Primitive values of quadratic polynomials in a finite field

Andrew R. Booker*
School of Mathematics
University of Bristol, England
andrew.booker@bristol.ac.uk

Stephen D. Cohen
School of Mathematics and Statistics,
University of Glasgow, Scotland
stephen.cohen@glasgow.ac.uk

Nicole Sutherland
Computational Algebra Group,
School of Mathematics and Statistics,
University of Sydney, Australia
nicole.sutherland@sydney.edu.au

Tim Trudgian†
School of Physical, Environmental and Mathematical Sciences
The University of New South Wales Canberra, Australia
t.trudgian@adfa.edu.au

June 14, 2018

Abstract

We prove that for all $q > 211$, there always exists a primitive root g in the finite field $\mathbb{F}_q$ such that $Q(g)$ is also a primitive root, where $Q(x) = ax^2 + bx + c$ is a quadratic polynomial with $a, b, c \in \mathbb{F}_q$ such that $b^2 - 4ac \neq 0$.

1 Introduction

For q a prime power, let $\mathbb{F}_q$ denote the finite field of order q, and let $g_1, g_2, \ldots, g_{\phi(q-1)}$ denote the primitive roots of q. Recently [6] the following conjecture of Cohen and Mullen [5] was established: that an arbitrary element of $\mathbb{F}_q$ can be written as a linear sum of two primitive roots provided $q > 61$. In fact, Cohen's survey of such problems [4] offered a preliminary treatment of a further result wherein the linear sum would be replaced by a

*Partially supported by EPSRC Grant EP/K034383/1.
†Supported by Australian Research Council Future Fellowship FT160100094.

quadratic function of primitive roots. It is the purpose of this paper to develop this theme and provide one complete existence result on the topic.

Let

$$a, b, c \in \mathbb{F}_q, \quad a \neq 0, \quad b^2 - 4ac \neq 0. \tag{1}$$

Is there some q_0 such that there is always at least one representation

$$g_n = ag_m^2 + bg_m + c, \tag{2}$$

for all $q > q_0$? We insist that a be non-zero, since otherwise the result follows from the work already quoted in [6]. We also insist that $b^2 - 4ac$ be non-zero so that g_n (given by (2)) is *not* of the form $a(g_m + b/(2a))^2$.

Han [7] showed under the assumption[1] of (1), and with the additional restriction that q be odd, that one could choose $q_0 = 2^{66} \approx 7.4 \times 10^{19}$. This was improved to $q_0 = 2^{62} \approx 4.7 \times 10^{18}$ by Chou et al. [3]. Moreover, Chou et al. provided a list of 24 genuine exceptions to (2), all of which were not greater than 211. Upon verifying that all odd values of $q \in [223, 457]$ satisfy (2), they conjectured that all $q \geq 223$ satisfy (2).

This was improved substantially by Cohen [4, §3] who showed that assuming (1) a representation of the form (2) always exists provided $q > 10^9$. We refine this result in Theorem 1 below.

Theorem 1. *Let $a, b, c \in \mathbb{F}_q$ with $a \neq 0$ and with $b^2 - 4ac \neq 0$. Then there are primitive roots g_n and g_m such that*

$$g_n = ag_m^2 + bg_m + c, \tag{3}$$

for all q with the exception of the values listed in (4).

The following values of q are genuine exceptions to (3) (for some triple (a, b, c)).

$$\{2, 3, 4, 5, 9, 7, 11, 13, 16, 19, 23, 25, 29, 31, 37, 41, 43, 49, 61, 67, 71, 73, 79, 121, 127, 151, 211\} \tag{4}$$

Note that this list of exceptions agrees with that of Chou et al. [3] (after noting that they only considered q odd).

The outline of this paper is as follows. In §2 we develop the necessary character sum machinery. In §3 we use a sieve to prove that there are at most 1528 exceptions to Theorem 1. We introduce a more refined sieve in §4 to reduce the number of possible exceptions to 1453. We then turn to computation in §5 to complete the proof of Theorem 1.

2 A cast of character sums

Given a positive integer m, let $\omega(m)$ denote the number of distinct prime factors of m so that $W(m) = 2^{\omega(m)}$ is the number of square-free divisors of m. Also, let $\theta(m) = \prod_{p|m}(1 - p^{-1})$. For any integer m define its radical $\mathrm{Rad}(m)$ as the product of all distinct prime factors of m.

[1] Han and Chou et al. considered the additional restriction that c be non-zero. We see no reason to make this distinction.

Let e be a divisor of $q-1$. Call $g \in \mathbb{F}_q$ *e-free* if $g \neq 0$ and $g = h^d$, where $h \in \mathbb{F}_q$ and $d \mid e$, implies $d = 1$. The notion of e-free depends (among divisors of $q-1$) only on $\mathrm{Rad}(e)$. Moreover, in this terminology a primitive root of $\mathbb{F}_q$ is a $(q-1)$-free element.

The definition of any multiplicative character χ on $\mathbb{F}_q^\times$ is extended to the whole of $\mathbb{F}_q$ by setting $\chi(0) = 0$. For any divisor d of $\phi(q-1)$, there are $\phi(d)$ characters of order d, a typical character being denoted by χ_d. In particular χ_1, the principal character, takes the value 1 at all non-zero elements of $\mathbb{F}_q$ (whereas $\chi_1(0) = 0$). A convenient shorthand notation to be employed for any divisor e of $q-1$ is

$$\int_{d|e} = \sum_{d|e} \frac{\mu(d)}{\phi(d)} \sum_{\chi_d},$$

where the sum over χ_d is the sum over all $\phi(d)$ multiplicative characters χ_d of $\mathbb{F}_q$ of exact order d. Its significance is that, for any $g \in \mathbb{F}_q$,

$$\theta(e) \int_{d|e} \chi_d(g) = \begin{cases} 1, & \text{if } g \text{ is non-zero and } e\text{-free,} \\ 0, & \text{otherwise.} \end{cases}$$

In this expression (and throughout) only characters χ_d with d square-free contribute (even if e is not square-free).

Let e_1, e_2 be divisors of $q-1$. Given a triple (a,b,c) satisfying (1) define $N(e_1,e_2)$ to be the number of e_1-free elements $g \in \mathbb{F}_q^\times$ such that $Q(g)$ is an e_2-free element in $\mathbb{F}_q^\times$. We wish to investigate when $N(q-1,q-1)$ is positive. The value of $N(e_1,e_2)$ can be expressed explicitly in terms of character sums over $\mathbb{F}_q$ as follows. We have

$$N(e_1,e_2) = \theta(e_1)\theta(e_2) \int_{d_1|e_1} \int_{d_2|e_2} S(\chi_{d_1}, \chi_{d_2}), \tag{5}$$

where

$$S(\chi_{d_1}, \chi_{d_2}) = \sum_{g \in \mathbb{F}_q} \chi_{d_1}(g)\chi_{d_2}(Q(g)) \tag{6}$$

with $Q(x) = ax^2 + bx + c$. We estimate $S(\chi_{d_1}, \chi_{d_2})$ in the following lemma.

Lemma 1. *Assume the triple $(a,b,c) \in \mathbb{F}_q$ satisfies (1). Suppose e_1, e_2 are divisors of $q-1$, $d_1 \mid e_1$ and $d_2 \mid e_2$. In (6), if $d_1 = d_2 = 1$ then $S(\chi_1,\chi_1) \geq q-3$. Otherwise,*

$$|S(\chi_{d_1}, \chi_{d_2})| \leq \begin{cases} 2, & \text{if } d_1 > 1, d_2 = 1, \\ \sqrt{q}+1, & \text{if } d_1 = 1, d_2 > 1, \\ 2\sqrt{q}, & \text{if } d_1 > 1, d_2 > 1. \end{cases}$$

Proof. This follows from Weil's theorem [8, Thm 5.41], taking into account (up to) 3 zeros of $gQ(g)$. □

Lemma 2. *Suppose the triple (a,b,c) satisfies (1). Suppose that e is a divisor of $q-1$ (with e even if q is odd). Then*

$$N(e,e) \geq \theta(e)^2 \left(q - 2W(e)\sqrt{q}\{W(e) - 3/2 + 1/(2W(e))\} - 3W(e)\right).$$

Proof. Write $W = W(e)$. Applying the estimates of Lemma 1 to (5) and (6) we obtain

$$N(e,e) \geq \theta(e)^2(q - 3 - (W-1)^2 2\sqrt{q} - (W-1)(\sqrt{q}+1) - 2(W-1))$$

and the result follows. □

We take $e = q-1$ to obtain a basic criterion to guarantee that $N(q-1, q-1) > 0$. In this situation the minor savings within Lemma 2 are insignificant and are ignored.

Theorem 2. *Suppose the triple (a,b,c) satisfies (1). If $q > 4W(q-1)^4$ then there exists a primitive root g such that $ag^2 + bg + c$ is also a primitive root.*

The condition in Theorem 2 is automatically satisfied if $\omega(q-1) \geq 17$. Hence we may assume $\omega(q-1) \leq 16$ and $q < 7.37 \times 10^{19}$. To obtain an improvement on Theorem 2 we proceed, as in [6], to introduce a sieving technique.

3 Introducing the sieve

Let e be a divisor of $q-1$. In practice, this *kernel* e will be chosen such that $\mathrm{Rad}(e)$ is the product of the smallest primes in $q-1$. In particular, if q is odd, then certainly e is even. If $\mathrm{Rad}(e) = \mathrm{Rad}(q-1)$, then set $s = 0$ and $\delta = 1$. Otherwise, if $\mathrm{Rad}(e) < \mathrm{Rad}(q-1)$ let $p_1, \ldots, p_s$, $s \geq 1$, be the primes dividing $q-1$ but not e and set $\delta = 1 - \sum_{i=1}^{s} 2p_i^{-1}$. In practice, it is essential to choose e so that $\delta > 0$. We first borrow a result from [6].

Lemma 3 (Lemma 1 [6])**.** *Suppose the triple (a,b,c) satisfies (1). Suppose e is a divisor of $q-1$. Then, in the above notation,*

$$N(q-1,q-1) \geq \sum_{i=1}^{s} N(p_i e, e) + \sum_{i=1}^{s} N(e, p_i e) - (2s-1)N(e,e).$$

Hence

$$N(q-1,q-1) \geq \sum_{i=1}^{s} \{[N(p_i e, e) - \theta(p_i)N(e,e)] + [N(e,p_i e) - \theta(p_i)N(e,e)]\} + \delta N(e,e). \quad (7)$$

We now proceed to use Lemma 1 to bound the terms appearing in (7).

Lemma 4. *Suppose the triple (a,b,c) satisfies (1). Let l be a prime dividing $q-1$ but not e. Then*

$$|N(e,le) - \theta(l)N(e,e)| \leq (1-1/l)\theta(e)^2(2W(e)^2\sqrt{q} - W(e)(\sqrt{q}-1)). \quad (8)$$

and

$$|N(le,e) - \theta(l)N(e,e)| \leq (1-1/l)\theta(e)^2(2W(e)^2\sqrt{q} - 2W(e)(\sqrt{q}-1)). \quad (9)$$

Proof. From (5)

$$N(le,e)-\theta(l)N(e,e)=\theta(le)\theta(e)\int_{d_1|e}\int_{d_2|e}S(\chi_{ld_1},\chi_{d_2}).$$

Hence, by Lemma 1

$$\begin{aligned}|N(e,le)-\theta(l)N(e,e)| &\le \theta(l)\theta(e)^2\left((W(le)-W(e))(W(e)-1)2\sqrt{q}+(W(le)-W(e))(\sqrt{q}+1)\right)\\ &= (1-\tfrac{1}{l})\theta(e)^2\left(2W(e)(W(e)-1)\sqrt{q}+W(e)(\sqrt{q}+1)\right),\end{aligned}$$

since $W(le)=2W(e)$ and $\theta(l)=1-1/l$; (8) follows.

Similarly,

$$|N(le,e)-\theta(l)N(e,e)|\le\theta(l)\theta(e)^2\left(W(e)(W(e)-1)2\sqrt{q}+2W(e)\right)$$

and (9) follows.

□

Theorem 3. *Let q be a prime power. Suppose the triple $(a,b,c)\in\mathbb{F}_q$ satisfies (1). Let $p_1,\dots,p_s$, $s\ge 1$, be the primes dividing $q-1$ but not e and set $\delta=1-2\sum_{i=1}^s p_i^{-1}$. Suppose that δ is positive and that*

$$q>\left\{\left(\frac{2s-1}{\delta}+2\right)\left(2W(W-3/2)+\frac{3W}{2\sqrt{q}}\right)+1+\frac{3W}{2\sqrt{q}}\right\}^2, \tag{10}$$

where $W=W(e)$. Then there is a primitive root g such that ag^2+bg+c is also primitive.

Proof. Assume $\delta>0$. Write N for $N(q-1,q-1)$ and W for $W(e)$. From (7) and Lemmas 2 and 4

$$\begin{aligned}N &\ge \theta(e)^2\left\{\delta\left(q-\left(2W(W-\frac{3}{2})+1+\frac{3W}{\sqrt{q}}\right)\sqrt{q}\right)-\sum_{i=1}^{s}2\left(1-\frac{1}{p_i}\right)\left(2W(W-\frac{3}{2})+\frac{3W}{2\sqrt{q}}\right)\sqrt{q}\right\}\\ &= \delta\theta(e)^2\sqrt{q}\left\{\sqrt{q}-\left(2W(W-\frac{3}{2})+1+\frac{3W}{\sqrt{q}}\right)-\left(\frac{2s-1}{\delta}+1\right)\left(2W(W-\frac{3}{2})+\frac{3W}{2\sqrt{q}}\right)\right\}. \qquad (11)\end{aligned}$$

The conclusion follows. □

We now illustrate the utility of Theorem 3. Recall that Theorem 2 implies that we need only consider those q satisfying $\omega(q-1)\le 16$. A simple computation shows that, for $9\le\omega(q-1)\le 16$ and $s=5$, the inequality in (10) is satisfied. As an example, consider the case $\omega(q-1)=9$, so that $q\ge 2\cdot3\cdot5\cdot7\cdot11\cdot13\cdot17\cdot19\cdot23+1=223,092,871$. For $s=5$ we have $W=W(e)=16$ and $\delta\ge 1-2\left(\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\frac{1}{23}\right)$. Therefore the right hand side of (10) is at most $161,546,452$. Hence there is bound to be a representation of the form (3).

We now consider $1\le\omega(q-1)\le 8$ following the procedure in §2 of [6]. Consider $\omega(q-1)=8$: there is no value of $s\in[1,7]$ for which (10) is true. Nevertheless, we find that $s=5$ gives the smallest bound for the right-hand side of (10). For $s=5$ we have

$W = W(e) = 8$ and $\delta \geq 1 - 2\left(\frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \frac{1}{17} + \frac{1}{19}\right)$. Therefore the right hand side of (10) is at most $38,228,191$. We now enumerate the values of q that require checking: that is, those q satisfying $q \leq 38,228,191$ with q a prime power and $\omega(q-1) = 8$. We find that there are 23 such values of q. For each of these values of q we list the prime factorisation, finding the exact value of δ in each case. With this tailored approach we apply Theorem 3 once more. We find that only 5 values of q do not satisfy (10).

We continue in this way for[2] $\omega(q-1) \leq 7$. In Table 1 we collect our results. We run the above procedure over all values of $s \in [1, \omega(q-1) - 1]$. The second column indicates the largest element in the final list. The third column contains the final number of elements of these lists, discriminating primes (on the left of the summation sign) and prime powers (on the right of the summation sign).

We have a total of 1528 possible exceptions to Theorem 1. In the next section we introduce the modified prime sieve, which, as can be seen in the fourth column of Table 1, reduces the number of possible exceptions to 1453.

Table 1: Improved bounds for q

$\omega(q-1)$	Largest q	Final list size (primes + prime powers)	MPS list size
8	18888871	$5 + 0$	$5 + 0$
7	8678671	$104 + 1$	$104 + 1$
6	2402401	$417 + 6$	$403 + 6$
5	591361	$477 + 11$	$464 + 11$
4	52501	$378 + 20$	$331 + 20$
3	4861	$73 + 9$	$73 + 9$
2	109	$14 + 6$	$14 + 5$
1	32	$3 + 4$	$3 + 4$
Total		$1471 + 57$	$1397 + 56$

4 The modified prime sieve

We modify the notation and argument used in Theorem 3 and follow the approach of [1]. Suppose that $\mathrm{Rad}(q-1)$ is written as ePL, where e is a divisor of $q-1$ and that for $s \geq 1$ we have $P = p_1 \cdots p_s$ is a product of distinct primes (*the main sieving primes*) and $L = l_1 \cdots l_r (r \geq 1)$ (*the large primes*). In practice, e is the product of the smallest primes in $q-1$ that cannot be used as sieving primes and L involves those primes that are somewhat larger than the rest (if there are any). Write $m = \theta(e)$ and $W(e)$. Define $\delta = 1 - 2\sum_{i=1}^{s} \frac{1}{p_i}$ and $\varepsilon = \sum_{j=1}^{r} \frac{1}{l_j}$.

[2]When $\omega(q-1) = 0$ we have $q = 2$, whence (3) is clearly false for $a = b = 1$ and $c = 0$.

Theorem 4. *Let $e \mid q-1$ as in Theorem 3 and define* $\mathrm{Rad}(q-1) = ePL$, δ, ε, W, *as above. Assume $m^2\delta > 2\varepsilon$, where $m = \theta(e)$. Suppose*

$$\sqrt{q} > \frac{m^2(2s-1+2\delta)\left(2W(W-\frac{3}{2})+\frac{3W}{2\sqrt{q}}\right)+\delta+r-\varepsilon+\frac{1}{\sqrt{q}}\left(\frac{3m^2\delta W}{2}+2r-\varepsilon\right)}{m^2\delta-2\varepsilon}.$$

Then there is a primitive root g such that ag^2+bg+c is also primitive.

Proof. Begin with the fact that $N = N(q-1, q-1) = N(ePL, ePL)$. Then, clearly,

$$N \geq N(eP, eP) + N(L, L) - N(1, 1).$$

Observe that, now (11) serves as a lower bound for the value of $N(eP, eP)$. Moreover,

$$N(L, L) \geq \sum_{j=1}^{r} [N(l_j, 1) + N(1, l_j)] - (2r-1)N(1, 1), \tag{12}$$

because each pair $(g, Q(g)), g \in \mathbb{F}_q^\times$ contributes 1 to the right side of (12) only if both g and $Q(g)$ are l_j-free for each $j = 1, \ldots, r$, and otherwise contributes a non-positive integer.

From (12), with $\Delta = N(L, L) - N(1, 1)$,

$$\Delta \geq \sum_{j=1}^{r} \left[\left(N(l_j, 1) - \left(1-\frac{1}{l_j}\right)N(1,1)\right) + \left(N(1, l_j) - \left(1-\frac{1}{l_j}\right)N(1,1)\right)\right] - 2\varepsilon(q-1). \tag{13}$$

From (8) and (9), for $j = 1, \ldots, r$,

$$\left|N(l_j, 1) - \left(1-\frac{1}{l_j}\right)\right| \leq 2\left(1-\frac{1}{l_j}\right)$$

and

$$\left|N(1, l_j) - \left(1-\frac{1}{l_j}\right)\right| \leq \left(1-\frac{1}{l_j}\right)(\sqrt{q}+1).$$

It follows that (13) yields

$$N(L, L) - N(1, 1) \geq 2\varepsilon(q-1) - (r-\varepsilon)\sqrt{q} - (2r-3\varepsilon). \tag{14}$$

Combining (14) with the relevant version of (10) we obtain Theorem 4. □

The modified prime sieve allows us to eliminate more values of q theoretically. We fed all outstanding q with $2 \leq \omega(q-1) \leq 8$, as detailed in our Table 1, into the criterion of Theorem 4. We have listed the final tally of possible exceptions in the final column of Table 1. The use of Theorem 4 reduces the total number of possible exceptions to 1453: this list includes the following six even values of q: $4, 8, 16, 32, 256, 4096$. The total impact of the modified prime sieve is about a 5% improvement on previous work. We note that in every case $r = 1$ was used to eliminate a value of q.

While the gain in using the modified prime sieve is small, we have included it to emphasise the limits of the theoretical approach. Indeed, it does not seem obvious how to extend these theoretical calculations further. We now turn to computational techniques to resolve Theorem 1.

5 Computation

5.1 Small values of q

For each possible exception q, we run over all admissible combinations of $a, b, c \in \mathbb{F}_q$ to find an appropriate primitive root. We do this in Algorithm 1 where we consider the equivalent $a(g^2 + bg + c)$, with $b^2 - 4c \neq 0$.

Let R be the radical of $q - 1$; then γ^k is primitive iff k is coprime to R. This property is unchanged by reduction modulo R; hence we need only consider $a = \gamma^k$ with $k < R$.

Algorithm 1: Check whether q has the quadratic primitive property

```
1  Procedure check_q(q)
2      Construct F_q and primitive element γ
3      for c ∈ [γ^j : 0 ≤ j < q − 1] ∪ [0] do
4          for b ∈ [γ^i : 0 ≤ i < q − 1] ∪ [0] do
5              if b^2 − 4c = 0 then
6                  next b
7              for a ∈ [γ^k : 0 ≤ k < R] do
8                  for l in stored_logs do
9                      if GCD(k+l, R) = 1 then
10                         next k
11                 for 1 ≤ m < q − 1 do
12                     if GCD(m, R) = 1 then
13                         g ← γ^m; l ← log_γ(g^2 + bg + c)
14                         Store l in stored_logs
15                         if GCD(k+l, R) = 1 then
16                             next k
17                 if m = q − 1 then
18                     FAIL
```

To maximise efficiency in Algorithm 1 we store the logarithms we have computed as well as the elements that have already been determined to be primitive. In this way we can first check through our list of stored primitive elements a and only generate more primitive elements as needed.

We record these results in Table 2. A comparison with Table 1 shows that we can eliminate all of those q with $1 \leq \omega(q-1) \leq 4$. However, as can be seen from Table 2 this approach becomes infeasible to pursue for q with $\omega(q-1) \geq 5$. The largest q we have checked this way is 11971, the smallest q we did not finish checking in 3 weeks is 11131. Algorithm 1 was, however, effective in treating the six remaining even values of q.

$\omega(q-1)$	1	2	3	4	5
Number of q checked	7	19	82	351	22 (out of 475)
Time	1s	3.22s	7.8 hrs	1076.3 days	139.52 days

Table 2: Total timings for checking whether q has the quadratic primitive property.

5.2 A further algorithm for odd q

Assume q is odd. Fix a primitive root g of $\mathbb{F}_q^\times$, and let $P = \{g^n : n \in \mathbb{Z},\ (n, q-1) = 1\} \subseteq \mathbb{F}_q^\times$ be the set of all primitive roots. For a prime $p \mid q-1$, let r_p denote the composition

$$\mathbb{F}_q^\times \xrightarrow{\log_g} \mathbb{Z}/(q-1)\mathbb{Z} \xrightarrow{\bmod p} \mathbb{Z}/p\mathbb{Z}.$$

For $d \mid q-1$, let $H_d = \langle g^d \rangle \leq \mathbb{F}_q^\times$ denote the unique subgroup of index d.

Let d be an odd unitary divisor of $q-1$ — so that $(d, (q-1)/d) = 1$ — and set

$$e = \prod_{p \mid \frac{q-1}{d}} p \quad \text{and} \quad A_d = \big\{g^{nd} : 0 \leq n < e\big\}.$$

Then A_d is a set of coset representatives for H_d/H_{de}, and it follows that any element of $\mathbb{F}_q^\times$ can be expressed uniquely in the form $\alpha h h'$, where $\alpha \in A_d$, $h \in H_{de}$ and $h' \in H_{\frac{q-1}{d}}$.

Let S_d denote the set of prime factors of d, and for each $p \in S_d$ set

$$R_p = \left\{ n + p\mathbb{Z} : 1 \leq n \leq \frac{p-1}{2} \right\} \subset (\mathbb{Z}/p\mathbb{Z})^\times.$$

Note that R_p is a set of coset representatives for $(\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}$. For $\varepsilon = (\varepsilon_p)_{p \in S_d} \in \{\pm 1\}^{S_d}$, define

$$X_d(\varepsilon) = \big\{x \in \mathbb{F}_q^\times : r_p(x) \in \varepsilon_p R_p \cup \{0\} \text{ for all } p \in S_d\big\}.$$

Then

$$\mathbb{F}_q^\times = \bigcup_{\varepsilon \in \{\pm 1\}^{S_d}} X_d(\varepsilon). \tag{15}$$

Lemma 5. *Let d be an odd unitary divisor of $q-1$, and define A_d, S_d and $X_d(\varepsilon)$ as above. Suppose, for all $\alpha, \beta \in A_d$ and $\varepsilon, \delta \in \{\pm 1\}^{S_d}$, that*

$$\big\{(\alpha x + 1)^2 - \beta y : x \in P \cap X_d(\varepsilon), y \in P \cap X_d(\delta)\big\} \supseteq \mathbb{F}_q^\times \tag{16}$$

and

$$\big\{x^2 - \beta y : x \in P, y \in P \cap X_d(\delta)\big\} \supseteq \mathbb{F}_q^\times.$$

Then the conclusion of Theorem 1 holds for q.

Proof. Let $a, b, c \in \mathbb{F}_q$ with $a(b^2 - 4ac) \neq 0$. If $b \neq 0$ then the relation $y = ax^2 + bx + c$ is equivalent to

$$\gamma = (\alpha x + 1)^2 - \beta y,$$

where $\alpha = 2ab^{-1}$, $\beta = 4ab^{-2}$ and $\gamma = b^{-2}(b^2 - 4ac)$. Similarly, for $b = 0$, $y = ax^2 + bx + c$ is equivalent to

$$\gamma = x^2 - \beta y,$$

where $\beta = a^{-1}$ and $\gamma = -ca^{-1}$. Hence, it suffices to show that

$$\big\{(\alpha x + 1)^2 - \beta y : x, y \in P\big\} \supseteq \mathbb{F}_q^\times \quad \text{for all } \alpha, \beta \in \mathbb{F}_q^\times \tag{17}$$

and

$$\big\{x^2 - \beta y : x, y \in P\big\} \supseteq \mathbb{F}_q^\times \quad \text{for all } \beta \in \mathbb{F}_q^\times. \tag{18}$$

Consider fixed $\alpha, \beta, \gamma \in \mathbb{F}_q^\times$. Let $\alpha_0, \beta_0 \in A_d$, $h_1, h_2 \in H_{de}$ and $h_1', h_2' \in H_{\frac{q-1}{d}}$ be the elements such that $\alpha = \alpha_0 h_1^{-1} h_1'^{-1}$ and $\beta = \beta_0 h_2^{-1} h_2'^{-1}$. By (15) we can choose $\varepsilon, \delta \in \{\pm 1\}^{S_d}$ such that $h_1' \in X_d(\varepsilon)$ and $h_2' \in X_d(\delta)$.

Now, by hypothesis, there exist $x_0 \in P \cap X_d(\varepsilon)$ and $y_0 \in P \cap X_d(\delta)$ such that

$$(\alpha_0 x_0 + 1)^2 - \beta_0 y_0 = \gamma.$$

Hence, writing $x = h_1 h_1' x_0$ and $y = h_2 h_2' y_0$, we have $\alpha x = \alpha_0 x_0$ and $\beta y = \beta_0 y_0$, so that

$$(\alpha x + 1)^2 - \beta y = \gamma.$$

Further, for any $p \mid q - 1$, we have $r_p(h_1) = 0$, so

$$r_p(x) = r_p(h_1') + r_p(x_0).$$

If $p \notin S_d$ then $r_p(h_1') = 0$ so that $r_p(x) = r_p(x_0)$, while if $p \in S_d$ then

$$r_p(x) \in (\varepsilon_p R_p \cup \{0\}) + \varepsilon_p R_p = (\mathbb{Z}/p\mathbb{Z})^\times.$$

In either case, we see that $r_p(x) \neq 0$. Therefore $x \in P$, and by a similar argument we find that $y \in P$. Since α, β, γ were arbitrary, we conclude that (17) holds.

Similarly, in the $b = 0$ case we choose $x \in P$ and $y_0 \in P \cap X_d(\delta)$ such that $x^2 - \beta_0 y_0 = \gamma$, and we set $y = h_2 h_2' y_0$. As above we see that $y \in P$ and $x^2 - \beta y = \gamma$. Thus (18) holds. □

For given α, β, ε and δ, using a fast convolution algorithm we can compute the set (16) using $O(q \log q)$ arithmetic operations on numbers with $O(\log q)$ bits. Thus, the total time to check the criterion given in Lemma 5 is

$$\ll (e2^{\omega(d)})^2 q (\log q)^{O(1)} \ll_\varepsilon e^2 q^{1+\varepsilon}.$$

For very large q we expect the criterion to be satisfied even with $e = 2$, so that Theorem 1 can be verified in quasi-linear time $O(q^{1+\varepsilon})$. However, that is slightly misleading, since we

will only apply the algorithm to those q satisfying $q \leq 4W(q-1)^4$, in which case the running time is

$$\gg W(q-1)^2 q \log q \gg q^{3/2} \log q.$$

There is also significant overhead in the convolution algorithm, to the point that we found the naive method of enumerating all values of $(\alpha x+1)^2-\beta y$ to be faster in practice. That method requires approximately $(e\phi(q-1))^2$ arithmetic operations in $\mathbb{F}_q$, which is still reasonable for $q \leq 18,888,871$ on modern computers, provided that e is not too large.

Write the prime factorisation of $q-1$ as $\prod_{i=1}^{s} p_i^{e_i}$, where $2 = p_1 < \cdots < p_s$. We coded the criterion of Lemma 5 with $d = \prod_{n<i\leq s} p_i^{e_i}$ for some $n \in \{1, \ldots, s\}$. We first try $n = 1$ (corresponding to $e = 2$), then $n = 2$, and so on, until either the criterion is satisfied or we reach $n = s$ without success. Note that when $n = s$ (corresponding to $d = 1$), our algorithm becomes an exhaustive search, so it must eventually succeed whenever the conclusion of Theorem 1 holds for q.

Applying this procedure (see [2]) to the 1447 odd values of q that were not covered by Theorems 3 and 4, we found that most succeeded with $n = 1$ or 2. In particular, for all $q > 150,151$ the algorithm succeeded for some choice of $e \leq 6$.

Acknowledgements

The second and fourth authors would like to thank Tomás Oliveira e Silva with whom we had several discussions on preliminary versions of this paper.

References

[1] G. Bailey, S. D. Cohen, N. Sutherland, and T. Trudgian, *Existence results for primitive elements in cubic and quartic extensions of a finite field*, Math. Comp., *to appear*.

[2] A.R. Booker, S.D. Cohen, N. Sutherland, and T. Trudgian. *Computer code*, `https://arxiv.org/src/1803.01435v2/anc/`, 2018.

[3] W.-S. Chou, G. L. Mullen, J.-S. Shiue, and Q. Sun, *Pairs of primitive element modulo p^l*, J. Sichuan U. Nat. Sci. Ed., **26** (1991), 189–195.

[4] S. D. Cohen, *Primitive elements and polynomials: existence results*, Finite fields, coding theory and advances in communications and computing (New York), Lecture Notes in Pure and Appl. Math. 141, Dekker, 1993.

[5] S. D. Cohen and G. L. Mullen, *Primitive elements in finite fields and Costas arrays*, AAECC **2** (1991), 45–53.

[6] S. D. Cohen, T. Oliveira e Silva, and T. Trudgian, *A proof of the conjecture of Cohen and Mullen on sums of primitive roots*, Math. Comp., **84**(296) (2015), 2979–2986.

[7] W.-B. Han, *On polynomials and primitive elements over finite fields*, Acta Math. Sinica, **32** (1983), 13–21.

[8] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, 1997.