
Peer reviewed version

License (if available): CC BY-NC-ND

Link to published version (if available): 10.1017/S0004972722000442

Link to publication record in Explore Bristol Research

PDF-document

This is the accepted author manuscript (AAM). The final published version (version of record) is available online via Cambridge University Press at https://doi.org/10.1017/S0004972722000442. Please refer to any applicable terms of use of the publisher.

**University of Bristol - Explore Bristol Research**

**General rights**

This document is made available in accordance with publisher policies. Please cite only the published version using the reference above. Full terms of use are available: http://www.bristol.ac.uk/red/research-policy/pure/user-guides/ebr-terms/
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

Abstract. We prove that for any prime power $q \in \{3, 4, 5\}$, the cubic extension $F_{q^3}$ of the finite field $F_q$ contains a primitive element $\xi$ such that $\xi + \xi^{-1}$ is also primitive, and $\text{Tr}_{F_{q^3}/F_q}(\xi) = a$ for any prescribed $a \in F_q$. This completes the proof of a conjecture of Gupta, Sharma, and Cohen concerning the analogous problem over an extension of arbitrary degree $n \geq 3$.

1. Introduction

Let $q$ be a prime power and $n$ an integer at least 3, and let $F_{q^n}$ denote a degree-$n$ extension of the finite field $F_q$. We say that $(q, n) \in \mathcal{P}$ if, for any $a \in F_q$, we can find a primitive element $\xi \in F_{q^n}$ such that $\xi + \xi^{-1}$ is also primitive and $\text{Tr}(\xi) = a$. This problem was considered by Gupta, Sharma, and Cohen [3], who proved a complete result for $n \geq 5$. We refer the reader to [3] for an introduction to similar problems. Cohen and Gupta [2] extended the work of [3], providing a complete result for $n = 4$ and some preliminary results for $n = 3$. We improved the latter results in [1, §7], showing in particular that $(q, 3) \in \mathcal{P}$ 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 [3, Conjecture 1].

Theorem 1.1. We have $(q, n) \in \mathcal{P}$ 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).

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

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

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

(1) \[\theta^2 \delta > 2\varepsilon \quad \text{and} \quad q^{1/2} > \frac{C_q\left(\theta^2 4^{\omega(k)}(2\omega(P) - 1 + 2\delta) + \omega(L) - \varepsilon\right)}{\theta^2 \delta - 2\varepsilon}.\]

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) reduces to

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

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 \( u = (q^2 + q + 1) \prod_{p < X} p^{- \text{ord}_p(q^2 + q + 1)} \) 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

\[
\sum_{i=1}^{s} \frac{1}{p_i} \leq \frac{\lfloor \log u \rfloor}{X}.
\]

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 379512 = 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 [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 \( \text{Tr}(\xi) = a \).

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 set \( P = x^3 - x^2 + g^{d-1}x - g^d \in \mathbb{F}_q[x] \). 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 \( \xi_0 \) is not a \( p \)-th power in \( \mathbb{F}_{q^3} \) for any \( p | q^2 + q + 1 \). 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 \( \text{Tr}(\xi_k) = g^k \) and \( \text{Tr}(\xi_k^{-1}) = g^{-k-1} \).

**Proof.** Note that \( \xi_0 \) has trace 1 and norm \( g^d \), so \( \xi_k \) has trace \( g^k \) and norm \( g^{k+q+1} \). Furthermore,

\[
\xi_0^{-3} - \xi_0^{-2} + g^{d-1} \xi_0 - g^d = 0 \implies \xi_0^{-3} - g^{-1} \xi_0^{-2} + g^{-d} \xi_0^{-1} - g^{-d} = 0,
\]

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

Let \( p \) be a prime dividing \( q^3 - 1 \). If \( p | q^2 + q + 1 \) then

\[
\xi_k^{\frac{q^3 - 1}{p}} = (g^k \xi_0)^{\frac{q^3 - 1}{p}} = g^{\frac{k+q+1}{p}(q-1)} \xi_0^{\frac{q^3 - 1}{p}} = \xi_0^\frac{q^3 - 1}{p} \neq 1,
\]

since \( \xi_0 \) is not a \( p \)-th power. On the other hand, if \( p | q - 1 \) then

\[
\frac{q^3 - 1}{p} = \frac{(q^2 + q + 1)q - 1}{p} = g^{(3k+d)q - 1} \neq 1,
\]

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

\[
\xi_0^{\frac{q^3 - 1}{p}} = \xi_0^\frac{q^3 - 1}{p} \neq 1.
\]
since $\gcd(3k + d, q - 1) = 1$. Hence $\xi_k$ is a primitive root.

\begin{remark}
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 $\gcd(k + d, r) = 1$, where $r = \prod_{p \neq 3} p$ and $3d \equiv d \pmod{r}$.

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

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

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 $d \mod (q - 1)$ 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 $\bar{d} = d/3 \mod r$ and $g^{-d}$, so we can quickly compute $\xi_k + \xi_k^{-1} = a^{-1}g^{-d}(\xi_0^d - \xi_0) + a\xi_0 + a^{-1}g^{-1}$ given the pair $(a, a^{-1}) = (g^k, g^{-k})$. Then for each $k$ we run through the precomputed values of $d$ satisfying $\gcd(k + d, r) = 1$, 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 $\xi_k$ itself is a primitive root is very fast (just a coprimality check), so we save a factor of roughly $(q^3 - 1)/\varphi(q^3 - 1)$ over a more naive approach that tests both $\xi$ 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 0 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 $\xi$ of trace $g^k$ and $g^{-k^{-1}}$.

We used \texttt{PARI/GP} \cite{pari} 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 \texttt{C} library \texttt{ff_poly} \cite{suth} for arithmetic in $\mathbb{F}_q[x]/(P)$, together with an implementation of the Bos–Coster algorithm for vector addition chains described in \cite{bc} §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.

\begin{references}

\footnote{In fact, since we run through values of $k$ in linear order, we could avoid computing the gcd by keeping track of $k \mod p$ and $-d \mod p$ 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.}
\end{references}


**University of Bristol, England**
*Email address*: andrew.booker@bristol.ac.uk

**University of Glasgow, Scotland**
*Email address*: Stephen.Cohen@glasgow.ac.uk

**The University of New South Wales Canberra, Australia**
*Email address*: nicol.leong@adfa.edu.au
*Email address*: t.trudgian@adfa.edu.au