Serdica
Mathematical Journal
Сердика
Математическо списание

For further information on
Serdica Mathematical Journal
which is the new series of
Serdica Bulgaricae Mathematicae Publicationes
visit the website of the journal http://www.math.bas.bg/~serdica
or contact: Editorial Office
Serdica Mathematical Journal
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Telephone: (+359-2)9792818, FAX:(+359-2)971-36-49
e-mail: serdica@math.bas.bg

Serdica Math. J. **30** (2004), 177–194

Serdica
Mathematical Journal

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

DICKSON POLYNOMIALS THAT ARE PERMUTATIONS

Mihai Cipu*

Communicated by P. Pragacz

Abstract. A theorem of S.D. Cohen gives a characterization for Dickson polynomials of the second kind that permutes the elements of a finite field of cardinality the square of the characteristic. Here, a different proof is presented for this result.

1. Permutation polynomials of finite fields. In recent years cryptographers became interested in finding polynomials that induce a bijection of a finite field under substitution. This property has been used in several constructions of cryptographic systems for the secure transmission of data (see, for instance, [19], [22, Ch. IX], [23]). Permutations of this type have also notable applications in combinatorics (cf., e.g., [8], [28], [29]). However, the interest in permutation polynomials (shortly, PP) is not as recent as it might seem. A classical result of Hermite [17] provides a necessary and sufficient condition for

2000 *Mathematics Subject Classification:* 11T06, 13P10.

Key words: Dickson polynomial, Gröbner basis, permutation polynomial.

*Research supported by the CERES program of the Ministry of Education, Research and Youth, contract nr. 39/2002.

a polynomial function to permute the elements of a finite field $\mathbb{F}_q$, $q = p^d$, p a prime and d a positive integer.

Theorem 1 ([17]). *$f \in \mathbb{F}_q[X]$ is a permutation polynomial over $\mathbb{F}_q$ if and only if*

a) f has exactly one root in $\mathbb{F}_q$, and

b) the reduction of $f^t \mod (X^q - X)$, $1 \leq t \leq q-2$, with $t \not\equiv 0 \pmod p$, has degree at most $q-2$.

Brison [6] has generalized this criterion to polynomials that induce a permutation on the elements of a finite subgroup of the multiplicative group of an arbitrary field. Various other generalizations are given by many authors, including Brawley, Carlitz, and Levine [4], Brawley and Schnibben [5], James and Lidl [18].

Usually it is not possible to decide the permutation property directly. An obvious exception is the monomial case: X^n permutes $\mathbb{F}_q$ if and only if $\gcd(n, q-1) = 1$. For each class of PP a specific approach was needed.

London and Ziegler [24] and Mollin and Small [27] gave criteria for f to be a permutation in terms of the coefficients of f. Two sufficient conditions can be found in [7].

In [29] there are given necessary and sufficient conditions for binomials $X^{(q+1)/2} + aX$ to be PP on $\mathbb{F}_q$. Surprisingly enough, the PP in the class of cyclotomic polynomials can easily be identified.

Theorem 2 ([27]). *The cyclotomic polynomial Φ_m is a PP over $\mathbb{F}_q$ if and only if $m = 2$ or m and q are powers of 2.*

The class of "all one" polynomials $1 + X + \cdots + X^n$ has been investigated by Matthews [26]. His approach is based on a result of B. Segre on ovals in the projective plane of odd order q.

Theorem 3 ([26]). *If q is odd then $1 + X + \cdots + X^n$ is a PP on $\mathbb{F}_q$ if and only if $n \equiv 1 \mod p(q-1)$.*

The same technique yields several examples of polynomials of this shape which induce permutations of finite fields of characteristic 2, but a complete description has not appeared yet.

The permutation properties of the ubiquitous Chebyshev polynomials (also known as Dickson polynomials) have been also analysed. For any positive integer n one defines the *Dickson polynomial of the first kind* (DPFK) g_n by

$$g_n(X) := \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-1)^i X^{n-2i},$$

and the *Dickson polynomial of the second kind* (DPSK) f_n by

$$f_n(X) := \sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n-i}{i} (-1)^i X^{n-2i}.$$

Dickson polynomials played a major role in the proof of the so-called Schur conjecture concerning integral polynomials which induce permutations on the field $\mathbb{F}_p$ for infinitely many primes p [13]. Their importance has been again highlighted in the proof of Carlitz's conjecture asserting that for each even positive integer k there is a constant C_k such that, for each finite field of odd order $q > C_k$, there does not exist a PP of degree k over $\mathbb{F}_q$. After several partial results due to various authors, Fried, Guralnick, and Saxl [14] settled in the affirmative Carlitz's conjecture. Cohen [9] proved that, for p sufficiently large prime, all permutations of small degree on $\mathbb{F}_p$ come from Dickson polynomials.

It has been proved by Dickson [12] (see also [30] or [22]) that g_n permutes $\mathbb{F}_q$ if and only if n is coprime to q^2-1. The proof is easy. It is much more difficult to ascertain the permutation properties of DPSK. In his thesis, Mathews [25] pointed out a sufficient condition: if n satisfies the system of congruences

$$C(q): \begin{cases} n+1 \equiv \pm 2 \bmod p\ , \\ n+1 \equiv \pm 2 \bmod \dfrac{1}{2}(q-1)\ , \\ n+1 \equiv \pm 2 \bmod \dfrac{1}{2}(q+1)\ , \end{cases}$$

then $f_n(x) = \pm x$ for all elements x of $\mathbb{F}_q$, so f_n is a PP of $\mathbb{F}_q$. Several authors (see, for instance, [18], [20]) conjectured that condition $C(q)$ is also necessary in order that f_n permute $\mathbb{F}_q$. S. D. Cohen [10] solved in the affirmative this conjecture. Refining the proof ideas, he obtains a stronger result:

Theorem 4 ([11])**.** *Assume f_n permutes the elements of $\mathbb{F}_q$, where $q = p$ is an odd prime or $q = p^2$, $p \geq 7$ prime. Then the condition C(q) holds.*

Cohen's result is quite satisfactory since, for $p = 3$ or 5 and q composite ($d \geq 2$), there are known examples of DPSK which are PP on $\mathbb{F}_q$ and do not

satisfy $C(q)$. By extensive computer search, James and Lidl [18] established the permutation properties of several DPSK. For instance, f_{21} is a PP on $\mathbb{F}_3$ and $\mathbb{F}_9$, f_{177} is a PP on $\mathbb{F}_3$, $\mathbb{F}_9$, and $\mathbb{F}_{27}$, though Matthews' conditions $C(9)$ and $C(27)$ are not fulfilled. Computer experiments showed that f_{57} is a PP on $\mathbb{F}_5$ and $\mathbb{F}_{25}$, despite the fact that the congruences $C(25)$ do not hold.

Henderson and Matthews [16] describe classes of DPSK which are PP on fields of characteristic not covered by Cohen's theorem. The conditions they found is expressed in terms of residues of the degree modulo appropriate moduli. For p odd and $q = p^d$, let $n+1$ be congruent to N, M and L to the moduli p, $\frac{1}{2}(q-1)$ and $\frac{1}{2}(q+1)$, respectively. The sign class of n consists of all triples of the form $(\pm N, \pm M, \pm L)$, where each component and each negative is interpreted modulo the appropriate modulus. For $p = 2$, the definition of sign classes refers to the moduli 2, $q-1$, $q+1$ instead of p, $\frac{1}{2}(q-1)$ and $\frac{1}{2}(q+1)$, respectively. With this terminology, one has the next result.

Theorem 5 ([16]). 1) *If $q = 2^d$, then f_n is a PP of $\mathbb{F}_q$ if n belongs to any of the following classes:*

a) $\{0, 2^e, 2^e\}$, *with* $\gcd(n, e) = 1$,

b) $\{1, 2(2^s-1)^{-1}+1, 2(2^t-1)^{-1}+1\}$, *with* $\gcd(t, d) = \gcd(s, 2d) = 1$.

2) *For $p = 3$, f_n is a PP of $\mathbb{F}_q$ in the following cases:*

a) $\{2, 10, 10\}$ *and* $d = 3$,

b) $\{2, 4, 4\}$ *and d odd,*

c) $\{1, ((3^t-1)/2)^{-1}+1, ((3^s-1)/2)^{-1}+1\}$, *where* $\gcd(t, d) = \gcd(s, 2d) = 1$.

3) *Let $q = 5^d$. Then f_n is a PP of $\mathbb{F}_q$ if the sign class of n contains either* $\{2, 2, 2\}$ *or* $\{2, 2, (q-1)/4\}$.

Some results on the permutation behaviour of generalized Chebyshev polynomials (obtained by homogenising with respect to a variable of weight twice the weight of X) are also known. We refer the reader to [21, Chapter 2] for DPFK and respectively to [15] for DPSK.

Our purpose in this paper is to provide a new approach to Theorem 4 that we feel is more transparent and, moreover, capable of generalizations. In the next Section we will present a sketch of Cohen's proof of Theorem 4 because, on the one hand, some of the results needed in his proof will be also used in

the new proof, and, on the other hand, in order to appreciate the novelty of our approach. Section 3 is devoted to details of our treatment of Theorem 4.

2. Sketch of the proof of Theorem 4. It is well-known that Chebyshev polynomials take a particularly simple form by substituting $Y+Y^{-1}$ for X:

$$f_n(Y+Y^{-1}) = Y^n + Y^{n-2} + Y^{n-4} + \cdots + Y^{-n} = \frac{Y^{n+1} - Y^{-n-1}}{Y - Y^{-1}}. \tag{1}$$

From this identity it should be clear why, in the study of Dickson polynomials, $n+1$ rather than the degree n is relevant.

Although the problem we discuss makes sense when n is even, we shall assume it is odd because $f_{2n} \in \mathbb{F}_q[X^2]$. Another obvious remark is: If f_n is a PP of $\mathbb{F}_q$, then f_n is a PP of $\mathbb{F}_p$. In particular, the first congruence of $C(q)$ is a general constraint on the degree of a PP of $\mathbb{F}_q$.

From now on we suppose that f_n is a PP of $\mathbb{F}_q$, where $q = p^d$ and n are odd integers. It is not difficult to see that $C(7)$ is a consequence of the congruence $n+1 \equiv \pm 2 \bmod 7$, so we shall assume for the rest of the paper that $p \geq 11$.

Cohen shows [11, Section 4] that for $q \geq 11$ we may proceed with the following normalisation:

$$n+1 \equiv \pm M \bmod \frac{1}{2}(q-1),\ 2 \leq M \leq (q-3)/4, \tag{2}$$

$$n+1 \equiv \pm L \bmod \frac{1}{2}(q+1),\ 2 \leq L \leq (q-1)/4. \tag{3}$$

The first of Mathews' congruences is proved in [11, Lemma 3.1], so Theorem 4 is established (for prime fields) if we show that relations (2)–(3) only hold for $M = L = 2$. Cohen's strategy for the proof is to generate integer polynomials in D and P, and show that the unique solution in $\mathbb{F}_p$ of this system is $D = 0$, $P = 4$, where D and P denotes the difference and respectively the product of M and L. Indeed, note that $D \equiv 0$, $P \equiv 4 \bmod p$ imply $M \equiv \pm 2 \bmod p$; but $M \equiv -2$ is forbidden since $M = p-2$ contradicts the restriction $M \leq (p-3)/4$. Such subtle transfers back and forth from integers M and L in the specified ranges to their residue classes modulo $(q-1)/2$ and $(q+1)/2$, respectively, play a prominent role throughout the proof.

To implement this idea, we need an equation-producing machinery. The technology is based on the next result, proved in [11, Section 4].

Key-Lemma. *Let ζ and η be primitive root of the unity of order $q-1$ and $q+1$, respectively. For each $r = 1, 2, \ldots, \frac{1}{2}(q-3)$*

$$\sum_{i=0}^{q-2}\left[f_{M-1}(\zeta^i+\zeta^{-i})\right]^{2r}+\sum_{j=0}^{q}\left[f_{L-1}(\eta^j+\eta^{-j})\right]^{2r}+2^{2r+2}=2(M^{2r}+L^{2r}).$$

So we have to compute the coefficients of the Laurent polynomial obtained by expanding even powers of DPSK evaluated in $Y+Y^{-1}$. We find the relevant information in the result below, known to people working in invariant theory.

Proposition ([1])**.**

$$(1+X+\cdots+X^s)^r=\sum_{m=0}^{rs}\sum_{j\geq 0}(-1)^j\binom{r}{j}\binom{m-j(s+1)+r-1}{r-1}X^m.$$

As usual, a binomial coefficient whose upper index is smaller than the lower index has zero value.

As a consequence of the fact that a primitive root of unity generates a cyclic group, one has

Well-known Lemma. *Let s be an integer and ε a primitive root of unity of order s. For any integer t*

$$\sum_{i=0}^{s-1}\varepsilon^{it}=\begin{cases}-1 & \text{if } s \text{ divides } t,\\ 0 & \text{otherwise.}\end{cases}$$

Combining this result with the Proposition above and the Key-Lemma we are actually left with very few coefficients.

Let us start the machinery. The square of DPSK, as computed according to Proposition, has the form

$$f_t(Y+Y^{-1})^2=Y^{2t}+2Y^{2t-2}+\cdots+tY^2+(t+1)+tY^{-2}+\cdots+2Y^{-2t+2}+Y^{-2t}.$$

Having in view the values permitted to M, only the constant term has a non-zero contribution to the first sum in the Key-Lemma, so that

$$\sum_{i=0}^{q-2}f_{M-1}(\zeta^i+\zeta^{-i})^2=M(q-1)=-M \text{ in } \mathbb{F}_q.$$

Similarly, the second sum is congruent to $L \bmod p$. So we get a quadratic polynomial in M and L

$$Pol1 := 2(M^2 + L^2) + M - L - 16. \tag{4}$$

Since this polynomial is symmetrical in M and $-L$, it can be expressed polynomially in terms of D and P, which results in

$$Q1 := 2D^2 + D + 4P - 16. \tag{5}$$

Repeat the procedure for $r = 2$. From

$$f_t(Y+Y^{-1})^4 = Y^{4t} + 4Y^{4t-2} + \cdots + \frac{1}{3}(t+1)(2t^2+4t+3) + \cdots + 4Y^{-4t+2} + Y^{-4t}$$

and $4(M-1) < q-1$ and $4(L-1) < q$, it follows again that only the constant terms may have a non-zero contribution to the sums in the left side of the equality from the Key-Lemma. The polynomial generated is

$$Pol2 := 6(M^4 + L^4) + 2M^3 + M - 2L^3 - L - 192. \tag{6}$$

Passing to variables D and P, one finds the corresponding polynomial

$$Q2 := 6D^4 + 24PD^2 + 12P^2 + 2D^3 + 6PD + D - 192. \tag{7}$$

Invoke the Key-Lemma with the next value of r. This time, the normalisation no longer guarantees that we need only regard the constant term in the expansion of f_t^6; the coefficient of $Y^{\pm(q\pm1)}$ can also be significant. Accordingly, we have to distinguish four cases:

a) $M < (q+5)/6$ and $L < (q+7)/6$,

b) $(q+5)/6 \le M \le (q-3)/4$ and $(q+7)/6 \le L \le (q-1)/4$,

c) $(q+5)/6 \le M \le (q-3)/4$ and $L < (q+7)/6$,

d) $M < (q+5)/6$ and $(q+7)/6 \le L \le (q-1)/4$.

a) We first examine the case M and L are both so small that the expansion only involves powers smaller than $q-1$. In this situation, only the constant terms in $f_t^6(Y+Y^{-1})$ $(t = M-1, L-1)$ matter. Thus, for $M < (q+5)/6$, $L < (q+7)/6$ we get the polynomial

$$h3a := 40M^6 + 40L^6 + M(11M^4 + 5M^2 + 4) - L(11L^4 + 5L^2 + 4) - 5120.$$

Let me briefly present the arguments Cohen uses to exclude the primes that occur this way. First, he finds the common root of the two polynomials in the prime field. Cohen rewrites equation $Q1 = 0$ as

$$P = 4 - \frac{1}{4}D - \frac{1}{2}D^2. \tag{8}$$

Introducing this into equation $Q2 = 0$ results in

$$12D^4 + 16D^3 - 189D^2 - 4D = 0. \tag{9}$$

Hence, we get either $D = 0$ (so that, by equation (8), $P \equiv 4 \mod p$ and we are done), or a polynomial over $\mathbb{F}_p$

$$12D^3 + 16D^2 - 189D - 4. \tag{10}$$

Similarly from $h3a$ one gets

$$40D^6 + 240PD^4 + 360P^2D^2 + 80P^3 + 11D^5 + 55PD^3 + 55P^2D + 5D^3 + 15PD + 4D - 5120,$$

so, eliminating again P by means of (8), one concludes that

$$196D^5 - 3600D^4 - 7685D^3 + 60580D^2 - 256D \equiv 0 \mod p. \tag{11}$$

Therefore, either D is multiple of p or its residue mod p is a root in $\mathbb{F}_p$ of

$$196D^4 - 3600D^3 - 7685D^2 + 60580D - 256. \tag{12}$$

The proof is complete if the only common root of equations (9) and (11) in $\mathbb{F}_p$ is $D \equiv 0 \mod p$. Otherwise the polynomials (10) and (12) have a common root mod p. This only happens if the characteristic p divides their resultant

$$1493463162316800 = 2^{11} \cdot 3 \cdot 5^2 \cdot 5569 \cdot 1745927.$$

Thus we have to further examine the situation for $p = 5569$ or 1 745 927. For $p = 5569$, the common root in $\mathbb{F}_p$ is $D \equiv 14 \mod p$, so, by (8), $P \equiv 2687 \mod p$. By direct computation one finds $D^2 + 4P \equiv 5375 \mod p$, which is not a square residue mod 5569. Hence integers M, L do not exist with $(M + L)^2 \equiv D^2 + 4P \equiv 5375 \mod p$. The same argument works for $p = 1\ 745\ 927$. Thus is case a) one obtains the desired conclusion.

b) Let us examine what happens when M and L are both big. Here "big" means that in the expansion of $f_{M-1}(Y+Y^{-1})^6$ and $f_{L-1}(Y+Y^{-1})^6$ one encounters the powers $Y^{\pm(q\pm1)}$. For $(q+5)/6 \le M \le (q-3)/4$ and $(q+7)/6 \le L \le (q-1)/4$, the Key-Lemma yields

$$2(M^6+L^6)+c_0(M)-c_0(L)+2c_{q-1}(M)-2c_{q+1}(L)=256, \tag{13}$$

where $c_j(t)$ is the coefficient of Y^j in $f_{t-1}(Y+Y^{-1})^6$. By Proposition above, one has for these values of M and L

$$c_0(T)=\binom{3T+2}{5}-6\binom{2T+2}{5}+15\binom{T+2}{5}=\frac{11T^5+5T^3+4T}{20},$$

$$c_{q-1}(M)=\binom{3M+\frac{5-q}{2}}{5},$$

$$c_{q+1}(L)=\binom{3L+\frac{3-q}{2}}{5}.$$

Substituting in equation (13), one gets a sextic polynomial, symmetric in M and $-L$.

$$\begin{aligned} h3b :=\ & 640(M^6+L^6)+1472(M^5-L^5)+1080(M^4+L^4)-280(M^3-L^3) \\ & -300(M^2+L^2)+73(M-L)-81905. \end{aligned}$$

Passing to polynomials D and P, one gets

$$\begin{aligned} & 640D^6+3840PD^4+5760P^2D^2+1280P^3+1472D^5+7360PD^3 \\ & +7360P^2D+1080D^4+4320PD^2+2160P^2-280D^3-840PD \\ & -300D^2-600P+73D-81905. \end{aligned} \tag{14}$$

After eliminating P it results the polynomial

$$128D^5+4140D^4+7640D^3-56665D^2-94943D-32175. \tag{15}$$

Let us call f_n exceptional on $\mathbb{F}_q$ if it is PP on $\mathbb{F}_q$ and does not satisfy Matthews' condition $C(q)$. Exceptional DPSK may only exist on fields whose characteristic divides the resultant of polynomials (10) and (15). Using the computer algebra package PARI/GP [2] one finds that this only happens for five values of $p \ge 11$, namely $p=11$, $p=19$, $p=47$, $p=1\ 693$ and $p=390\ 357\ 049$. These values do not coincide with those found in the original proof because Cohen's calculations produced a sextic polynomial instead of the quintic (15).

c) The next case is M big and L small, i.e. $(q+5)/6 \le M \le (q-3)/4$ and $L < (q+7)/6$, so that

$$2(M^6 + L^6) + c_0(M) - c_0(L) + 2c_{q-1}(M) = 256.$$

Performing the calculations, it results the polynomial

$$\begin{aligned} h3c := {} & 1280(M^6 + L^6) + 352(M^5 - L^5) + 160(M^3 - L^3) + 128(M - L) \\ & + 2592M^5 + 2160M^4 - 720M^3 - 600M^2 + 18M - 163825. \end{aligned} \tag{16}$$

Since the resulting polynomial is no longer symmetric in M and $-L$, one cannot obtain a polynomial in D and P. It is possible to rewrite $h3c$ as a polynomial $Q3c$ in M and D. Similarly $Q1$ gives rise to a polynomials $Q1c$ of M and D. Cohen searches for primes for which $Q1c$, $Q2$, and $Q3c$ are simultaneously soluble mod p by successively computing R, the resultant of $Q1c$ and $Q3c$ with respect to variable M, and then the resultant of R and the polynomial given by relation (10) with respect to D. The computations performed with PARI/GP yield a number with 52 digits and prime decomposition

$$2^{51} \cdot 3^4 \cdot 5^5 \cdot 11 \cdot 31 \cdot 424\,928\,167 \cdot 70\,588\,464\,402\,288\,705\,233.$$

The prime numbers greater than 11 in this factorization are candidates for characteristic of fields in which Matthews' condition does not hold, and therefore subsequent work is required in order to settle these cases.

d) Finally, one has to consider $M < (q+5)/6$, $(q+7)/6 \le L \le (q-1)/4$. This situation is similar to case c): just replace M by $-L$ in the second line of relation (16), as well as in the polynomial $Q3c$.

At this point we have a few polynomial systems and several primes p such that these systems have solutions in the prime field of characteristic p. We want to show that the only solution in the ranges permitted by normalisation is $M = L = 2$. For prime fields, of characteristic p computed in case b), Cohen explicitly finds the common root mod p of polynomials (10) and (15) and obtains the desired conclusion by showing that no integers M, L in the indicated ranges are congruent to this root mod p.

This task is considerably more difficult when q is composite. Cohen uses the fact that $C(p)$ and normalisation for $q = p^2$ are simultaneously satisfied only by four values of M. By ingenious, though *ad-hoc*, reasoning, the desired conclusion is obtained in all but the following cases:

$$\begin{aligned} q = {} & 31^2, \ M = 62, \ \text{ and } L = 177, 208, \ \text{ or } 239, \\ q = {} & 31^2, \ M = 238, \ \text{ and } L = 12, 105, \ \text{ or } 136, \\ q = {} & 151^2, \ M = 2, \ \text{ and } L = 2267. \end{aligned}$$

The specific arguments needed in order to complete the proof vary from case a) to b) or c). The finishing touch is possible thanks to a p-adic version of the Key-Lemma which permits to eliminate the unyielding cases listed above. The approach sketched above has several drawbacks:

1. The necessity to find all solutions of quintic or sextic univariate polynomials in large prime fields is a non-trivial task (for instance, recall that in case b) occurs a prime with 9 decimal digits, while in case c) a prime with 20 digits made appearance).

2. Performing elimination by successively taking resultants has the potential of introducing fake factors. To the best of our knowledge, there is known no general procedure to distinguish them from true factors.

3. The need to apply a p-adic version of the Key-Lemma is somewhat unsatisfactory.

3. Details of the alternate proof. Our approach is based on Gröbner bases computations. Though still machine-dependent, it obviates so many case-by-case arguments and confirms Cohen's hope that his result can be extended to higher d.

We generate one more polynomial $Pol4) \in \mathbb{Z}[M, L]$ applying the Key-Lemma with $r = 4$. (This is legitimate only for $q \geq 11$.) The coefficients vary according to whether M is $<$ or $\geq (q+7)/8$, and L is $<$ or $\geq (q+9)/8$, see Table 1.

The free term of $f_{T-1}(Y+Y^{-1})^8$ $(T = M, L)$ is, according to Proposition above,

$$c_0^4(T) = \binom{4T+3}{7} - 8\binom{3T+3}{7} + 28\binom{2T+3}{7} - 56\binom{T+3}{7}$$
$$= \frac{151T^7 + 70T^5 + 49T^3 + 45T}{315}.$$

Since $8M < 2(q-1)$ by our normalisation (2), the only monomials in the expansion of $f_{M-1}(Y+Y^{-1})^8$ with exponents divisible by $q-1$ are $Y^{\pm(q-1)}$. As seen from Proposition, the formula for the coefficients of these powers of Y involves one or two binomial coefficients, according to whether $3M + \dfrac{1-q}{2} + 3$ is less than or greater than 7. Let us denote

$$c_{q-1}^1(M) = \binom{4M + \frac{1-q}{2} + 3}{7} \quad \text{for} \quad M \leq (q+5)/6,$$

$$c^2_{q-1}(M) = c^1_{q-1}(M) - 8\binom{3M + \frac{1-q}{2} + 3}{7} \quad \text{for} \quad (q+7)/6 \le M \le (q-3)/4,$$

and similarly

$$c^1_{q+1}(L) = \binom{4L - \frac{1+q}{2} + 3}{7} \quad \text{for} \quad L \le (q+7)/6,$$

$$c^2_{q+1}(L) = c^1_{q+1}(L-1) - 8\binom{3L - \frac{1+q}{2} + 3}{7} \quad \text{for} \quad (q+9)/6 \le L \le (q-1)/4.$$

Clearly, $c^2_{q-1}(M)$ exists only for $q \ge 23$, and $c^2_{q+1}(L)$ only for $q \ge 29$.

The Key-Lemma yields one of the following primitive polynomials with integer coefficients:

$$\begin{aligned}
h41 &:= 315\big(2M^8 + 2L^8 - 2^{10} + c^4_0(M) - c^4_0(L)\big),\\
h42 &:= 1024\big(h41 + 630c^1_{q-1}(M)\big),\\
h43 &:= 1024\big(h41 + 630c^2_{q-1}(M)\big),\\
h44 &:= 1024\big(h41 - 630c^1_{q+1}(L)\big),\\
h45 &:= \frac{1}{2}h44 + 1024 \cdot 315c^1_{q-1}(M),\\
h46 &:= \frac{1}{2}h44 + 1024 \cdot 315c^2_{q-1}(M),\\
h47 &:= 1024\big(h41 - 630c^2_{q+1}(L)\big),\\
h48 &:= \frac{1}{2}h42 - 1024 \cdot 315c^2_{q+1}(L),\\
h49 &:= \frac{1}{2}h43 - 1024 \cdot 315c^2_{q+1}(L).
\end{aligned}$$

We consider the ideal I generated in the polynomial ring $\mathbb{Z}[M, L]$ by $Pol1$, $Pol2$, $Pol3$, $Pol4$, given respectively by equations (4), (6) and Table 1.

In order to make computations depend as little as possible on the characteristic of the field, we choose to compute Gröbner bases over integers. Thus we need to keep track not only of the leading monomials, but also of the leading coefficients of all polynomials entering the Gröbner bases. MAGMA [3] is one of the computer algebra systems with such capabilities.

Let us number with Roman digits the 16 cases described in Table 1, starting from the upper-left corner and going right and down. From the output of

		M	$\le (q+5)/8$	$\le (q+3)/6$	$= (q+5)/6$	$\le (q-3)/4$
L	$\le (q+7)/8$		$h3a$, $h41$	$h3a$, $h42$	$h3c$, $h42$	$h3c$, $h43$
	$\le (q+5)/6$		$h3a$, $h44$	$h3a$, $h45$	$h3c$, $h45$	$h3c$, $h46$
	$= (q+7)/6$		$h3d$, $h44$	$h3d$, $h45$	$h3b$, $h45$	$h3b$, $h46$
	$\le (q-1)/4$		$h3d$, $h47$	$h3d$, $h48$	$h3b$, $h48$	$h3b$, $h49$

Table 1. The third and fourth generator of the ideal I

a MAGMA session we see that the ideal I is generated in Case I by six polynomials:

$$\begin{aligned}
&M^2 + 8M + 31L^2 - 8L - 128,\\
&ML + 2M + 4L^3 + 111L^2 - 18L - 448,\\
&15M + 60L^2 - 15L - 240,\\
&4L^4 + 20L^2 - 144,\\
&8L^3 + 72L^2 - 32L - 288,\\
&120L^2 - 480.
\end{aligned}$$

In every polynomial ring over a field of characteristic greater than 5, these polynomials generate the same ideal as the polynomials $M - L$ and $L^2 - 4$. This means that in this case $M \equiv L \equiv \pm 2 \pmod{p}$ for $p > 5$.

In Cases II–XVI the ideal I contains a constant polynomial (the largest entry in the second column of Table 2). Therefore, the polynomials $Pol1$, $Pol2$, $Pol3$, $Pol4$ we are interested in may have a common solution only in fields of characteristic dividing one of the leading coefficients appearing in Gröbner bases. Table 2 contains relevant information.

Case	Coefficients > 1	Prime divisors
I	4, 8, 15, 120	2, 3, 5
II, V	15, 14549535, 15058768725	3, 5, 7, 11, 13, 17, 19, 23
III, VII	15, 45, 6435, 765765	3, 5, 7, 11, 13, 17
IV	15, 495, 6435, 2297295	3, 5, 7, 11, 13, 17
VI	15, 101846745	3, 5, 7, 11, 13, 17, 19
VIII	15, 495, 6435, 765765	3, 5, 7, 11, 13, 17
IX	15, 1035	3, 5, 23
X, XIV	15, 45	3, 5
XI, XII, XV, XVI	4095	3, 5, 7, 13
XIII	15, 405	3, 5

Table 2. Leading coefficients in bivariate Gröbner bases over $\mathbb{Z}$

A first remark is that exceptional DPSK may exist only on fields of very small characteristic. These computations already suffice to conclude the necessity of Matthews' condition $C(p)$ if $p > 23$. Moreover, the conclusion of Theorem 4 is reached in each of the Cases I, X, XIII, XIV. It remains to establish the same conclusion when p is between 11 and 23.

For each prime $p > 7$ appearing in the last column of Table 2 we computed a Gröbner basis of the image of the ideal I in the polynomial ring $\mathbb{F}_p[M, L]$. A synopsis of the output is given in Table 3 below.

Case	Polynomials
II, V	$M \equiv L \equiv \pm 2 \pmod{p}$ $(p \leq 19)$, $M \equiv L \equiv 2 \pmod{23}$
III, IV, VII, VIII	$M \equiv L \equiv \pm 2 \pmod{13}$, $M \equiv L \equiv 2 \pmod{17}$
VI	$M \equiv L \equiv \pm 2 \pmod{p}$, $(13 \leq p \leq 19)$
IX	$M \equiv L \equiv 2 \pmod{23}$
XI, XII, XV, XVI	$M \equiv L \equiv \pm 2 \pmod{13}$

Table 3. Gröbner bases over $\mathbb{F}_p$, $(p > 11)$

It is obvious that these computations suffice for $q = p > 11$ but for $q = p^2$ or $q = p = 11$ yield only congruences for M, $L \pmod{p}$ and so require further work.

For $p = 11$, in all cases but IV and VIII the computer delivered the same Gröbner basis over $\mathbb{F}_p$, namely $M - L$, $M^2 - 4$. In the case IV or VIII we obtain the polynomials $M^2 + 6M + 5L + 7$, $ML + 9M + 2L + 7$, $L^2 + 7$. It is easy to find all solutions of this polynomial system: $(2, 2)$, $(3, 2)$, $(-2, -2) \in \mathbb{F}_{11}$. The second entry in this list does not fulfil Matthews' condition $C(11)$. It is perfectly legitimate in the realm of ideal theory, but not relevant in our initial context. Indeed, the case IV, resp. VIII, is defined by the polynomial $h43$, resp. $h46$, involving the coefficient $c_{q-1}^2(M)$. As remarked before, this value does not actually appear for $q < 23$. Therefore, Theorem 1.4 is established for prime fields of characteristic greater than 7. The considerations below refer to q composite.

For each of the 16 cases described by Table 1 the computation ended in less than 4 seconds. Subsequent computations described below are even easier.

Let us now suppose that $q = p^2$. Recall that normalisation described by equations (2) and (3) is in force. The fact that $\frac{1}{2}(p^2 - 1)$ is multiple of the two consecutive integers $\frac{1}{2}(p - 1)$ and $\frac{1}{2}(p + 1)$ means that M is congruent to either 2 or -2 modulo $\frac{1}{2}(p \pm 1)$. These congruences are satisfied only by four integers in the range $2 \leq M \leq (q - 3)/4$, namely 2, $2p$, $(p^2 - 8p - 1)/4$ and $(p^2 - 9)/4$.

$M = 2p$		$M = (p^2 - 8p - 1)/4$		$M = (p^2 - 9)/4$	
Case	Constant	Case	Constant	Case	Constant
I	48	VI	315	I–IV, VI–VIII	255
II–XVI	3	IX, X, XIII, XIV	9	V	1275
		I–V, VII, VIII	63	IX, X, XIII, XIV	15
		XI, XII, XV, XVI	63	XI, XII, XV, XVI	3

Table 4. Constant polynomials in univariate Gröbner bases over $\mathbb{Z}$

We specialize *Pol*1, *Pol*2, *Pol*3, *Pol*4 by letting M take one of the last three values in the list above and compute Gröbner bases of the resulting univariate integer polynomial ideals. Each Gröbner basis contains a constant polynomial, cf. Table 4. From the data given in Table 4 we conclude that the proof of Theorem 4 is completed, except when $p = 17$, $M = (p^2 - 9)/4$ and $L \le (q + 5)/6$. From Table 1 it is clear that, for these values of M and L, the ideal I is generated by *Pol*1, *Pol*2, *h*3*c* and either *h*43 or *h*46. We apply once more the Key-Lemma with $r = 5$. Since $2(q - 1) < 10M < 3(q - 1)$ and $10L < 2q$, this means that we have to consider a polynomial of the form

$$2(M^{10} + L^{10}) - 2^{12} + s_0(M) - s_0(L) + 2s_1(M) + 2s_2(M) - 2s_3(L),$$

where

$$\begin{aligned} s_0(T) &= \binom{5T+4}{9} - 10\binom{4T+4}{9} + 45\binom{3T+4}{9} - 120\binom{2T+4}{9} \\ &\quad + 210\binom{T+4}{9} \quad (T = M, L), \\ s_1(M) &= \binom{5M + \frac{9-q}{2}}{9} - 10\binom{4M + \frac{9-q}{2}}{9} + 45\binom{3M + \frac{9-q}{2}}{9}, \\ s_2(M) &= \binom{5M + 5 - q}{9}, \end{aligned}$$

and

$$s_3(L) = \begin{cases} \binom{5L + \frac{7-q}{2}}{9} & \text{for } (q+11)/10 \le L \le (q+9)/8, \\ \binom{5L + \frac{7-q}{2}}{9} - 10\binom{4L + \frac{7-q}{2}}{9} & \text{for } (q+11)/8 \le L \le (q+5)/6. \end{cases}$$

The coefficients of the resulting primitive integer polynomial *Pol*5 vary according to the location of L. Considerations similat to those detailed before lead to distinguish four cases:

A) Case IV for $L \leq (q+9)/10$,

B) Case IV for $(q+11)/10 \leq L \leq (q+7)/8$,

C) Case VIII for $L = (q+9)/8$,

D) Case VIII for $(q+11)/8 \leq L \leq (q+5)/6$.

MAGMA computes Gröbner bases of the ideal generated by the specializations of the polynomials $Pol1$, $Pol2$, $Pol3$, $Pol4$, $Pol5$ to $M = -9/4$. The output contains the constant polynomial 15 in cases A), B) and D), and the constant polynomial 3 in case C). Therefore we conclude that polynomials $Pol1$, $Pol2$, $Pol3$, $Pol4$, $Pol5$ have no common roots in $\mathbb{F}_{17}$.

As a result of these computations we obtain $M = 2$ and $L \equiv 2 \pmod{p}$. Cohen proves [11, Section 6] that equations obtained by applying the Key-Lemma for $r = (p+1)/2$ and $r = p+1$ eliminates all possibilities but $p = 443$ and $L = 9305$ or $p = 151$ and $L = 2267$. However, it turns out that each of these putative solutions is incompatible with what results for $r = 5$.

This ends the proof of Theorem 4.

Acknowledgements. The author is grateful to Professor S.D. Cohen for useful discussions.

REFERENCES

[1] G. ALMKVIST. Commutative and noncommutative invariant theory. In: Topics in Algebra, Part 2 (Warsaw, 1988), Banach Center Publ., vol. **26**, Part 2, PWN, Warsaw, 1990, 259–268.

[2] C. BATUT, K. BELABAS, D. BERNARDI, H. COHEN, M. OLIVIER. User's guide to PARI/GP, Univ. Bordeaux, Nov. 2000. (see also http://www.parigp-home.de/)

[3] W. BOSMA, J. CANNON, C. PLAYOUST. The Magma algebra system. *J. Symb. Comp.* **24** (1997), 235–265. (see also http://magma.maths.usyd.edu.au/magma/)

[4] J. BRAWLEY, L. CARLITZ, J. LEVINE. Scalar polynomial functions on the $n \times n$ matrices over a finite field. *Linear Algebra Appl.* **10** (1975), 199–217.

[5] J. Brawley, G. E. Schnibben. Polynomials which permute the matrices over a field. *Linear Algebra Appl.* **86** (1987), 145–160.

[6] O. J. Brison. On group permutation polynomials. *Portug. Math.* **50** (1993), 365–383.

[7] L. Carlitz, J. A. Lutz. A characterization of permutation polynomials over a field. *Amer. Math. Monthly* **85** (1978), 746–748.

[8] S. D. Cohen, M. J. Ganley. Some classes of translation planes. *Quart. J. Math. Oxford Ser.* (2) **35** (1984), 101–113.

[9] S. D. Cohen. Proof of a conjecture of Chowla and Zassenhaus. *Canad. Math. Bull.* **33** (1990), 230–234.

[10] S. D. Cohen. Dickson polynomials of the second kind that are permutations. *Canad. Math. Bull.* **46** (1994), 225–238.

[11] S. D. Cohen. Dickson permutations. In: Number Theoretic and Algebraic Methods in Computer Science, Proc. Internat. Conf. Moscow June/July 1993 (Eds Alf J. van der Poorten, I. Shparlinski, Horst G. Zimmer), World Scientific, Singapore, New Jersey, London, Hong Kong, 1995, 29–51.

[12] L. E. Dickson. Linear Groups with an Exposition of the Galois Field Theory. Teubner, Leipzig, 1901; Dover, New York, 1958.

[13] M. Fried. On a conjecture of Schur. *Michigan Math. J.* **17** (1970), 41–55.

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

[15] M. Henderson. A note on the permutation behaviour of the Dickson polynomials of the second kind. *Bull. Australl. Math. Soc.* **56** (1997), 499–505.

[16] M. Henderson, R. Matthews. Permutation properties of Chebyshev polynomials of the second kind over a finite field. *Finite Fields Appl.* **1** (1995), 115–125.

[17] C. Hermite. Sur les fonctions de sept lettres. *C. R. Acad. Sci. Paris* **57** (1863), 750–757; *Oeuvres*, vol. **2**, Gauthier-Villars, Paris, 1908, 280–288.

[18] N. S. James, R. Lidl. Permutation polynomials on matrices, *Linear Algebra Appl.* **96** (1987), 181–190.

[19] J. Levine, J. V. Brawley. Some cryptographic applications of permutation polynomials. *Cryptologia*, **1** (1977), 76–92.

[20] R. Lidl, G. L. Mullen. When does a polynomial over a finite field permute the elements of the field? *Amer. Math. Monthly*, **95** (1988), 243–246.

[21] R. Lidl, G. L. Mullen, G. Turnwald. Dickson Polynomials. Pitman Monographs and Surveys in Pure and Appl. Math., vol. **65**, Longman Scientific and Technical, Essex, England, 1993.

[22] R. Lidl, H. Niederreiter. Finite Fields. Encyclopedia Math. Appl., vol. **20**, Addison-Wesley, Reading, Mass., 1983.

[23] R. Lidl, W. B. Müller. A note on polynomials and functions in algebraic cryptography. *Ars Comb.* **171** (1984), 223–229.

[24] D. London, Z. Ziegler. Functions over the residue field modulo a prime. *J. Austral. Math. Soc. Ser. A* **7** (1967), 410–416.

[25] R. W. Matthews. Permutation Polynomials in One and Several Variables. Ph.D. Dissertation, Univ. of Tasmania, 1982.

[26] R. Matthews. Permutation properties of the polynomials $1 + x + \cdots + x^k$ over a finite field. *Proc. Amer. Math. Soc.* **120** (1994), 47–51.

[27] R. A. Mollin, C. Small. On permutation polynomials over finite fields. *Internat. J. Math. Math. Sci.* **10** (1987), 535–544.

[28] H. Niederreiter, K. H. Robinson. Bol loops of order pq. *Math. Proc. Cambridge Philos. Soc.* **89** (1981), 241–256.

[29] H. Niederreiter, K. H. Robinson. Complete mappings of finite fields. *J. Austral. Math. Soc. Ser. A* **33** (1982), 197–212.

[30] W. Nöbauer. Uber Permutationspolynome und Permutationsfunktionen für Primzahlpotenzen. *Monats. M.* **69** (1965), 230–238.

Institute of Mathematics "Simion Stoilow" of the Romanian Academy
P. O. Box 01-764
RO-014700 Bucharest, Romania
e-mail: mihai.cipu@imar.ro

Received March 18, 2004