Designs, Codes and Cryptography
https://doi.org/10.1007/s10623-022-01041-3

High order elements in finite fields arising from recursive towers

Valerio Dose[1] · Pietro Mercuri[2] · Ankan Pal[3] · Claudio Stirpe[4]

Received: 11 March 2021 / Revised: 10 March 2022 / Accepted: 25 March 2022

Abstract
We illustrate a general technique to construct towers of fields producing high order elements in $\mathbb{F}_{q^{2^n}}$, for odd q, and in $\mathbb{F}_{2^{2\cdot 3^n}}$, for $n \geq 1$. These towers are obtained recursively by $x_n^2 + x_n = v(x_{n-1})$, for odd q, or $x_n^3 + x_n = v(x_{n-1})$, for $q = 2$, where $v(x)$ is a polynomial of small degree over the prime field $\mathbb{F}_q$ and x_n belongs to the finite field extension $\mathbb{F}_{q^{2^n}}$, for an odd q, or to $\mathbb{F}_{2^{2\cdot 3^n}}$. Several examples are provided to show the numerical efficacy of our method. Using the techniques of Burkhart et al. (Des Codes Cryptogr 51(3):301–314, 2009) we prove similar lower bounds on the orders of the groups generated by x_n, or by the discriminant δ_n of the polynomial. We also provide a general framework which can be used to produce many different examples, with the numerical performance of our best examples being slightly better than in the cases analyzed in Burkhart et al. (2009).

Keywords Finite field · High order elements · Recursive towers · Galois towers

Mathematics Subject Classification 11T55 · 11T71

Communicated by O. Ahmadi.

✉ Pietro Mercuri
mercuri.ptr@gmail.com

Valerio Dose
valerio.dose@uniroma1.it

Ankan Pal
ankanpal100@gmail.com

Claudio Stirpe
clast@inwind.it

1 Department of Computer, Control and Management Engineering (DIAG), "Sapienza" Università di Roma, Rome, Italy

2 Department of SBAI, "Sapienza" Università di Roma, Rome, Italy

3 Department of Mathematics, University of L'Aquila, L'Aquila, Italy

4 Convitto Nazionale R. Margherita, Anagni, Italy

Published online: 21 April 2022

1 Introduction

Finding elements of high multiplicative order in a finite field is an interesting problem in computational number theory and has applications in cryptography (for instance: Discrete Logarithm Problem). A general method to find high order elements was given in [11], later improved in [8, 18]. Another general result in this area is an algorithmic technique for finding primitive elements which is devised in [12]. Such technique is efficient in finite fields of small characteristic. Other strategies which allow to construct elements of high order usually address specific sequences of finite fields. In this regard, methods involving Gauss periods were first proposed in the results summarized in [26]. After that, an extensive literature followed with works such as [1, 5, 16, 17, 19]. Recently, Artin-Schreier extensions were also effectively used in [13, 21]. Another interesting approach is to look for high order elements which arise as coordinates of points on an algebraic curve defined over a finite field (see for example [4, 24, 25]). One way which has been explored for generating elements of this type is through the iterative use of polynomial equations of type $f(x_{n-1}, x_n) = 0$, defining suitable towers of fields, which we address as *recursive towers* in this work. Examples of this can be found in [3, 20, 22, 25].

In [3], a recursive tower defined by $f(x_{n-1}, x_n)$ is used to produce elements δ_n with high multiplicative order in $\mathbb{F}_{q^{2^n}}$, for an odd q, and in $\mathbb{F}_{q^{3^n}}$, for $q \neq 3$. The choice of the polynomial f for the recursive process to generate high order elements in finite field extensions, was limited to the equations of the modular curve towers in [10].

In this work, we attempt to generalize the choice of the polynomials. We illustrate in detail several interesting towers of fields defined by $x_n^2 + x_n = v(x_{n-1})$, where $v(x) \in \mathbb{F}_q[x]$, for an odd q, or $x_n^3 + x_n = v(x_{n-1})$, for $v(x) \in \mathbb{F}_2[x]$. These towers generate elements of high orders in $\mathbb{F}_{q^{2^n}}$ and in $\mathbb{F}_{2^{2\cdot 3^n}}$, for $n \geq 1$. We also give a recipe for finding other towers of the same form which have similar properties. The simple algebraic conditions given in Sections 3 and 4, which differ partially from the conditions required in [3] (Remark 3.1 below), seem to play an important role toward this. In fact, in many of the cases we studied, these conditions are useful to prove the existence of high order elements x_n, in the field extension.

Throughout this paper, δ_n in $\mathbb{F}_{q^{2^n}}$ is the discriminant of the polynomial $f(x_n, y)$ in $\mathbb{F}_{q^{2^n}}[y]$. In Corollary 3.5, we prove that the multiplicative orders of x_n and δ_n grow very fast if x_{n-j}^2 and δ_{n-j}^2 do not belong to $\mathbb{F}_{q^{2^{n-j-1}}}$, for all $j < n-1$. Similar results hold also in even characteristic, see Corollary 4.3. Notably, despite the bounds obtained are similar and have no advantage with respect to the ones in [3], the even characteristic case turns out to be completely new. In particular, no additional conditions on the discriminant are required, and the details of the proof are worked out in a different manner. Furthermore the numerical performance of some of our examples improves slightly on [3], in the iterations we were able to compute. As already mentioned above, the polynomials used in [3] are the models of certain modular curves given in [10]. Despite this fact, a possible relation of the construction of high order elements with the arithmetic properties of such curves does not seem to play a role in the proof of the lower bounds. Instead, in one case, we do make use of some arithmetic properties of the algebraic curve considered by us (Lemma 5.4).

A comparative study with other relevant literature has also been carried-out. For example, a specific construction of high order elements in the same type of fields of odd characteristic q can be found in [7], and some variations on it are in [6, 15]. Comparing the numerical performance of their construction with our variety of examples, we observe that the results are similar for $q \equiv 1 \pmod 4$, while for $q \equiv 3 \pmod 4$ our construction performs better (see Sect. 7 for examples with $q = 3, 11$).

In Sect. 2, we introduce the notation that we use in the paper. In Sects. 3 and 4, we give the main results which allow us to obtain the lower bounds on the order of x_n and δ_n. Section 3 deals with odd characteristic and Sect. 4 deals with even characteristic. The lists of towers satisfying the properties given in Sects. 3 and 4 are provided in Sects. 5 and 6, respectively. Finally, in Sect. 7, we list numerical results obtained using MAGMA [2], about the seven towers listed in Sects. 5 and 6.

2 Background and notation

Let q be a prime and let $\mathbb{F}_q$ and $\mathbb{F}_q^*$ denote the finite field with q elements and its multiplicative group, respectively. We recall that every extension $\mathbb{F}_{q^r}/\mathbb{F}_q$ of finite fields, for a positive integer r, is cyclic and the Galois group is generated by the Frobenius automorphism $a \mapsto a^q$, for each $a \in \mathbb{F}_{q^r}$.

By *tower of fields*, or simply a *tower*, we mean a sequence of field extensions

$$K_1 \subset K_2 \subset \ldots \subset K_n \subset \ldots.$$

We are interested in infinite towers, namely towers such that the degree $[K_n : K_1]$ grows to infinity. All the towers considered in this paper are actually finite, normal and separable, i.e., each extension K_n/K_{n-1} is finite, normal and separable, for every $n > 1$. When q is odd, for each positive integer n, let $K_n = \mathbb{F}_q(x_n)$, where the element $x_n \in \mathbb{F}_{q^{2^n}}$ is given by a recursive formula $f(x_{n-1}, x_n) = 0$, for a polynomial $f(x, y) \in \mathbb{F}_q[x, y]$. In this case, we say that the tower $K_1 \subset K_2 \subset \ldots \subset K_n \subset \ldots$ is defined by $f(x_{n-1}, x_n)$ and we address this kind of towers as *recursive towers*. We focus on towers defined by $f(x_{n-1}, x_n) = x_n^2 + x_n - v(x_{n-1})$, for $n \geq 2$, with $x_1 \in \mathbb{F}_{q^2}$, and where $v(x)$ is a polynomial in $\mathbb{F}_q[x]$. We denote by δ_n the discriminant $\delta_n = 1 + 4v(x_n)$, for $n \geq 1$. We point out that both elements x_n and δ_n belong to $\mathbb{F}_{q^{2^n}}$, but they could also lie in a smaller extension $\mathbb{F}_{q^{2^k}}$ for some $k < n$. Given the tower defined by $f(x_{n-1}, x_n)$, we denote by $g(x, y) \in \mathbb{F}_q[x, y]$ a polynomial giving the relation between two consecutive discriminants δ_{n-1} and δ_n, namely $g(\delta_{n-1}, \delta_n) = 0$. In the case of even characteristic (Sects. 4 and 6), we deal with towers defined by $f(x_{n-1}, x_n) = x_n^3 + x_n + v(x_{n-1})$, with $x_n \in \mathbb{F}_{2^{2\cdot 3^n}}$, for $n \geq 1$, and $v(x)$ being a polynomial in $\mathbb{F}_2[x]$.

Given two positive integers j and n, such that $j < n$, we denote the norm of the field extension $\mathbb{F}_{q^{2^n}}/\mathbb{F}_{q^{2^{n-j}}}$ by, $\mathrm{N}_{n,j} : \mathbb{F}_{q^{2^n}} \to \mathbb{F}_{q^{2^{n-j}}}$. The norm in the odd case is $\mathrm{N}_{n,j}(x) = x^{\prod_{i=1}^{j}(q^{2^{n-i}}+1)}$. In order to apply the same techniques to even characteristic, we also denote by $\mathrm{N}_{n,j} : \mathbb{F}_{2^{2\cdot 3^n}} \to \mathbb{F}_{2^{2\cdot 3^{n-j}}}$ the norm of the extension $\mathbb{F}_{2^{2\cdot 3^n}}/\mathbb{F}_{2^{2\cdot 3^{n-j}}}$, namely $\mathrm{N}_{n,j}(x) = x^{\prod_{i=1}^{j}(4^{2\cdot 3^{n-i}}+4^{3^{n-i}}+1)}$. For every characteristic, we use the conventions $\mathrm{N}(x) := \mathrm{N}_{n,1}(x)$ and $\mathrm{N}_{n,0}(x) = x$.

We use the following lemma for estimating the order of the elements in finite fields.

Lemma 2.1 *Let ℓ be a prime and let $\Phi_{\ell^n}(x) = \sum_{j=0}^{\ell-1} x^{j\ell^{n-1}}$ be the ℓ^n-th cyclotomic polynomial for a positive integer n. Let a, b and c be positive integers such that $b < c$ and $a \equiv 1 \bmod \ell$. Then $\gcd\left(\Phi_{\ell^{b+1}}(a), \Phi_{\ell^{c+1}}(a)\right) = \ell$, in particular $\frac{1}{\ell}\Phi_{\ell^{b+1}}(a)$ and $\frac{1}{\ell}\Phi_{\ell^{c+1}}(a)$ are coprime. Moreover, if p is a prime dividing $\frac{1}{\ell}\Phi_{\ell^{b+1}}(a)$, then $p > \ell^{b+1}$.*

Proof See [3, Lemmas 1 and 2]. □

In order to prove that a cubic polynomial is irreducible, we need the following results.

Lemma 2.2 *If $u \in \mathbb{F}_{2^{2\cdot 3^n}}$ and $c := u + u^{-1} \in \mathbb{F}_{2^{2\cdot 3^{n-1}}}$, then $u \in \mathbb{F}_{2^{2\cdot 3^{n-1}}}$.*

Proof If $u \notin \mathbb{F}_{2^{2\cdot 3^{n-1}}}$, then $x^2 + cx + 1$ is the minimum polynomial of u over $\mathbb{F}_{2^{2\cdot 3^{n-1}}}$. So $u \in \mathbb{F}_{2^{2\cdot 3^n}} \cap \mathbb{F}_{2^{4\cdot 3^{n-1}}} = \mathbb{F}_{2^{2\cdot 3^{n-1}}}$ and we get a contradiction. □

Lemma 2.3 *Let $u^3 \in \mathbb{F}_{2^{2\cdot 3^{n-1}}}$ be a root of the quadratic polynomial $x^2 + tx + 1$, with $t \in \mathbb{F}_{2^{2\cdot 3^{n-1}}}$. Then $y := u + u^{-1} \in \mathbb{F}_{2^{2\cdot 3^n}}$ is a root of the cubic polynomial $x^3 + x + t$, and furthermore $y \in \mathbb{F}_{2^{2\cdot 3^{n-1}}}$ if and only if $u \in \mathbb{F}_{2^{2\cdot 3^{n-1}}}$.*

Proof This is Cardano's formula for solving cubic equations in even characteristic. The second statement follows by Lemma 2.2 taking $y = c = u + u^{-1}$. □

3 Towers in odd characteristic

In order to find good towers we restrict our search to polynomials $f(x, y) = y^2 + y - v(x)$, with $v(x) \in \mathbb{F}_q[x]$ being a non-zero polynomial, which satisfy Condition **(1)** below and at least one of the last two conditions:

(1) $\frac{f(x_{n-1},0)}{x_{n-1}}$ is a square in $\mathbb{F}_{q^{2^{n-1}}}$ for $n \geq 2$;
(2) $\frac{g(\delta_{n-1},0)}{x_{n-1}}$ is a square in $\mathbb{F}_{q^{2^{n-1}}}$ for $n \geq 2$;
(2') $\frac{g(\delta_{n-1},0)}{\delta_{n-1}}$ is a square in $\mathbb{F}_{q^{2^{n-1}}}$ for $n \geq 2$.

Remark 3.1 We have found examples, in the literature, of towers of fields which satisfy Condition **(2')** above, but do not verify Condition **(1)** (see [3, Section 4, formula (5)]). We wonder whether such examples satisfy a suitable analog of **(1)** which ensures that Proposition 3.3 below holds anyway.

Remark 3.2 These conditions are not sufficient for obtaining high order elements from each tower, but, for our particular choices of f, they are sufficient to construct a recursive tower defined by $f(x_{n-1}, x_n)$ as Proposition 3.3 below shows.

The following key proposition ensures that all the polynomials $f(x_{n-1}, x_n)$ listed in Sect. 5 define infinite towers of fields. In particular it shows that $[K_n : K_{n-1}] = 2$, for all $n > 1$. The argument of the proof is the corresponding analogue of [3, Proposition 1] but it could be applied to many different towers.

Proposition 3.3 *Let $v(x) \in \mathbb{F}_q[x]$ be a polynomial and assume that $f(x_{n-1}, x_n) = x_n^2 + x_n - v(x_{n-1})$ satisfies Conditions **(1)** and **(2)**, or Conditions **(1)** and **(2')**. If x_{n-1} and δ_{n-1} are not squares in the multiplicative group $\mathbb{F}^*_{q^{2^{n-1}}}$ for a suitable $n \geq 2$, then x_j and δ_j are not squares in the multiplicative group $\mathbb{F}^*_{q^{2^j}}$, for $j \geq n$.*

Proof The element x_n is not in $\mathbb{F}_{q^{2^{n-1}}}$ because δ_{n-1} is not a square in $\mathbb{F}_{q^{2^{n-1}}}$, therefore $f(x_{n-1}, y)$ is the minimal polynomial of x_n. We need to ensure that $x_n^{(q^{2^n}-1)/2} = -1$. As in [3, Proposition 1], we obtain:

$$\begin{aligned} x_n^{(q^{2^n}-1)/2} &= (x_n^{q^{2^{n-1}}+1})^{(q^{2^{n-1}}-1)/2} = \mathrm{N}(x_n)^{(q^{2^{n-1}}-1)/2} \\ &= f(x_{n-1}, 0)^{(q^{2^{n-1}}-1)/2} = -1, \end{aligned}$$

where $\mathrm{N}(x_n) = x_n^{q^{2^{n-1}}+1} = f(x_{n-1}, 0)$ is the norm of x_n over $\mathbb{F}_{q^{2^{n-1}}}$ and we use Condition **(1)** in last equality to show that $f(x_{n-1}, 0)$ is not a square in $\mathbb{F}_{q^{2^{n-1}}}$ for $n > 1$.

Consider the discriminant δ_n. Again $g(\delta_{n-1}, y)$ is the minimal polynomial of $\delta_n = 1 + 4v(x_n)$. Since, in $\mathbb{F}_{q^{2^n}}$, we know that $\frac{f(x_n,0)}{x_n}$ is a square by Condition **(1)**, -1 is a square and x_n is not a square as above, then $v(x_n) = -f(x_n, 0)$ is not a square in $\mathbb{F}_{q^{2^n}}$. Hence, $\delta_n \notin \mathbb{F}_{q^{2^{n-1}}}$. The same computation as above yields:

$$\begin{aligned}\delta_n^{(q^{2^n}-1)/2} &= (\delta_n^{q^{2^{n-1}}+1})^{(q^{2^{n-1}}-1)/2} = \mathrm{N}(\delta_n)^{(q^{2^{n-1}}-1)/2} \\ &= g(\delta_{n-1}, 0)^{(q^{2^{n-1}}-1)/2} = -1,\end{aligned}$$

where we use Condition **(2)**, respectively **(2')**, in last equality to show that $g(\delta_{n-1}, 0)$ is not a square in $\mathbb{F}_{q^{2^{n-1}}}$, because x_{n-1}, (respectively δ_{n-1}), is a non-square by hypothesis. It follows that x_n and δ_n are non-squares in $\mathbb{F}_{q^{2^n}}$. Repeating the same argument, we find that x_j and δ_j are not squares in $\mathbb{F}_{q^{2^j}}$, for all $j > n$, which completes the proof. □

The importance of this proposition is evident if we consider Corollary 3.5 below, which is an analogue of [3, Proposition 2]. We first state the following property of the norm that is used in the proof of the corollary.

Lemma 3.4 *Let $n \geq 2$ and $j < n$ be positive integers, then*

$$\frac{\mathrm{N}_{n,j}(x_n)}{x_{n-j}} = \prod_{k=1}^{j} \mathrm{N}_{n-k,j-k}\left(\frac{\mathrm{N}_{n-k+1,1}(x_{n-k+1})}{x_{n-k}}\right).$$

Moreover $\frac{\mathrm{N}_{n,j}(x_n)}{x_{n-j}}$ is a square in $\mathbb{F}_{q^{2^{n-j}}}$.

Proof The case $j = 1$ is trivial. By induction on j, let $j \geq 2$ and assume the result holds for $j - 1$, then

$$\begin{aligned}\frac{\mathrm{N}_{n,j}(x_n)}{x_{n-j}} &= \frac{x_n^{(q^{2^{n-1}}+1)\prod_{i=2}^{j}(q^{2^{n-i}}+1)}}{x_{n-j}} \\ &= \left(\frac{x_n^{q^{2^{n-1}}+1}}{x_{n-1}}\right)^{\prod_{i=2}^{j}(q^{2^{n-i}}+1)} \frac{x_{n-1}^{\prod_{i=2}^{j}(q^{2^{n-i}}+1)}}{x_{n-j}} \\ &= \left(\frac{\mathrm{N}_{n,1}(x_n)}{x_{n-1}}\right)^{\prod_{i=2}^{j}(q^{2^{n-i}}+1)} \frac{\mathrm{N}_{n-1,j-1}(x_{n-1})}{x_{n-j}} \\ &= \left(\frac{\mathrm{N}_{n,1}(x_n)}{x_{n-1}}\right)^{\prod_{i=1}^{j-1}(q^{2^{n-1-i}}+1)} \prod_{k=1}^{j-1} \mathrm{N}_{n-k-1,j-k-1}\left(\frac{\mathrm{N}_{n-k,1}(x_{n-k})}{x_{n-k-1}}\right) \\ &= \mathrm{N}_{n-1,j-1}\left(\frac{\mathrm{N}_{n,1}(x_n)}{x_{n-1}}\right) \prod_{k=2}^{j} \mathrm{N}_{n-k,j-k}\left(\frac{\mathrm{N}_{n-k+1,1}(x_{n-k+1})}{x_{n-k}}\right).\end{aligned}$$

The remaining part of the proof follows by Condition **(1)**. □

Corollary 3.5 *Let $v(x)$ be a polynomial in $\mathbb{F}_q[x]$ and assume that $f(x_{n-1}, x_n) = x_n^2 + x_n - v(x_{n-1})$ satisfies Conditions **(1)** and **(2)**, or Conditions **(1)** and **(2')**, and that x_1 and δ_1 are not squares in $\mathbb{F}_{q^2}$. Then $x_n^2 \notin \mathbb{F}_{q^{2^{n-1}}}$ and the order of x_n is greater than*

$$2^{\frac{1}{2}(n^2+3n)+\mathrm{ord}_2(q-1)-2},$$

for all $n > 1$. The same lower bound also holds for the order of δ_n if $\delta_n^2 \notin \mathbb{F}_{q^{2^{n-1}}}$ for all $n > 1$.

Proof We know that $x_n \notin \mathbb{F}_{q^{2^{n-1}}}$ by Proposition 3.3, therefore we have that $x_n^2 = -x_n + v(x_{n-1}) \notin \mathbb{F}_{q^{2^{n-1}}}$ for all $n > 1$. We show that the order of x_n has a common factor with the odd number $\frac{q^{2^{n-j}}+1}{2}$ proving that $x_n^{\frac{2(q^{2^n}-1)}{q^{2^{n-j}}+1}} \neq 1$, for $j = 1, 2, \ldots, n-1$. For $j = 1$, we have

$$x_n^{\frac{2(q^{2^n}-1)}{q^{2^{n-1}}+1}} = x_n^{2(q^{2^{n-1}}-1)} \neq 1,$$

since $x_n^2 \notin \mathbb{F}_{q^{2^{n-1}}}$, as we have just seen. For $j \geq 2$, we get

$$x_n^{\frac{2(q^{2^n}-1)}{q^{2^{n-j}}+1}} = \left(x_n^{\prod_{k=1}^{j-1}(q^{2^{n-k}}+1)}\right)^{2(q^{2^{n-j}}-1)} = \mathrm{N}_{n,j-1}(x_n)^{2(q^{2^{n-j}}-1)}$$

and the last member above is 1 only if $\mathrm{N}_{n,j-1}(x_n)^2 \in \mathbb{F}_{q^{2^{n-j}}}$. We show that this is not possible. Consider $\mathrm{N}_{n,j}(x_n) = \mathrm{N}_{n-j+1,1}(\mathrm{N}_{n,j-1}(x_n))$. If $\mathrm{N}_{n,j-1}(x_n)^2 \in \mathbb{F}_{q^{2^{n-j}}}$, then either $\mathrm{N}_{n,j}(x_n) = \mathrm{N}_{n,j-1}(x_n)^2$ or $\mathrm{N}_{n,j}(x_n) = \mathrm{N}_{n,j-1}(x_n)$. The latter equality is not possible since $\mathrm{N}_{n,j-1}(x_n)$ is not a square in $\mathbb{F}_{q^{2^{n-j+1}}}$ by Lemma 3.4 but $\mathrm{N}_{n,j}(x_n) \in \mathbb{F}_{q^{2^{n-j}}}$ is a square in $\mathbb{F}_{q^{2^{n-j+1}}}$. The former equality, by Lemma 3.4, gives:

$$\begin{aligned}
1 &= \frac{x_{n-j}\prod_{k=1}^{j}\mathrm{N}_{n-k,j-k}\left(\frac{\mathrm{N}_{n-k+1,1}(x_{n-k+1})}{x_{n-k}}\right)}{x_{n-j+1}^2\prod_{k=1}^{j-1}\left(\mathrm{N}_{n-k,j-k-1}\left(\frac{\mathrm{N}_{n-k+1,1}(x_{n-k+1})}{x_{n-k}}\right)\right)^2} \\
&= \frac{x_{n-j}\frac{\mathrm{N}_{n-j+1,1}(x_{n-j+1})}{x_{n-j}}\prod_{k=1}^{j-1}\mathrm{N}_{n-k,j-k}\left(\frac{\mathrm{N}_{n-k+1,1}(x_{n-k+1})}{x_{n-k}}\right)}{x_{n-j+1}^2\prod_{k=1}^{j-1}\left(\mathrm{N}_{n-k,j-k-1}\left(\frac{\mathrm{N}_{n-k+1,1}(x_{n-k+1})}{x_{n-k}}\right)\right)^2} \\
&= \frac{\mathrm{N}_{n-j+1,1}(x_{n-j+1})\prod_{k=1}^{j-1}\mathrm{N}_{n-j+1,1}\left(\mathrm{N}_{n-k,j-k-1}\left(\frac{\mathrm{N}_{n-k+1,1}(x_{n-k+1})}{x_{n-k}}\right)\right)}{x_{n-j+1}^2\prod_{k=1}^{j-1}\left(\mathrm{N}_{n-k,j-k-1}\left(\frac{\mathrm{N}_{n-k+1,1}(x_{n-k+1})}{x_{n-k}}\right)\right)^2} \\
&= \frac{(x_{n-j+1})^{q^{2^{n-j}}+1}\prod_{k=1}^{j-1}\left(\mathrm{N}_{n-k,j-k-1}\left(\frac{\mathrm{N}_{n-k+1,1}(x_{n-k+1})}{x_{n-k}}\right)\right)^{q^{2^{n-j}}+1}}{x_{n-j+1}^2\prod_{k=1}^{j-1}\left(\mathrm{N}_{n-k,j-k-1}\left(\frac{\mathrm{N}_{n-k+1,1}(x_{n-k+1})}{x_{n-k}}\right)\right)^2} \\
&= x_{n-j+1}^{q^{2^{n-j}}-1}\prod_{k=1}^{j-1}\left(\mathrm{N}_{n-k,j-k-1}\left(\frac{\mathrm{N}_{n-k+1,1}(x_{n-k+1})}{x_{n-k}}\right)\right)^{q^{2^{n-j}}-1}.
\end{aligned}$$

Since the last term is 1, then

$$x_{n-j+1}\prod_{k=1}^{j-1}\mathrm{N}_{n-k,j-k-1}\left(\frac{\mathrm{N}_{n-k+1,1}(x_{n-k+1})}{x_{n-k}}\right)\in\mathbb{F}_{q^{2^{n-j}}},$$

but this is impossible because x_{n-j+1} is a non-square in $\mathbb{F}_{q^{2^{n-j+1}}}$, by Proposition 3.3, but

$$\mathrm{N}_{n-k,j-k-1}\left(\frac{\mathrm{N}_{n-k+1,1}(x_{n-k+1})}{x_{n-k}}\right)=\mathrm{N}_{n-k,j-k-1}\left(\frac{f(x_{n-k},0)}{x_{n-k}}\right)$$

is a square in $\mathbb{F}_{q^{2^{n-j+1}}}$, for each $k<j$, by Condition **(1)** and by multiplicativity of the norm.

This odd common factor ensures, by Lemma 2.1 with $a=q$, $b=n-j$ and $\ell=2$, the existence of a lower bound on the order of x_n, namely $p_j>2^{n-j+1}$, for every $j=1,2,\ldots,n-1$. Hence, the order is bounded below by

$$2^{\frac{n(n+1)}{2}-1}=\prod_{j=1}^{n-1}2^{n-j+1}<\prod_{j=1}^{n-1}p_j.$$

The remaining term $2^{n+\mathrm{ord}_2(q-1)-1}$ follows as in [3, Proposition 2]. By the repetition of the difference of squares formula, we get:

$$\mathrm{ord}_2\left(\frac{q^{2^n}-1}{2}\right)=\sum_{j=0}^{n-1}\mathrm{ord}_2(q^{2^j}+1)+\mathrm{ord}_2(q-1)-1=n+\mathrm{ord}_2(q-1)-1,$$

for all $n\geq 1$. It follows that $2^{n+\mathrm{ord}_2(q-1)-1}$ divides the order of x_n because $x_n^{\frac{q^{2^n}-1}{2}}=-1$ by Proposition 3.3. The proof for δ_n is similar. □

4 Towers in even characteristic

The even analogue of Conditions **(1)** and **(2)** in the odd case for polynomials $f(x,y)=y^3+y+v(x)$, with $v(x)\in\mathbb{F}_2[x]$, is:

(3) There exists an integer $e\geq 0$ such that $f(x_{n-1},0)=x_{n-1}^{2^e}$ for all $n\geq 2$.

This means that we can restrict our study to polynomials in the form $f(x,y)=y^3+y+x^{2^e}$, with $e\geq 0$, and deduce similar results as in the previous section. In Sect. 6, we find some cases where the towers defined by polynomials $f(x_{n-1},x_n)$ are infinite and Galois. This is achieved by finding a suitable initial element $x_1\in\mathbb{F}_{2^6}$. Under these hypotheses we have an analogue of Proposition 3.3.

Proposition 4.1 *Consider an infinite normal tower defined by $f(x_{n-1},x_n)=x_n^3+x_n+x_{n-1}^{2^e}$ for a certain $e\geq 0$, for all $n>1$. Let p be a prime divisor of $|\mathbb{F}^*_{2^{2\cdot 3^{n-1}}}|$, for a suitable $n>1$, and assume that x_{n-1} is not a p-th power in the multiplicative group $\mathbb{F}^*_{2^{2\cdot 3^{n-1}}}$. Then x_j is not a p-th power in the multiplicative group $\mathbb{F}^*_{2^{2\cdot 3^j}}$, for $j\geq n$.*

Proof By assumption $f(x_{n-1},y)$ is irreducible, so $x_n\notin\mathbb{F}_{2^{2\cdot 3^{n-1}}}$ and $f(x_{n-1},y)$ is the minimum polynomial of x_n. We need to check that $x_n^{(4^{3^n}-1)/p}\neq 1$. As in the proof of Proposition 3.3, we obtain:

$$x_n^{(4^{3^n}-1)/p} = (x_n^{4^{2\cdot 3^{n-1}}+4^{3^{n-1}}+1})^{(4^{3^{n-1}}-1)/p}$$
$$= \mathrm{N}(x_n)^{(4^{3^{n-1}}-1)/p} = f(x_{n-1},0)^{(4^{3^{n-1}}-1)/p},$$

where $\mathrm{N}(x_n) = x_n^{4^{2\cdot 3^{n-1}}+4^{3^{n-1}}+1} = f(x_{n-1},0)$ is the norm of x_n over $\mathbb{F}_{2^{2\cdot 3^{n-1}}}$. The last term is not equal to 1 because x_{n-1} is not a p-th power in $\mathbb{F}_{2^{2\cdot 3^{n-1}}}$, hence, by Condition **(3)**, $f(x_{n-1},0)$ is not a p-th power as well. □

The analogue of Lemma 3.4 in even characteristic is the following:

Lemma 4.2 *Let $e \geq 0$, $n \geq 2$ and $j < n$ be positive integers, then*

$$\frac{\mathrm{N}_{n,j}(x_n)}{x_{n-j}^{2^{ej}}} = \prod_{k=1}^{j} \mathrm{N}_{n-k,j-k}\left(\frac{\mathrm{N}_{n-k+1,1}(x_{n-k+1})}{x_{n-k}^{2^e}}\right)^{2^{e(k-1)}}.$$

*In particular, if the tower defined by $f(x_{n-1},x_n)$ satisfies Condition **(3)** for a certain $e \geq 0$, then $\mathrm{N}_{n,j}(x_n) = x_{n-j}^{2^{ej}}$.*

Proof By induction on j. For $j = 1$ the result is trivial. Let $j \geq 2$ and assume the result holds for $j-1$, then:

$$\frac{\mathrm{N}_{n,j}(x_n)}{x_{n-j}^{2^{ej}}} = \frac{x_n^{(4^{2\cdot 3^{n-1}}+4^{3^{n-1}}+1)\prod_{i=2}^{j}(4^{2\cdot 3^{n-i}}+4^{3^{n-i}}+1)}}{x_{n-j}^{2^{ej}}}$$
$$= \left(\frac{x_n^{4^{2\cdot 3^{n-1}}+4^{3^{n-1}}+1}}{x_{n-1}^{2^e}}\right)^{\prod_{i=2}^{j}(4^{2\cdot 3^{n-i}}+4^{3^{n-i}}+1)} \left(\frac{x_{n-1}^{\prod_{i=2}^{j}(4^{2\cdot 3^{n-i}}+4^{3^{n-i}}+1)}}{x_{n-j}^{2^{e(j-1)}}}\right)^{2^e}$$
$$= \left(\frac{\mathrm{N}_{n,1}(x_n)}{x_{n-1}^{2^e}}\right)^{\prod_{i=2}^{j}(4^{2\cdot 3^{n-i}}+4^{3^{n-i}}+1)} \left(\frac{\mathrm{N}_{n-1,j-1}(x_{n-1})}{x_{n-j}^{2^{e(j-1)}}}\right)^{2^e}$$
$$= \mathrm{N}_{n-1,j-1}\left(\frac{\mathrm{N}_{n,1}(x_n)}{x_{n-1}^{2^e}}\right) \prod_{k=1}^{j-1} \mathrm{N}_{n-k-1,j-k-1}\left(\frac{\mathrm{N}_{n-k,1}(x_{n-k})}{x_{n-k-1}^{2^e}}\right)^{2^{ek}}$$
$$= \mathrm{N}_{n-1,j-1}\left(\frac{\mathrm{N}_{n,1}(x_n)}{x_{n-1}^{2^e}}\right) \prod_{k=2}^{j} \mathrm{N}_{n-k,j-k}\left(\frac{\mathrm{N}_{n-k+1,1}(x_{n-k+1})}{x_{n-k}^{2^e}}\right)^{2^{e(k-1)}}.$$

The remaining part of the proof follows by Condition **(3)**. □

Corollary 4.3 *Consider an infinite normal tower defined by $f(x_{n-1},x_n) = x_n^3 + x_n + x_{n-1}^{2^e}$, for a certain $e \geq 0$, for all $n > 1$. If x_1 is not a cube in $\mathbb{F}_{2^6}$, then $x_n^3 \notin \mathbb{F}_{2^{2\cdot 3^{n-1}}}$ for all $n \geq 2$ and the order of x_n in the tower defined by $f(x_{n-1},x_n)$ is greater than*

$$3^{\frac{1}{2}(n^2+3n)-1}.$$

Proof The proof is similar to the proofs of Corollary 3.5 and [3, Proposition 4]. We know that $x_n \notin \mathbb{F}_{2^{2\cdot 3^{n-1}}}$ by Proposition 4.1, so $x_n^3 = x_n + v(x_{n-1}) \notin \mathbb{F}_{2^{2\cdot 3^{n-1}}}$. It follows that $\left(x_n^3\right)^{2^e} \notin$

$\mathbb{F}_{2^{2\cdot 3^{n-1}}}$. In order to show that the order of x_n has a common factor with $\frac{1}{3}(4^{2\cdot 3^{n-j}}+4^{3^{n-j}}+1)$, we show that $x_n^{\frac{3(4^{3^n}-1)}{4^{2\cdot 3^{n-j}}+4^{3^{n-j}}+1}} \neq 1$, for $j = 1, 2, \ldots, n-1$. We have:

$$x_n^{\frac{3(4^{3^n}-1)}{4^{2\cdot 3^{n-j}}+4^{3^{n-j}}+1}} = x_n^{\frac{4^{3^n}-1}{4^{3^{n-j}}-1}\cdot\frac{3(4^{3^{n-j}}-1)}{4^{2\cdot 3^{n-j}}+4^{3^{n-j}}+1}} = x_n^{\frac{3(4^{3^n}-1)(4^{3^{n-j}}-1)}{4^{3^{n-j+1}}-1}}$$
$$= x_n^{3(4^{3^{n-j}}-1)\prod_{i=1}^{j-1}(4^{2\cdot 3^{n-i}}+4^{3^{n-i}}+1)} = \mathrm{N}_{n,j-1}(x_n)^{3(4^{3^{n-j}}-1)}.$$

By Lemma 4.2 we have that $\mathrm{N}_{n,j}(x_n) = x_{n-j}^{2^{ej}}$, for $j = 1, 2, \ldots, n-1$. But $\left(x_{n-j+1}^{2^{e(j-1)}}\right)^3 \notin \mathbb{F}_{2^{2\cdot 3^{n-j}}}$ for all $j \geq 1$. It follows that $\mathrm{N}_{n,j-1}(x_n)^{3(4^{3^{n-j}}-1)}$ cannot be equal to 1. This ensures, by Lemma 2.1 with $a = 4$, $b = n-j$ and $\ell = 3$, the existence of a lower bound on the order of x_n, namely $p_j > 3^{n-j+1}$, for every $j = 1, 2, \ldots, n-1$. Hence, we get a lower bound for the order of x_n, which is

$$3^{\frac{n(n+1)}{2}-1} = \prod_{j=1}^{n-1} 3^{n-j+1} < \prod_{j=1}^{n-1} p_j.$$

The remaining term 3^n follows by the computation of the power of 3 dividing the order of x_n. By the repetition of the difference of cubes formula, we have:

$$\mathrm{ord}_3\left(\frac{4^{3^n}-1}{3}\right) = \sum_{j=0}^{n-1} \mathrm{ord}_3(4^{2\cdot 3^j}+4^{3^j}+1) + \mathrm{ord}_3(4-1) - 1 = n,$$

for all $n \geq 1$. This term divides the order of x_n, since $x_n^{\frac{4^{3^n}-1}{3}} \neq 1$, by Proposition 4.1. □

5 Examples of good towers in odd characteristic

In this section we find high order elements in $\mathbb{F}_{q^{2^n}}$, for odd q, using five good towers. In this section, we denote by ε the element 4^{-1} inside $\mathbb{F}_q$. We consider the polynomials $f_i(x_{n-1}, x_n) := x_n^2 + x_n - v_i(x_{n-1})$, for $i \in \{1, 2, \ldots, 5\}$, where $v_i(x)$ is a polynomial chosen as follows:

(1) $v_1(x) := \varepsilon x$;
(2) $v_2(x) := 4x(x+3\varepsilon)^2$;
(3) $v_3(x) := 2\varepsilon x$;
(4) $v_4(x) := 8x(2x+3\varepsilon)^2$;
(5) $v_5(x) := 8x(x+3\varepsilon)^2$.

Remark 5.1 Condition **(1)** holds for all the previous polynomials and the relation between two consecutive discriminants is given respectively by:

$$g_1(\delta_{n-1}, \delta_n) = \delta_n^2 - \delta_n - \varepsilon\delta_{n-1} + \varepsilon;$$
$$g_2(\delta_{n-1}, \delta_n) = \delta_n^2 - \delta_n - 4\delta_{n-1}^3 + 6\delta_{n-1}^2 - 9\varepsilon\delta_{n-1} + \varepsilon;$$
$$g_3(\delta_{n-1}, \delta_n) = \delta_n^2 - \delta_{n-1};$$
$$g_4(\delta_{n-1}, \delta_n) = \delta_n^2 + 48\delta_{n-1}\delta_n - 256\delta_{n-1}^3 + 288\delta_{n-1}^2 - 81\delta_{n-1};$$
$$g_5(\delta_{n-1}, \delta_n) = \delta_n^2 - 16\delta_{n-1}^3 + 24\delta_{n-1}^2 - 9\delta_{n-1}.$$

The first two towers satisfy Condition **(2)**. In fact

$$g_1(\delta_{n-1}, 0) = -\varepsilon(1 + 4x_{n-1}) + \varepsilon = -x_{n-1};$$
$$g_2(\delta_{n-1}, 0) = x_{n-1}(x_{n-1} + 3\varepsilon)^2(x_{n-1}^3 + 6x_{n-1}^2 + 9\varepsilon^2 x_{n-1} + 3\varepsilon^3)^2.$$

Similarly the last three towers satisfy Condition **(2')**. In fact,

$$g_3(\delta_n, 0) = -\delta_n;$$
$$g_4(\delta_n, 0) = -256\delta_n(\delta_n - 9\varepsilon^2)^2;$$
$$g_5(\delta_n, 0) = -16\delta_n(\delta_n - 3\varepsilon)^2.$$

Hence, Proposition 3.3 applies to $f_i(x_{n-1}, x_n)$, for $i \in \{1, 2, \ldots, 5\}$ once we have some starting points.

The next two lemmas ensures the existence of a non-square x_1 such that δ_1 is a non-square in $\mathbb{F}_{q^2}$ as well. This would be the corresponding analogue of [3, Lemma 3], but here we also need that *both* x_1 and δ_1 must be non-squares. This requires more effort, especially for the last tower $f_5(x_{n-1}, x_n)$ below, but, as a balance, this gives a lower bound for the order of x_n, also.

The present proof relies mainly on elementary combinatorial arguments.

Lemma 5.2 *Let $c \in \mathbb{F}_q$ be a non-zero element. There is at least a non-square $x_1 \in \mathbb{F}_{q^2}$ such that $x_1 + c$ is a non-square as well.*

Proof Consider the action ρ of $\mathbb{F}_q$ on $\mathbb{F}_{q^2}$ as an additive group, namely we have $\rho_g(x) = x+g$, for $g \in \mathbb{F}_q$ and $x \in \mathbb{F}_{q^2}$. Then, $\mathbb{F}_{q^2}$ is partitioned into q orbits. There are exactly $\frac{1}{2}(q^2 + 1)$ squares in $\mathbb{F}_{q^2}$. Among these, there are all the elements of the orbit $\mathbb{F}_q$. It follows that there are exactly $\frac{1}{2}(q^2 - 2q + 1)$ square elements in $q - 1$ orbits. Hence, there is at least one orbit with at most $\frac{1}{2}(q - 1)$ square elements and at least $\frac{1}{2}(q + 1)$ non-square elements. We denote this orbit by S. It follows that there are at least two consecutive non-squares in S under the repeated action of ρ_c, namely a and $\rho_c(a) = a + c$. The lemma follows by choosing $x_1 = a$. □

Example 5.3 Consider, $q = 3$ and $c = 1$. Denote by z a generator of $\mathbb{F}_{3^2}^*$ satisfying $z^2 = z+1$. There are exactly 5 squares in $\mathbb{F}_{3^2}^*$, but 3 of them are in the same orbit $\mathbb{F}_3$. The remaining ones are $z^2 = z + 1$ and $z^6 = 2z + 2$. One can check that they belong to the orbits

$$S_1 = (z;\ z + 1 = z^2;\ z + 2 = z^7) \text{ and } S_2 = (2z = z^5;\ 2z + 1 = z^3;\ 2z + 2 = z^6).$$

As x_1 we can choose the element $2z$ or $z+2$. They are both roots of the polynomial $x^2 = 2x+1$, so we use this polynomial for $q = 3$ in Sect. 7.

In order to show the existence of a suitable initial element x_1 for the tower defined by $f_5(x_{n-1}, x_n)$ we prove the following lemma.

Lemma 5.4 *Let q be an odd prime and let $p(x)$ be a cubic polynomial in $\mathbb{F}_q[x]$ without multiple roots, such that $p(0) \neq 0$. Then:*

(i) *The curve $C_1 : y^2 = p(x)$ has at most $q^2 + 2q$ affine $\mathbb{F}_{q^2}$-rational points and the curve $C_2 : y^2 = p(x^2)$ has at least $q^2 - 4q - 1$ affine $\mathbb{F}_{q^2}$-rational points.*

(ii) *If $q \geq 11$, then there is at least a non-square $x_1 \in \mathbb{F}_{q^2}$ such that $p(x_1)$ is a non-square in $\mathbb{F}_{q^2}$ as well.*

Proof (i) We note that $p(x^2)$ is square-free since $p(x)$ is square-free and $p(0) \neq 0$ by hypothesis. The first statement follows by Weil bound $|N - (q^2+1)| \leq 2gq$, for every smooth projective curve of genus g with N points over $\mathbb{F}_{q^2}$, since C_1 is an elliptic curve and C_2 has genus at most 2, see [23, Propositions 6.1.3 (a) and 6.2.3 (b)]. It is well known that the number of points at infinity is 1 in an elliptic curve and it is at most 2 in a genus 2 curve. Hence, (i) is proved.

(ii) By contradiction we assume that $p(\alpha)$ is a square for all non-square $\alpha \in \mathbb{F}_{q^2}$. Let $\beta \in \mathbb{F}_{q^2}$ be a square root of $p(\alpha)$. Since there are exactly $\frac{1}{2}(q^2-1)$ non-squares in $\mathbb{F}_{q^2}$ and $\beta \neq 0$, except at most for 3 choices of α, then the pairs (α, β) and $(\alpha, -\beta)$ produce at least q^2-4 distinct points of C_1. We show that such points are too many. We estimate the number of squares α such that $p(\alpha)$ is also a square in $\mathbb{F}_{q^2}$. Each point (t, y) in C_2 corresponds to the point (x, y) in C_1 with $x = t^2$. This correspondence is not $1-1$ because, when $t \neq 0$, the point $(-t, y)$ determines the same point in C_1. Let N be the number of affine $\mathbb{F}_{q^2}$-rational points of C_2, then C_1 must have more than $\frac{N}{2}$ affine $\mathbb{F}_{q^2}$-rational points (x, y) with x being a square in $\mathbb{F}_{q^2}$. By Part (i), we have $N \geq q^2 - 4q - 1$. Counting the points of C_1 we get, again by Part (i), $q^2 - 4 + \frac{1}{2}(q^2 - 4q - 1) \leq q^2 + 2q$ which yields, after a straightforward computation, $q^2 - 8q - 9 \leq 0$. It follows that $q \leq 9$, which is contrary to our assumption on q. Hence, there is at least one non-square $x_1 \in \mathbb{F}_{q^2}$ such that $p(x_1)$ is a non-square too. □

Remark 5.5 The condition $q \geq 11$ in the previous lemma is not necessary and here we show that Part (ii) also holds for $q = 3, 5, 7$ for the polynomial $p(x) = 1 + 4v_5(x)$, which is not square-free for $q = 3$. This is useful in the proof of Corollary 5.6. We are interested in this polynomial since the discriminant δ_1 of f_5 above is $p(x_1)$ and so we need to be able to choose an element $x_1 \in \mathbb{F}_{q^2}$ such that both x_1 and δ_1 are non-squares.

For $q = 7$, we choose x_1 in $\mathbb{F}_{7^2}$ as a root of $x^2 + 5x + 5$. Then a straightforward computation shows that both x_1 and $p(x_1) = 4x_1^3 - x_1^2 + 4x_1 + 1$ are non-squares in $\mathbb{F}_{7^2}$ since $x_1^{24} = p(x_1)^{24} = -1$.

Similarly, for $q = 5$, if we choose x_1 being a root of the polynomial $x^2 + 4x + 2$, in $\mathbb{F}_{5^2}$, then $p(x_1) = 2x_1^3 + 3x_1^2 + 3x_1 + 1$ and $x_1^{12} = p(x_1)^{12} = -1$. Hence, both x_1 and $p(x_1)$ are non-square in $\mathbb{F}_{5^2}$.

Finally, for $q = 3$, if we choose x_1 as a root of the polynomial $x^2 + 2x + 2$, as in Example 5.3 above, then $p(x_1) = 1 - x_1^3$ and $x_1^4 = p(x_1)^4 = -1$, hence x_1 and $p(x_1)$ are non-squares in $\mathbb{F}_{3^2}$ as well.

We use the aforementioned examples in Sect. 7.

The following corollary ensures the existence of towers defined by $f_i(x_{n-1}, x_n)$ generating high order elements for $i \in \{1, 2, \ldots, 5\}$.

Corollary 5.6 *The polynomials $f_i(x_{n-1}, x_n)$, for $i \in \{1, 2, \ldots, 5\}$, define infinite towers of fields. Moreover, for a suitable choice of x_1, the order of x_n in $\mathbb{F}_{q^{2^n}}$ is greater than $2^{\frac{1}{2}(n^2+3n)+\mathrm{ord}_2(q-1)-2}$. The same bound holds for δ_n in the towers defined by $f_1(x_{n-1}, x_n)$ and $f_2(x_{n-1}, x_n)$ and, when $q > 3$, for δ_n in the tower defined by $f_4(x_{n-1}, x_n)$.*

Proof First, for each tower considered, we show the existence of a non-square starting point x_1 such that the discriminant δ_1 is a non-square as well. A straightforward computation shows that $\delta_1 = x_1 + 1$ for f_1 and that $\delta_1 = 16x_1^3 + 24x_1^2 + 9x_1 + 1 = (x_1+1)(4x_1+1)^2$ for f_2. Hence, for the first two polynomials, it is enough to choose x_1 as in Lemma 5.2 with $c = 1$. A straightforward computation also shows that $\delta_1 = 2\left(x_1 + \frac{1}{2}\right)$ for f_3 and that $\delta_1 = 128\left(x_1 + \frac{1}{2}\right)(x_1 + 2\varepsilon^2)^2$ for f_4. Hence, for the third and the fourth polynomial, it is

enough to choose x_1 as in Lemma 5.2 with $c = \frac{1}{2}$. For the last tower, by Remark 5.5, we can take x_1 as in Remark 5.5 for $q \leq 7$ and we can take x_1 as in Lemma 5.4 for $q \geq 11$.

Now, we know, by Remark 5.1, that all the considered towers satisfy Conditions **(1)** and **(2)**, or Conditions **(1)** and **(2')**. Therefore, the result for x_n follows by Corollary 3.5. For δ_n we have to check that $\delta_n^2 \notin \mathbb{F}_{q^{2^{n-1}}}$ for $n > 1$, in the tower defined by $f_1(x_{n-1}, x_n)$ and $f_2(x_{n-1}, x_n)$, for $q \geq 3$, and by $f_4(x_{n-1}, x_n)$ for $q > 3$. But this follows by the expression of $g_1(\delta_{n-1}, \delta_n)$, $g_2(\delta_{n-1}, \delta_n)$ and $g_4(\delta_{n-1}, \delta_n)$ in Remark 5.1. □

As in [3], the bound of the previous corollary does not seem to be sharp, in fact in many cases we were able to construct generators of the multiplicative group $\mathbb{F}^*_{q^{2^n}}$, whose order is $q^{2^n} - 1$, which is much higher than $2^{\frac{n^2}{2}}$. The interested reader can compare the tables in Sect. 7 with the experimental results of [3].

Remark 5.7 The bound in the Corollary 5.6 above, does not hold for δ_n in the tower defined by $f_3(x_{n-1}, x_n)$ and $f_5(x_{n-1}, x_n)$. In fact, $\delta_n^2 \in \mathbb{F}_{q^{2^{n-1}}}$, for all $n > 1$, which can be verified easily. The interested reader can see the numerical results in Sect. 7. A careful comparison between the results for these two polynomials reveals an interesting difference when $q > 3$. In fact, the order of the discriminant δ_n turns out to grow very slowly using f_3 in comparison to f_5. The reason is that in the former tower the discriminants satisfy the relation $g_3(\delta_{n-1}, \delta_n) = \delta_n^2 - \delta_{n-1} = 0$, which yields $\delta_n^{2^{n-1}} = \delta_{n-1}^{2^{n-2}} = \ldots = \delta_1 \in \mathbb{F}_{q^2}$. This implies that we can estimate the order of δ_n, which turns out to be lower than $2^{n-1+\mathrm{ord}_2(q^2-1)}$. In the tower defined by $f_5(x_{n-1}, x_n)$, we have that $\delta_n^{2^j} \in \mathbb{F}_{q^{2^{n-j}}}$ holds for $j = 1$, but not for all $j < n$. This explains why the order grows comparatively faster when $q > 3$. In the case $q = 3$ the polynomial equation $g_5(\delta_{n-1}, \delta_n) = \delta_n^2 - \delta_{n-1}^3 = 0$ gives $\delta_n^{2^{n-1}} = \delta_1^{3^{n-1}} \in \mathbb{F}_{3^2}$. This explains why the numerical results for the order of δ_n are similar to the tower defined by $f_3(x_{n-1}, x_n)$.

Remark 5.8 From the relation $g_4(\delta_{n-1}, \delta_n) = 0$ between δ_n and δ_{n-1} in the fourth tower, for $q = 3$, we get $g_4(\delta_{n-1}, \delta_n) = \delta_n^2 - \delta_{n-1}^3 = 0$. Hence, we observe that the proof of last corollary does not work when $q = 3$. We also point out that $f_4(x_{n-1}, x_n) = f_5(x_{n-1}, x_n)$ when $q = 3$. This fact explains why the numerical results in the corresponding tables in Sect. 7 have the same values in the first two columns.

Of course could exist other towers satisfying analogues of Conditions **(1)** and **(2)** or Conditions **(1)** and **(2')** above. An extensive computer search could show the non-existence of similar examples of the form $f(x_{n-1}, x_n) = x_n^2 + x_n + v(x_{n-1})$, with $\deg(v(x)) \leq 3$, at least for small prime fields.

6 Examples of good towers in even characteristic

In this section we list polynomials generating high order elements, as in Sect. 5. We have to adapt some proofs in even characteristic, since we have to prove that our cubic polynomials $f(x_{n-1}, y)$ are irreducible in $\mathbb{F}_{2^{2\cdot 3^{n-1}}}[y]$. Let e be a non-negative integer. In the following results, we prove that $f(x_{n-1}, x_n) := x_n^3 + x_n + x_{n-1}^{2^e}$ actually defines an infinite normal separable tower.

Lemma 6.1 *Let e and n be integers such that $e \geq 0$ and $n \geq 2$, and let $x_{n-1} \in \mathbb{F}_{2^{2\cdot 3^{n-1}}}$. Assume that $u_n^3 \in \mathbb{F}_{2^{2\cdot 3^{n-1}}}$ is a root of the quadratic polynomial $y^2 + x_{n-1}^{2^e} y + 1$ and that*

$x_n := u_n + u_n^{-1} \notin \mathbb{F}_{2^{2\cdot 3^{n-1}}}$ is a root of the cubic polynomial $y^3 + y + x_{n-1}^{2^e}$. Let $u_{n+1} \in \mathbb{F}_{2^{2\cdot 3^{n+1}}}$ be a third root of $u_n^{2^e}$. Then:

(i) $u_{n+1} \notin \mathbb{F}_{2^{2\cdot 3^n}}$;
(ii) u_{n+1}^3 *and* u_{n+1}^{-3} *are the roots of* $y^2 + x_n^{2^e} y + 1$;
(iii) $x_{n+1} := u_{n+1} + u_{n+1}^{-1}$ *is a root of* $y^3 + y + x_n^{2^e}$ *and* $x_{n+1} \notin \mathbb{F}_{2^{2\cdot 3^n}}$.

Proof Part (i) follows since $u_{n+1}^9 = (u_{n+1}^3)^3 = (u_n^{2^e})^3 = (u_n^3)^{2^e}$ belongs to $\mathbb{F}_{2^{2\cdot 3^{n-1}}}$ and since $\mathbb{F}_{2^{2\cdot 3^n}}$ does not contain any 9-th root of non-cubic elements in $\mathbb{F}_{2^{2\cdot 3^{n-1}}}$ because 9 does not divide

$$\frac{|\mathbb{F}^*_{2^{2\cdot 3^n}}|}{|\mathbb{F}^*_{2^{2\cdot 3^{n-1}}}|} = 1 + 4^{3^{n-1}} + 4^{2\cdot 3^{n-1}},$$

for all $n \geq 1$.

Part (ii) follows by straightforward verification.

The last part follows by Lemma 2.3 and by Parts (i) and (ii). □

Part (iii) in the previous lemma shows by induction that if $f(x_1, y) = y^3 + y + x_1^{2^e}$ is irreducible in $\mathbb{F}_{2^6}[y]$, then $f(x_n, y) = y^3 + y + x_n^{2^e}$ is also irreducible in $\mathbb{F}_{2^{2\cdot 3^n}}[y]$ for all $n > 1$. It follows that the Galois group of the splitting field of $f(x_n, y)$ is the cyclic group $\mathbb{Z}/3\mathbb{Z}$.

We summarize the results above in the following corollary, which provides a good initial choice for x_1, resulting in $f(x_{n-1}, x_n)$ to be a normal separable recursive tower.

Corollary 6.2 *Let $e \geq 0$ be an integer. Then $f(x_{n-1}, x_n) := x_n^3 + x_n + x_{n-1}^{2^e}$ defines an infinite tower of fields and, for a suitable choice of x_1, the order of $x_n \in \mathbb{F}_{2^{2\cdot 3^n}}$, for $n \geq 2$, is greater than $3^{\frac{1}{2}(n^2+3n)-1}$.*

Proof Let x_1 be one of the roots of $h(x) := x^6 + x^5 + x^3 + x^2 + 1$. The reader can verify that each root of this polynomial is not a cube in $\mathbb{F}_{2^{18}}$. By Lemma 6.1, Part (iii), the fact that the roots of $y^2 + x_1^{2^e} y + 1$ are not cubes implies that $f(x_n, y) = y^3 + y + x_n^{2^e}$ is irreducible for each $n \geq 1$. Hence $f(x_{n-1}, x_n)$ defines an infinite tower of fields which is Galois because they are extensions of finite fields. Since f clearly satisfies Condition **(3)** of Sect. 4, so the proof follows by Corollary 4.3. □

In Sect. 7 we collated the numerical results for $f_6(x_{n-1}, x_n) := x_n^3 + x_n + x_{n-1}$ and $f_7(x_{n-1}, x_n) := x_n^3 + x_n + x_{n-1}^2$ corresponding to $e = 0$ and $e = 1$, respectively. The initial element x_1 is one of the roots of $h(x) := x^6 + x^5 + x^3 + x^2 + 1$ as explained in the proof of Corollary 6.2.

7 Numerical results

In this section, we have collated the multiplicative orders $o(x_n)$ (and $o(\delta_n)$ for q odd) for small n in the towers defined by $f_i(x_{n-1}, x_n)$, for $i = 1, 2, \ldots, 7$. In most of the cases we obtained generators of the multiplicative groups $\mathbb{F}^*_{q^{2^n}}$ and $\mathbb{F}^*_{2^{2\cdot 3^n}}$. We tabulated base 2 logarithm of the orders as they grow exponentially. In particular, in Tables 1, 2, 3, 4, 5 we list the numerical results in odd characteristic for $f_1, \ldots, f_5$. The interested reader can also find the lower and upper bounds for $o(x_n)$ and $o(\delta_n)$ listed in Tables 6 and 7, for odd and even characteristic

Table 1 Results for $f_1(x_{n-1}, x_n)$ for odd $q \leq 11$

q	3	3	5	5	7	7	11	11
$x_1^2 =$	$2x_1 + 1$	$2x_1 + 1$	$3x_1 + 2$	$3x_1 + 2$	$x_1 + 4$	$x_1 + 4$	$4x_1 + 9$	$4x_1 + 9$
n	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$
1	3.0	3.0	4.6	3.0	5.6	5.6	6.9	5.3
2	6.3	6.3	9.3	9.3	11.2	11.2	13.8	13.8
3	12.7	12.7	18.6	18.6	22.5	22.5	27.7	27.7
4	25.4	25.4	37.2	37.2	44.9	44.9	55.4	55.4
5	50.7	50.7	74.3	74.3	89.8	89.8	110.7	110.7
6	101.4	101.4	148.6	148.6	179.7	179.7	221.4	221.4
7	202.9	202.9	297.2	297.2	359.3	359.3	442.8	442.8
8	405.8	405.8	594.4	594.4	718.7	718.7	883.3	885.6
9	811.5	811.5	1188.8	1188.8	1437.4	1437.4	1771.2	1771.2

Table 2 Results for $f_2(x_{n-1}, x_n)$ for odd $q \leq 11$

q	3	3	5	5	7	7	11	11
$x_1^2 =$	$2x_1 + 1$	$2x_1 + 1$	$3x_1 + 2$	$3x_1 + 2$	$x_1 + 4$	$x_1 + 4$	$4x_1 + 9$	$4x_1 + 9$
n	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$
1	3.0	3.0	4.6	4.6	5.6	5.6	6.9	4.6
2	6.3	6.3	9.3	9.3	11.2	11.2	13.8	12.3
3	12.7	12.7	18.6	18.6	20.9	22.5	26.1	27.7
4	25.4	25.4	37.2	37.2	44.9	44.9	55.4	48.9
5	50.7	50.7	74.3	74.3	88.3	89.8	106.6	110.7
6	101.4	101.4	148.6	148.6	179.7	179.7	221.4	219.8
7	202.9	202.9	297.2	297.2	357.8	359.3	441.2	442.8
8	405.8	405.8	594.4	594.4	718.7	718.7	885.6	879.2
9	811.5	811.5	1188.8	1188.8	1435.8	1437.4	1767.1	1771.2

Table 3 Results for $f_3(x_{n-1}, x_n)$ for odd $q \leq 11$

q	3	3	5	5	7	7	11	11
$x_1^2 =$	$x_1 + 1$	$x_1 + 1$	$2x_1 + 2$	$2x_1 + 2$	$3x_1 + 2$	$3x_1 + 2$	$4x_1 + 9$	$4x_1 + 9$
n	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$
1	3.0	3.0	4.6	4.6	5.6	4.0	6.9	5.3
2	6.3	4.0	9.3	5.6	11.2	5.0	13.8	6.3
3	12.7	5.0	18.6	6.6	22.5	6.0	25.4	7.3
4	25.4	6.0	37.2	7.6	44.9	7.0	51.3	8.3
5	50.7	7.0	74.3	8.6	89.8	8.0	106.6	9.3
6	101.4	8.0	148.6	9.6	179.7	9.0	217.3	10.3
7	202.9	9.0	297.2	10.6	359.3	10.0	436.4	11.3
8	405.8	10.0	594.4	11.6	718.7	11.0	881.5	12.3
9	811.5	11.0	1188.8	12.6	1437.4	12.0	1767.1	13.3

Table 4 Results for $f_4(x_{n-1}, x_n)$ for odd $q \leq 11$

q	3	3	5	5	7	7	11	11
$x_1^2 =$	$x_1 + 1$	$x_1 + 1$	$4x_1 + 3$	$4x_1 + 3$	$2x_1 + 4$	$2x_1 + 4$	$7x_1 + 4$	$7x_1 + 4$
n	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$
1	3.0	3.0	4.6	4.6	5.6	5.6	6.9	4.6
2	6.3	4.0	9.3	7.7	11.2	11.2	13.8	13.8
3	12.7	5.0	17.0	17.0	22.5	20.9	27.7	27.7
4	25.4	6.0	35.6	37.2	41.0	43.3	55.4	55.4
5	50.7	7.0	72.7	72.7	89.8	89.8	110.7	109.1
6	101.4	8.0	147.0	148.6	177.3	179.7	221.4	219.8
7	202.9	9.0	295.6	295.6	359.3	357.8	442.8	441.2
8	405.8	10.0	592.8	594.4	717.1	717.1	885.6	884.0
9	811.5	11.0	1187.2	1188.8	1435.8	1435.8	1769.6	1771.2

Table 5 Results for $f_5(x_{n-1}, x_n)$ for odd $q \leq 11$

q	3	3	5	5	7	7	11	11
$x_1^2 =$	$x_1 + 1$	$x_1 + 1$	$x_1 + 3$	$x_1 + 3$	$2x_1 + 2$	$2x_1 + 2$	$4x_1 + 4$	$4x_1 + 4$
n	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$
1	3.0	3.0	4.6	4.6	5.6	5.6	6.9	3.0
2	6.3	4.0	9.3	5.6	8.9	5.0	13.8	5.6
3	12.7	5.0	18.6	8.7	22.5	12.2	27.7	14.8
4	25.4	6.0	35.6	18.0	42.6	23.5	55.4	28.7
5	50.7	7.0	72.7	38.2	89.8	45.9	110.7	56.4
6	101.4	8.0	147.0	73.7	179.7	89.3	221.4	110.1
7	202.9	9.0	295.6	149.6	359.3	179.1	442.8	220.8
8	405.8	10.0	592.8	296.6	718.7	358.8	883.3	442.8
9	811.5	11.0	1187.2	595.4	1437.4	718.1	1771.2	885.0

Table 6 Upper bounds for odd $q \leq 11$ and lower bound

q	3	5	7	11	Lower bound
n	$\log_2(q^{2^n}-1)$	$\log_2(q^{2^n}-1)$	$\log_2(q^{2^n}-1)$	$\log_2(q^{2^n}-1)$	$\log_2(2^{(n^2+3n)/2})$
1	3.0	4.6	5.6	6.9	2.0
2	6.3	9.3	11.2	13.8	5.0
3	12.7	18.6	22.5	27.7	9.0
4	25.4	37.2	44.9	55.4	14.0
5	50.7	74.3	89.8	110.7	20.0
6	101.4	148.6	179.7	221.4	27.0
7	202.9	297.2	359.3	442.8	35.0
8	405.8	594.4	718.7	885.6	44.0
9	811.5	1188.8	1437.4	1771.2	54.0

Table 7 Results for $f_6(x_{n-1}, x_n)$ and $f_7(x_{n-1}, x_n)$ for $q = 2$ and related lower and upper bounds

$f(x_{n-1}, x_n) =$	$f_6(x_{n-1}, x_n)$	$f_7(x_{n-1}, x_n)$	Lower bound	Upper bound
n	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(x_n))$	$\log_2(3^{n(n+3)/2})$	$\log_2(4^{3^n}-1)$
1	6.0	6.0	3.2	6.0
2	18.0	18.0	7.9	18.0
3	54.0	54.0	14.3	54.0
4	162.0	162.0	22.2	162.0
5	486.0	486.0	31.7	486.0
6	1458.0	1458.0	42.8	1458.0

respectively. Finally, in Table 8, we compare one of our examples in characteristic 3, with the constructions of [3] and [7].

MAGMA [2] computational algebra system was used for the experiments and a sample MAGMA code and output, for $q = 11$ can be found in [9]. The performance of the code depends on the efficiency of the *root* finding algorithm that one uses. We have used the standard function of MAGMA [2] for finding roots.

8 Conclusion and future work

In [3], the choice of polynomials for the recursive process to generate high order elements in finite field extensions, was limited to the equations of the modular curve towers in [10]. In this work, we attempted to generalize the choice of the polynomials. This provides us with more examples with similar properties. A central theme of this research work is to find a recipe to choose polynomials to use the recursive process. There might be other equations which could help to attain similar bounds. It would be interesting to understand in general which equations are good and which ones are not. We also point out that there could be other explicit towers satisfying similar properties. We were in fact attracted previously by other interesting examples with $v(x)$ being a polynomial of higher degree over $\mathbb{F}_q$, which turned out to give high order elements, although the proof seems to be much harder. A possible relation

Table 8 Comparative analysis

n	$\log_2(\lvert\mathbb{F}^*_{32^n}\rvert)$	Our Model	Burkhart's Model [3]	Cohen's Model [7]	McNay's Model [14]
1	3.0	3.0	3.0	3.0	3.0
2	6.3	6.3	5.3	4.0	4.3
3	12.7	12.7	10.7	5.0	7.4
4	25.4	25.4	22.4	6.0	13.7
5	50.7	50.7	46.8	7.0	26.4
6	101.4	101.4	96.5	8.0	51.7
7	202.9	202.9	197.0	9.0	102.4
8	405.8	405.8	399.0	10.0	203.9
9	811.5	811.5	804.0	11.0	406.8

linking together these equations could allow to obtain other families of towers with good parameters. We also expect to improve our results by extending the construction of Sect. 3 to higher degree polynomials and extending the construction of Sect. 4 to odd characteristic $q > 3$.

Another question that would be interesting to explore is the possible relation with some geometric construction. In fact, since the tower in [3] is obtained from the equation of a modular curve, it is a natural question to ask whether our results have a geometric interpretation or not. We hope that a finer understanding of the subject might also possibly provide a recipe for finding high order elements from towers obtained from different forms.

Acknowledgements The second author was partially supported by the research grant "Ing. Giorgio Schirillo" of the Istituto Nazionale di Alta Matematica "F. Severi", Rome. The third author would like to thank the High Performance Computing facility of University of L'Aquila (UAQ), which enabled us to implement the algorithm on MAGMA [2] computer algebra system, and run the experiments to validate our results. The third author is grateful to the fruitful and illuminating discussions with Professor Norberto Gavioli, UAQ. The third author is thankful to Professor Kalyan Chakraborty for arranging his research visit to Harish-Chandra Institute (HRI), Prayagraj, India, where the possible modularity aspects of this research work were explored. The third author thanks Dr. Kalyan Banerjee (Post-Doctoral Fellow, HRI) for his interest in exploring the geometric meaning of such towers and the modularity connections.

Funding Open access funding provided by Universitá degli Studi di Roma La Sapienza within the CRUI-CARE Agreement.

Code availability Not applicable.

Declarations

Conflict of interest All Authors declare that they have no competing interest.

References

1. Ahmadi O., Shparlinski I.E., Voloch J.F.: Multiplicative order of Gauss periods. Int. J. Number Theory **6**(4), 877–882 (2010).
2. Bosma W., Cannon J.J., Fieker C., Steel A.: Handbook of Magma Functions. http://magma.maths.usyd.edu.au/magma/handbook/.
3. Burkhart J.F., Calkin N.J., Gao S., Hyde-Volpe J.C., James K., Maharaj H., Manber S., Ruiz J., Smith E.: Finite field elements of high order arising from modular curves. Des. Codes Cryptogr. **51**(3), 301–314 (2009).
4. Chang M.-C.: Elements of large order in prime finite fields. Bull. Aust. Math. Soc. **88**(1), 169–176 (2013).
5. Chang M.-C.: Order of Gauss periods in large characteristic. Taiwanese J. Math. **17**(2), 621–628 (2013).
6. Chapman R.: Completely normal elements in iterated quadratic extensions of finite fields. Finite Fields Their Appl. **3**(1), 1–10 (1997).
7. Cohen S.D.: The explicit construction of irreducible polynomials over finite fields. Des. Codes Cryptogr. **2**(2), 169–174 (1992).

8. Conflitti A.: On elements of high order in finite fields. In: Cryptography and Computational Number Theory (Singapore, 1999). Progress in Computer Science and Applied Logic, vol. 20, pp. 11–14. Birkhäuser, Basel (2001).
9. Dose V., Mercuri P., Pal A., Stirpe C.: Sample code for recursive tower $q = 11$ in MAGMA (2020). https://www.dropbox.com/sh/qsq6iw9oh0lsvql/AACEV9ZGEL587IDDQSjirHfza?dl=0.
10. Elkies N.D.: Explicit modular towers (2001). arXiv:math/0103107.
11. Gao S.: Elements of provable high orders in finite fields. Proc. Am. Math. Soc. **127**(6), 1615–1623 (1999).
12. Huang M.-D., Narayanan A.K.: Finding primitive elements in finite fields of small characteristic. In: Topics in Finite Fields. Contemporary Mathematics, vol.632, pp. 215–228. American Mathematical Society, Providence, RI (2015).
13. Martínez F.E.B., Reis L.: Elements of high order: in Artin-Schreier extensions of finite fields $\mathbb{F}_q$. Finite Fields Appl. **41**, 24–33 (2016).
14. McNay G.: Topics in Finite Fields. PhD, University of Glasgow, Glasgow, UK (1995).
15. Meyn H.: Explicit n-polynomials of 2-power degree over finite fields, I. Des. Codes Cryptogr. **6**(2), 107–116 (1995).
16. Popovych R.: Elements of high order in finite fields of the form $F_q[x]/\Phi_r(x)$. Finite Fields Appl. **18**(4), 700–710 (2012).
17. Popovych R.: Elements of high order in finite fields of the form $F_q[x]/(x^m - a)$. Finite Fields Appl. **19**, 86–92 (2013).
18. Popovych R.: On elements of high order in general finite fields. Algebra Discret. Math. **18**(2), 295–300 (2014).
19. Popovych R.: Sharpening of the explicit lower bounds for the order of elements in finite field extensions based on cyclotomic polynomials. Ukrainian Math. J. 66(6):916–927 (2014). Reprint of Ukraïn. Mat. Zh. **6**6, 815–825 (2014).
20. Popovych R.: On the multiplicative order of elements in Wiedemann's towers of finite fields. Carpathian Math. Publ. **7**(2), 220–225 (2015).
21. Popovych R.: Some primitive elements for the Artin-Schreier extensions of finite fields. J. Math. Sci. (N.Y.) **210**(1), 67–75 (2015). Translation of Ukr. Mat. Visn. **1**2, 86–96 (2015).
22. Popovych R.: Multiplicative orders of elements in Conway's towers of finite fields. Algebra Discret. Math. **25**(1), 137–146 (2018).
23. Stichtenoth H.: Algebraic Function Fields and Codes, vol. 254, 2nd edn Springer, Berlin (2009).
24. Voloch J.F.: On the order of points on curves over finite fields. Integers **7**(A49), 4 (2007).
25. Voloch J.F.: Elements of high order on finite fields from elliptic curves. Bull. Aust. Math. Soc. **81**(3), 425–429 (2010).
26. von zur Gathen J., Shparlinski I.: Gaußperiods in finite fields. In: Finite Fields and Applications (Augsburg, 1999), pp. 162–177. Springer, Berlin (2001).