.8. Note also that if $F(t) = (t-\alpha)^2$ with $\alpha \in \mathbb{F}_\ell$, then $F(0) = \alpha^2 = q$, so q must be a square modulo ℓ. □

We point out that $F(t)$ is a product of 2 (linear) type 3 polynomials in case 1, a type 2 polynomial in case 2, and a square of a type 1 polynomial in case 3. So the above results could also have been obtained through Theorem 5.5 and Corollary 5.6. We also note that every factorization described above can happen, as evidenced by the example below. Here, $q = 5$ and $\ell = 11$. The first column in the table below lists a cubic polynomial $D(x) \in \mathbb{F}_5[x]$ so that $y^2 = D(x)$ is an elliptic curve over $\mathbb{F}_5$. The second column provides the factorization of $F(t) \equiv t^2 L(t^{-1}) \pmod{11}$, $F(t) \in \mathbb{F}_{11}[t]$, into monic irreducibles over $\mathbb{F}_{11}$. The third column specifies which of the cases in Proposition 6.1 this factorization corresponds to.

$D(x) \in \mathbb{F}_5[x]$	Factorization of $F(t)$ over $\mathbb{F}_{11}$	Case in Prop. 6.1
$x^3 + 2x + 1$	$(t+3)(t+9)$	1
$x^3 + 1$	$t^2 + 5$	2
$x^3 + x + 1$	$(t+7)^2$	3

For genus 2 curves, bounds on the field of rationality of the ℓ-torsion can be found in [7, Proposition 6.2]. That source assumes that the function field has complex multiplication by the ring of integers of a quartic CM field. Our result has no such restriction and is an improvement on [7] in some cases.

Proposition 6.2 *Let $L(t)$ be the L-polynomial of a function field $\mathbb{K}/\mathbb{F}_q$ of genus 2, and set $F(t) = t^4 L(t^{-1}) \pmod{\ell}$, $F(t) \in \mathbb{F}_\ell[t]$. Let n_ℓ be the degree of the field of rationality of $\mathcal{J}[\ell]$ over $\mathbb{F}_q$.*

1. *Suppose first that $F(t)$ is square-free.*
   (a) *If $F(t)$ splits into four (distinct) linear factors in $\mathbb{F}_\ell[t]$, then*
   $$n_\ell = \operatorname{lcm}(\operatorname{ord}_\ell(\alpha_i)) \mid \ell - 1 \ ,$$
   where the $\alpha_i \in \mathbb{F}_\ell$ run through all the roots of F.
   (b) *If $F(t)$ splits into either two or three distinct irreducible factors in $\mathbb{F}_\ell[t]$, then $n_\ell \mid \ell^2 - 1$.*
   (c) *If $F(t)$ is irreducible in $\mathbb{F}_\ell[t]$, then $n_\ell \mid \operatorname{ord}_\ell(q)(\ell^2+1) \mid (\ell-1)(\ell^2+1)$.*
2. *Suppose now that $F(t)$ is not square-free.*
   (a) *If $F(t)$ has a quadratic irreducible factor in $\mathbb{F}_\ell[t]$, then $n_\ell \mid \ell(\ell^2-1)$.*
   (b) *If $F(t)$ is the fourth power of a linear factor in $\mathbb{F}_\ell[t]$, then for the root α of $F(t)$,*
   $$n_\ell \mid \ell^{\lceil \log_\ell(4) \rceil} \operatorname{ord}_\ell(\alpha) \mid \begin{cases} \ell^2(\ell-1) & \text{if } \ell = 2 \text{ or } \ell = 3\,, \\ \ell(\ell-1) & \text{if } \ell \geq 5\,. \end{cases}$$
   This can only occur when q is a square modulo ℓ.
   (c) *In every other case, we have*
   $$n_\ell \mid \operatorname{lcm}(\operatorname{ord}_\ell(\alpha_i)) \mid \ell(\ell-1),$$
   where the $\alpha_i \in \mathbb{F}_\ell$ run through all the roots of F.

Proof First note that $F(t)$ cannot have an irreducible factor of degree 3, as such a factor would be a type 2 factor, which cannot have odd degree by Lemma

5.1. Neither can $F(t)$ split into a cube of a linear factor and a second different linear factor. To see this, suppose that three of the roots of $F(t)$ in $\mathbb{F}_\ell^*$ are identical, say $\alpha = \beta = q/\alpha$. Then $\alpha = \beta$ implies $q/\beta = q/\alpha$, so all four roots must be identical. Hence the list above exhausts all possible cases.

The claim for irreducible $F(t)$ follows from Corollary 5.8. The other results are a consequence of Theorem 4.3, or of Theorem 5.5 and Corollary 5.6. Note again that if $F(t) = (t-\alpha)^4$ with $\alpha \in \mathbb{F}_\ell$, then the coefficient of t in $F(t)$ is equal to q times that of t^3. Thus, $-4\alpha q = -4\alpha^3$, which implies that $q = \alpha^2$ must be a square modulo ℓ. □

Once again, each of the above factorizations can occur: in the example below, $q = 11$ and $\ell = 7$. The first column lists a polynomial $D(x) \in \mathbb{F}_{11}[x]$ of degree 5 so that $y^2 = D(x)$ is a hyperelliptic curve of genus 2 over $\mathbb{F}_{11}$. The second and third columns are analogous to those of the previous table, with column 3 specifying which of the cases in Proposition 6.2 the factorization case of $F(t)$ over $\mathbb{F}_7$ corresponds to.

$D(x) \in \mathbb{F}_{11}[x]$	Factorization of $F(t)$ over $\mathbb{F}_7$	Case in Prop. 6.2
$x^5+x^4+x^3+x^2+6x+10$	$(t+1)(t+3)(t+4)(t+6)$	1 (a)
$x^5+x^4+x^3+x^2+x+6$	$(t^2+t+3)(t^2+6t+3)$	1 (b)
$x^5+x^4+x^3+x^2+x+3$	$(t+3)(t+6)(t^2+6t+4)$	1 (b)
$x^5+x^4+x^3+x^2+x+1$	$t^4+4t^3+6t^2+2t+2$	1 (c)
$x^5+x^4+x^3+x^2+x+2$	$(t+5)^2(t^2+6t+4)$	2 (a)
$x^5+x^4+x^3+x^2+3x+8$	$(t^2+t+4)^2$	2 (a)
$x^5+x^4+x^3+x^2+x$	$(t+2)^2(t+5)^2$	2 (b)
$x^5+x^4+x^3+x^2+x+10$	$(t+2)^2(t+3)(t+6)$	2 (b)
$x^5+x^4+x^3+x^2+x+4$	$(t+5)^4$	2 (c)

We point out that the last line of the above table represents an example where Theorem 4.3 (and hence Theorem 5.5 as well) do not give a sharp bound on n_ℓ. Both theorems yield the multiple 42 of n_7, whereas computations of the ℓ-rank of the Jacobian in Magma reveal that $n_7 = 21$.

7 Incremental increases in ℓ-rank

Rather than achieving full ℓ-rank $2g$, we now turn to the question of incremental increases in ℓ-rank that was already addressed in Proposition 3.4. We provide an improvement to that proposition. In particular, we will see how to achieve multiple such increases over intermediate base fields $\mathbb{F}_q \subseteq \mathbb{F}_{q^n} \subseteq \mathbb{F}_{q^{n\ell}}$. We begin with some useful preliminary results.

Lemma 7.1 *Let ℓ be a prime, $\lambda \in \overline{\mathbb{F}}_\ell^*$, and $m \in \mathbb{N}$ with $m \geq 2$. Then for any $n \in \mathbb{N}$, the eigenspace of the Jordan matrix $J_{m,\lambda}^n \in \mathrm{GL}_m(\overline{\mathbb{F}}_\ell)$ has dimension 1 if and only if $\ell \nmid n$.*

Proof The matrix $J_{m,\lambda}^n$ has λ^n as its only eigenvalue, and the corresponding eigenspace is the null space of the matrix $J_{m,\lambda}^n - \lambda^n I_m$. This matrix is of the form $\begin{pmatrix} 0 & A \\ 0 & 0 \end{pmatrix}$, where A is an $(m-1)\times(m-1)$ matrix whose i-th row $(1 \leq i \leq m-1)$ has the form

$$\begin{pmatrix} 0 & 0 & \dots & 0 & \binom{n}{1}\lambda^{n-1} & \binom{n}{2}\lambda^{n-2} & \cdots & \binom{n}{m-i}\lambda^{n-m+i} \end{pmatrix}.$$

Here, for ease of notation, we adopt the convention $\binom{n}{j} = 0$ for $j > n$. Thus, A is an upper triangular matrix of determinant $(n\lambda^{n-1})^{m-1}$. So A has maximal rank (i.e. trivial null space) if and only if $\ell \nmid n$, and this holds exactly when the null space of $J_{m,\lambda}^n - \lambda^n I_m$ has dimension 1. □

Corollary 7.2 *With the notation of Lemma 7.1, if $\ell \nmid n$ and $\mathrm{ord}_\ell(\lambda) \mid n$, then $J_{m,\lambda}^n$ is similar to $J_{m,1}$.*

Lemma 7.3 *Let $P \in \mathbb{F}_\ell[t]$ be an irreducible polynomial, $m \in \mathbb{N}$, and A_P, A_{P^m} the companion matrices of P and P^m, respectively. Then for any multiple n of $\mathrm{ord}(A_P)$, the matrix $A_{P^m}^n$ has 1 as its only eigenvalue. The corresponding eigenspace contains a direct sum of $\deg(P)$ one-dimensional spaces, and is equal to this direct sum if $m = 1$ or $\ell \nmid n$.*

Proof For brevity, set $d = \deg(P)$. Then over $\overline{\mathbb{F}}_\ell$, A_P^n is similar to the $d \times d$ identity matrix I_d, and thus has 1 as its only eigenvalue, with d linearly independent eigenvectors. Since A_P^n and I_d have entries in $\mathbb{F}_\ell$, so does the kernel of their difference $\ker(A_P^n - I_d)$. Thus, $\dim_{\mathbb{F}_\ell} \ker(A_P^n - I_d) = d$ and the result holds for $m = 1$.

Now suppose $m \geq 2$. Then over $\overline{\mathbb{F}}_\ell$, A_{P^m} is similar to its Jordan canonical form $J_{A_{P^m}} = \mathrm{diag}(J_{m,\lambda_1}, J_{m,\lambda_2}, \ldots, J_{m,\lambda_d})$, where $\lambda_1, \lambda_2, \ldots, \lambda_d \in \overline{\mathbb{F}}_\ell$ are the roots of $P(t)$. So A_{P^m} has d distinct eigenvalues $\lambda_j \in \overline{\mathbb{F}}_\ell$, $1 \leq j \leq d$, each of which corresponds to a one-dimensional eigenspace W_j over $\overline{\mathbb{F}}_\ell$. Since $\mathrm{ord}_\ell(\lambda_j) = \mathrm{ord}(A_P)$ divides n for $1 \leq j \leq d$, each power J_{m,λ_j}^n has 1 as its only eigenvalue. It follows that the only eigenvalue of $A_{P^m}^n$ is 1, and $A_{P^m}^n$ acts trivially on each W_j for $1 \leq j \leq d$. Therefore, $\dim_{\overline{\mathbb{F}}_\ell} \ker(A_{P^m}^n - I_{md}) \geq d$, where I_{md} is the $md \times md$ identity matrix. Since $A_{P^m}^n$ and I_{md} have entries in $\mathbb{F}_\ell$, so does $\ker(A_{P^m}^n - I_{md})$. Thus, $\dim_{\mathbb{F}_\ell} \ker(A_{P^m}^n - I_{md}) \geq d$, and the eigenspace of $A_{P^m}^n$ corresponding to 1 contains the direct sum $W = \bigoplus_{j=1}^d W_j$.

If $\ell \nmid n$, then Corollary 7.2 implies that J_{m,λ_j}^n is similar to $J_{m,1}$ for all $1 \leq j \leq d$. So over $\overline{\mathbb{F}}_\ell$, $A_{P^m}^n$ is similar to the matrix $\mathrm{diag}(J_{m,1}, J_{m,1}, \ldots, J_{m,1})$, and thus has 1 as its only eigenvalue, with d Jordan blocks. Therefore, $\dim_{\overline{\mathbb{F}}_\ell} \ker(A_{P^m}^n - I_{md}) = d$. Again, since $A_{P^m}^n$ and I_{md} both have entries in $\mathbb{F}_\ell$, we have $\dim_{\mathbb{F}_\ell} \ker(A_{P^m}^n - I_{md}) = d$, and the eigenspace of $A_{P^m}^n$ corresponding to the only eigenvalue 1 is equal to W. □

We can now ascertain lower bounds on the ℓ-rank of $\mathcal{J}_n = \mathrm{Jac}_{\mathbb{K}_n}(\mathbb{F}_{q^n})$ for any $n \in \{1, 2, \ldots, n_\ell\}$, and sometimes even the exact ℓ-rank.

Theorem 7.4 *Let $L(t)$ be the L-polynomial of a function field $\mathbb{K}/\mathbb{F}_q$ of genus g, and set $F(t) \equiv t^{2g} L(t^{-1}) \pmod{\ell}$, $F(t) \in \mathbb{F}_\ell[t]$. Let $P_1, P_2, \cdots, P_s \in \mathbb{F}_\ell[t]$ be the collection of distinct monic irreducible factors of $F(t)$, with respective companion matrices A_{P_i}, $1 \leq i \leq s$. Let $n \in \mathbb{N}$, and set*

$$\mathcal{I}_n = \{i \mid 1 \leq i \leq s \text{ and } \mathrm{ord}(A_{P_i}) \text{ divides } n\} \ .$$

Then the following hold:

1. $\ell\text{-rank}(\mathcal{J}_n) \geq \sum_{i \in \mathcal{I}_n} \deg(P_i)$, *with equality if $v_{P_i}(F) = 1$ for all $i \in \mathcal{I}_n$.*
2. $\ell\text{-rank}(\mathcal{J}_1) \geq 1$ *if and only if* $t - 1 \mid F(t)$. *Moreover,* $\ell\text{-rank}(\mathcal{J}_1) = 1$ *if* $v_{t-1}(F) = 1$.

3. *Suppose* $\mathrm{ord}(A_{P_i}) \nmid n$ *for all* $1 \le i \le s$ *such that* $P_i(t) \ne t-1$. *If* $v_{t-1}(F) \le 1$ *or* $\ell \nmid n$, *then* $\ell\text{-rank}(\mathcal{J}_n) = \ell\text{-rank}(\mathcal{J}_1)$.

Proof We note that an element of $\mathcal{J}[\ell]$ is defined over $\mathbb{F}_{q^n}$, i.e. belongs to $\mathcal{J}_n[\ell]$, if and only if it is fixed by the Frobenius π_{q,n_ℓ}^n acting on $\mathcal{J}[\ell]$.

Let $P_i^{m_{ij}}$ $(1 \le i \le s,\ 1 \le j \le k_i)$ be the elementary divisors of π_{q,n_ℓ}. Then the primary rational canonical form of π_{q,n_ℓ} is $A_{\pi_{q,n_\ell}} = \mathrm{diag}(A_{P_i^{m_{ij}}})$. Thus, the n-th power π_{q,n_ℓ}^n of π_{q,n_ℓ} has a matrix representation $A^n_{\pi_{q,n_\ell}} = \mathrm{diag}(A^n_{P_i^{m_{ij}}})$. By Lemma 7.3, for $i \in \mathcal{I}_n$, $A^n_{P_i^{m_{ij}}}$ has 1 as its only eigenvalue, and the corresponding eigenspace W_{ij} contains a subspace that is isomorphic to $\mathbb{F}_\ell^{\deg(P_i)}$. It follows that π_{q,n_ℓ}^n has 1 as an eigenvalue, and the corresponding eigenspace $W = \bigoplus_{i,j} W_{ij}$ contains a subspace that is $\mathbb{F}_\ell$-isomorphic to $\mathbb{F}_\ell^{d_n}$, where $d_n = \sum_{i\in\mathcal{I}_n} \deg(P_i)$. Moreover, the eigenvalue 1 results in a trivial action of π_{q,n_ℓ}^n on W, so $w^{q^n} = w$ for all $w \in W$. Hence, elements in W must be defined over $\mathbb{F}_{q^n}$, implying that $W \subseteq \mathcal{J}_n[\ell]$. Thus, $\ell\text{-rank}(\mathcal{J}_n) \ge d_n$, yielding the inequality of part 1.

To obtain equality in the case when $F(t)$ is square-free, note that $k_i = m_{i1} = 1$ for $1 \le i \le s$. Thus, each W_{i1} is isomorphic to $\mathbb{F}_\ell^{\deg(P_i)}$ by Lemma 7.3, and hence $W \cong \mathbb{F}_\ell^{d_n}$. Moreover, for $i \notin \mathcal{I}_n$, the matrix $A^n_{P_i^{m_{i1}}}$ has only eigenvalues distinct from 1, so π_{q,n_ℓ}^n does not act trivially on any element outside W. It follows that $\ell\text{-rank}(\mathcal{J}_n) = d_n$.

For part 2 of Theorem 7.4, if $t-1 \mid F(t)$, then $\ell\text{-rank}(\mathcal{J}_1) \ge \deg(t-1) = 1$ by part 1 of the theorem applied to $n = 1$. Conversely, if $\ell\text{-rank}(\mathcal{J}_1) \ge 1$, then $t-1 \mid F(t)$ by Proposition 3.3 (with $r = 1$). Similarly, $v_{t-1}(F) = 1$ implies $t-1 \mid F(t)$, and hence $\ell\text{-rank}(\mathcal{J}_1) \ge 1$. Then the same proposition yields $\ell\text{-rank}(\mathcal{J}_1) = 1$.

For part 3, suppose first that $t-1 \nmid F(t)$. Then neither π_{q,n_ℓ} nor π_{q,n_ℓ}^n has 1 as an eigenvalue, so neither map acts trivially on any non-zero element of $\mathcal{J}[\ell]$. Thus, $\ell\text{-rank}(\mathcal{J}_1) = \ell\text{-rank}(\mathcal{J}_n) = 0$.

Now assume that $t-1 \mid F(t)$. Then $\mathcal{I}_n = \mathcal{I}_1$. If $v_{t-1}(F) = 1$, then by parts 1 and 2 of the theorem, $\ell\text{-rank}(\mathcal{J}_n) = \ell\text{-rank}(\mathcal{J}_1) = 1$. If $(t-1)^2 \mid F(t)$, then let $(t-1)^{m_j}$, $1 \le j \le k$, be the elementary divisors of π_{q,n_ℓ} corresponding to the factor $t-1$ of $F(t)$. Then $A_{\pi_{q,n_\ell}}$ is similar to $\mathrm{diag}(J_{m_1,1}, \ldots, J_{m_k,1}, B)$, where B is a matrix whose eigenvalues are all distinct from 1. By Corollary 7.2, $A_{\pi^n_{q,n_\ell}}$ is similar to $\mathrm{diag}(J_{m_1,1}, \ldots, J_{m_k,1}, C)$, where C also has only eigenvalues distinct from 1. It follows that π_{q,n_ℓ} and π_{q,n_ℓ}^n act trivially on k-dimensional subspaces of $\mathcal{J}_1[\ell]$ and $\mathcal{J}_n[\ell]$, respectively, but do not act trivially on any elements outside these respective subspaces. So $\ell\text{-rank}(\mathcal{J}_n) = \ell\text{-rank}(\mathcal{J}_1) = k$. □

For brevity, we henceforth refer to the tuple of ℓ-ranks of the Jacobians $\mathcal{J}_n$, $1 \le n \le n_\ell$, as the *ℓ-rank structure* of the extension $\mathbb{K}/\mathbb{F}_q$. The results of Theorem 7.4, combined with Theorem 4.3 (or Theorem 5.5) can sometimes yield the entire ℓ-rank structure of a given function field. Before we illustrate this, we discuss a particularly simple case.

Corollary 7.5 *Let* $L(t)$ *be the L-polynomial of a function field* $\mathbb{K}/\mathbb{F}_q$ *of genus* g, *set* $F(t) \equiv t^{2g}L(t^{-1}) \pmod{\ell}$, $F(t) \in \mathbb{F}_\ell[t]$, *and let* A_F *be the companion matrix of* $F(t)$. *If* $F(t)$ *is irreducible, then* $\ell\text{-rank}(\mathcal{J}_{\mathrm{ord}(A_F)}) = 2g$ *and* $\ell\text{-rank}(\mathcal{J}_k) = 0$ *for any* $k < \mathrm{ord}(A_F)$.

Proof ℓ-rank$(\mathcal{J}_{\mathrm{ord}(A_F)}) = \deg(F) = 2g$ by part 1 of Theorem 7.4. Since $F(t)$ is irreducible and $\deg(F)$ is even, we have $t-1 \nmid F(t)$, so ℓ-rank$(\mathcal{J}_k) = \ell$-rank$(\mathcal{J}_1) = 0$ for any $k < \mathrm{ord}(A_F)$ by parts 3 and 2 of Theorem 7.4. □

We revisit Example 5.4 of [2] to apply this corollary:

Example 7.6 Consider $q = 373$, the hyperelliptic function field $\mathbb{K} = \mathbb{F}_{373}(x, y)$ of genus 4 with

$$y^2 = x^9 + 245\,x^8 + 175\,x^7 + 340\,x^6 + 122\,x^5 + 70\,x^4 + 196\,x^3 + 210\,x^2 + 316\,x + 337 \ ,$$

and $\ell = 3$. With the aid of Magma, we found that $\zeta(t) = L(t)/(373\,t^2 - 374\,t + 1)$ is the zeta function of $\mathbb{K}$ with

$$\begin{aligned} L(t) = {} & 373^4\,t^8 + 33 \cdot 373^3\,t^7 + 347 \cdot 373^2\,t^6 - 3785 \cdot 373\,t^5 - 188703\,t^4 \\ & - 3785\,t^3 + 347\,t^2 + 33\,t + 1 \ . \end{aligned}$$

Then $F(t) = t^8 + 2\,t^6 + t^5 + t^3 + 2\,t^2 + 1$ is irreducible over $\mathbb{F}_3$, and $\mathrm{ord}(A_F) = 41$. By Corollary 7.5, ℓ-rank$(\mathcal{J}_{41}) = 8$, and ℓ-rank$(\mathcal{J}_k) = 0$ for $1 \le k \le 40$.

We now illustrate with two examples how our previous results can be employed to obtain the complete ℓ-rank structure of a function field $\mathbb{K}/\mathbb{F}_q$. In fact, knowing the L-polynomial of $\mathbb{K}$ will often yield this entire structure; at times, it is also necessary to find the ℓ-rank of $\mathcal{J}_n$ for one or a few very small values of n via direct computation, for example, using Magma. Generally, it is even possible to deduce the elementary divisors of $\pi_{q,n\ell}$ using these techniques.

Example 7.7 We first revisit Example 5.5 of [2], which was already discussed in Examples 4.4 and 5.7. Here, $\mathbb{K} = \mathbb{F}(x, y)$ with y as given in Example 4.4 is a genus 4 hyperelliptic function field over $\mathbb{F}_{179}$. We wish to determine the 3-rank structure of $\mathbb{K}/\mathbb{F}_{179}$, i.e. the 3-rank of $\mathcal{J}_n$ with $1 \le n \le n_3$. Theorems 4.3 and 5.5 yield $n_3 \mid 24$.

Recall that $F = P_1 P_2 P_3^2 P_4 \in \mathbb{F}_3[t]$ where

$$P_1(t) = t + 1, \quad P_2(t) = t + 2, \quad P_3(t) = t^2 + 1, \quad P_4(t) = t^2 + t + 2$$

are all irreducible over $\mathbb{F}_3$, and $\mathrm{ord}(A_{P_1}) = 2$, $\mathrm{ord}(A_{P_2}) = 1$, $\mathrm{ord}(A_{P_3}) = 4$, $\mathrm{ord}(A_{P_4}) = 8$.

By part 2 of Theorem 7.4, 3-rank$(\mathcal{J}_1) = 1$, and by part 3 of the same theorem, 3-rank$(\mathcal{J}_n) = 1$ for all odd n. Using the notation of Theorem 7.4, we obtain the following sets $\mathcal{I}_n$:

n	1 (mod 2)	2 (mod 4)	4 (mod 8)	0 (mod 8)
$\mathcal{I}_n$	$\{2\}$	$\{1, 2\}$	$\{1, 2, 3\}$	$\{1, 2, 3, 4\}$

By part 1 of Theorem 7.4, 3-rank$(\mathcal{J}_n) = \deg(P_2) = 1$ for n odd (which we already observed), 3-rank$(\mathcal{J}_n) = \deg(P_1) + \deg(P_2) = 2$ for $n \equiv 2 \pmod 4$, 3-rank$(\mathcal{J}_n) \ge 4$ for $n \in \{4, 12, 20\}$, and 3-rank$(\mathcal{J}_n) \ge 6$ for $n \in \{8, 16, 24\}$. From Theorems 4.3 and 5.5, 3-rank$(\mathcal{J}_{24}) = 8$. This leaves the 3-ranks of $\mathcal{J}_n$ for $n = 4, 8, 12, 16$ and 20 only partially determined.

We first analyze $n = 12$; this will resolve all the ambiguous cases. The primary rational canonical form of π_{179,n_3} is one of

$$A_1 = \mathrm{diag}(A_{P_1}, A_{P_2}, A_{P_3}, A_{P_3}, A_{P_4}) \ \text{ or } \ A_2 = \mathrm{diag}(A_{P_1}, A_{P_2}, A_{P_3^2}, A_{P_4}) \ .$$

By considering the orders of the diagonal sub-matrices in A_1 and A_2, is easy to see that $A_1^{12} = A_2^{12} = \mathrm{diag}(I_6, -I_2)$. It follows that π_{179,n_3}^{12} acts trivially on a subspace of $\mathcal{J}[3]$ of dimension exactly 6. So 3-rank$(\mathcal{J}_{12}) = 6$.

Note that $\mathbb{F}_{179^{12}}$ is the largest proper subfield of $\mathbb{F}_{179^{24}}$, so this implies that $n_3 = 24$. Since A_1 has order 8, it follows that the primary rational canonical form of π_{179,n_3} must be A_2.

Now $A_{P_1}^n = A_{P_2}^n = (1)$ for all n even, and both these matrices have a one-dimensional eigenspace. By Lemma 7.3, $A_{P_3^2}^n$ has 1 as its only eigenvalue, with a 2-dimensional eigenspace, for $n = 4, 8, 16, 20$. Since $\mathrm{ord}(A_{P_4}) = 8$, $A_{P_4}^4 = A_{P_4}^{20}$ has a double eigenvalue -1. A_2^4 and A_2^{20} have 1 as a 6-fold eigenvalue with a 4-dimensional eigenspace, and -1 as a double eigenvalue. Hence, π_{179,n_3}^4 acts trivially on a subspace of $\mathcal{J}[3]$ of dimension 4. Thus, 3-rank$(\mathcal{J}_4) =$ 3-rank$(\mathcal{J}_{20}) = 4$. Similarly, $A_{P_4}^8 = A_{P_4}^{16} = I_2$, so A_2^8 and A_2^{16} each have 1 as their only eigenvalue, with a 6-dimensional eigenspace. Thus, 3-rank$(\mathcal{J}_8) =$ 3-rank$(\mathcal{J}_{16}) = 6$. This yields the following 3-rank structure for $\mathbb{K}/\mathbb{F}_{179}$:

n	3-rank
odd	1
2, 6, 10, 14, 18, 22	2
4, 20	4
8, 12, 16	6
24	8

To check our results, we used Magma to compute the 3-Sylow subgroups of $\mathcal{J}_n$ for all proper divisors n of 24, and for a few other values of n, and found

$$\mathrm{Syl}_3(\mathcal{J}_1) \cong \mathrm{Syl}_3(\mathcal{J}_3) \cong \mathbb{Z}/9,$$
$$\mathrm{Syl}_3(\mathcal{J}_2) \cong \mathrm{Syl}_3(\mathcal{J}_{10}) \cong (\mathbb{Z}/9)^2, \quad \mathrm{Syl}_3(\mathcal{J}_6) \cong (\mathbb{Z}/27)^2,$$
$$\mathrm{Syl}_3(\mathcal{J}_4) \cong \mathrm{Syl}_3(\mathcal{J}_{20}) \cong (\mathbb{Z}/9)^4,$$
$$\mathrm{Syl}_3(\mathcal{J}_8) \cong \mathrm{Syl}_3(\mathcal{J}_{16}) \cong (\mathbb{Z}/3)^2 \times (\mathbb{Z}/9)^4, \quad \mathrm{Syl}_3(\mathcal{J}_{12}) \cong (\mathbb{Z}/3)^2 \times (\mathbb{Z}/27)^4.$$

We were unable to compute $\mathrm{Syl}_3(J_{24})$ with Magma due to limited computer memory.

Example 7.8 Consider $q = 149$, the hyperelliptic function field $\mathbb{K} = \mathbb{F}_{149}(x, y)$ of genus 4 with

$$y^2 = x^9 + 43\,x^8 + 35\,x^7 + 11\,x^6 + 22\,x^5 + 38\,x^4 + 75\,x^3 + 28\,x^2 + 61\,x + 5 \ ,$$

and $\ell = 5$. With the aid of Magma, we computed the L-polynomial $L(t)$ of $\mathbb{K}/\mathbb{F}_{149}$ and obtained $F(t) \equiv t^8 L(t^{-1}) \pmod 5$. We found that

$$F(t) = t^8 + 4t^7 + 3t^6 + 2t^5 + 2t^4 + 3t^3 + 3t^2 + t + 1 \in \mathbb{F}_5[t]$$

factors as $F = P_1 P_2 P_3^2 P_4 P_5$, where

$$P_1(t) = t + 4,\ P_2(t) = t + 1,\ P_3(t) = t + 3,\ P_4(t) = t^2 + t + 2,\ P_5 = t^2 + 2t + 3$$

are all irreducible over $\mathbb{F}_5$. One easily verifies that $\mathrm{ord}(A_{P_1}) = 1$, $\mathrm{ord}(A_{P_2}) = 2$, $\mathrm{ord}(A_{P_3}) = 4$, and $\mathrm{ord}(A_{P_4}) = \mathrm{ord}(A_{P_5}) = 24$. Both Theorems 4.3 and 5.5 imply $n_5 \mid 120$.

As in the previous example, we deduce that 5-rank$(\mathcal{J}_n) = 1$ for n odd and obtain

n	1 (mod 2)	2 (mod 4)	4, 8, 12, 16, 20 (mod 24)	0 (mod 24)
$\mathcal{I}_n$	$\{1\}$	$\{1,2\}$	$\{1,2,3\}$	$\{1,2,3,4,5\}$

By part 1 of Theorem 7.4, 5-rank$(\mathcal{J}_n) = 1$ for n odd, 5-rank$(\mathcal{J}_n) = 2$ for $n \equiv 2 \pmod 4$, 5-rank$(\mathcal{J}_n) \geq 3$ for $n \equiv 4, 8, 16, 20 \pmod{24}$, and 5-rank$(\mathcal{J}_n) \geq 7$ for $n \equiv 0 \pmod{24}$. Also, from Theorems 4.3 and 5.5, 5-rank$(\mathcal{J}_{120}) = 8$. This leaves the 5-ranks of $\mathcal{J}_n$ for $n \equiv 0 \pmod 4$ with $n < 120$ only partially determined.

The primary rational canonical form $A_{\pi_{149,n_5}}$ of π_{149,n_5} is one of

$$\begin{aligned} A_1 &= \operatorname{diag}(A_{P_1}, A_{P_2}, A_{P_3}, A_{P_3}, A_{P_4}, A_{P_5}) \text{ or} \\ A_2 &= \operatorname{diag}(A_{P_1}, A_{P_2}, A_{P_3^2}, A_{P_4}, A_{P_5}) \ . \end{aligned}$$

Hence, $n_5 = \operatorname{ord}(A_1) = 24$ or $n_5 = \operatorname{ord}(A_2) = 120$.

We consider multiples n of 20 less than 120; note that $\operatorname{ord}(A_{P_3^2}) = 20$ by Lemma 4.1. For such n, we have $A_1^n = A_2^n = \operatorname{diag}(I_4, A_{P_4}^n, A_{P_5}^n)$, and $A_{P_4}^n$ and $A_{P_5}^n$ do not have 1 as an eigenvalue. It follows that π_{149,n_5}^n acts trivially on a subspace of $\mathcal{J}[5]$ of dimension exactly 4. So 5-rank$(\mathcal{J}_n) = 4$ for these n.

Note that by Lemma 7.3, $A_{P_3^2}^4$ has 1 as its only eigenvalue, with a one-dimensional eigenspace. Also, $A_{P_4}^4$ and $A_{P_5}^4$ do not have 1 as an eigenvalue. Hence, 5-rank$(\mathcal{J}_4) = 4$ if $A_{\pi_{149,n_5}} = A_1$ and 5-rank$(\mathcal{J}_4) = 3$ if $A_{\pi_{149,n_5}} = A_2$. At this point, it is unclear how to resolve this ambiguity, so we resort to Magma to determine 5-rank$(\mathcal{J}_4)$. We obtain 5-rank$(\mathcal{J}_4) = 3$, so $A_{\pi_{149,n_5}} = A_2$ and $n_5 = 120$. This resolves the rest of the 5-rank structure completely as follows.

Since $7 \leq$ 5-rank$(\mathcal{J}_n) <$ 5-rank$(\mathcal{J}_{120}) = 8$ for $n \equiv 0 \pmod{24}$ and $n < 120$, we have 5-rank$(\mathcal{J}_n) = 7$ for such n. Also, for any multiple n of 4 not divisible by 20, $A_{P_3^2}^n$ has 1 as its only eigenvalue, with a one-dimensional eigenspace. So 5-rank$(\mathcal{J}_n) = 3$ for $n \equiv 0 \pmod 4$, $n \not\equiv 0 \pmod{20}$, $n \not\equiv 0 \pmod{24}$. This yields the following 5-rank structure for $\mathbb{K}/\mathbb{F}_{149}$:

Congruence class of n, $1 \leq n \leq 120$	5-rank
$n \equiv 1 \pmod 2$	1
$n \equiv 2 \pmod 4$	2
$n \equiv 0 \pmod 4$, $n \not\equiv 0 \pmod{20}$, $n \not\equiv 0 \pmod{24}$	3
$n \equiv 0 \pmod{20}$, $n < 120$	4
$n \equiv 0 \pmod{24}$, $n < 120$	7
$n = 120$	8

Again, we used Magma to compute $\mathcal{J}_n[5]$ for most of the divisors n of 120, and found

$$\begin{aligned} &\text{5-rank}(\mathcal{J}_1) = \text{5-rank}(\mathcal{J}_3) = \text{5-rank}(\mathcal{J}_5) = \text{5-rank}(\mathcal{J}_{15}) = 1, \\ &\text{5-rank}(\mathcal{J}_2) = \text{5-rank}(\mathcal{J}_6) = \text{5-rank}(\mathcal{J}_{10}) = \text{5-rank}(\mathcal{J}_{30}) = 2, \\ &\text{5-rank}(\mathcal{J}_4) = \text{5-rank}(\mathcal{J}_8) = \text{5-rank}(\mathcal{J}_{12}) = 3, \\ &\text{5-rank}(\mathcal{J}_{20}) = 4, \\ &\text{5-rank}(\mathcal{J}_{24}) = 7. \end{aligned}$$

We again could not compute 5-rank$(\mathcal{J}_n)$ for $n = 40, 60, 120$ using Magma because of limited memory.

8 Conclusion

For any function field $\mathbb{K}/\mathbb{F}_q$ of genus g, we have provided several tools for analyzing the ℓ-ranks of the Jacobians of constant field extensions $\mathbb{K}_n/\mathbb{F}_{q^n}$, with $n \in \mathbb{N}$ and ℓ a prime not dividing q. This includes the determination of the field

of definition of the absolute ℓ-torsion, or at least an upper bound on the extension degree of this field over $\mathbb{F}_q$.

Our investigation extends the previous results of [2]. Of key importance is the factorization of $F(t) \in \mathbb{F}_\ell[t]$ into monic irreducibles over $\mathbb{F}_\ell$, where $F(t) \equiv t^{2g}L(t^{-1}) \pmod{\ell}$ and $L(t)$ is the L-polynomial $L(t)$ of $\mathbb{K}/\mathbb{F}_q$. Assuming that $L(t)$ can be computed, our method can often determine the entire ℓ-rank structure of $\mathbb{K}/\mathbb{F}_q$. This is always true if $F(t)$ is square-free, and also in some other cases when $F(t)$ only contains small and few powers. In fact, oftentimes, our approach is able to identify the elementary divisors of the q-th power Frobenius, which in turn yield the complete ℓ-rank structure. At times, when $F(t)$ is not square-free, it may additionally be necessary to determine the ℓ-rank of $\mathcal{J}_n$ for one or a few very small values of n.

Apart from the L-polynomial, all the ingredients of our method stem from basic algebra and linear algebra. Obtaining $L(t)$ can be difficult and represents the main practical and computational obstacle to this approach. Magma computes the zeta function, and hence the L-polynomial, of a hyperelliptic function field of moderate size reasonably efficiently. For small ℓ, it can also find the ℓ-Sylow subgroups of an Abelian group quite quickly. Thus, our approach is very suitable for not too large base fields $\mathbb{F}_q$ and small values of ℓ, and is especially fruitful for hyperelliptic curves. Unfortunately, it is unclear whether it is possible to obtain $F(t)$ without computing $L(t)$, or to ascertain the elementary divisors of the Frobenius via some other means.

Acknowledgments. This work was begun at the *WIN — Women in Numbers* workshop, held at the Banff International Research Station (BIRS) in Banff, Alberta (Canada) November 2-7, 2008. The authors are grateful to BIRS for hosting this workshop at this beautiful venue and providing a stimulating work environment. The first four authors are also indebted to the University of Calgary's Department of Mathematics and Statistics for hosting them during a visit to finish this work. Finally, we owe thanks to an anonymous referee for her or his careful proof-reading and constructive comments that lead to considerable improvements of this paper.

References

[1] Achter, J. *The distribution of class groups of function fields.* J. Pure Appl. Algebra **2**04 (2006), 316–333.

[2] Bauer, M., Jacobson Jr, J. M., Lee, Y. and Scheidler, R. *Construction of Hyperelliptic Function Fields of High Three-Rank.* Math. Comp. **77**(261) (2008), 503–530.

[3] Balasubramanian, R. and Koblitz, N. *The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm.* J. Cryptology **11** (1998), 141–145.

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

[5] Chavdarov, N. *The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy.* Duke Math. J. **87** (1997), 151–180.

[6] Charles, D. and Lauter, K. *Computing modular polynomials.* LMS J. Comput. Math. **8** (2005), 195–204.

[7] Freeman D. and Lauter, K. *Computing Endomorphism Rings of Jacobians of Genus 2 Curves over Finite Fields.* Symp. Algebraic Geometry and its Applications, World Scientific, 2008, pp. 29–66.

[8] Hungerford, T. W. *Algebra.* Springer, New York 1974.

[9] Kowalski, E. *The large sieve, monodromy and zeta functions of curves.* J. Reine Angew. Math. **601** (2006), 29–69.

[10] Lee, Y. and Pacelli, A. M. *Class groups of imaginary function fields: the inert case.* Proc. Amer. Math. Soc. **133** (2005), 2883–2889.
[11] Lee Y. and Pacelli, A. M. *Higher rank subgroups in the class groups of imaginary function fields.* J. Pure Applied Algebra **207** (2006), 51–62.
[12] Miret, J., Pujolàs, J. and Rio, A. *Bisection for genus 2 curves in odd characteristic.* Proc. Japan Academy – Series A **85** (2009), 55–61.
[13] Pacelli, A. M., *Abelian subgroups of any order in class groups of global function fields.* J. Number Theory **106** (2004), 26–49.
[14] Pacelli, A. M. *The prime at infinity and the rank of the class group of global function fields.* J. Number Theory **116** (2006), 311–323.
[15] Rosen, M. *Number Theory in Function Fields.* Springer, Berlin 2002.
[16] Rozenhart, P. *Fast Tabulation of Cubic Function Fields.* Doctoral Dissertation, University of Calgary (Canada) 2009.
[17] Stichtenoth, H. *Algebraic Function Fields and Codes.* Second ed., Springer, Berlin 2009.
[18] Zhang, X.-K. *Ambiguous classes and 2-rank of class group of quadratic function field* (Chinese summary). J. China Univ. Sci. Tech. **17** (1987), 425–431.