Bull. Aust. Math. Soc. **101** (2020), 40–55
doi:10.1017/S0004972719000674

PERMUTATION POLYNOMIALS OF DEGREE 8 OVER FINITE FIELDS OF ODD CHARACTERISTIC

XIANG FAN

(Received 14 April 2019; accepted 14 May 2019; first published online 9 July 2019)

Abstract

We give an algorithmic generalisation of Dickson's method of classifying permutation polynomials (PPs) of a given degree d over finite fields. Dickson's idea is to formulate from Hermite's criterion several polynomial equations satisfied by the coefficients of an arbitrary PP of degree d. Previous classifications of PPs of degree at most 6 were essentially deduced from manual analysis of these polynomial equations, but this approach is no longer viable for $d > 6$. Our idea is to calculate some radicals of ideals generated by the polynomials, implemented by a computer algebra system. Our algorithms running in SageMath 8.6 on a personal computer work very fast to determine all PPs of degree 8 over an arbitrary finite field of odd order $q > 8$. Such PPs exist if and only if $q \in \{11, 13, 19, 23, 27, 29, 31\}$ and are explicitly listed in normalised form.

2010 *Mathematics subject classification*: primary 11T06; secondary 12Y05.

Keywords and phrases: permutation polynomial, Hermite's criterion, Carlitz conjecture, SageMath.

1. Introduction

Denote by $\mathbb{F}_q$ the finite field of order q and write $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$. An arbitrary map from $\mathbb{F}_q$ to itself can be represented by a polynomial f in $\mathbb{F}_q[x]$. We call f a *permutation polynomial* (PP) over $\mathbb{F}_q$ if it represents a permutation of $\mathbb{F}_q$.

Beginning with Hermite [11] and Dickson [4] in the nineteenth century, the study of PPs over finite fields aroused growing interest, partly due to its valuable applications in other areas of mathematics and engineering, such as cryptography, coding theory, combinatorial designs and so on. For example, a special class of PPs called Dickson polynomials (introduced in [4]) played a key role in the breakthrough construction by Ding and Yuan [5] of a new family of skew Hadamard difference sets in combinatorics.

Although dozens of classes of PPs (with good appearance or properties) have been found (see [12, 16] for recent surveys), the classification problems of PPs of prescribed forms are still challenging. In his pioneering thesis [4] on PPs, Dickson discussed the

This work was partially supported by the Natural Science Foundation of Guangdong Province (No. 2018A030310080). The author was also sponsored by the National Natural Science Foundation of China (No. 11801579).

classification of all PPs of a given degree d over an arbitrary finite field $\mathbb{F}_q$. Replacing PPs by their reductions modulo $x^q - x$ if necessary, it is assumed that $d < q$. Results obtained from Dickson's classification cover:

- $d \leqslant 5$ with any q and $d = 6$ with any odd q (Dickson [4], 1896–1897);
- $d = 6$ or 7 with any even q (Li, Chandler and Xiang [14], 2010);
- $d = 7$ with any odd q [7] and $d = 8$ with any even q [8].

The present paper classifies all PPs of degree 8 over an arbitrary $\mathbb{F}_q$ of odd order $q > 8$. More importantly, we provide an algorithmic generalisation of Dickson's method of classifying PPs of a given degree d over finite fields. Dickson's main idea is to formulate from Hermite's criterion several polynomial equations satisfied by the coefficients of an arbitrary PP of degree d. Previously known classifications of PPs of degree at most 6 were essentially deduced from manual analysis of these polynomial equations. However, the polynomials needed for that purpose when $d > 6$ are too complicated to solve by hand. Our idea is to make them more solvable by calculating some radicals of ideals generated by some of them, implemented on a computer algebra system. Our algorithms running in SageMath 8.6 on a personal computer work very fast to determine all PPs of degree 8 over finite fields of odd order, as described below.

THEOREM 1.1. *PPs of degree* 8 *exist over* $\mathbb{F}_q$ *of odd order* $q > 8$ *if and only if*

$$q \in \{11, 13, 19, 23, 27, 29, 31\}.$$

All PPs of degree 8 *in normalised form over such* $\mathbb{F}_q$ *are explicitly listed in Propositions 4.2–4.8.*

All previous classifications of PPs of degree at most 7 can be recovered very quickly by our approach, with calculations implemented on a personal computer. This approach is different from that used in [7] classifying PPs of degree 7. Roughly speaking, [7] uses only two simple equations provided by Hermite's criterion and its main algorithm is a brute-force search (though optimised by linear transformations), but this cannot work in an acceptable time for degree 8 with $q > 100$. The approach here will work for degrees a little larger than 8 on a more powerful computer. We have already done some computations for degree 9.

The structure of this paper is as follows. Section 2 establishes Algorithm 1 for explicit polynomial equations on coefficients of PPs of degree 8 by Hermite's criterion. Section 3 verifies the nonexistence of PPs of degree 8 over finite fields of odd order $q > 31$, by calculations of some radicals of ideals generated by polynomials provided by Algorithm 1. Section 4 explicitly lists all PPs of degree 8 in normalised form over $\mathbb{F}_q$ of odd order q such that $8 < q \leqslant 31$, by a brute-force search.

2. Hermite's criterion

The main tool for the classification is *Hermite's criterion* for PPs over finite fields. It was introduced by Dickson [4] as a generalisation of the prime field case

https://doi.org/10.1017/S0004972719000674 Published online by Cambridge University Press

in Hermite [11] and is sometimes called the Hermite–Dickson criterion. We state an explicit version of it from [15], using the following notation:

- $\mathbb{N} = \{n \in \mathbb{Z} : n \geqslant 0\}$;
- for $n \in \mathbb{N}$ and $f \in \mathbb{F}_q[x]$, the coefficient of x^n in $f(x)$ is $[x^n : f]$ and the degree of f is $\deg(f) = \max\{n \in \mathbb{N} : [x^n : f] \neq 0\}$, that is, $f(x) = \sum_{n=0}^{\deg(f)} [x^n : f] \cdot x^n$ for any nonzero $f \in \mathbb{F}_q[x]$;
- for $t \in \mathbb{R}$, let $\lfloor t \rfloor$ denote the largest integer $\leqslant t$.

Lemma 2.1 (Hermite's criterion [15, Theorem 7.6]). *Let $f \in \mathbb{F}_q[x]$. A necessary and sufficient condition for f to be a PP over $\mathbb{F}_q$ is that*

$$\sum_{w=1}^{\lfloor \deg(f^m)/(q-1) \rfloor} [x^{w(q-1)} : f^m] \begin{cases} = 0 & \text{for } 1 \leqslant m \leqslant q-2, \\ \neq 0 & \text{for } m = q-1. \end{cases}$$

Let us show how to calculate $[x^n : f^m]$ explicitly with the help of multinomial coefficients. Consider a polynomial f of degree d in $\mathbb{F}_q[x]$. Suppose that $\gcd(d, q) = 1$ (noting that we aim for $d = 8$ with an odd q). By linear transformations, we may assume f to be *in normalised form*, that is, $f(x) = x^d + \sum_{i=1}^{d-2} a_i x^i$ with all $a_i \in \mathbb{F}_q$. For integers $j, j_1, j_2, \ldots, j_d$, define the associated *multinomial coefficient*

$$\binom{j}{j_1, j_2, \ldots, j_d} := \begin{cases} \dfrac{j!}{j_1! j_2! \cdots j_d!} & \text{if } j = j_1 + j_2 + \cdots + j_d \text{ and all } j_1, \ldots, j_d \geqslant 0, \\ 0 & \text{otherwise.} \end{cases}$$

By the multinomial theorem,

$$f(x)^m = \sum_{\sum_{i=1}^{d-2} j_i + j_d = m} \binom{m}{j_1, j_2, \ldots, j_{d-2}, j_d} \cdot \prod_{i=1}^{d-2} a_i^{j_i} \cdot x^{\sum_{i=1}^{d-2} i j_i + d j_d}.$$

Therefore,

$$\begin{aligned} [x^n : f(x)^m] &= \sum_{\substack{\sum_{i=1}^{d-2} j_i + j_d = m \\ \sum_{i=1}^{d-2} i j_i + d j_d = n.}} \binom{m}{j_1, j_2, \ldots, j_{d-2}, j_d} \prod_{i=1}^{d-2} a_i^{j_i} \\ &= \sum_{\sum_{i=1}^{d-2} (d-i) j_i = dm - n} \binom{m}{j_1, j_2, \ldots, j_{d-2}, m - \sum_{i=1}^{d-2} j_i} \prod_{i=1}^{d-2} a_i^{j_i}. \end{aligned}$$

Define a multivariate polynomial $\mathbf{HC}_d(q, m)$ in $\mathbb{F}_q[x_1, x_2, \ldots, x_{d-2}]$ by

$$\mathbf{HC}_d(q, m) := \sum_{w=1}^{\lfloor dm/(q-1) \rfloor} \sum_{\sum_{i=1}^{d-2} (d-i) j_i = dm - w(q-1)} \binom{m}{j_1, j_2, \ldots, j_{d-2}, m - \sum_{i=1}^{d-2} j_i} \prod_{i=1}^{d-2} x_i^{j_i}.$$

https://doi.org/10.1017/S0004972719000674 Published online by Cambridge University Press

Then Hermite's criterion asserts that $f(x) = x^d + \sum_{i=1}^{d-2} a_i x^i$ (with all $a_i \in \mathbb{F}_q$) is a PP over $\mathbb{F}_q$ if and only if

$$\mathbf{HC}_d(q,m)(a_1, a_2, \ldots, a_{d-2}) \begin{cases} = 0 & \text{for } 1 \leqslant m \leqslant q-2, \\ \neq 0 & \text{for } m = q-1. \end{cases}$$

In particular, when $q \equiv 1 \pmod{d}$, there is no PP of degree d over $\mathbb{F}_q$ because $\mathbf{HC}_d(q, (q-1)/d) = 1$. On the other hand, if $q \not\equiv 0, 1 \pmod{d}$, then $\mathbf{HC}_d(q,m) = 0$ when $m \leqslant \lfloor q/d \rfloor = \lfloor (q-1)/d \rfloor < (q-1)/d$.

When $\gcd(d,q) = 1$, previous classifications of PPs of degree $d \leqslant 6$ were essentially deduced from manual analysis of the equations $\mathbf{HC}_d(q,m)(a_1, a_2, \ldots, a_{d-2}) = 0$ for $\lfloor q/d \rfloor + 1 \leqslant m \leqslant \lfloor q/d \rfloor + d - 2$, which nearly determine $(a_1, a_2, \ldots, a_{d-2}) \in \mathbb{F}_q^{d-2}$ when $q > d(d-2)$. However, when $d > 6$, these polynomials $\mathbf{HC}_d(q,m)$ are too long to write down explicitly, let alone to solve by hand. Our main idea is to solve them by calculating some radicals of ideals generated by some $\mathbf{HC}_d(q,m)$, implemented on a computer algebra system (CAS) running on a personal computer.

All algorithms of this paper run in SageMath [17] (version 8.6), a free open-source CAS combining the power of many existing open-source packages, such as NumPy, SciPy, Sympy, Maxima, R, GAP, Singular and many more, into a common Python-based interface.

For $d = 8$, the multivariate polynomial $\mathbf{HC}_8(q,m)$ in $\mathbb{F}_q[x_1, x_2, \ldots, x_6]$ is

$$\mathbf{HC}_8(q,m) := \sum_{\substack{7j_1+6j_2+5j_3+4j_4+3j_5+2j_6=8m-n \\ n\in\{w(q-1):\ 1\leqslant w\leqslant\lfloor 8m/(q-1)\rfloor\}}} \binom{m}{j_1, j_2, \ldots, j_6, m - \sum_{i=1}^{6} j_i} \prod_{i=1}^{6} x_i^{j_i}.$$

Algorithm 1 realises $\mathbf{HC}_8(q,m)$ as a SageMath function `HC8`(q,m), outputting a multivariate polynomial in $\mathbb{F}_q[x_1, x_2, \ldots, x_6]$.

3. Nonexistence for odd $q > 31$

In an address before the Mathematical Association of America in 1966, Carlitz conjectured the existence of a constant C_n for each positive even integer n such that no PP of degree n exists over $\mathbb{F}_q$ of odd order $q > C_n$. When $\gcd(n,q) = 1$, this was verified by Hayes [10] in the following stronger form.

Lemma 3.1 [10, Theorem 3.4]. *Given a positive integer n, there is a constant C_n (depending only on n) such that for any prime power $q > C_n$ with* $\gcd(n,q) = 1$, *a PP of degree n exists over $\mathbb{F}_q$ only if* $\gcd(n, q-1) = 1$.

Lemma 3.1 without the assumption $\gcd(n,q) = 1$ is called the *Carlitz–Wan conjecture*, now a theorem by [2, 9]. For Lemma 3.1 (and the Carlitz–Wan conjecture) to hold, C_n can be taken as n^4 by von zur Gathen [18], as $n^2(n-2)^2$ by Chahal and Ghorpade [1] and as

$$\left\lfloor \left(\frac{(n-2)(n-3) + \sqrt{(n-2)^2(n-3)^2 + 8n - 12}}{2} \right)^2 \right\rfloor$$

https://doi.org/10.1017/S0004972719000674 Published online by Cambridge University Press

Algorithm 1 To calculate $\mathbf{HC}_8(q, m)$ in $\mathbb{F}_q[x_1, x_2, \ldots, x_6]$

```
def HC8(q,m):
    HC = 0; K.<x1,x2,x3,x4,x5,x6> = PolynomialRing(GF(q))
    for n in range(q-1,8*m+1,q-1):
        u = 8*m-n
        for j1 in range(u//7+1):
            for j2 in range((u-7*j1)//6+1):
                for j3 in range((u-7*j1-6*j2)//5+1):
                    for j4 in range((u-7*j1-6*j2-5*j3)//4+1):
                        for j5 in range((u-7*j1-6*j2-5*j3-4*j4)//3+1):
                            v = u-7*j1-6*j2-5*j3-4*j4-3*j5
                            if is_odd(v): continue
                            j6 = v//2; j = j1+j2+j3+j4+j5+j6
                            if j>m: continue
                            c = multinomial(j1,j2,j3,j4,j5,j6,m-j)
                            HC+=c*x1^j1*x2^j2*x3^j3*x4^j4*x5^j5*x6^j6
    return HC
```

by [6]. In particular, when $n = 8$, the above expression is 925. The greatest prime power below 925 is 919. So, C_8 can be taken as 919.

We will refine the bound for C_8 to 31 for the original version of the Carlitz conjecture: no PP of degree 8 exists over $\mathbb{F}_q$ of odd order $q > 31$. The method is to calculate some radicals of ideals generated by some $\mathbf{HC}_8(q, m)$ as follows.

Consider a PP $f \in \mathbb{F}_q[x]$ of degree 8 over $\mathbb{F}_q$ of odd order $q = 8t + s$ with $1 \leqslant t \in \mathbb{Z}$ and $s \in \{3, 5, 7\}$, where $s \neq 1$ by Hermite's criterion. Without loss of generality, let $f(x) = x^8 + \sum_{i=1}^{6} a_i x^i$ (in normalised form) with all $a_i \in \mathbb{F}_q$. Hermite's criterion ensures that $(a_1, a_2, \ldots, a_6) \in \mathbb{F}_q^6$ is a vanishing point of each $\mathbf{HC}_8(q, m)$ with $1 \leqslant m \leqslant q - 2$, and thus of every polynomial in the radical of any ideal in $\mathbb{F}_q[x_1, x_2, \ldots, x_6]$ generated by some of them. The *radical* $\sqrt{I}$ of an ideal I in a ring R is

$$\sqrt{I} := \{g \in R : g^m \in I \text{ for some positive integer } m\}.$$

In particular, for $1 \leqslant k \in \mathbb{Z}$, we calculate the radical $\mathbf{Rad}_8(q, k)$ of the ideal generated by k polynomials $\mathbf{HC}_8(q, m)$ with $\lfloor q/8 \rfloor + 1 \leqslant m \leqslant \lfloor q/8 \rfloor + k$, by the SageMath function Rad8(q, k) defined in Algorithm 2.

Algorithm 2 To calculate the radical $\mathbf{Rad}_8(q, k)$

```
def Rad8(q,k):
    return Ideal([HC8(q,q//8+1+i) for i in range(k)]).radical()
```

SageMath uses Singular [3] to implement the calculation for radicals of ideals in multivariate polynomial rings over fields, based on the algorithm of Kemper [13] in positive characteristic.

https://doi.org/10.1017/S0004972719000674 Published online by Cambridge University Press

Below, we list the following $\mathbf{Rad}_8(q,k)$ for the odd prime powers $q \not\equiv 1 \pmod 8$ with $31 < q \leqslant 919$ as outputs of Algorithm 2 in SageMath 8.6, in the form $\texttt{Ideal}(g_1, g_2, \ldots, g_s)$ denoting the ideal generated by $g_1, g_2, \ldots, g_s$ in $\mathbb{F}_q[x_1, x_2, \ldots, x_6]$. By definition, every g_i in the output vanishes at $(a_1, a_2, \ldots, a_6) \in \mathbb{F}_q^6$ for any PP of the form $f(x) = x^8 + \sum_{i=1}^{6} a_i x^i$ over $\mathbb{F}_q$. For each q, we choose a suitable k to manufacture the g_i good enough for our purpose. Our choice of k might not be minimal, but it makes the running time of $\texttt{Rad8}(q,k)$ for the same result as short as possible.

- $\mathbf{Rad}_8(37,8) = \texttt{Ideal}(1)$. So, no PP of degree 8 exists over $\mathbb{F}_{37}$.
- $\mathbf{Rad}_8(43,7) = \texttt{Ideal}(x_6, x_5, x_4, x_{3,}x_2, x_1)$. Since $f(x) = x^8$ is clearly not a PP over $\mathbb{F}_{43}$, no PP of degree 8 exists over $\mathbb{F}_{43}$.
- $\mathbf{Rad}_8(47,7) = \texttt{Ideal}(x_6, x_5, x_4, x_{3,}x_2, x_1)$. So, no PP of degree 8 exists over $\mathbb{F}_{47}$.
- $\mathbf{Rad}_8(53,7) = \texttt{Ideal}(1)$. So, no PP of degree 8 exists over $\mathbb{F}_{53}$.

The above calculations indicate that no PP of degree 8 exists over $\mathbb{F}_q$ of odd order q if $31 < q \leqslant 53$.

- For any prime power $q \equiv 7 \pmod 8$ with $53 < q \leqslant 919$,

$$\mathbf{Rad}_8(q,7) = \texttt{Ideal}(x_6, x_5, x_{3,}x_2, x_1)$$

  by the output of the following piece of SageMath code:

```
for q in range(54,920):
    if q%8==7 and is_prime_power(q): print Rad8(q,7)
```

  Then $f(x) = x^8 + a_4x^4$. Now $q = 8t + 7$ with $1 \leqslant t \in \mathbb{Z}$. For $m = \lfloor q/4 \rfloor + 1 = 2t + 2 < q - 1$, by Hermite's criterion,

$$0 = \mathbf{HC}_8(q,m)(0,0,0,a_4,0,0) = \sum_{\substack{4j_4 = 16t+16-n \\ n \in \{w(8t+6):\ 1 \leqslant w \leqslant \lfloor (16t+16)/(8t+6) \rfloor\}}} \binom{m}{j_4, m-j_4} a_4^{j_4}$$

$$= \sum_{4j_4 = 16t+16-2(8t+6)} \binom{m}{j_4, m-j_4} a_4^{j_4} = ma_4 \in \mathbb{F}_q.$$

  Note that $\gcd(m,q) = 1$, as $q = 4m - 1$; thus, $a_4 = 0$. Since $f(x) = x^8$ is not a PP over $\mathbb{F}_q$, no PP of degree 8 exists over $\mathbb{F}_q$ if $q \equiv 7 \pmod 8$ and $53 < q \leqslant 919$.
- For any prime $q \equiv 3 \pmod 8$ with $53 < q \leqslant 919$,

$$\mathbf{Rad}_8(q,7) = \texttt{Ideal}(x_5, x_3, x_1, x_4x_6 - 10x_2, x_6^3 - 32x_2).$$

- For any prime $q \equiv 5 \pmod 8$ with $53 < q \leqslant 919$,

$$\mathbf{Rad}_8(q,7) = \texttt{Ideal}(x_5, x_3, x_1, x_6^2 + \alpha(q)x_4, x_4x_6 - 10x_2),$$

  where $\alpha(q) \in \mathbb{F}_q$ depends on q.

https://doi.org/10.1017/S0004972719000674 Published online by Cambridge University Press

- For any nonprime prime power $q \equiv 3$ or $5 \pmod 8$ with $53 < q \leqslant 919$, that is, $q = 5^3$ or 3^5,

$$\mathbf{Rad}_8(5^3, 9) = \mathtt{Ideal}(x_5, x_4, x_3, x_1, x_6^3 - 2x_2),$$
$$\mathbf{Rad}_8(3^5, 19) = \mathtt{Ideal}(x_5, x_3, x_1, x_4x_6 - x_2, x_6^3 + x_2, x_2x_6^2 + x_2x_4, x_2x_4^2 + x_2^2x_6).$$

For any prime power $q \equiv 3$ or $5 \pmod 8$ with $53 < q \leqslant 919$, the above calculations imply that $a_1 = a_3 = a_5 = 0$ by Hermite's criterion. We calculate $\mathbf{HC}_8(q, m)(0, x_2, 0, x_4, 0, x_6)$ by the SageMath function $\mathtt{HC8new}(q, m)$ in Algorithm 3.

Algorithm 3 To calculate $\mathbf{HC}_8(q, m)(0, x_2, 0, x_4, 0, x_6)$

```
def HC8new(q,m):
    HC = 0; K.<x1,x2,x3,x4,x5,x6> = PolynomialRing(GF(q))
    for n in range(q-1,8*m+1,q-1):
        u = 8*m-n
        for j2 in range(u//6+1):
            for j4 in range((u-6*j2)//4+1):
                v = u-6*j2-4*j4
                if is_odd(v): continue
                j6 = v//2; j = j2+j4+j6
                if j<=m:
                    HC += multinomial(j2,j4,j6,m-j)*x2^j2*x4^j4*x6^j6
    return HC
```

Inspired by the case $q \equiv 7 \pmod 8$, we try to run $\mathtt{HC8new}(q, m)$ with $m = \lfloor q/4 \rfloor + 1$. After some experiments, we fortunately see that the output of Algorithm 4 in SageMath 8.6, which prints $\mathtt{Ideal}(x_6, x_5, x_4, x_3, x_2, x_1)$ for every prime power $q \equiv 3$ or $5 \pmod 8$ with $53 < q \leqslant 919$, verifies the nonexistence of PPs of degree 8 over $\mathbb{F}_q$ for these q.

Algorithm 4 Nonexistence of degree 8 PPs over $\mathbb{F}_q$ for $q \equiv 3, 5 \pmod 8$, $53 < q \leqslant 919$

```
for q in prime_range(54,920)+[5^3,3^5]:
    if q%8 in [1,7]: continue
    K.<x1,x2,x3,x4,x5,x6> = PolynomialRing(GF(q))
    if q == 5^3: k = 9
    elif q == 3^5: k = 19
    else: k = 7
    R = Rad8(q,k).gens()
    if x1 in R and x3 in R and x5 in R:
        print(Ideal(R+[HC8new(q,q//4+1)]).radical())
    else: print("Fail when q = "+str(q))
```

In conclusion, the above calculations for the odd prime powers $q \not\equiv 1 \pmod 8$ with $31 < q \leqslant 919$, together with Lemma 3.1 in which we can take $C_8 = 919$ by [6], ensure the following nonexistence result.

THEOREM 3.2. *No PP of degree* 8 *exists over any finite field* $\mathbb{F}_q$ *of odd order* $q > 31$.

https://doi.org/10.1017/S0004972719000674 Published online by Cambridge University Press

4. Explicit results

This section aims for a complete list of all PPs of degree 8 in normalised form over $\mathbb{F}_q$ of odd order $q > 8$. Since $q \not\equiv 1 \pmod 8$ by Hermite's criterion and $q \leqslant 31$ by Theorem 3.2, we indeed have $q \in \{11, 13, 19, 23, 27, 29, 31\}$.

To make the resulting list as short as possible, we first investigate the linear relations among polynomials of degree 8. Two polynomials f and g in $\mathbb{F}_q[x]$ are said to be *related by linear transformations* (*linearly related* for short) if there exist $s, t \in \mathbb{F}_q^*$ and $u, v \in \mathbb{F}_q$ such that $g(x) = sf(tx + u) + v$. Note that linearly related f and g have the same degree and f is a PP over $\mathbb{F}_q$ if and only if so is g.

Proposition 4.1. *Let q be an odd prime power. Then each polynomial of degree 8 in $\mathbb{F}_q[x]$ is linearly related to some $f \in \mathbb{F}_q[x]$ in normalised form, $f(x) = x^8 + \sum_{i=1}^{6} a_i x^i$ with all $a_i \in \mathbb{F}_q$. Moreover, for another $g(x) = x^8 + \sum_{i=1}^{6} b_i x^i \in \mathbb{F}_q[x]$ with all $b_i \in \mathbb{F}_q$, f and g are linearly related if and only if $f(x) = t^8 g(t^{-1}x)$ for some $t \in \mathbb{F}_q^*$, that is,*

$$(a_6, a_5, a_4, a_3, a_2, a_1) = (t^2 b_6, t^3 b_5, t^4 b_4, t^5 b_3, t^6 b_2, t^7 b_1).$$

Proof. Each polynomial h of degree 8 in $\mathbb{F}_q[x]$ can be written as $h(x) = \sum_{i=1}^{8} c_i x^i$ with all $c_i \in \mathbb{F}_q$ and $c_8 \neq 0$. Then $f(x) = c_8^{-1} h(x - 8^{-1} c_8^{-1} c_7) - c_8^{-1} h(-8^{-1} c_8^{-1} c_7)$ is in normalised form and linearly related to h.

Suppose that $f(x) = x^8 + \sum_{i=1}^{6} a_i x^i$ and $g(x) = x^8 + \sum_{i=1}^{6} b_i x^i$ (with all $a_i, b_i \in \mathbb{F}_q$) are linearly related, say $g(x) = sf(tx + u) + v$ with $s, t \in \mathbb{F}_q^*$ and $u, v \in \mathbb{F}_q$. Clearly, $st^8 = 1$ and $8st^7 u = 0$, considering the coefficients of x^8 and x^7, respectively. So, $s = t^{-8}$ and $u = 0$. Then $g(x) = t^{-8} f(tx) + v$, where $v = g(0) - t^{-8} f(0) = 0$. □

The following subsections carry out a brute-force search for $(a_1, a_2, \ldots, a_6) \in \mathbb{F}_q^6$ corresponding to a PP $f(x) = x^8 + \sum_{i=1}^{6} a_i x^i$ over $\mathbb{F}_q$ in normalised form, on a case-by-case basis for each odd prime power $q \not\equiv 1 \pmod 8$ with $8 < q \leqslant 31$. The candidates are reduced up to linear transformations by Proposition 4.1. The search employs the SageMath function isPP8$(q, a_6, a_5, a_4, a_3, a_2, a_1)$ defined in Algorithm 5 to examine whether f is a PP over $\mathbb{F}_q$ or not. By Wan [19], it suffices to test whether the value set $\{f(c) : c \in \mathbb{F}_q\}$ contains $\lfloor q - (q-1)/8 \rfloor + 1$ distinct values.

Algorithm 5 To examine whether $f(x) = x^8 + \sum_{i=1}^{6} a_i x^i$ is a PP over $\mathbb{F}_q$

```
def isPP8(q,a6,a5,a4,a3,a2,a1):
    V = []
    for x in list(GF(q,'e'))[0:1+int(q-(q-1)/8)]:
        t = x^8+a6*x^6+a5*x^5+a4*x^4+a3*x^3+a2*x^2+a1*x
        if t in V: return False
        else: V.append(t)
    return True
```

https://doi.org/10.1017/S0004972719000674 Published online by Cambridge University Press

4.1. Case $q = 31$. The following piece of SageMath code prints polynomials with at most two terms among the given generators of $\mathbf{Rad}_8(31, 12)$.

```
for g in Rad8(31,12).gens():
    if g.number_of_terms()<3: print g
```

The output prints x_6, $x_2^5 - 1$, $x_3^6 - 1$, $x_4^{15} - 1$ and $x_1^{30} - 1$, all of which vanish at $(a_1, a_2, \ldots, a_6) \in \mathbb{F}_{31}^6$. So, $a_6 = 0 \neq a_1$ and $a_2^5 = a_3^6 = a_4^{15} = 1$.

Note that $f(x)$ is linearly related to

$$t^8 f(t^{-1}x) = x^8 + t^2 a_6 x^6 + t^3 a_5 x^5 + t^4 a_4 x^4 + t^5 a_3 x^3 + t^6 a_2 x^2 + t^7 a_1 x.$$

As $q - 1 = 30$ is coprime to 7, $a_1 = a^7$ for some $a \in \mathbb{F}_{31}^*$. Replacing $f(x)$ by $a^{-8} f(ax)$ if necessary, we assume that $a_1 = 1$ without loss of generality. So, Algorithm 6 lists PPs of degree 8 in normalised form over $\mathbb{F}_{31}$, up to linear transformations.

Algorithm 6 To list PPs of degree 8 in normalised form over $\mathbb{F}_{31}$

```
q = 31; F = GF(q)
for a5 in F:
    for a4 in [a4 for a4 in F if a4^15==1]:
        for a3 in [a3 for a3 in F if a3^6==1]:
            for a2 in [a2 for a2 in F if a2^5==1]:
                if isPP8(q,0,a5,a4,a3,a2,1): print(0,a5,a4,a3,a2,1)
```

The output of Algorithm 6 is $(0, 19, 25, 6, 2, 1)$, which gives Proposition 4.2.

Proposition 4.2. *All PPs of degree* 8 *in normalised form over* $\mathbb{F}_{31}$ *are exactly*

$$x^8 + 19t^3x^5 + 25t^4x^4 + 6t^5x^3 + 2t^6x^2 + t^7x$$

with t running through $\mathbb{F}_{31}^*$.

4.2. Case $q = 29$. The following piece of SageMath code prints polynomials with at most three terms among the given generators of $\mathbf{Rad}_8(29, 7)$.

```
for g in Rad8(29,7).gens():
    if g.number_of_terms()<4: print g
```

The output prints $x_6^2 - 9x_4$, $x_1^8 + 4x_1^4 - 5$, $x_2^{15} - x_2$ and $x_3^{29} - x_3$, all of which vanish at $(a_1, a_2, \ldots, a_6) \in \mathbb{F}_{29}$. So, $a_4 = a_6^2/9$, $a_1^8 + 4a_1^4 = 5$ and $a_2^{15} = a_2$.

As $q - 1 = 28$ is coprime to 3, without loss of generality we can assume that $a_5 \in \{0, 1\}$ (by linear transformations if necessary). So, Algorithm 7 lists PPs of degree 8 in normalised form over $\mathbb{F}_{29}$, up to linear transformations.

The output of Algorithm 7 prints

$$(0, 0, 0, 0, 0, 4),\ (0, 0, 0, 0, 0, 10),\ (0, 0, 0, 0, 0, 19),\ (0, 0, 0, 0, 0, 25),\ (26, 1, 1, 4, 20, 1).$$

Note that $\{4t^7 : t \in \mathbb{F}_{29}^*\} = \{4, 10, 19, 25\}$. This gives the following proposition.

https://doi.org/10.1017/S0004972719000674 Published online by Cambridge University Press

Algorithm 7 To list PPs of degree 8 in normalised form over $\mathbb{F}_{29}$

```
q = 29; F = GF(q)
for a6 in F:
    a4 = a6^2/F(9)
    for a5 in [0,1]:
        for a3 in F:
            for a2 in [a2 for a2 in F if a2^15==a2]:
                for a1 in [a1 for a1 in F if a1^8+4*a1^4==5]:
                    if isPP8(q,a6,a5,a4,a3,a2,a1):
                        print(a6,a5,a4,a3,a2,a1)
```

Proposition 4.3. *All PPs of degree* 8 *in normalised form over* $\mathbb{F}_{29}$ *are exactly*

$$x^8 + 4t^7x, \quad x^8 + 26t^2x^6 + t^3x^5 + t^4x^4 + 4t^5x^3 + 20t^6x^2 + t^7x$$

with t running through $\mathbb{F}_{29}^*$.

4.3. Case $q = 27$.

Note that $(a_1, a_3) \neq (0, 0)$ by the output of the SageMath code.

```
K.<x1,x2,x3,x4,x5,x6> = PolynomialRing(GF(27))
Ideal([HC8(27,4+i) for i in range(10)]+[x1,x3]).radical()
```

The output is `Ideal`(1), which indicates that polynomials x_1 and x_3 cannot both vanish at $(a_1, a_2, \ldots, a_6) \in \mathbb{F}_{27}$. By linear transformations if necessary, we can assume that $a_1 \in \{0, 1\}$, as $q - 1 = 26$ is coprime to 7. Further, when $a_1 = 0$ (and thus $a_3 \neq 0$), we can assume that $a_3 = 1$, as $q - 1 = 26$ is coprime to 5. Note that $a_2 = -a_6^3$ since $\mathbf{HC}_8(27, 4) = x_6^3 + x_2$. So, Algorithm 8 lists PPs of degree 8 in normalised form over $\mathbb{F}_{27}$ up to linear transformations and Proposition 4.4 is read off from its output.

Algorithm 8 To list PPs of degree 8 in normalised form over $\mathbb{F}_{27}$

```
q = 3^3; F = GF(q,'e')
print("The minimal polynomial of e is "+str(F.modulus()))
for (a3,a1) in [(1,0)]+[(a3,1) for a3 in F]:
    for a6 in F:
        a2 = -a6^3
        for a5 in F:
            for a4 in F:
                if isPP8(q,a6,a5,a4,a3,a2,a1):
                    print(a6,a5,a4,a3,a2,a1)
```

Proposition 4.4. *Let e be a root of the polynomial $x^3 + 2x + 1$ in $\mathbb{F}_{27}$, which is a generator of $\mathbb{F}_{27}^*$. All PPs of degree* 8 *in normalised form over $\mathbb{F}_{27}$ are exactly those of*

https://doi.org/10.1017/S0004972719000674 Published online by Cambridge University Press

the form $x^8 + \sum_{i=1}^{6} t^{8-i} a_i x^i$ *with* $t \in \mathbb{F}_{27}^*$ *and* $(a_6, a_5, a_4, a_3, a_2, a_1)$ *listed as follows:*

$$\begin{array}{lll}
(1,0,2,1,2,0), & (1,1,2,1,2,0), & \\
(e^2, 2e, 2e^3, e^{10}, 2e^6, 1), & (e^6, 2e^3, 2e^9, e^4, e^5, 1), & (2e^5, 2e^9, 2e, e^{12}, 2e^2, 1), \\
(e^2, 2e^4, e^7, e^6, 2e^6, 1), & (e^6, 2e^{12}, 2e^8, 2e^5, e^5, 1), & (2e^5, 2e^{10}, e^{11}, e^2, 2e^2, 1), \\
(e^4, 2e^2, e^7, e^4, 2e^{12}, 1), & (e^{12}, 2e^6, 2e^8, e^{12}, 2e^{10}, 1), & (e^{10}, e^5, e^{11}, e^{10}, 2e^4, 1), \\
(2e^4, e^{10}, 2e^{12}, 2e^{11}, e^{12}, 1), & (2e^{12}, e^4, 2e^{10}, 2e^7, e^{10}, 1), & (2e^{10}, e^{12}, 2e^4, e^8, e^4, 1).
\end{array}$$

4.4. Case $q = 23$.

The following piece of SageMath code prints polynomials with at most four terms among the given generators of $\mathbf{Rad}_8(23, 9)$.

```
for g in Rad8(23,9).gens():
    if g.number_of_terms()<5: print g
```

The output prints x_6, $x_4x_5^2 - 11x_3^2 + x_2x_4 + x_1x_5$, $x_5^{22} - 1$, $x_4^{22} - 1$, $x_3^{22} - 1$ and $x_1^{22} - 1$, all of which vanish at $(a_1, a_2, \ldots, a_6) \in \mathbb{F}_{23}$. So, $a_6 = 0 \neq a_j$ for $j \in \{1, 3, 4, 5\}$ and $a_4a_5^2 - 11a_3^2 + a_2a_4 + a_1a_5 = 0$.

As $q - 1 = 22$ is coprime to 3, without loss of generality we can assume that $a_5 = 1$ by linear transformations if necessary. So, Algorithm 9 lists PPs of degree 8 in normalised form over $\mathbb{F}_{23}$ up to linear transformations and Proposition 4.5 is read off from its output.

Algorithm 9 To list PPs of degree 8 in normalised form over $\mathbb{F}_{23}$

```
q = 23; F = GF(q)
for a4 in [a4 for a4 in F if a4!=0]:
    for a3 in [a3 for a3 in F if a3!=0]:
        for a2 in F:
            a1 = -a4+11*a3^2-a2*a4
            if isPP8(q,0,1,a4,a3,a2,a1): print(0,1,a4,a3,a2,a1)
```

Proposition 4.5. *All PPs of degree* 8 *in normalised form over* $\mathbb{F}_{23}$ *are exactly those of the form* $x^8 + t^3x^5 + t^4a_4x^4 + t^5a_3x^3 + t^6a_2x^2 + t^7a_1x$ *with* $t \in \mathbb{F}_{23}^*$ *and* (a_4, a_3, a_2, a_1) *listed as follows:*

$$\begin{array}{llll}
(11,1,12,6), & (11,1,21,22), & (15,8,16,12), & (15,16,13,7), \\
(16,8,7,1), & (19,5,10,20), & (20,12,2,6). &
\end{array}$$

4.5. Case $q = 19$.

Note that $(a_1, a_3) \neq (0, 0)$ by the output of the SageMath code.

```
K.<x1,x2,x3,x4,x5,x6> = PolynomialRing(GF(19))
Ideal([HC8(19,3+i) for i in range(7)]+[x3,x1]).radical()
```

https://doi.org/10.1017/S0004972719000674 Published online by Cambridge University Press

TABLE 1. PPs $x^8 + \sum_{i=1}^{6} a_i x^i$ of degree 8 over $\mathbb{F}_{19}$ up to linear transformations.

(a_3, a_1)	(a_6, a_5, a_4, a_2)			(a_3, a_1)	(a_6, a_5, a_4, a_2)		
(1, 0)	(0, 1, 3, 18),	(8, 1, 7, 14),	(15, 1, 1, 3)	(10, 1)	(6, 17, 3, 2),	(17, 12, 6, 3)	
(0, 1)	(9, 9, 18, 17),	(17, 16, 2, 8)		(11, 1)	(11, 2, 8, 16),	(11, 9, 1, 17),	(18, 0, 18, 11)
(1, 1)	(4, 7, 17, 9),	(8, 16, 10, 15),	(15, 4, 9, 14)	(12, 1)	(9, 15, 12, 0)		
(2, 1)	(1, 8, 1, 16),	(3, 6, 3, 13),	(6, 18, 2, 17)	(13, 1)	(12, 6, 8, 13),	(13, 17, 8, 12)	
(3, 1)	(12, 11, 10, 13)			(14, 1)	(10, 15, 14, 4),	(12, 12, 4, 1),	(17, 3, 9, 17),
					(18, 12, 4, 10),	(18, 17, 13, 16)	
(4, 1)	(2, 5, 8, 10),	(10, 10, 11, 18)		(15, 1)	(0, 5, 4, 13),	(8, 13, 8, 1)	
(5, 1)	(0, 4, 4, 3),	(0, 9, 9, 14),	(10, 0, 0, 15),	(16, 1)	(2, 11, 6, 17),	(3, 17, 17, 18),	(9, 18, 16, 0),
	(14, 5, 15, 2)				(11, 8, 9, 10)		
(6, 1)	(0, 14, 12, 13),	(13, 16, 2, 11),	(16, 7, 1, 4)	(17, 1)	(1, 8, 12, 13),	(3, 8, 12, 7),	(3, 16, 1, 14)
(7, 1)	(0, 6, 12, 2),	(3, 7, 16, 17)		(18, 1)	(8, 3, 18, 1),	(11, 3, 5, 1),	(18, 11, 0, 6)

The output is `Ideal`(1), which indicates that polynomials x_1 and x_3 cannot both vanish at $(a_1, a_2, \ldots, a_6) \in \mathbb{F}_{19}$. By linear transformations if necessary, we can assume that $a_1 \in \{0, 1\}$, as $q - 1 = 18$ is coprime to 7. Further, when $a_1 = 0$ (and thus $a_3 \neq 0$), we can assume that $a_3 = 1$, as $q - 1 = 18$ is coprime to 5. Note that $a_2 = -a_6^3/3 - a_5^2 - 2a_4a_6$ since $\mathbf{HC}_8(19, 3) = x_6^3 + 3x_5^2 + 6x_4x_6 + 3x_2$. So, Algorithm 10 lists PPs of degree 8 in normalised form over $\mathbb{F}_{19}$ up to linear transformations. There are exactly 48 linearly related classes of PPs of degree 8 over $\mathbb{F}_{19}$ as listed in Proposition 4.6, corresponding to 48 output tuples of Algorithm 10.

Algorithm 10 To list PPs of degree 8 in normalised form over $\mathbb{F}_{19}$

```
q = 19; F = GF(q)
for (a3,a1) in [(1,0)]+[(a3,1) for a3 in F]:
    for a6 in F:
        for a5 in F:
            for a4 in F:
                a2 = -a6^3/F(3)-a5^2-2*a4*a6
                if isPP8(q,a6,a5,a4,a3,a2,a1):
                    print(a6,a5,a4,a3,a2,a1)
```

PROPOSITION 4.6. *All PPs of degree 8 in normalised form over $\mathbb{F}_{19}$ are exactly those of the form $x^8 + \sum_{i=1}^{6} t^{8-i} a_i x^i$ with $t \in \mathbb{F}_{19}^*$ and $(a_6, a_5, a_4, a_3, a_2, a_1)$ listed in Table 1.*

4.6. Case $q = 13$. Note that $a_4 = -a_6^2/2$ since $\mathbf{HC}_8(13, 2) = x_6^2 + 2x_4$. By linear transformations if necessary, we can assume that $a_1 \in \{0, 1\}$, as $q - 1 = 12$ is coprime to 7. When $a_1 = 0$, we can assume that $a_3 \in \{0, 1\}$, as $q - 1 = 12$ is coprime to 5. When $a_1 = a_3 = 0$, we can assume that $a_5 \in \{0, 1, 2, 4\}$, as $\{1, 2, 4\}$ is a complete set of coset representatives of $\mathbb{F}_{13}^*/\{t^3 : t \in \mathbb{F}_{13}^*\}$. So, Algorithm 11 lists PPs of degree 8 in normalised form over $\mathbb{F}_{13}$ up to linear transformations.

The output of Algorithm 11 prints 119 tuples $(a_6, a_5, \ldots, a_1)$, among which three tuples $(4, 2, 5, 0, 4, 0)$, $(10, 2, 2, 0, 4, 0)$ and $(12, 2, 6, 0, 4, 0)$ give three linearly related

Algorithm 11 To list PPs of degree 8 in normalised form over $\mathbb{F}_{13}$

```
q = 13; F = GF(q)
for (a3,a1) in [(0,0),(1,0)]+[(a3,1) for a3 in F]:
    if (a3,a1)==(0,0): A5 = [0,1,2,4]
    else: A5 = F
    for a6 in F:
        a4 = -a6^2/F(2)
        for a5 in A5:
            for a2 in F:
                if isPP8(q,a6,a5,a4,a3,a2,a1):
                    print(a6,a5,a4,a3,a2,a1)
```

Table 2. PPs $x^8 + \sum_{i=1}^{6} a_i x^i$ of degree 8 over $\mathbb{F}_{13}$ up to linear transformations.

(a_3, a_1)	(a_6, a_5, a_4, a_2)							
(0, 0)	(0, 1, 0, 5),	(0, 1, 0, 7),	(0, 4, 0, 9),	(4, 2, 5, 4)				
(1, 0)	(0, 7, 0, 12),	(2, 0, 11, 12),	(4, 8, 5, 2),	(7, 7, 8, 9)				
(0, 1)	(2, 7, 11, 6),	(3, 1, 2, 2),	(3, 2, 2, 12),	(4, 11, 5, 8),	(7, 11, 8, 1),	(10, 5, 2, 1),	(10, 9, 2, 2),	(12, 11, 6, 1)
(1, 1)	(1, 9, 6, 4),	(4, 2, 5, 10),	(4, 3, 5, 7),	(4, 4, 5, 12),	(7, 5, 8, 5),	(9, 5, 5, 10),	(9, 8, 5, 7),	(12, 10, 6, 3)
(2, 1)	(0, 3, 0, 0),	(1, 8, 6, 5),	(1, 9, 6, 3),	(2, 9, 11, 1),	(5, 8, 7, 6),	(6, 12, 8, 4),	(7, 4, 8, 12),	(8, 0, 7, 11)
(3, 1)	(1, 3, 6, 10),	(1, 4, 6, 12),	(4, 5, 5, 5),	(8, 1, 7, 12),	(8, 5, 7, 7),	(8, 5, 7, 12),	(8, 6, 7, 2),	(9, 12, 5, 7),
	(12, 5, 6, 8)							
(4, 1)	(1, 10, 6, 6),	(4, 4, 5, 5),	(5, 6, 7, 9),	(9, 2, 5, 6),	(9, 10, 5, 12),	(10, 10, 2, 9),	(12, 1, 6, 7)	
(5, 1)	(0, 1, 0, 8),	(3, 5, 2, 12),	(4, 0, 5, 7),	(5, 11, 7, 1),	(6, 12, 8, 8),	(10, 12, 2, 4)		
(6, 1)	(0, 10, 0, 12),	(3, 0, 2, 9),	(5, 2, 7, 10),	(6, 7, 8, 3),	(6, 10, 8, 6),	(10, 0, 2, 11),	(11, 11, 11, 2)	
(7, 1)	(0, 1, 0, 6),	(1, 7, 6, 10),	(1, 11, 6, 4),	(4, 4, 5, 6),	(10, 7, 2, 10),	(11, 1, 11, 1),	(11, 3, 11, 11),	(11, 10, 11, 2),
	(12, 10, 6, 6)							
(8, 1)	(0, 0, 0, 1),	(1, 1, 6, 1),	(4, 9, 5, 2),	(7, 11, 8, 1),	(8, 11, 7, 10),	(9, 8, 5, 1),	(9, 10, 5, 10),	(12, 0, 6, 2)
(9, 1)	(0, 2, 0, 2),	(1, 11, 6, 5),	(3, 9, 2, 2),	(4, 9, 5, 6),	(4, 12, 5, 0),	(7, 1, 8, 2),	(7, 2, 8, 5),	(7, 12, 8, 0),
	(11, 1, 11, 0),	(12, 6, 6, 8),	(12, 10, 6, 8)					
(10, 1)	(0, 3, 0, 3),	(0, 10, 0, 1),	(4, 5, 5, 5),	(5, 1, 7, 10),	(5, 12, 7, 9),	(9, 4, 5, 5),	(9, 5, 5, 11),	(10, 5, 2, 9),
	(10, 7, 2, 0),	(10, 10, 2, 7),	(12, 1, 6, 4)					
(11, 1)	(0, 3, 0, 7),	(1, 12, 6, 12),	(2, 4, 11, 10),	(2, 6, 11, 0),	(3, 0, 2, 12),	(6, 8, 8, 3),	(7, 7, 8, 12),	(9, 0, 5, 6)
(12, 1)	(3, 5, 2, 1),	(4, 9, 5, 0),	(5, 4, 7, 10),	(6, 8, 8, 9),	(6, 12, 8, 2),	(7, 10, 8, 9),	(8, 3, 7, 2),	(9, 5, 5, 5),
	(11, 9, 11, 10)							

PPs of degree 8. Indeed, for $t = 3 \in \mathbb{F}_{13}^*$, we have $t^3 = 1$, $t^{-1} = 9$ and

$$(10, 2, 2, 0, 4, 0) = (4t^2, 2t^3, 5t^4, 0, 4t^6, 0) = (12t^{-2}, 2t^{-3}, 6t^{-4}, 0, 4t^{-6}, 0).$$

No other linear transformation relations exist among the output tuples. Therefore, there are exactly 117 linearly related classes of PPs of degree 8 over $\mathbb{F}_{13}$, as listed in Proposition 4.7 read off from the output of Algorithm 11.

Proposition 4.7. *All PPs of degree* 8 *in normalised form over* $\mathbb{F}_{13}$ *are exactly those of the form* $x^8 + \sum_{i=1}^{6} t^{8-i} a_i x^i$ *with* $t \in \mathbb{F}_{13}^*$ *and* $(a_6, a_5, a_4, a_3, a_2, a_1)$ *listed in Table* 2.

4.7. Case $q = 11$. Note that $a_2 = -a_5^2/2 - a_4 a_6$ since $\mathbf{HC}_8(11, 2) = x_5^2 + 2x_4x_6 + 2x_2$. We can assume that $a_1 \in \{0, 1\}$, as $q - 1 = 10$ is coprime to 7. When $a_1 = 0$, we can assume that $a_5 \in \{0, 1\}$, as $q - 1 = 10$ is coprime to 3. When $a_1 = a_5 = 0$, we

https://doi.org/10.1017/S0004972719000674 Published online by Cambridge University Press

TABLE 3. PPs $x^8 + \sum_{i=1}^{6} a_i x^i$ of degree 8 over $\mathbb{F}_{11}$ up to linear transformations.

(a_5, a_1)	(a_6, a_4, a_3, a_2)							
(0, 0)	(0, 0, 2, 0),	(0, 0, 4, 0),	(2, 6, 2, 10),	(2, 7, 3, 8)				
(1, 0)	(0, 2, 0, 5),	(1, 1, 0, 4),	(1, 4, 0, 1),	(1, 4, 5, 1),	(1, 9, 1, 7),	(1, 10, 5, 6),	(2, 1, 4, 3),	(2, 4, 0, 8),	(2, 5, 0, 6),
	(3, 2, 3, 10),	(4, 1, 0, 1),	(4, 6, 4, 3),	(4, 7, 0, 10),	(4, 8, 3, 6),	(4, 9, 9, 2),	(4, 10, 9, 9),	(5, 6, 5, 8),	(6, 6, 5, 2),
	(7, 7, 5, 0),	(8, 0, 0, 5),	(8, 2, 0, 0),	(9, 3, 4, 0),	(9, 5, 0, 4),	(9, 5, 5, 4),	(9, 7, 0, 8),	(10, 0, 9, 5)	
(0, 1)	(0, 1, 3, 0),	(0, 2, 9, 0),	(0, 8, 5, 0),	(2, 3, 5, 5),	(3, 2, 3, 5),	(3, 4, 1, 10),	(3, 9, 4, 6),	(3, 10, 1, 3),	(4, 3, 9, 10),
	(4, 8, 4, 1),	(5, 10, 3, 5),	(6, 2, 4, 10),	(6, 4, 0, 9),	(7, 5, 0, 9),	(7, 6, 1, 2),	(8, 5, 9, 4),	(9, 3, 1, 6),	(9, 10, 1, 9),
	(10, 0, 1, 0),	(10, 1, 4, 1),	(10, 3, 3, 3),	(10, 5, 1, 5),	(10, 7, 4, 7)				
(1, 1)	(0, 4, 6, 5),	(1, 9, 10, 7),	(2, 0, 0, 5),	(2, 10, 10, 7),	(4, 3, 7, 4),	(4, 5, 5, 7),	(4, 6, 3, 3),	(5, 2, 5, 6),	(5, 8, 1, 9),
	(6, 0, 3, 5),	(6, 0, 6, 5),	(6, 0, 7, 5),	(8, 1, 3, 8),	(8, 10, 7, 2),	(9, 1, 3, 7),	(9, 2, 3, 9),	(9, 5, 0, 4),	(9, 6, 7, 6),
	(9, 9, 2, 1),	(10, 0, 7, 5),	(10, 3, 7, 8),	(10, 7, 2, 1)					
(2, 1)	(0, 1, 5, 9),	(0, 3, 5, 9),	(1, 4, 2, 5),	(1, 4, 9, 5),	(1, 7, 6, 2),	(1, 10, 2, 10),	(2, 5, 5, 10),	(4, 0, 7, 9),	(4, 5, 4, 0),
	(5, 2, 9, 10),	(5, 10, 6, 3),	(6, 0, 4, 9),	(6, 1, 9, 3),	(6, 8, 4, 5),	(7, 0, 9, 9),	(7, 1, 5, 2),	(7, 3, 6, 10),	(8, 2, 5, 4),
	(8, 3, 4, 7),	(8, 8, 4, 0),	(9, 1, 9, 0),	(9, 6, 6, 10),	(9, 10, 9, 7),	(10, 10, 5, 8)			
(3, 1)	(0, 4, 3, 1),	(0, 5, 8, 1),	(0, 7, 0, 1),	(0, 8, 0, 1),	(1, 4, 5, 8),	(1, 8, 0, 4),	(3, 8, 3, 10),	(3, 8, 8, 10),	(4, 2, 8, 4),
	(4, 8, 5, 2),	(5, 9, 6, 0),	(6, 4, 4, 10),	(7, 6, 6, 3),	(7, 8, 3, 0),	(8, 7, 6, 0),	(9, 0, 4, 1),	(9, 3, 10, 7),	(9, 7, 2, 4),
	(9, 7, 3, 4),	(9, 10, 3, 10),	(10, 2, 6, 3),	(10, 8, 3, 9)					
(4, 1)	(0, 3, 0, 3),	(1, 1, 10, 2),	(1, 4, 10, 10),	(2, 3, 8, 8),	(2, 7, 9, 0),	(3, 0, 5, 3),	(3, 1, 7, 0),	(3, 1, 9, 0),	(3, 3, 9, 5),
	(3, 5, 0, 10),	(3, 5, 7, 10),	(4, 1, 2, 10),	(5, 5, 10, 0),	(5, 10, 1, 8),	(5, 10, 7, 8),	(6, 3, 9, 7),	(6, 7, 2, 5),	(7, 2, 8, 0),
	(7, 5, 10, 1),	(7, 9, 0, 6),	(8, 3, 10, 1),	(8, 6, 8, 10),	(8, 8, 7, 5),	(9, 7, 10, 6),	(9, 9, 1, 10),	(10, 3, 5, 6)	
(5, 1)	(0, 9, 1, 4),	(0, 10, 6, 4),	(1, 2, 2, 2),	(1, 3, 9, 1),	(1, 5, 6, 10),	(1, 7, 8, 8),	(2, 2, 1, 0),	(2, 5, 2, 5),	(2, 9, 0, 8),
	(3, 3, 4, 6),	(3, 6, 7, 8),	(4, 2, 6, 7),	(4, 3, 1, 3),	(4, 4, 7, 10),	(5, 0, 8, 4),	(5, 1, 6, 10),	(5, 8, 8, 8),	(5, 10, 0, 9),
	(6, 4, 8, 2),	(7, 3, 9, 5),	(7, 10, 7, 0),	(8, 2, 1, 10),	(8, 2, 7, 10),	(8, 3, 1, 2),	(8, 5, 9, 8),	(8, 6, 2, 0),	(8, 8, 0, 6),
	(8, 8, 7, 6),	(9, 8, 4, 9),	(10, 9, 1, 2)						
(6, 1)	(0, 7, 9, 4),	(1, 6, 8, 9),	(1, 9, 2, 6),	(2, 1, 3, 2),	(3, 7, 8, 5),	(4, 6, 9, 2),	(5, 10, 10, 9),	(6, 0, 2, 4),	(6, 7, 10, 6),
	(7, 9, 3, 7),	(9, 3, 9, 10),	(9, 6, 1, 5),	(9, 7, 9, 7),	(10, 9, 1, 2)				
(7, 1)	(1, 0, 1, 3),	(1, 0, 4, 3),	(1, 0, 6, 3),	(2, 7, 1, 0),	(2, 9, 5, 7),	(3, 9, 5, 9),	(4, 0, 4, 3),	(4, 6, 6, 1),	(5, 2, 10, 4),
	(5, 3, 1, 10),	(5, 10, 7, 8),	(7, 4, 4, 8),	(8, 1, 10, 6),	(8, 3, 7, 1),	(8, 10, 10, 0),	(9, 0, 7, 3),	(9, 10, 10, 1),	(10, 8, 10, 0)
(8, 1)	(0, 10, 4, 1),	(1, 9, 3, 3),	(2, 2, 7, 8),	(2, 10, 10, 3),	(3, 2, 4, 6),	(3, 4, 1, 0),	(3, 4, 3, 0),	(4, 1, 3, 8),	(4, 4, 1, 7),
	(4, 6, 8, 10),	(5, 9, 4, 0),	(6, 9, 10, 2),	(7, 0, 8, 1),	(7, 2, 8, 9),	(8, 6, 4, 8),	(8, 9, 8, 6),	(9, 0, 8, 1),	(10, 0, 7, 1)
(9, 1)	(0, 0, 4, 9),	(0, 6, 3, 9),	(1, 0, 6, 9),	(1, 8, 6, 1),	(1, 8, 8, 1),	(1, 10, 8, 10),	(2, 1, 10, 7),	(2, 4, 0, 1),	(2, 5, 0, 10),
	(3, 0, 0, 9),	(3, 5, 3, 5),	(3, 9, 10, 4),	(4, 3, 10, 8),	(4, 4, 4, 4),	(4, 7, 6, 3),	(4, 10, 4, 2),	(5, 9, 4, 8),	(6, 2, 9, 8),
	(6, 5, 4, 1),	(6, 6, 0, 6),	(6, 10, 10, 4),	(7, 1, 0, 2),	(7, 10, 8, 5),	(8, 1, 8, 1),	(8, 6, 7, 5),	(8, 8, 10, 0),	(9, 3, 0, 4),
	(9, 5, 9, 8),	(9, 6, 6, 10),	(10, 6, 8, 4),	(10, 7, 8, 5),	(10, 9, 4, 7)				
(10, 1)	(0, 1, 8, 5)	(0, 5, 2, 5),	(0, 6, 5, 5),	(1, 0, 2, 5),	(2, 4, 9, 8),	(3, 5, 8, 1),	(3, 6, 6, 9),	(3, 8, 9, 3),	(4, 2, 3, 8),
	(5, 10, 5, 10)	(7, 3, 8, 6),	(7, 5, 9, 3),	(8, 2, 8, 0),	(8, 3, 5, 3),	(8, 6, 9, 1),	(9, 1, 3, 7),	(9, 9, 6, 1),	(10, 1, 6, 6)

can assume that $a_6 \in \{0, 1, 2\}$, as $\{1, 2\}$ is a complete set of coset representatives of $\mathbb{F}_{11}^*/\{t^2 : t \in \mathbb{F}_{11}^*\}$. So, Algorithm 12 lists PPs of degree 8 in normalised form over $\mathbb{F}_{11}$ up to linear transformations.

The output of Algorithm 12 prints 281 tuples $(a_6, a_5, \ldots, a_1)$. By Proposition 4.1 and our assumptions, linear transformation relations exist only among those with $a_1 = a_5 = 0$, which are indeed the first eight tuples in the output, corresponding to four distinct linearly related classes. No other linear transformation relations exist among the output tuples. So, there are exactly 277 linearly related classes of PPs of degree 8 over $\mathbb{F}_{11}$, as listed in Proposition 4.8 read off from the output of Algorithm 12.

PROPOSITION 4.8. *All PPs of degree* 8 *in normalised form over* $\mathbb{F}_{11}$ *are exactly those of the form* $x^8 + \sum_{i=1}^{6} t^{8-i} a_i x^i$ *with* $t \in \mathbb{F}_{11}^*$ *and* $(a_6, a_5, a_4, a_3, a_2, a_1)$ *listed in Table* 3.

https://doi.org/10.1017/S0004972719000674 Published online by Cambridge University Press

Algorithm 12 To list PPs of degree 8 in normalised form over $\mathbb{F}_{11}$

```
q = 11; F = GF(q)
for (a5,a1) in [(0,0),(1,0)]+[(a5,1) for a5 in F]:
    if (a5,a1)==(0,0): A6 = [0,1,2]
    else: A6 = F
    for a6 in A6:
        for a4 in F:
            a2 = -a5^2/F(2)-a4*a6
            for a3 in F:
                if isPP8(q,a6,a5,a4,a3,a2,a1):
                    print(a6,a5,a4,a3,a2,a1)
```

Acknowledgements

The author would like to thank the anonymous referee for helpful suggestions to improve this paper. Special thanks go to my lovely newborn daughter, without whose birth this paper should have come out much earlier.

References

[1] J. S. Chahal and S. R. Ghorpade, 'Carlitz–Wan conjecture for permutation polynomials and Weil bound for curves over finite fields', *Finite Fields Appl.* **54** (2018), 366–375.

[2] S. D. Cohen and M. D. Fried, 'Lenstra's proof of the Carlitz–Wan conjecture on exceptional polynomials: an elementary version', *Finite Fields Appl.* **1**(3) (1995), 372–375.

[3] W. Decker, G.-M. Greuel, G. Pfister and H. Schönemann, 'Singular 4-1-2: A computer algebra system for polynomial computations', 2019, https://www.singular.uni-kl.de.

[4] L. E. Dickson, 'The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group', *Ann. of Math. (2)* **11**(1–6) (1896–1897), 65–120.

[5] C. Ding and J. Yuan, 'A family of skew Hadamard difference sets', *J. Combin. Theory Ser. A* **113**(7) (2006), 1526–1535.

[6] X. Fan, 'The Weil bound and non-exceptional permutation polynomials over finite fields', Preprint, 2018, arXiv:1811.12631.

[7] X. Fan, 'A classification of permutation polynomials of degree 7 over finite fields', *Finite Fields Appl.* **59** (2019), 1–21.

[8] X. Fan, 'Permutation polynomials of degree 8 over finite fields of characteristic 2', Preprint, 2019, arXiv:1903.10309.

[9] M. D. Fried, R. Guralnick and J. Saxl, 'Schur covers and Carlitz's conjecture', *Israel J. Math.* **82**(1–3) (1993), 157–225.

[10] D. R. Hayes, 'A geometric approach to permutation polynomials over a finite field', *Duke Math. J.* **34** (1967), 293–305.

[11] C. Hermite, 'Sur les fonctions de sept lettres', *C. R. Acad. Sci. Paris* **57** (1863), 750–757.

[12] X.-D. Hou, 'Permutation polynomials over finite fields — a survey of recent advances', *Finite Fields Appl.* **32** (2015), 82–119.

[13] G. Kemper, 'The calculation of radical ideals in positive characteristic', *J. Symbolic Comput.* **34**(3) (2002), 229–238.

[14] J. Li, D. B. Chandler and Q. Xiang, 'Permutation polynomials of degree 6 or 7 over finite fields of characteristic 2', *Finite Fields Appl.* **16**(6) (2010), 406–419.

[15] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd edn, Encyclopedia of Mathematics and its Applications, 20 (Cambridge University Press, Cambridge, 1997).

https://doi.org/10.1017/S0004972719000674 Published online by Cambridge University Press

[16] G. L. Mullen (ed), *Handbook of Finite Fields*, Discrete Mathematics and its Applications (CRC Press, Boca Raton, FL, 2013).

[17] The Sage Developers, *SageMath, the Sage Mathematics Software System*, version 8.6, 2019, https://www.sagemath.org.

[18] J. von zur Gathen, ‘Values of polynomials over finite fields’, *Bull. Aust. Math. Soc.* **43**(1) (1991), 141–146.

[19] D. Q. Wan, ‘A *p*-adic lifting lemma and its applications to permutation polynomials’, in: *Finite Fields, Coding Theory, and Advances in Communications and Computing (Las Vegas, NV, 1991)*, Lecture Notes in Pure and Applied Mathematics, 141 (Dekker, New York, 1993), 209–216.

XIANG FAN, School of Mathematics,
Sun Yat-sen University, Guangzhou 510275, China
e-mail: fanx8@mail.sysu.edu.cn

https://doi.org/10.1017/S0004972719000674 Published online by Cambridge University Press