Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
Finite Fields and Their Applications 13 (2007) 58–70
FINITE FIELDS AND THEIR APPLICATIONS
http://www.elsevier.com/locate/ffa

Permutation polynomials and applications to coding theory

Yann Laigle-Chapuy*

INRIA, Domaine de Voluceau, BP 105, 78153 Rocquencourt, Le Chesnay Cedex, France

Received 30 November 2004; revised 18 May 2005

Communicated by Rudolf Lidl

Available online 29 September 2005

Abstract

We present different results derived from a theorem stated by Wan and Lidl [Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure, Monatsh. Math. 112(2) (1991) 149–163] which treats specific permutations on finite fields. We first exhibit a new class of permutation binomials and look at some interesting subclasses. We then give an estimation of the number of permutation binomials of the form $X^r(X^{(q-1)/m} + a)$ for $a \in \mathbb{F}_q^*$. Finally we give applications in coding theory mainly related to a conjecture of Helleseth.

Keywords: Finite fields; Permutation; Permutation binomial; Complete permutation; Niho exponent; Balanced codeword; Cross-correlation function; Boolean function

1. Introduction

The study of permutation polynomials started with Hermite [9] for prime fields, and Dickson [5] for arbitrary finite fields. Recently, the applications of permutations of finite fields for cryptography [11–13,16,17,20] bring this subject back to the front scene. The articles of Lidl and Mullen [14,15] list some open problems of interest and one of them is to find new classes of permutation polynomials. Despite the

* Fax: +33 1 3963 5051.
E-mail address: yann.laigle-chapuy@inria.fr.

1071-5797/$ - see front matter © 2005 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2005.08.003

interest of numerous authors, still very little is known about which polynomials are permutation ones.

This article is based on a characterization of permutation polynomials from Niederreiter [21] generalized by Lidl and Wan [26] from which we derive a new class of permutation polynomials. We then exhibit interesting subclasses it contains: permutation binomials [4,10,23,24,6,27], complete permutations [19,21,25] and power permutation with Niho exponents [3,7,22]. In a second part, we establish a lower bound on the number of permutation polynomials of the form $X^r(X^{(q-1)/m}+a)$.

Finally, we state some consequences in coding theory. This work was first motivated by the study of an old conjecture by Helleseth [8]

Conjecture 1.1. *For all integer k coprime with 2^n-1, there exists $a \in \mathbb{F}_{2^n}^*$ such that* $\mathrm{Trace}(x^k+ax)$ *is a balanced word.*

The links between this conjecture and the preceding results are given in the third part.

2. Preliminary

In this article, p will be a prime number, q a power of p, and $\mathbb{F}_q$ will denote the finite field of order q. $\mathbb{F}_q[X]$ is the set of polynomials with coefficients in $\mathbb{F}_q$ and indeterminate X. α will be a primitive element in $\mathbb{F}_q$.

Definition 2.1. A polynomial with coefficients in $\mathbb{F}_q$ for which the associated polynomial function is a permutation of $\mathbb{F}_q$ is called *permutation polynomial of* $\mathbb{F}_q$.

In [26], Wan and Lidl give a useful characterization of permutation polynomials we will use extensively.

Theorem 2.2. *Let m and r be two positive integers such that m divides $q-1$. Let α be a primitive element in $\mathbb{F}_q$ and assume P is a polynomial in $F_q[X]$. Then $Q = X^r P(X^{(q-1)/m})$ is a permutation polynomial of $\mathbb{F}_q$ if and only if the following conditions are satisfied*:

(i) $\mathrm{Gcd}(r, \frac{q-1}{m}) = 1$.

(ii) $\forall i;\ 0 \leqslant i < m,\ P(\alpha^{i\frac{q-1}{m}}) \neq 0$.

(iii) $\forall i, j;\ 0 \leqslant i < j < m,\ Q(\alpha^i)^{\frac{q-1}{m}} \neq Q(\alpha^j)^{\frac{q-1}{m}}$.

Remark 1. If m is small, this also gives an efficient way to test whether Q is a permutation polynomial.

Remark 2. If $m = q-1$, we get $Q = X^r P(X)$ is a permutation polynomial if and only if the associated function on $\mathbb{F}_q$ is injective.

Remark 3. If $m = 1$, we get $Q = P(1)X^r$ is a permutation polynomial if and only if

(i) $\mathrm{Gcd}(r, q-1) = 1$.
(ii) $P(1) \neq 0$.

In the third section, we will need a classical theorem on character sums.

Definition 2.3. Let G be a finite group of order m. A morphism $\psi : G \to \mathbb{C}$ is called a *character* of the group G. When G is the multiplicative group $\mathbb{F}_q^*$, ψ is extended using $\psi(0) = 0$.

Theorem 2.4 (*see Lidl and Niederreiter [18, Theorem 5.41]*). *Let ψ be a multiplicative character of $\mathbb{F}_q$ of order $m > 1$ and let $P \in \mathbb{F}_q[X]$ be a monic polynomial of positive degree that is not an mth power of a polynomial. Let d be the number of distinct roots of P in its splitting field over $\mathbb{F}_q$. Then for every $x \in \mathbb{F}_q$ we have*

$$\left|\sum_{a\in\mathbb{F}_q} \psi(xP(a))\right| \leqslant (d-1)\sqrt{q}.$$

3. A new class of permutation polynomials

We will derive from Theorem 2.2 a new class of permutation polynomials, with coefficients lying in an appropriate subfield.

Theorem 3.1. *Let p be a prime, m be a positive integer and k be the order of p in $\mathbb{Z}/m\mathbb{Z}$. Let ℓ be a positive integer, take $q = p^{k\ell m}$. Assume r is a positive integer coprime with $q-1$ and P is a polynomial in $F_{p^{k\ell}}[X]$.*

Then the polynomial $Q = X^r P\left(X^{\frac{q-1}{m}}\right)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if

$$\text{(iv)}\ \forall \omega \in \mathbb{F}_q \text{ such that } \omega^m = 1, \quad P(\omega) \neq 0.$$

Proof. We use Theorem 2.2. Note that (iv) is (ii). Thus we have to prove that Q satisfies (i) and (iii).

The integer r is coprime with $q-1$ and thus coprime with $(q-1)/m$ too. Condition (i) is thus satisfied.

For (iii), we first note that

$$\frac{q-1}{m} = \frac{p^{k\ell}-1}{m} \sum_{j=0}^{m-1} p^{k\ell j}. \tag{1}$$

Let ω be a generator of the cyclic subgroup of order m of $\mathbb{F}_q^*$. As it lies in $\mathbb{F}_{p^{k\ell}}$, we have $P(\omega^i)^{p^{k\ell}} = P(\omega^i)$ for $0 \leqslant i < m$. We then obtain

$$\begin{aligned}
P(\omega^i)^{\frac{q-1}{m}} &= P(\omega^i)^{\frac{p^{k\ell}-1}{m}\sum_{j=0}^{m-1} p^{k\ell j}} \quad \text{via Eq. (1)} \\
&= \left(\prod_{j=0}^{m-1} P(\omega^i)^{p^{k\ell j}}\right)^{\frac{p^{k\ell}-1}{m}} \\
&= \left(P(\omega^i)^m\right)^{\frac{p^{k\ell}-1}{m}} \quad \text{because } P(\omega^i) \text{ lies in } \mathbb{F}_{p^{k\ell}} \\
&= P(\omega^i)^{p^{k\ell}-1} \\
&= 1
\end{aligned}$$

and thus, we get $Q(\omega^i) = \omega^{ri}$. The ω^{ri}, $0 \leqslant i < m$, are pairwise distinct because r is coprime with $q-1$. Condition (iii) is then always satisfied by Q and being a permutation polynomial is equivalent to condition (ii); the necessary and sufficient condition we give is just a rewrite of it. $\square$

Remark 4. This gives an easy way to construct sparse permutation polynomials.

Example 1. Let $p := 2$, $m := 3$ and $\ell := 3$, which give $k := 2$ and $q := 2^{18}$.
Let

$$\mathbb{F}_q = \mathbb{F}_2[y]/(y^{18} + y^3 + 1)$$

we have

$$\begin{aligned}
\mathbb{F}_{p^{k\ell}} = \mathbb{F}_{2^6} &= \mathbb{F}_2\left[y^3\right]/(y^{18} + y^3 + 1) \\
&= \mathbb{F}_2[z]/(z^6 + z + 1).
\end{aligned}$$

The polynomial $P(X) = X^2 + (z^5 + z^4 + z^2)X + (z^4 + z) \in \mathbb{F}_{2^6}[X]$ is irreducible on $\mathbb{F}_{2^6}$ and then has no root in $\mathbb{F}_{2^6}$. Since $r = 29$ is coprime with $2^{18} - 1$, the polynomial

$$\begin{aligned}
Q &= X^r\left(X^{2\frac{q-1}{3}} + (y^{15} + y^{12} + y^6)X^{\frac{q-1}{3}} + (y^{12} + y^3)\right) \\
&= X^{174791} + (y^{15} + y^{12} + y^6)X^{87410} + (y^{12} + y^3)X^{29}
\end{aligned}$$

is a permutation trinomial of $\mathbb{F}_{2^{18}}$.

We will now consider several interesting subclasses.

4. Permutation binomials

Many authors have been interested in binomials as this is the simplest non trivial case. One can find results on such polynomials in [4,23,24] or for more recent work [10,27].

Our new class of permutation polynomials gives clearly a class of permutation binomials taking $P = X + a$.

Corollary 4.1. *Let p be a prime and $(m, \ell) \in \mathbb{N}^2$. Let k be the order of p in $\mathbb{Z}/m\mathbb{Z}$. Take $q = p^{k\ell m}$ and r a positive integer coprime with $q-1$.*

If $a \in \mathbb{F}_{p^{k\ell}}$, then the binomial $X^r\left(X^{\frac{q-1}{m}} + a\right)$ is a permutation polynomial if and only if $(-a)^m \neq 1$.

Remark 5. In [1,2] Carlitz established the existence of permutation polynomials of the form

$$X(X^{\frac{q-1}{m}} + a)$$

provided q is large enough. However he did not give any construction.

We can remark that the two monomials $X^{r+\frac{q-1}{m}}$ and aX^r are permutations since the exponents are coprime with $q-1$ as shown in the following lemma.

Lemma 4.2. *Let k, ℓ and p be positive integers. Let m be a divisor of $p^k - 1$ and r be coprime with $p^{k\ell m} - 1$,*

$$\operatorname{Gcd}\left(p^{k\ell m} - 1, \frac{p^{k\ell m} - 1}{m} + r\right) = 1.$$

Proof. Let $q = p^{k\ell m}$. We note that

$$\frac{q-1}{m} = \frac{p^k - 1}{m} \sum_{i=0}^{\ell m - 1} \left[(p^k - 1) + 1\right]^i \equiv \frac{p^k - 1}{m} \sum_{i=0}^{\ell m - 1} 1 \equiv 0 \pmod{m}$$

as m divides $p^k - 1$, and thus m divides $\frac{q-1}{m}$. $q-1$ and $\frac{q-1}{m}$ have then exactly the same prime divisors. Take d a prime divisor of $q-1$, it divides $\frac{q-1}{m}$ but not r since r and $q-1$ are coprime. The lemma is thus proven. $\square$

4.1. Complete permutations

An important problem is to find *complete permutations*, i.e. permutations f such that $x \mapsto f(x) + x$ is also a permutation (see Niederreiter and Robinson [21]). We will see that for many values of p, m and ℓ we obtain complete permutations.

Theorem 4.3. *Let p be a prime and $(m, \ell) \in \mathbb{N}^2$. Let k be the order of p in $\mathbb{Z}/m\mathbb{Z}$. Take $q = p^{k\ell m}$ and r a positive integer coprime with $q-1$. Assume $a \in \mathbb{F}_{p^{k\ell}}$ is such that $(-a)^m \neq 1$. Then the polynomials*

$$P = X(X^{\frac{q-1}{m}} + a)$$

and

$$Q = aX^{\frac{q-1}{m}+1}$$

are complete permutation polynomials.

Proof. From Corollary 4.1, P is a permutation polynomial. If a lies in $\mathbb{F}_{p^{k\ell}}$ and is such that $(-a)^m \neq 1$, so does $a+1$. Thus, again with Corollary 4.1, $P+X$ is a permutation polynomial.

Q is a permutation polynomial since, via Lemma 4.2, $\mathrm{Gcd}(q-1, \frac{q-1}{m}+1) = 1$. Finally, $Q+X$ is a permutation polynomial via Corollary 4.1. $\square$

4.2. An asymptotic result

We obtained a family of permutation binomials of the type $X^r(X^{(q-1)/m} + a)$ for specific values of a. A natural question is how many such polynomials are permutation ones.

Definition 4.4. We define

$$\mathcal{B}(q, m, r) = \left\{a \in \mathbb{F}_q^* \text{ such that } X^r\left(X^{\frac{q-1}{m}} + a\right) \text{ is a permutation polynomial}\right\}$$

and

$$N(q, m, r) = \#\mathcal{B}(q, m, r).$$

It is known that $\left|N(q, m, r) - \frac{m!}{m^m}q\right| = \mathcal{O}(\sqrt{q})$, but it seems that no exact upper bound has been explicited. Theorem 2.2 gives us a quick way to do this.

Theorem 4.5. *Let q be a power of a prime. Assume r is a positive integer coprime with $q-1$ and m is a divisor of $q-1$. Then*:

$$\left|N(q, m, r) - \frac{m!}{m^m}q\right| \leqslant m!\left(\frac{1}{m^m} + (m-2)\right)\sqrt{q} + (m+1)!$$

Proof. We work in $\mathbb{F}_q$ with m dividing $q-1$; we can thus consider $\mathcal{G}$ the cyclic subgroup of $\mathbb{F}_q^*$ of order m and take β a generator, i.e. $\mathcal{G} = \langle\beta\rangle$. Take ω a primitive mth root of unity in $\mathbb{C}$.

We will denote by ϕ the application from $\mathcal{G}$ to the set of mth roots of unity in $\mathbb{C}$: $\phi(\beta^i) = \omega^i$, and extend it with $\phi(0) = 0$.

For $a \in \mathbb{F}_q$, Theorem 2.2 ensures that $Q_a(X) = X^r\left(X^{\frac{q-1}{m}} + a\right)$ is a permutation polynomial if and only if the following two conditions are satisfied:

$$\left(\forall i, 0 \leqslant i < m,\ \beta^i + a \neq 0\right) \text{ which is equivalent to } (-a)^m \neq 1 \tag{2}$$

$$\text{the function} \begin{cases} \{1, \ldots, m\} \to \{1, \ldots, m\} \\ i \mapsto \log_\beta\left(Q(\alpha^i)^{\frac{q-1}{m}}\right) \end{cases} \quad \text{is a permutation.} \tag{3}$$

For $f : \{1, \ldots, m\} \to \{1, \ldots, m\}$, we define

$$P_f(X_1, \ldots, X_m) = \prod_{i=1}^{m} \left(\sum_{j=0}^{m-1} \left[X_i \omega^{-f(i)}\right]^j \right). \tag{4}$$

Let Ψ be the character $x \mapsto \phi(x^{\frac{q-1}{m}})$.

For $x = (x_1, \ldots, x_m)$ a m-tuplet of elements in $\mathbb{F}_q^*$, we use the notation $\Psi(x) = (\Psi(x_1), \ldots, \Psi(x_m))$. We then have

$$P_f(\Psi(x)) = \begin{cases} m^m & \text{if } \log_\beta\left(x_i^{\frac{q-1}{m}}\right) = f(i) \text{ for all } i, \\ 0 & \text{otherwise.} \end{cases} \tag{5}$$

We also have $P(0) = 1$.

Let $\mathcal{S}$ be the set of permutations of $\{1, \ldots, m\}$. The first important thing to note is that according to (5)

$$\frac{1}{m^m} \sum_{\sigma \in \mathcal{S}} P_\sigma\Big(\Psi\big(Q_a(\alpha^1), \ldots, Q_a(\alpha^m)\big)\Big) = \begin{cases} 1 & \text{if (3) is satisfied,} \\ 0 & \text{otherwise.} \end{cases} \tag{6}$$

Therefore,

$$N(q, m, r) = \frac{1}{m^m} \sum_{\substack{a \in \mathbb{F}_q^* \\ (-a)^m \neq 1}} \sum_{\sigma \in \mathcal{S}} P_\sigma\Big(\Psi\big(Q_a(\alpha^1), \ldots, Q_a(\alpha^m)\big)\Big). \tag{7}$$

Our goal is now to estimate this sum.

Let $\mathcal{M}(P)$ be the set of monomials of P. For a monomial M, let $ind(M)$ be the number of indeterminates appearing in M.

The character Ψ is multiplicative and we then have

$$M \circ \Psi(x_1, \cdot, x_m) = \Psi \circ M(x_1, \cdot, x_m).$$

Therefore, for any $\sigma \in \mathcal{S}$

$$\begin{aligned}
&\left|\sum_{a\in\mathbb{F}_q} P_\sigma(\Psi(Q_a(\alpha^1), \dots, Q_a(\alpha^m))) - q\right| \\
&\quad = \left|\sum_{a\in\mathbb{F}_q} \sum_{\substack{M\in\mathcal{M}(P)\\ ind(M)>0}} M(\Psi(Q_a(\alpha^1), \dots, Q_a(\alpha^m)))\right| \\
&\quad \leqslant \sum_{k=1}^{m} \sum_{\substack{M\in\mathcal{M}(P)\\ ind(M)=k}} \left|\sum_{a\in\mathbb{F}_q} \Psi(M(Q_a(\alpha^1), \dots, Q_a(\alpha^m)))\right|.
\end{aligned}$$

If $M = \prod_{i\in I} X_i^{k_i}$, we obtain

$$M(Q_a(\alpha^1), \dots, Q_a(\alpha^m)) = \prod_{i\in I} \left[\alpha^{ir}(\beta^i + a)\right]^{k_i}$$

which—seen as a polynomial with indeterminate a—has exactly $\#I = ind(M)$ roots which are $\{-\beta^i \mid i \in I\}$. They have multiplicity k_i which are here strictly lower than m. Using Theorem 2.4 on character sums we thus obtain

$$\left|\sum_{a\in\mathbb{F}_q} P_\sigma(\Psi(Q_a(\alpha^1), \dots, Q_a(\alpha^m))) - q\right| \leqslant \sum_{k=1}^{m} \sum_{\substack{M\in\mathcal{M}(P)\\ ind(M)=k}} (k-1)\sqrt{q}. \tag{8}$$

Finally, as each indeterminate appears exactly in one of the m terms of the product (4) defining P, we have $\#\{M \in \mathcal{M}(P) | ind(M) = k\} = (m-1)^k \binom{m}{k}$ and thus

$$\left|\sum_{a\in\mathbb{F}_q} P_\sigma(\Psi(Q_a(\alpha^1), \dots, Q_a(\alpha^m))) - q\right| \leqslant \left(\sum_{k=1}^{m} (m-1)^k \binom{m}{k} (k-1)\right)\sqrt{q}. \tag{9}$$

The classical formula for binomial coefficients $k\binom{m}{k} = m\binom{m-1}{k-1}$ gives

$$\begin{aligned}\sum_{k=1}^{m}(m-1)^k\binom{m}{k}(k-1) &= m\sum_{k=1}^{m}(m-1)^k\binom{m-1}{k-1} - \sum_{k=1}^{m}(m-1)^k\binom{m}{k}\\ &= m(m-1)m^{m-1} - (m^m - 1)\\ &= 1 + m^m(m-2).\end{aligned}$$

Summing inequality (9) for $\sigma \in \mathcal{S}$, we obtain

$$\begin{aligned}\left|N(q,m,r) - \frac{m!}{m^m}q\right| &= \frac{1}{m^m}\left|\sum_{\sigma\in\mathcal{S}}\left(\sum_{\substack{a\in\mathbb{F}_q^*\\(-a)^m\neq 1}} P_\sigma\left(\Psi(Q_a(\alpha^1),\ldots,Q_a(\alpha^m))\right) - q\right)\right|\\ &\leqslant \frac{1}{m^m}\sum_{\sigma\in\mathcal{S}}\left(\left|\sum_{a\in\mathbb{F}_q} P_\sigma\left(\Psi(Q_a(\alpha^1),\ldots,Q_a(\alpha^m))\right) - q\right|\right.\\ &\quad\left. + \left|\sum_{\{a\mid(-a)^m=1\}\cup\{0\}} P_\sigma\left(\Psi(Q_a(\alpha^1),\ldots,Q_a(\alpha^m))\right)\right|\right)\\ &\leqslant \frac{m!}{m^m}(1+m^m(m-2))\sqrt{q} + \sum_{\sigma\in\mathcal{S}}\sum_{\{a\mid(-a)^m=1\}\cup\{0\}} 1\\ &\leqslant \frac{m!}{m^m}\left(1+m^m(m-2)\right)\sqrt{q} + m!(m+1)\end{aligned}$$

and this completes the proof. □

Thus we are able to derive a lower bound on q providing a sufficient condition for the existence of polynomials in $\mathcal{B}(q,m,r)$.

Corollary 4.6. *Let $q = p^n$, p a prime. Let m divide $q-1$ and r coprime with $q-1$. Assume that $q > \left(1 + \frac{m+1}{m^{m+2}}\right)^2 m^{2m+2}$. Then there exists $a \in \mathbb{F}_q^*$ such that the polynomial $X^r(X^{\frac{q-1}{m}} + a)$ is a permutation polynomial of $\mathbb{F}_q$.*

Proof. The existence is equivalent to $N(q,m,r) > 0$. According to Theorem 4.5, a sufficient condition is thus

$$0 < \frac{1}{m^m}q - \left(\frac{1}{m^m} + (m-2)\right)\sqrt{q} - (m+1).$$

The biggest root of this degree two polynomial is

$$\frac{m^{m+1}}{2}\left(\left(1+\frac{1}{m^{m-1}}-\frac{2}{m}\right)+\sqrt{\left(1+\frac{1}{m^{m-1}}-\frac{2}{m}\right)^2+4\frac{m+1}{m^{m+2}}}\right)$$

which is lower than

$$\frac{m^{m+1}}{2}\left(1+\sqrt{1+4\frac{m+1}{m^{m+2}}}\right).$$

Using the fact that $\sqrt{1+x}<1+x/2$ we obtain the bound

$$m^{m+1}\left(1+\frac{m+1}{m^{m+2}}\right).$$

This is a lower bound on $\sqrt{q}$, squaring this value gives the result. □

Remark 6. In [1] Carlitz proved that for q large enough, $N(q,m,1)$ is strictly positive but he doesn't give a bound, except for $m=2$.

5. Consequences in coding theory

5.1. Preliminary

To any Boolean function $f:\mathbb{F}_{2^n}\to\mathbb{F}_2$ one can associate the binary word $(f(x))_{x\in\mathbb{F}_{2^n}}$. This implies an order on the element of $\mathbb{F}_{2^n}$ which can be obtained using a fixed primitive element α.

Definition 5.1. Let f be a Boolean function. We will use the notation $(f(x))_{x\in\mathbb{F}_{2^n}}$ for the binary word $f(0)f(\alpha)\cdots f(\alpha^{2^n-1})$.

In cryptography, we are interested in words giving little information to the opponent.

Definition 5.2. A binary word is said *balanced* if it contains as many 0 as 1.

The field $\mathbb{F}_{2^n}$ is a vector space of dimension n over $\mathbb{F}_2$. An element $a\in\mathbb{F}_{2^n}$ can thus be seen as a n-tuplet of elements a_i in $\mathbb{F}_2$, and a function $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ as a n-tuplet of Boolean functions f_i. The next proposition gives a characterization of permutation functions, it is proven in a more general context in [18] (Theorem 7.17).

Proposition 5.3. *F is a permutation of $\mathbb{F}_{2^n}$ if and only if for all $a \in \mathbb{F}_{2^n}^*$ the word*

$$(a_1 f_1(x) + \cdots + a_n f_n(x))_{x \in \mathbb{F}_{2^n}}$$

is a balanced word.

5.2. Helleseth's conjecture

There are many applications of results on permutation polynomials. We will present a conjecture made by Helleseth [8], and the results derived from the first part.

The conjecture in [8] was in terms of cross-correlation functions, but it is equivalent to the following one.

Conjecture 5.4. *For all integers k coprime with $2^n - 1$, there exists $a \in \mathbb{F}_{2^n}^*$ such that $(\mathrm{Trace}(x^k + ax))_{x \in \mathbb{F}_{2^n}}$ is a balanced word.*

Remark 7. The original conjecture is more general, it deals not only with the case 2 but with a prime p. Some of the following results could easily be extended to this case.

Proposition 5.3 tells us that if $X^k + aX$ is a permutation polynomial, then $(\mathrm{Trace}(x^k + ax))_{x \in \mathbb{F}_{2^n}}$ is a balanced word. Finding permutation binomials is thus a way to answer partially to this conjecture.

From this point of view, Corollaries 4.1 and 4.6 give the following:

Theorem 5.5. *Let m and ℓ be two positive integers, and k be the order of 2 in $\mathbb{Z}/m\mathbb{Z}$. Note $q = 2^{k\ell m}$, then Helleseth's conjecture is satisfied for $k = \frac{q-1}{m} + 1$.*

Theorem 5.6. *For all $m \geqslant 3$, for all $n > 2\log_2\left(1 + \frac{m+1}{m^{m+2}}\right) + (2m+2)\log_2(m)$ such that m divides $2^n - 1$, Helleseth's conjecture is satisfied for $k = \frac{2^n-1}{m} + 1$.*

5.3. Niho exponents

Another important class of polynomials are the polynomials X^k when k is a so-called *Niho exponent*. Those exponents have been introduced by Niho in his thesis [22] for the definition of interesting binary sequences. Niho proposed several conjectures which are being considered for instance in [3,7].

Definition 5.7. Let $n = p^{2t} - 1$ and k be a positive integer lower than n. Then k is a *Niho exponent* if and only if

- $\mathrm{Gcd}(k, n) = 1$.
- $k \notin \{1, p, p^p, \ldots, p^{t-1}\}$.
- $k \equiv p^j \pmod{p^t - 1}$ for some j, $0 \leqslant j < t - 1$.

We will show that some of our binomials are of the form $X^k + aX$ with k a Niho exponent.

Proposition 5.8. *$\frac{p^{2t}-1}{m} + 1$ is a Niho exponent in normal form in $\mathbb{F}_{p^{2t}}$ if and only if m divides $p^t + 1$.*

Proof. Writing $q = p^{2t}$, we have:

$$\frac{q-1}{m} + 1 = \lambda(p^t - 1) + p^j \;\Leftrightarrow\; q - 1 + m = \lambda(p^t - 1)m + p^j m$$
$$\Leftrightarrow\; m = \frac{(p^t - 1)(p^t + 1)}{\lambda(p^t - 1) + p^j - 1}.$$

With $j = 0$, we obtain the result. $\square$

Using the results we have on permutation binomials, we obtain some Niho exponent and we have moreover a property of their spectrum.

Proposition 5.9. *Let m and ℓ be positive integers, k be the order of 2 in $\mathbb{Z}/m\mathbb{Z}$. Take $q = 2^{k\ell m}$. If m divides $1 + \sqrt{q}$, then*

$$k = \frac{q-1}{m} + 1$$

is a Niho exponent and there exists $a \in \mathbb{F}_{q^*}$ such that the word $(\mathrm{Trace}(x^k + ax))_{x \in \mathbb{F}_q}$ is balanced.

Proof. Proposition 5.8 ensures that k is a Niho exponent, while Proposition 4.1 gives some a such that $X^k + aX$ is a permutation polynomial and therefore $\sum_{x \in \mathbb{F}_{2^k}} (-1)^{\mathrm{Trace}(x^k + ax)} = 0$. $\square$

Acknowledgments

This author would like to thank the CODES project at INRIA, and especially Pascale Charpin for her assistance throughout the preparation of this work and Daniel Augot for helpful discussion. He also wants to thank the reviewers for their constructive comments.

References

[1] L. Carlitz, Some theorems on permutation polynomials, Bull. Amer. Math. Soc. 68 (1962) 120–122.

[2] L. Carlitz, C. Wells, The number of solutions of a special system of equations in a finite field, Acta Arith. 12 (1966/1967) 77–84.

[3] P. Charpin, Cyclic codes with few weights and Niho exponents, J. Combin. Theory Ser. A 108 (2004) 247–259.

[4] W.S. Chou, Binomial permutations of finite fields, Bull. Austral. Math. Soc. 38 (3) (1988) 325–327.

[5] 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. 11 (1–6) (1896/97) 161–183.

[6] H. Dobbertin, Kasami power functions, permutation polynomials and cyclic difference sets, in: Difference Sets, Sequences and Their Correlation Properties, Bad Windsheim, 1998, NATO Advanced Sciences Institutes Series C Mathematical and Physical Sciences, vol. 542, Kluwer Academic Publishers, Dordrecht, 1999, pp. 133–158.

[7] H. Dobbertin, P. Felke, T. Helleseth, P. Rocendalh, Niho type cross-correlation functions via dickson polynomials and klosterman sums, preprint.

[8] T. Helleseth, Some results about the cross-correlation function between two maximal linear sequences, Discrete Math. 16 (3) (1976) 209–232.

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

[10] S. Janphaisaeng, V. Laohakosol, A. Harnchoowong, Some new classes of permutation polynomials, Sci. Asia 28 (2002) 401–405.

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

[12] J. Levine, R. Chandler, Some further cryptographic applications of permutation polynomials, Cryptologia 11 (4) (1987) 211–218.

[13] R. Lidl, On cryptosystems based on polynomials and finite fields, in: Advances in Cryptology, Paris, 1984, Lecture Notes in Computer Science, vol. 209, Springer, Berlin, 1985, pp. 10–15.

[14] 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.

[15] R. Lidl, G.L. Mullen, When does a polynomial over a finite field permute the elements of the field?, Amer. Math. Monthly 100 (1993) 71–74.

[16] R. Lidl, W.B. Müller, A note on polynomials and functions in algebraic cryptography, Ars Combin. 17 (A) (1984) 223–229.

[17] R. Lidl, W.B. Müller, Permutation polynomials in RSA-cryptosystems, in: Advances in Cryptology, Santa Barbara, CA, 1983, Plenum Press, New York, 1984, pp. 293–301.

[18] R. Lidl, H. Niederreiter, Finite fields, Encyclopedia of Mathematics and its Applications, vol. 20, second ed., Cambridge University Press, Cambridge, 1997 (With a foreword by P.M. Cohn).

[19] G.L. Mullen, H. Niederreiter, Dickson polynomials over finite fields and complete mappings, Canad. Math. Bull. 30 (1) (1987) 19–27.

[20] W.B. Müller, W. Nöbauer, Some remarks on public-key cryptosystems, Studia Sci. Math. Hungar. 16 (1–2) (1981) 71–76.

[21] H. Niederreiter, K.H. Robinson, Complete mappings of finite fields, J. Austral. Math. Soc. Ser. A 33 (2) (1982) 197–212.

[22] Y. Niho, Multi-valued cross-correlation function between two maximal linear recursive sequences, Ph.D. Thesis, University of Southern California, Los Angeles, CA, 1975.

[23] C. Small, Permutation binomials, Internat. J. Math. Math. Sci. 13 (2) (1990) 337–342.

[24] G. Turnwald, Permutation polynomials of binomial type, Contributions to General Algebra, vol. 6, Hölder-Pichler-Tempsky, Vienna, 1988, pp. 281–286.

[25] D.Q. Wan, On a problem of Niederreiter and Robinson about finite fields, J. Austral. Math. Soc. Ser. A 41 (3) (1986) 336–338.

[26] D.Q. Wan, R. Lidl, Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure, Monatsh. Math. 112 (2) (1991) 149–163.

[27] L. Wang, On permutation polynomials, Finite Fields Appl. 8 (3) (2002) 311–322.