On a Class of APN Permutation Polynomials

Ayça Çeşmelioğlu, Wilfried Meidl and Alev Topuzoğlu

Sabancı University, MDBF, Orhanlı, 34956 Tuzla, İstanbul, Turkey

Abstract

The permutations $\mathcal{P}(x) = (a_0x + a_1)^{p-2} + a_2$ over a prime field $\mathbb{F}_p$ are APN if and only if $p \equiv 5 \bmod 6$. We present results on the dispersion and p-dispersion of $\mathcal{P}(x)$, and relate this concept to Costas property. Results on the construction and enumeration of permutations $\mathcal{P}(x)$ with prescribed dispersion and cycle structure are given. Applications in coding theory are described.

Key Words: Permutation polynomial, APN permutation, inversive generator, dispersion, Costas permutation

Almost perfect nonlinear (APN) functions are mainly studied over fields of characteristic two, since there are no *perfect nonlinear* (PN) functions in characteristic 2. On the other hand PN "permutations" do not exist in odd characteristic either, hence APN permutations of $\mathbb{F}_p$ are of interest for odd p also.
This talk is concerned with the class of permutations $\mathcal{P}(x) \in \mathbb{F}_p[x]$, where

$$\mathcal{P}(x) = (a_0x + a_1)^{p-2} + a_2, \tag{1}$$

$a_0 \neq 0$ and p is an odd prime. We first observe that $\mathcal{P}(x)$ is APN if and only if $p \equiv 5 \bmod 6$.
These polynomials give rise to the well-known inversive pseudorandom number generators (u_n), which are defined recursively by $u_n = \mathcal{P}(u_{n-1}), u_0 \in \mathbb{F}_p$, for $a_1 = 0$. Since their *randomness* is well established, they are good candidates for use in turbo codes as interleavers. Indeed our results on the values of dispersion of these polynomials show that one can select the parameters a_0, a_1 and a_2 to yield permutations with prescribed dispersion (e.g. close to that of a random permutation). We recall that dispersion of a permutation P of the set $\{0, 1, \ldots, n-1\}$ is the cardinality $|D(P)|$ of the set

$$D(P) = \{(j - i, P(j) - P(i)) | 0 \leq i < j \leq n - 1\}.$$

Permutations with maximum possible dispersion $n(n-1)/2$ are, of course, those which satisfy *Costas property* (see [4, 6] for a recent survey on Costas

arrays). Accordingly the normalized dispersion is defined as

$$\gamma(P) = \frac{2\,|D(P)|}{n(n-1)},$$

and hence $\gamma(P) \leq 1$ for any permutation P of the set $\{0, 1, \ldots, n-1\}$. We note that the expected value of normalized dispersion of a random permutation is approximately 0.8, see, [3], [7]. Hence a permutation P can be considered as being random (and hence as a favourable interleaver) if $\gamma(P)$ is close to 0.8. We note that there are only a few non-empirical results on the normalized dispersion of permutation polynomials over finite fields, and only about monomials.
Since we need to calculate both in $\mathbb{Z}$ and in $\mathbb{F}_p$, we denote addition and subtraction in $\mathbb{F}_p$ by "$\oplus$", and "$\ominus$", to avoid confusion. Studying permutations of $\mathbb{F}_p$, we naturally consider the *p-dispersion* $|D(P, \mathbb{F}_p)|$ of $P \in \mathbb{F}_p[x]$, which we define as the cardinality of the set

$$D(P, \mathbb{F}_p) = \{(k, P(i \oplus k) \ominus P(i)) | 1 \leq k \leq p-1, 0 \leq i \leq p-1-k\}.$$

Our main results concerning dispersion of permutations $\mathcal{P}(x)$ are stated below. The element (the *pole*) $\ominus\frac{a_1}{a_0} \in \mathbb{F}_p$, is denoted by x_p. We denote the integer in $\{0, 1, \ldots, p-1\}$, which x_p is identified with, by x_I.

Theorem 1. *Let $p \equiv 5 \bmod 6$ and $\mathcal{P}(x) = (a_0 x \oplus a_1)^{p-2} \oplus a_2 \in \mathbb{F}_p[x]$, $a_0 \neq 0$. Then*

$$|D(\mathcal{P}, \mathbb{F}_p)| = \begin{cases} \frac{(p+3)(p-1)+4x_I(p-2x_I-2)}{4} & : \quad 0 \leq x_I \leq \frac{p-1}{2}, \\ \frac{(p+3)(p-1)+4(p-1-x_I)(2x_I-p)}{4} & : \quad \frac{p-1}{2} < x_I \leq p-1. \end{cases}$$

Theorem 2. *Let $p \equiv 5 \mod 6$ and let $\underline{\mathcal{P}}(x) = (a_0 x \oplus a_1)^{p-2} \in \mathbb{F}_p[x]$, $a_0 \neq 0$. The dispersion $|D(\underline{\mathcal{P}})|$ of $\underline{\mathcal{P}}(x)$ is then given by*

$$|D(\underline{\mathcal{P}})| = \begin{cases} \frac{(p+3)(p-1)+4x_1(p-2x_1-1)}{4} & : \quad 0 \leq x_1 \leq \frac{p-1}{2}, \\ \frac{(p+3)(p-1)+4(p-1-x_1)(2x_1-p+1)}{4} & : \quad \frac{p-1}{2} < x_1 \leq p-1. \end{cases}$$

Corollary 3. *Let $p \equiv 5 \bmod 6$ and let $\underline{\mathcal{P}}(x) = (a_0 x \oplus a_1)^{p-2} \in \mathbb{F}_p[x]$, $a_0 \neq 0$ The maximum value for the normalized dispersion $\gamma(\underline{\mathcal{P}})$ is $\gamma(\underline{\mathcal{P}}) = 0.75 + \frac{5}{4p}$. This value is attained for $x_I = \lfloor \frac{p-1}{4} \rfloor$ and $x_I = \lfloor \frac{3p-1}{4} \rfloor$.*

Corollary 4. *Let $p \equiv 5 \bmod 6$ and let $\underline{\mathcal{P}}(x) = (a_0 x \oplus a_1)^{p-2} \in \mathbb{F}_p[x]$, $a_0 \neq 0$. Then $|D(\underline{\mathcal{P}}, \mathbb{F}_p)| = |D(\underline{\mathcal{P}})|$ if and only if $\underline{\mathcal{P}}(x) = a_0 x^{p-2}$ or $\underline{\mathcal{P}}(x) = (a_0 x + a_0)^{p-2}$ where $a_0 \in \mathbb{F}_p^*$ is arbitrary.*

It is suggested that the cycle structure of a permutation P also affects the performance of P when used as an interleaver. Of particular interest are the permutations that decompose into cycles of the same length (see [8, 9]). We therefore present results on the cycle decomposition of $\mathcal{P}(x) = (a_0x \oplus a_1)^{p-2} \oplus a_2$ in relation to its dispersion. Since p-dispersion of $\mathcal{P}$ depends only on $\ominus a_1/a_0$, we show how to choose the remaining parameters in order to obtain a prescribed cycle structure, assuming $p \equiv 5 \bmod 6$. Furthermore we determine the number of permutations $\mathcal{P}(x) = (a_0x \oplus a_1)^{q-2} \oplus a_2 \in \mathbb{F}_p[x]$ with prescribed p-dispersion and cycle structure. The polynomial,

$$f(x) = x^2 \ominus (a_0a_2 \oplus a_1)x \ominus a_0. \tag{2}$$

associated to $\mathcal{P}(x)$, plays the central role in studying the cycle structure of $\mathcal{P}(x)$. Let $\alpha, \beta \in \mathbb{F}_{p^2}$ be the roots of $f(x)$, then the multiplicative order m of α/β either divides $p-1$ or $p+1$. The cycle structure of $\mathcal{P}(x)$ depends on this order m of α/β as can be seen in the following proposition. When a permutation P is decomposed into a product of disjoint cycles, we write $\mathcal{C}_P = [n_1 \times l_1, n_2 \times l_2, \ldots, n_s \times l_s]$ to indicate that the permutation is composed of n_1 cycles of length l_1, n_2 cycles of length l_2,...,n_s cycles of length l_s, $l_1 > l_2 > \cdots > l_s \geq 1$.

Proposition 5. *[1, Theorem 2] For a permutation $\mathcal{P}(x) = (a_0x \oplus a_1)^{p-2} \oplus a_2$, let f be the associated polynomial as in (2), and α, β be the roots of f. Suppose that m is the order of α/β in $\mathbb{F}_{p^2}$. Then $\mathcal{C}_\mathcal{P} = \mathcal{C}_\mathcal{P}(m)$ depends on m as follows:*

$$\mathcal{C}_\mathcal{P}(m) = \begin{cases} [(t-1) \times m, 1 \times (m-1)] & : \ m = (p+1)/t, \\ & \quad 1 \leq t < (p+1)/2, \\ [(t-1) \times m, 1 \times (m-1), 2 \times 1] & : \ m = (p-1)/t, \\ & \quad 1 \leq t < (p-1)/2, \\ [1 \times (p-1), 1 \times 1] & : \ m = 1, \\ [((p-1)/2 - \delta(f)) \times 2, (1 + 2\delta(f)) \times 1] & : \ m = 2, \end{cases}$$

with $\delta(f) = 0$ if f is irreducible and $\delta(f) = 1$ if f is reducible.

It follows that for $m = p \pm 1$ we have only one nontrivial cycle (of length > 1) having length $m-1$. If $2 < m < p-1$, all nontrivial cycles have the same length m, except for one of length $m-1$. If $m = 2$, all nontrivial cycles have length 2.

Theorem 6. *Let $p \equiv 5 \bmod 6$. For any $x_p \in \mathbb{F}_p$ and any integer m dividing $p-1$ or $p+1$, there is a permutation $\mathcal{P}(x) = (a_0x \oplus a_1)^{q-2} \oplus a_2 \in \mathbb{F}_p[x]$ with cycle decomposition $\mathcal{C}_\mathcal{P}(m)$ and $x_p = \ominus a_1/a_0$.*

Theorem 7. *Suppose* $p \equiv 5 \mod 6$. *Let* m *be a divisor of* $p-1$ *or* $p+1$ *and let* $\mathcal{N}(\mathcal{C}_{\mathcal{P}}(m), x_p)$ *be the number of permutations* $\mathcal{P}(x) = (a_0 x \oplus a_1)^{p-2} \oplus a_2 \in \mathbb{F}_p[x]$ *with given* $x_p = \ominus a_1/a_0 \in \mathbb{F}_p$ *and cycle decomposition* $\mathcal{C}_{\mathcal{P}}(m)$, *then*

$$\begin{aligned} \mathcal{N}(\mathcal{C}_{\mathcal{P}}(m), x_p) &= p-1 \quad \text{if } m = 1, 2, \quad \text{and} \\ \mathcal{N}(\mathcal{C}_{\mathcal{P}}(m), x_p) &= \frac{p-1}{2}\varphi(m) \quad \text{if } m > 2. \end{aligned}$$

An entirely different point of view regarding dispersion may help understanding the relation between APN and Costas permutations , see ([5]) for related work.
As mentioned above, the maximum possible dispersion is attained by permutations with Costas property. Recall that Costas permutation is precisely the one, which has no repetitions in the rows of its *difference triangle*, where the difference triangle of a permutation $P \in \mathbb{F}_p[x]$ is a triangular array $DT(P)$ of integers, which has $p-1$ *rows* $T_1(P), \ldots, T_{p-1}(P)$, with

$$T_k(P) = (P(k) - P(0), P(1+k) - P(1), \ldots, P(p-1) - P(p-k-1)),$$

for $k = 1, \ldots, p-1$. Calculating in $\mathbb{F}_p$, we obtain a p-difference triangle $DT_p(P)$ of P, whose rows are:

$$T_{p,k}(P) = (P(k) \ominus P(0), P(1 \oplus k) \ominus P(1), \ldots, P((p \ominus 1) \ominus P(p \ominus k \ominus 1)),$$

for $k = 1, \ldots, p-1$. Denoting the number of distinct integers appearing in $T_k(P)$ by $|T_k(P)|$ and distinct elements appearing in $T_{p,k}(P)$ by $|T_{p,k}(P)|$, one has $|D(P)| = \sum |T_k(P)|$ and $|D(P, \mathbb{F}_p)| = \sum |T_{p,k}(P)|$. There are no permutations of $\mathbb{F}_p$ with $|D(P, \mathbb{F}_p)| = p(p-1)/2$, see ([5]). Hence one can consider permutations with at most two repetitions in each row of their p-difference (or difference) triangles. By definition all APN permutations have at most two repetitions in each row of their difference triangles. See ([5]) for a study of the relation between APN and Costas permutations. In particular the APN permutations $\mathcal{P}$ we consider are not Costas for $p > 5$. On the other hand, though they are affine equivalent to x^{p-2}, the number of repeated terms in rows of their difference triangles show a great variety. In view of this fact we regard a permutation P as being close to having Costas property if $\gamma(P)$ is close to 1. We end this talk by describing how the choice of parameters a_0, a_1, a_2 affects $\mathcal{P}$ to being close to or far away from being Costas.
Further remarks and proofs of above results can be found in ([2]).

References

[1] A. Çeşmelioğlu, W. Meidl, A. Topuzoğlu, On the cycle structure of permutation polynomials, *Finite Fields Appl.* 14 (2008), 593–614.

[2] A. Çeşmelioğlu, W. Meidl, A. Topuzoğlu, On a class of APN permutation polynomials, preprint (2010).

[3] C.J. Corrada-Bravo, I.M. Rubio, Deterministic interleavers for Turbo codes with random-like performance and simple implementation, Proc. of the 3rd International Symposium on Turbo Codes and Related Topics, Brest, France, 2003, 555–558.

[4] K. Drakakis, A review on Costas arrays, J. Appl. Math. 2006.

[5] K. Drakakis, G. McGuire, APN permutations on $\mathbb{Z}_n$ and Costas arrays, Discrete Applied Mathematics 157, 3320–3326.

[6] S.W. Golomb, G. Gong, The status of Costas arrays, IEEE Trans. Inform. Theory 53 (2007), 4260–4265.

[7] C. Heegard, S.B. Wicker, Turbo Coding, Kluwer Academic Publishers, Dordrecht, 1999.

[8] I.M. Rubio, C.J. Corrada-Bravo, Cyclic decomposition of permutations of finite fields obtained using monomials, In: A. Poli, H. Stichtenoth H (Eds.), Proc. of Finite fields and applications 7, Lecture Notes in Computer Science Vol 2948., pp. 254–261, Springer-Verlag, Berlin (2004).

[9] I.M. Rubio, G.L. Mullen, C.J. Corrada, F.N. Castro, Dickson permutation polynomials that decompose in cycles of the same length, In: G.L. Mullen, D. Panario, I. Shparlinski (Eds.), Proc. of Finite fields and applications 8, Contemporary Mathematics Vol 461, 229–239.