# THE DIFFERENCE BETWEEN PERMUTATION POLYNOMIALS OVER FINITE FIELDS 

STEPHEN D. COHEN, GARY L. MULLEN, AND PETER JAU-SHYONG SHIUE<br>(Communicated by William Adams)


#### Abstract

Recently S. D. Cohen resolved a conjecture of Chowla and Zassenhaus (1968) in the affirmative by showing that, if $f(x)$ and $g(x)$ are integral polynomials of degree $n \geq 2$ and $p$ is a prime exceeding $\left(n^{2}-3 n+4\right)^{2}$ for which $f$ and $g$ are both permutation polynomials of the finite field $F_{p}$, then their difference $h=f-g$ cannot be such that $h(x)=c x$ for some integer $c$ not divisible by $p$. In this note we provide a significant generalization by proving that, if $h$ is not a constant in $F_{p}$ and $t$ is the degree of $h$, then $t \geq 3 n / 5$ and, provided $t \leq n-3, t$ and $n$ are not relatively prime. In a sense this measures the isolation of permutation polynomials of the same degree over large finite prime fields.


## 1. Introduction

For each prime $p$ let $F_{p}$ denote the finite field of order $p$. A polynomial $f(x)$ is said to be a permutation polynomial (PP) of the field $F_{p}$ if $f$ induces a 1-1 mapping of $F_{p}$ onto itself; see Lidl and Niederreiter [5, Chapter 7]. The Chowla and Zassenhaus conjecture was recently proved by Cohen [2] in the following more precise form:
Theorem 1. Let $f(x)$ be a polynomial with integral coefficients and degree $n \geq$ 2. Then for any prime $p>\left(n^{2}-3 n+4\right)^{2}$ for which $f$ (considered modulo $p$ ) is a PP of degree $n$ of $F_{p}$, there is no integer $c$ with $1 \leq c<p$ for which $f(x)+c x$ is also a PP of $F_{p}$.

The purpose of this note is to provide a rather substantial generalization of Theorem 1. There are numerous ways to consider extending Theorem 1, for example, if one considers $f(x)$ to be a PP over $F_{p}$, one could consider replacing the monomial $x$ by a more general PP over $F_{p}$, in fact by an arbitrary PP, say $g(x)$, over $F_{p}$. This however does not really provide a generalization since if we replace $x$ by the polynomial over $F_{p}$ representing $g^{-1}(x)$, we have $f\left(g^{-1}(x)\right)+c x=h(x)+c x$, which is of course in the original form. Thus if

[^0]$f(x)$ is a PP over $F_{p}$, we consider the question of when $f(x)+g(x)$ can be a PP, where $g(x)$ need not itself be a PP of $F_{p}$.

There is also a related viewpoint. Let $f$ and $g$ be a pair of PPs of degree $n$ over $F_{p}$ not trivially connected by $f(x)=g(x)+c, c \in F_{p}$. Let $h=f-g$, and let $t$ be the degree of $h$. Then $t \neq 0$ and Theorem 1 implies that, for large primes $p, h(x) \neq c x, c \in F_{p}$. That is, $f$ and $g$ cannot be so close as to differ merely by a linear term $c x$. The question naturally arises as to whether $f$ and $g$ can be separated by another polynomial of smallish degree. We show that, in fact, necessarily $t \geq 3 n / 5$. Moreover, provided $t \leq n-3$, $t$ and $n$ cannot be relatively prime. In this connection, note that trivially, if $f(x)=g(x+c), c \neq 0$, and $p>n$, then $t=n-1$ and there are examples with $t=n-2$ (see below). We stress that we have demonstrated that PPs of given degree are isolated (in the described sense) over sufficiently large prime fields. It is an open question as to how far such isolation prevails in the most general setting.

## 2. Generalization

Suppose $f(x)$ is a PP of $F_{p}$ of degree $n \geq 2$ and $h(x)$ is any polynomial over $F_{p}$ of degree $t$ where $1 \leq t<3 n / 5$. Then we show that $f(x)-h(x)$ cannot be a PP of $F_{p}$. The bound $t=3 n / 5$ is attained because for $p \equiv$ $\pm 2(\bmod 5)$, if we let $f(x)=D_{5}\left(a, x^{m}\right)$ where $D_{5}(a, x)=x^{5}-5 a x^{3}+5 a^{2} x$ is the Dickson polynomial of degree 5 with $(m, p-1)=1$ and let $g(x)=x^{5 m}$ so that $g(x)$ is a PP of $F_{p}$, then $t=3 m=3 n / 5$. Here we recall that $D_{5}(a, x)$ is a PP of $F_{p}$ if and only if $\left(5, p^{2}-1\right)=1$; see [5, Theorem 7.16]. This example (with $m=1$ ) also shows that it is possible that $t=n-2$.

In particular we prove
Theorem 2. Suppose $f$ and $g$ are monic PPs of degree $n \geq 3$ over $F_{p}$ where $p>\left(n^{2}-3 n+4\right)^{2}$. Set $f-g=h$, and let $t$ be the degree of $h$. Suppose $t \geq 1$. Then $t \geq 3 n / 5$. Moreover, provided $n \geq 5$ and $t \leq n-3$, then $(t, n)>1$.

As a special case of Theorem 2 we note that if $g(x)=f(x)-c x$ is a PP for some $1 \leq c<p$, then $h(x)=c x$ so that $t=1$, and hence $n \leq 5 / 3$, a contradiction. Hence Theorem 2 implies Theorem 1. It is worth pointing out that from results of Cohen [2], $n$ must be odd, and so we make this assumption throughout the rest of the paper.

## 3. Proof of Theorem 2

Since $n \geq 3$, we can assume $t<n-1$. As in Cohen's proof [2] of the Chowla and Zassenhaus conjecture, we first normalize $f$ and $g$ so that $f$ and $g$ are both monic and have the coefficient of $x^{n-1}$ equal to zero (this requires that $t \neq n-1)$. Suppose that $f=f_{0}(\ell)$ and $g=g_{0}(\ell)$ for some normalized PP $\ell(x)$. Choose such a polynomial $\ell$ whose degree $d$ is maximal and write degree $\left(f_{0}\right)=\operatorname{degree}\left(g_{0}\right)=n_{0}$ where $n=d n_{0}$. Of course $d<n$ since $1 \leq t \leq n-2$. Then $h=h_{0}(\ell)$ where degree $\left(h_{0}\right)=t_{0}$ and $t=d t_{0}$.

Suppose $d>1$. Then $(t, n)>1$. Moreover, $t<3 n / 5$ if and only if $t_{0}<3 n_{0} / 5$ and so we may replace $f$ and $g$ by $f_{0}$ and $g_{0}$ and assume $d=1$. Hence, in every case we may suppose that $d=1$.

Next suppose that $t=n-2$. Then $n \neq 3$ and $t \geq 3 n / 5$ with equality only
if $n=5, t=3$ (as in the example preceding the statement of Theorem 2). Thus we may also assume that $t \leq n-3$ (with $n \geq 5$ ).

From Corollary 6 of [2] we have that $f=f_{2}\left(f_{1}\right), g=g_{2}\left(g_{1}\right)$ where $f_{2}$ and $g_{2}$ are normalized and

$$
\begin{align*}
& f_{1}(x)=D_{m_{1}}\left(a, x^{m_{2}}\right)+\alpha, \quad a \neq 0, \alpha \in F_{p}, \quad m=m_{1} m_{2} \geq 3, \\
& g_{1}(x)=D_{k_{1}}\left(b, x^{k_{2}}\right)+\beta, \quad b \neq 0, \quad \beta \in F_{p}, \quad k=k_{1} k_{2} \geq 3 . \tag{*}
\end{align*}
$$

Moreover in $\left.{ }^{*}\right)$ if $m_{1}=1$, then $\alpha \neq 0$ unless $f(x)=x^{n}$ and a similar statement holds for $g$. Further at one point in Case 3 below we shall assume that in $\left.{ }^{*}\right), m$ and $k$ have been chosen to be maximal in a natural sense; see the discussion of that case for details. We recall that $D_{m}(a, x)$ is the Dickson polynomial of degree $m$ with $a \in F_{p}$ defined by

$$
D_{m}(a, x)=\sum_{j=0}^{\lfloor m / 2\rfloor} \frac{m}{m-j}\binom{m-j}{j}(-a)^{j} x^{m-2 j} ;
$$

see [5, p. 355]. It is worth pointing out here that the results in (*) follow from a result of Fried [3] which is a critical part of his proof of the Schur conjecture.

We now prove Theorem 2 by considering three cases.
Case 1: $f_{1}(x)=x^{m}+\alpha$ and $g_{1}(x)=x^{k}+\beta$ with $\alpha \beta \neq 0$. Since $d=1$, we have $(m, k)=1$, and from [2, Lemma 4], $t=\max \{n-m, n-k\}$ and $k m \mid n$. Hence $(t, n)=k>1$ or $m>1$ and $t \geq n-n / 3=2 n / 3>3 n / 5$.
Case 2: $f_{1}(x)=D_{m_{1}}\left(a, x^{m_{2}}\right)+\alpha$ and $g_{1}(x)=x^{k}+\beta$ with $m_{1}>1$. Then $\left(k, m_{2}\right)=1$ and $t=\max \left\{n-2 m_{2}, n-k\right\}$, where $m_{2}>1$ since $t \neq n-2$. Also $(t, n)>1$ and if $k<2 m_{2}$, then because $m_{2}>1,1-k / n \geq 1-1 / m_{2} \geq 2 / 3$. If $k \geq 2 m_{2}$, then $1-2 m_{2} / n \geq 1-2 / m_{1} \geq 1-2 / 5=3 / 5$.
Case 3: $f_{1}(x)=D_{m_{1}}\left(a, x^{m_{2}}\right)+\alpha$ and $g_{1}(x)=D_{k_{1}}\left(b, x^{k_{2}}\right)+\beta$, where $m_{1}>1$, $k_{1}>1$. In this case ( $m_{2}, k_{2}$ )=1 and [2, Lemma 4] implies

$$
t=\max \left\{n-2 m_{2}, n-2 k_{2}\right\},
$$

unless $m_{2}=k_{2}=1$ and $a=b$ (if $a \neq b$ then $t=n-2$, a contradiction). Thus, except in this last situation,

$$
1-\frac{2 m_{2}}{n} \geq 1-\frac{2}{m_{1}} \geq \frac{3}{5}
$$

On the other hand if $m_{2}=k_{2}=1$ and $a=b$ we have $(k, m)=1$, for otherwise $f_{1}=f_{0}\left(D_{r}(a, x)\right)$ and $g_{1}=g_{0}\left(D_{r}(a, x)\right)$ with $r=(k, m)$. As noted at (*), we assume here that $m$ is maximal in the sense that, if $\alpha=0$, then $f_{2}(x) \neq H\left(D_{r}\left(a^{m}, x\right)\right), r \geq 5$, for any polynomial $H$, and, similarly, $k$ is maximal. We also have

$$
\begin{aligned}
h\left(x+\frac{a}{x}\right)= & f_{2}\left(x^{m}+\frac{a^{m}}{x^{m}}+\alpha\right)-g_{2}\left(x^{k}+\frac{a^{k}}{x^{k}}+\beta\right) \\
= & \frac{n}{m} \alpha x^{n-m}+\cdots+\left(\frac{n}{m} a^{m}+A\right) x^{n-2 m}+\cdots \\
& -\left(\frac{n}{k} \beta x^{n-k}+\cdots+\left(\frac{n}{k} a^{k}+B\right) x^{n-2 k}+\cdots\right)
\end{aligned}
$$

where $f_{2}(x)=x^{N}+A x^{N-2}+\ldots, N=n / m$, and similarly for $g_{2}$.

We note that $n-m$ and $n-k$ are even while $n-2 m$ and $n-2 k$ are odd so that no cancellation occurs among the displayed terms. Moreover, by the maximality of $m$, if $\alpha=0$, the coefficient of $x^{n-2 m}$ is non-zero, and similarly that of $x^{n-2 k}$ is non-zero if $\beta=0$. Also $k$ and $m$ both divide $n$ with $k \geq 5, m \geq 5$. Depending upon whether $\alpha$ or $\beta$ are zero we have the cases:

$$
t= \begin{cases}\max \{n-2 m, n-2 k\} & \text { if } \alpha=\beta=0  \tag{1}\\ \max \{n-m, n-2 k\} & \text { if } \alpha \neq 0, \beta=0 \\ \max \{n-m, n-k\} & \text { if } \alpha \beta \neq 0\end{cases}
$$

We also note that if $\alpha=0, \beta \neq 0$ we have a situation analogous to (2). Clearly in each case $(t, n)=k$ or $m$ so that $(t, n)>1$. For (1) assume $m<k$. Then

$$
\frac{t}{n}=1-\frac{2 m}{n} \geq 1-\frac{10}{35}=\frac{5}{7}>\frac{3}{5}
$$

For (2), if $m<2 k$, then $t / n \geq 1-7 / 35=4 / 5$; while if $m>2 k$, then $t / n \geq 1-2 / 11=9 / 11>3 / 5$. Finally for (3), $t / n \geq 6 / 7>3 / 5$. This completes the proof.

Theorem 2 can be applied to the theory of uniform distribution of sequences over finite fields. A sequence $\left(x_{n}\right), n=0,1, \ldots$, of elements of $F_{q}$ is said to be equidistributed (or uniformly distributed) in $F_{q}$ if

$$
\lim _{N \rightarrow \infty} \frac{A(c, N)}{N}=\frac{1}{q}
$$

where $A(c, N)=A\left(c, N,\left(x_{n}\right)\right)$ denotes the number of $n$ with $0 \leq n \leq N-1$ for which $x_{n}=c$ (compare with [4, p. 331, Exercise 3.5]). For a periodic sequence $\left(x_{n}\right)$, this definition is obviously equivalent to the requirement that each element of $F_{q}$ occurs equally often in the full period of $\left(x_{n}\right)$.

Corollary. Suppose $f(x)$ is a PP of $F_{p}$ of degree $n \geq 3$ with $p>\left(n^{2}-3 n+4\right)^{2}$ and $h(x)$ is any polynomial over $F_{p}$ of degree $t \geq 1$ where $t<3 n / 5$ or $t \leq n-3$ and $(t, n)=1$. Then the sequence $(f(m)+h(m)), m=0,1, \ldots$, cannot be equidistributed in $F_{p}$.

Before closing we remark that as with Cohen's Theorem 2 of [2], we could extend our Theorem 2 above to "tame" PPs over general finite fields.

## Acknowledgment

We would like to thank the referee and G. Turnwald for a number of helpful suggestions and comments.

## References

1. S. Chowla and H. Zassenhaus, Some conjectures concerning finite fields, Norske Vid. Selsk. Forh. (Trondheim) 41 (1968), 34-35.
2. S. D. Cohen, Proof of a conjecture of Chowla and Zassenhaus on permutation polynomials, Canad. Math. Bull. 33 (1990), 230-234.
3. M. Fried, On a conjecture of Schur, Michigan Math. J. 17 (1970), 41-55 .
4. L. Kuipers and H. Niederreiter, Uniform distribution of sequences, Wiley-Interscience, New York, 1974.
5. R. Lidl and H. Niederreiter, Finite fields, Encyclopedia Math. Appl., vol. 20, AddisonWesley, Reading, MA, 1983 (now distributed by Cambridge Univ. Press).

Department of Mathematics, University of Glasgow, University Gardens, Glasgow G12 8QW, Scotland

E-mail address: sdc@maths.gla.ac.uk
Department of Mathematics, Pennsylvania State University, University Park, PennSYLVANIA 16802

E-mail address: mullen@math.psu.edu
Department of Mathematical Sciences, University of Nevada, Las Vegas 4505 Maryland Parkway, las Vegas, Nevada 89154

E-mail address: shiue@nevada.edu


[^0]:    Received by the editors May 24, 1992 and, in revised form, November 22, 1992 and November 22, 1993.

    1991 Mathematics Subject Classification. Primary 11T06.
    Key words and phrases. Finite field, permutation polynomial.
    This author would like to thank the NSA for partial support under grant agreement \#MDA904-87- H-2023.

