Bull. Aust. Math. Soc. **106** (2022), 458–462
doi:10.1017/S0004972722000442

PRIMITIVE ELEMENT PAIRS WITH A PRESCRIBED TRACE IN THE CUBIC EXTENSION OF A FINITE FIELD

ANDREW R. BOOKER, STEPHEN D. COHEN, NICOL LEONG and TIM TRUDGIAN ✉

(Received 3 March 2022; accepted 25 March 2022; first published online 25 April 2022)

Abstract

We prove that for any prime power $q \notin \{3, 4, 5\}$, the cubic extension $\mathbb{F}_{q^3}$ of the finite field $\mathbb{F}_q$ contains a primitive element ξ such that $\xi + \xi^{-1}$ is also primitive, and $\mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(\xi) = a$ for any prescribed $a \in \mathbb{F}_q$. This completes the proof of a conjecture of Gupta *et al.* ['Primitive element pairs with one prescribed trace over a finite field', *Finite Fields Appl.* **54** (2018), 1–14] concerning the analogous problem over an extension of arbitrary degree $n \geq 3$.

2020 *Mathematics subject classification*: primary 12E20; secondary 11T23.

Keywords and phrases: finite field, field extension, primitive element, prime sieve algorithm.

1. Introduction

Let q be a prime power and n an integer at least 3, and let $\mathbb{F}_{q^n}$ denote a degree-n extension of the finite field $\mathbb{F}_q$. We say that $(q, n) \in \mathfrak{P}$ if, for any $a \in \mathbb{F}_q$, we can find a primitive element $\xi \in \mathbb{F}_{q^n}$ such that $\xi + \xi^{-1}$ is also primitive and $\mathrm{Tr}(\xi) = a$. This problem was considered by Gupta *et al.*, who proved a complete result for $n \geq 5$ [4]. We refer the reader to [4] for an introduction to similar problems. Cohen and Gupta [2] extended the work of [4], providing a complete result for $n = 4$ and some preliminary results for $n = 3$. We improved the latter results in [1, Section 7], showing in particular that $(q, 3) \in \mathfrak{P}$ for all $q \geq 8 \times 10^{12}$. It is a formidable task to try to prove the result for the remaining values of q and, indeed, the computation involved in [2] is extensive.

In this paper, we combine theory and novel computation to resolve the remaining cases with $n = 3$, proving the following theorem and affirming [4, Conjecture 1].

THEOREM 1.1. *We have $(q, n) \in \mathfrak{P}$ for all q and all $n \geq 3$, with the exception of the pairs $(3, 3)$, $(4, 3)$ and $(5, 3)$.*

The main theoretical input that we need is the following result, which Cohen and Gupta term the 'modified prime sieve criterion' (MPSC).

T. Trudgian was supported by Australian Research Council Future Fellowship FT160100094.

THEOREM 1.2 [2, Theorem 4.1]. *Let q be a prime power, and write* $\mathrm{rad}(q^3-1) = kPL$, *where k, P, L are positive integers. Define*

$$\delta = 1 - 2\sum_{p\mid P}\frac{1}{p}, \quad \varepsilon = \sum_{p\mid L}\frac{1}{p}, \quad \theta = \frac{\varphi(k)}{k} \quad \textit{and} \quad C_q = \begin{cases} 2 & \textit{if } 2 \mid q, \\ 3 & \textit{if } 2 \nmid q. \end{cases}$$

Then $(q,3) \in \mathfrak{P}$ *provided that*

$$\theta^2\delta > 2\varepsilon \quad \textit{and} \quad q^{1/2} > \frac{C_q(\theta^2 4^{\omega(k)}(2\omega(P) - 1 + 2\delta) + \omega(L) - \varepsilon)}{\theta^2\delta - 2\varepsilon}. \tag{1.1}$$

In practice, we take k to be the product of the first few prime factors of q^3-1 and L the product of the last few. In particular, taking $L = 1$, we recover the simpler 'prime sieve criterion' (PSC) [2, Theorem 3.2], in which the hypothesis (1.1) reduces to

$$\delta > 0 \quad \text{and} \quad q^{1/2} > C_q 4^{\omega(k)}\Big(\frac{2\omega(P)-1}{\delta} + 2\Big).$$

We will use this simpler criterion in most of what follows.

2. Proof of Theorem 1.1

2.1. Applying the modified prime sieve. Thanks to [1, Theorem 7.2], to complete the proof of Theorem 1.1 for $n = 3$, it suffices to check all $q < 8 \times 10^{12}$. To reduce this to a manageable list of candidates, we seek to apply the MPSC. For prime $q < 10^{10}$ and composite $q < 8 \times 10^{12}$, we do this directly with a straightforward implementation in `PARI/GP` [6], first trying the PSC and then the general MPSC when necessary.

For larger primes q, the direct approach becomes too time-consuming, mostly because of the time taken to factor q^3-1. To remedy this, we developed and coded in `C` the following novel strategy that makes use of a partial factorisation. Using sliding window sieves, we find the complete factorisation of $q-1$, as well as all prime factors of q^2+q+1 below $X = 2^{20}$. Let $u = (q^2+q+1)\prod_{p<X} p^{-\mathrm{ord}_p(q^2+q+1)}$ denote the remaining unfactored part. If $u < X^2$, then u must be 1 or a prime number, so we have enough information to compute the full prime factorisation of q^3-1 and can apply the PSC directly.

Otherwise, let $\{p_1, \ldots, p_s\}$ be the set of prime factors of u. Although the p_i are unknown to us, we can bound their contribution to the PSC via

$$s \le \lfloor \log_X u \rfloor \quad \text{and} \quad \sum_{i=1}^{s}\frac{1}{p_i} \le \frac{\lfloor \log_X u \rfloor}{X}.$$

We then check the PSC with all possibilities for P divisible by $p_1 \cdots p_s$. This sufficed to rule out all primes $q \in [10^{10}, 8 \times 10^{12}]$ in less than a day using one 16-core machine.

The end result is a list of 46896 values of q that are not ruled out by the MPSC, the largest of which is 4708304701. Of these, 483 are composite, the largest being

https://doi.org/10.1017/S0004972722000442 Published online by Cambridge University Press

$37951^2 = 1440278401$. We remark that with only the PSC, there would be 87157 exceptions, so using the MPSC reduces the number of candidates by 46% and reduces the time taken to test the candidates (see Section 2.2) by an estimated 61%. This represents an instance when the MPSC makes a substantial and not merely an incidental contribution to a computation.

2.2. Testing the possible exceptions. Next we aim to test each putative exception directly, by exhibiting, for each $a \in \mathbb{F}_q$, a primitive pair $(\xi, \xi + \xi^{-1})$ satisfying $\mathrm{Tr}(\xi) = a$. Although greatly reduced from the initial set of all $q < 8 \times 10^{12}$ from [1, Theorem 7.2], the candidate list is still rather large, so we employed an optimised search strategy based on the following lemma.

LEMMA 2.1. *Let $g \in \mathbb{F}_q^\times$ be a primitive root, let $d \in \mathbb{Z}$ and define the polynomial $P = x^3 - x^2 + g^{d-1}x - g^d \in \mathbb{F}_q[x]$. Suppose P is irreducible. Let $\xi_0 = x + (P)$ be a root of P in $\mathbb{F}_q[x]/(P) \cong \mathbb{F}_{q^3}$ and assume that ξ_0 is not a pth power in $\mathbb{F}_{q^3}$ for any $p \mid q^2 + q + 1$. Then for any $k \in \mathbb{Z}$ such that $\gcd(3k + d, q - 1) = 1$, $\xi_k := g^k \xi_0$ is a primitive root of $\mathbb{F}_{q^3}^\times$ satisfying $\mathrm{Tr}(\xi_k) = g^k$ and $\mathrm{Tr}(\xi_k^{-1}) = g^{-k-1}$.*

PROOF. Note that ξ_0 has trace 1 and norm g^d, so ξ_k has trace g^k and norm $\xi_k^{q^2+q+1} = g^{3k+d}$. Furthermore,

$$\xi_0^3 - \xi_0^2 + g^{d-1}\xi_0 - g^d = 0 \Longrightarrow \xi_0^{-3} - g^{-1}\xi_0^{-2} + g^{-d}\xi_0^{-1} - g^{-d} = 0,$$

so $\mathrm{Tr}(\xi_k^{-1}) = g^{-k}\,\mathrm{Tr}(\xi_0^{-1}) = g^{-k-1}$.

Let p be a prime dividing $q^3 - 1$. If $p \mid q^2 + q + 1$, then

$$\xi_k^{(q^3-1)/p} = (g^k\xi_0)^{(q^3-1)/p} = g^{k(q^2+q+1)(q-1)/p}\xi_0^{(q^3-1)/p} = \xi_0^{(q^3-1)/p} \neq 1,$$

since ξ_0 is not a pth power. However, if $p \mid q - 1$, then

$$\xi_k^{(q^3-1)/p} = \xi_k^{(q^2+q+1)(q-1)/p} = g^{(3k+d)(q-1)/p} \neq 1,$$

since $\gcd(3k + d, q - 1) = 1$. Hence ξ_k is a primitive root. □

REMARK 2.2. If $q \equiv 1 \pmod 3$, then the hypotheses of Lemma 2.1 imply that $3 \nmid d$. Hence there always exists k such that $\gcd(3k + d, q - 1) = 1$, and this condition is equivalent to $\gcd(k + \bar{d}, r) = 1$, where $r = \prod_{p \mid q-1,\, p \neq 3} p$ and $3\bar{d} \equiv d \pmod r$.

Thanks to the symmetry between ξ and ξ^{-1}, if we find a ξ that works for a given g^k via Lemma 2.1, we also obtain a solution for g^{-k-1}. Furthermore, when $q \equiv 1 \pmod 4$, $\alpha \in \mathbb{F}_{q^3}^\times$ is primitive if and only if $-\alpha$ is primitive, and thus a solution for g^k yields one for $-g^k$ by replacing ξ with $-\xi$. Therefore, to find a solution for every $a \in \mathbb{F}_q^\times$, it suffices to check $k \in \{0, \ldots, K - 1\}$, where

$$K = \begin{cases} \lfloor q/4 \rfloor & \text{if } q \equiv 1 \pmod 4, \\ \lfloor q/2 \rfloor & \text{otherwise.} \end{cases}$$

https://doi.org/10.1017/S0004972722000442 Published online by Cambridge University Press

Note that this does not handle $a = 0$, for which we conduct a separate search over randomly chosen $\xi \in \mathbb{F}_{q^3}$ of trace 0.

Our strategy for applying Lemma 2.1 is as follows. First we choose random values of $d \pmod{q-1}$ until we find sufficiently many (2^{10} in our implementation) satisfying the hypotheses. (We allow repetition among the d values, but for some small q there are no suitable d, in which case we fall back on a brute-force search strategy.) For each d, we precompute and store $\bar{d} = d/3 \bmod r$ and g^{-d}, so we can quickly compute $\xi_k + \xi_k^{-1} = a^{-1}g^{-d}(\xi_0^2 - \xi_0) + a\xi_0 + a^{-1}g^{-1}$ given the pair $(a, a^{-1}) = (g^k, g^{-k})$. Then for each k, we run through the precomputed values of d satisfying $\gcd(k + \bar{d}, r) = 1$, and check whether $(\xi_k + \xi_k^{-1})^{(q^3-1)/p} \neq 1]$ for every prime $p \mid q^3 - 1$.

Thanks to Lemma 2.1, our test for whether ξ_k itself is a primitive root, which is just a coprimality check, is very fast. In fact, since we run through values of k in linear order, we could avoid computing the gcd by keeping track of $k \bmod p$ and $-\bar{d} \bmod p$ for each prime $p \mid r$, and looking for collisions between them. However, in our numerical tests, this gave only a small reduction in the overall running time.

We are therefore able to save a factor of roughly $(q^3 - 1)/\varphi(q^3 - 1)$ over a more naive approach that tests both ξ and $\xi + \xi^{-1}$. Combined with the savings from symmetries noted above, we estimate that the total running time of our algorithm over the candidate set is approximately 1/15th of what it would be with a direct approach testing random $\xi \in \mathbb{F}_{q^3}$ of trace a for every $a \in \mathbb{F}_q$.

We are not aware of any reason why this strategy should fail systematically, though we observed that for some fields of small characteristic (the largest q we encountered is $3^{12} = 531441$), $\xi_k + \xi_k^{-1}$ is always a square for a particular k. Whenever this occurred, we fell back on a more straightforward randomised search for ξ of trace g^k and g^{-k-1}.

We used `PARI/GP` [6] to handle the brute-force search for $q \leq 211$, as well as the remaining composite q with a basic implementation of the above strategy. For prime $q > 211$, we used Andrew Sutherland's fast `C` library `ff_poly` [5] for arithmetic in $\mathbb{F}_q[x]/(P)$, together with an implementation of the Bos–Coster algorithm for vector addition chains described in [3, Section 4]. The total running time for all parts was approximately 13 days on a computer with 64 cores (AMD Opteron processors running at 2.5 GHz). The same system handles the largest value $q = 4708304701$ in approximately one hour. Our code is available upon request.

References

[1] A. R. Booker, S. D. Cohen, N. Leong and T. Trudgian, 'Primitive elements with prescribed traces', Preprint, 2022, arXiv:2112.10268.

[2] S. D. Cohen and A. Gupta, 'Primitive element pairs with a prescribed trace in the quartic extension of a finite field', *J. Algebra Appl.* **20**(6) (2021), Article no. 2150168.

[3] P. de Rooij, 'Efficient exponentiation using precomputation and vector addition chains', in: *Advances in Cryptology—EUROCRYPT'94 (Perugia)* (ed. A. De Santis), Lecture Notes in Computer Science, 950 (Springer, Berlin, 1995), 389–399.

[4] A. Gupta, R. K. Sharma and S. D. Cohen, 'Primitive element pairs with one prescribed trace over a finite field', *Finite Fields Appl.* **54** (2018), 1–14.

[5] A. V. Sutherland, ff_poly, version 1.2.7, 2015, available from https://math.mit.edu/~drew/ff_poly_v1.2.7.tar.
[6] The PARI Group, PARI/GP version 2.13.3, Univ. Bordeaux, 2021, available from http://pari.math.u-bordeaux.fr/.

ANDREW R. BOOKER, School of Mathematics,
University of Bristol, Bristol BS8 1UG, UK
e-mail: andrew.booker@bristol.ac.uk

STEPHEN D. COHEN, School of Mathematics and Statistics,
University of Glasgow, Glasgow G12 8QQ, UK
e-mail: Stephen.Cohen@glasgow.ac.uk

NICOL LEONG, School of Science,
The University of New South Wales Canberra, Canberra ACT 2610, Australia
e-mail: nicol.leong@adfa.edu.au

TIM TRUDGIAN, School of Science,
The University of New South Wales Canberra, Canberra ACT 2610, Australia
e-mail: t.trudgian@adfa.edu.au

https://doi.org/10.1017/S0004972722000442 Published online by Cambridge University Press