Nonlinear p-ary sequences

Ling, San; Sole, Patrick

2003

Ling, S., & Solé, P. (2003). Nonlinear p-ary Sequences. *Applicable Algebra in Engineering, Communication and Computing*, 14(2), 117-125.

<https://hdl.handle.net/10356/96417>

<https://doi.org/10.1007/s00200-003-0130-8>

© 2003 Springer-Verlag. This is the author created version of a work that has been peer reviewed and accepted for publication by *Applicable Algebra in Engineering, Communication and Computing*, Springer-Verlag. It incorporates referee's comments but changes resulting from the publishing process, such as copyediting, structural formatting, may not be reflected in this document. The published version is available at: [<http://dx.doi.org/10.1007/s00200-003-0130-8>].

Downloaded on 26 Apr 2023 21:37:46 SGT

Nonlinear p -ary Sequences

San Ling^{1,*}, Patrick Solé^{**, 2}

¹ Department of Mathematics, National University of Singapore, Singapore 117543, Republic of Singapore (e-mail: lings@math.nus.edu.sg)

² CNRS-I3S, ESSI, Route des Colles, 06 903 Sophia Antipolis, France (e-mail: ps@essi.fr)

Abstract. Low correlation p -ary sequences with p an odd prime are constructed. They are obtained as Gray images of codewords of a subcode of the generalized Kerdock codes over the ring $\mathbb{Z}_{p^2}$. They can be shown to be nonlinear in some precise sense.

Keywords: Galois rings, Gray map, Kerdock code, CDMA.

1 Introduction

In the domain of low correlation sequences, the Sidelnikov bound is an important design criterion. Given a family consisting of M pairwise cyclically non-equivalent sequences of period T , with maximum non-trivial correlation modulus θ_{max} , this bound says that for large T and for M of the order of magnitude of T , the best correlation we can expect is at least

$$\theta_{max} \geq \sqrt{\alpha T},$$

where α is a constant of value 2 for binary sequences and 1 for non binary sequences. This bound is known to be tight for binary sequences (Gold sequences), for quaternary sequences [13, 4]. Families of p -ary sequences ($p \geq 3$ a prime) meeting that bound were first constructed by Sidelnikov, then by Kumar and Moreno [7] by using linear cyclic codes over $\mathbb{F}_p$.

*The research of this author is partially supported by NUS-ARF research grant R-146-000-029-112 and DSTA research grant R-394-000-011-422.

**This research was done while this author was visiting Temasek Laboratories and Department of Mathematics, NUS. The author thanks them for their hospitality.

In this note, we construct, for every odd prime p and every integer $m \geq 1$, a family $F_{p,m}$ with the following parameters

$$\begin{aligned} T &= p(p^m - 1) \\ M &= p^{m-1} \\ \theta_{\max} &\leq (p - 1)p^{m/2+1}. \end{aligned}$$

For large m and fixed p , we see that M is of the order of T/p^2 and that $\theta_{\max}$ is of the order of $p^{3/2}\sqrt{T}$, so our sequences are not as close to Sidelnikov bound as the constructions of Sidelnikov and Kumar-Moreno. Still they present the advantage of being highly nonlinear which is an important asset from a steganographic standpoint.

In the present work, we construct sequences from nonlinear codes over $\mathbb{F}_p$ obtained by the Gray map from cyclic codes over $\mathbb{Z}_{p^2}$. The code we use is a subcode of the p^2 -ary Kerdock code introduced by van Asch and van Tilborg [3]. To ensure cyclicity of the image, we will use the generalized Nechaev-Gray map [11] instead of the usual Gray map. The derivation of the correlation estimate that we need relies on a new arithmetic property of the Gray map, which is of interest in its own right. For any undefined concept regarding low correlation sequences, we refer the reader to the excellent survey [7].

We remark that, in the case where $p = 2$, analogous constructions of such sequences and their properties have been studied by various authors (cf. [5, 9, 10]).

2 Construction

2.1 Cyclic Codes over $\mathbb{Z}_{p^2}$

We will define a free cyclic code of length $n := p^m - 1$ over $\mathbb{Z}_{p^2}$ by its parity-check polynomial. Let $\overline{h_m}$ denote a primitive irreducible polynomial over $\mathbb{F}_p$. Then it is well-known (see [3, Theorem 7] for a direct proof) that there exists a unique polynomial $h_m \in \mathbb{Z}_{p^2}[x]$ satisfying both

1. $h_m \mid x^n - 1$
2. $h_m \equiv \overline{h_m} \pmod{p}$.

This is a special case of Hensel's lifting, which is programmed in most symbolic computation packages. We can now define the smaller Kerdock code $k_{p^2,m}$ as the code with parity-check polynomial h_m . Thus $k_{p^2,m}$ is of codimension one in $GK_{p^2,m}^-$ of [3].

To handle a trace description of that code, we need to recall some Galois ring theory. Let $GR(p^2, m)$ denote the quotient ring $\mathbb{Z}_{p^2}[x]/(h_m)$. This ring is local of maximal ideal (p) , and residue field $\mathbb{F}_{p^m}$. Denote by $\mu(\cdot)$ the residue map. Representatives of that quotient can be given by powers of a fixed root ξ , say, of h_m . The set of these representatives

$$T_m := \{0, 1, \xi, \xi^2, \dots, \xi^{n-1}\}$$

is called the Teichmüller set. Let $T_m^* = T_m \setminus \{0\}$. The unique p -adic expansion of $x \in GR(p^2, m)$ is given by

$$x = u + pv,$$

where $u, v \in T_m$. The Frobenius operator F is defined for such an x as $F(a + pb) = a^p + pb^p$, and the trace Tr , from $GR(p^2, m)$ down to $\mathbb{Z}_{p^2}$, as

$$Tr := \sum_{j=0}^{m-1} F^j.$$

The following result is then either immediate or a consequence of [3, p.326].

Proposition 2.1

$$k_{p^2, m} = \{(Tr(A), Tr(A\xi), \dots, Tr(A\xi^{n-1})) \mid A \in GR(p^2, m)\}.$$

2.2 The Gray Map

Define the Gray map $\phi : \mathbb{Z}_{p^2}^n \longrightarrow \mathbb{Z}_p^{pn}$ as follows: for $x \in \mathbb{Z}_{p^2}^n$ with p -adic expansion $u + pv$, with $u, v \in \mathbb{Z}_p^n$,

$$\phi(x) = \phi(u + pv) = (v, v + u, v + 2u, \dots, v + (p-1)u).$$

Observe the analogy with the $\mathbb{Z}_4$ -Gray map of [6]. Note that $\phi(pv)$ is the constant vector $(v, v, \dots, v)$.

Let $(n, p) = 1$ and let n' be the unique integer satisfying $1 \leq n' \leq p-1$ and $nn' \equiv 1 \pmod{p}$.

Let π be the permutation on $\mathbb{Z}_p^{pn}$ defined as follows: for $a = (a_0, a_1, \dots, a_{pn-1})$, then $\pi(a) = (a'_0, a'_1, \dots, a'_{pn-1})$, where, for $0 \leq \epsilon \leq p-1$ and $0 \leq j \leq n-1$,

$$a'_{\epsilon n + j} = a_{(\epsilon + jn')_p n + j}.$$

Here, $(y)_p$ denotes the unique number in $\{0, 1, \dots, p-1\}$ congruent to y modulo p . The map π is a generalization of the Nechaev permutation (in the case $p = 2$).

Write $\Phi = \pi\phi$. This may be called the generalized Nechaev-Gray map.

In [11, Corollary 3.6], it is proved that a code $\mathcal{C}$ of length n over $\mathbb{Z}_{p^2}$ is cyclic if and only if $\pi\phi(\mathcal{C})$ is cyclic over $\mathbb{Z}_p$ of length pn .

To go from the world of codes to the world of sequences, we require a little character theory. For $x \in \mathbb{Z}_{p^i}$, $i = 1, 2$, define the standard additive character

$$\Psi_i(x) = w_i^x,$$

where

$$w_i = \exp(2\pi\sqrt{-1}/p^i).$$

We are now in a position to define our family $F_{p,m}$ as the set of pairwise non-equivalent sequences within the set

$$\{(\Psi_1(x_0), \dots, \Psi_1(x_{pn-1})) \mid x = (x_0, \dots, x_{pn-1}) \in \Phi(k_{p^2,m} \setminus pk_{p^2,m})\}.$$

Proposition 2.2 *The size of the family $F_{p,m}$ is*

$$|F_{p,m}| = p^{m-1}.$$

Proof. It is clear that words of $\Phi(pk_{p^2,m})$ have period $p^m - 1$. The only delicate point is the cyclicity of $\Phi(k_{p^2,m})$, which results from [11, Corollary 3.6]. $\square$

3 Correlation

With every vector $x = (x_0, \dots, x_{n-1}) \in \mathbb{Z}_{p^2}^n$, we attach the character sum

$$\theta_2(x) := \sum_{j=0}^{n-1} \Psi_2(x_j).$$

Equivalently, if $n_j(x)$ denotes the frequency of the letter $j \in \mathbb{Z}_{p^2}$ amongst the entries of the word x , this is

$$\theta_2(x) = \sum_{j=0}^{p^2-1} n_j(x) \Psi_2(j).$$

Similarly, with every vector $y = (y_0, \dots, y_{pn-1}) \in \mathbb{Z}_p^{pn}$, we attach the sum

$$\theta_1(y) := \sum_{j=0}^{pn-1} \Psi_1(y_j).$$

By abuse of notation, we write

$$\theta_1(y) = \sum_{j=0}^{p-1} n_j(y) \Psi_1(j).$$

In order to estimate θ_{max} , it is necessary to bound from above the modulus of $\theta_1(y)$ for $y \in \Phi(k_{p^2,m} \setminus pk_{p^2,m})$.

3.1 A Property of the Gray Map

To express $\theta_1(\Phi(x))$ as a function of $\theta_2(x)$, we require some familiarity with certain basic facts in Number Fields, as can be gleaned from, e.g., [12]. Denote by Tr_2 the trace from the cyclotomic field $\mathbb{Q}(w_2)$ down to $\mathbb{Q}(w_1)$. It can be shown that this number field is of degree p over $\mathbb{Q}(w_1)$. For instance $Tr_2(1) = p$ and $Tr_2(w_2^j) = 0$ for j not a multiple of p . We are now in a position to state the main result of this subsection.

Theorem 3.1 *For all $x \in \mathbb{Z}_{p^2}^n$, we have*

$$Tr_2(\theta_2(x)) = \theta_1(\Phi(x)).$$

To prove this theorem, it will be useful to describe the composition of $y := \Phi(x) = \Phi(x_0 + px_1)$.

Lemma 3.2 *Assume $n = 1$ for simplicity. Three cases and three cases only occur*

1. if $x = 0$, then $n_j(y) = \delta_{j,0}p$,
2. if $x \in (p) \setminus \{0\}$, then $n_j(y) = \delta_{j,x_1}p$,
3. if $x \in \mathbb{Z}_{p^2} \setminus (p)$, then $n_j(y) = 1$ for all $j \in \mathbb{Z}_p$.

Proof. In each of the three cases we see that, respectively:

1. if $x = 0$ then $y = 0$,
2. the condition $x \in (p) \setminus \{0\}$ is equivalent to $x_0 = 0, x_1 \neq 0$,
3. by the properties of linear forms over finite fields, we see that the entries of y take all possible values in $\mathbb{Z}_p$ equally often. $\square$

We proceed with the proof of Theorem 3.1.

Proof. Assume, for simplicity, that $n = 1$. In each of the three cases of Lemma 3.2, we have respectively that

1. if $x = 0$, then $\theta_2(x) = n_0(x) = 1 \in \mathbb{Q}(w_2)$ and therefore $Tr_2(\theta_2(x)) = p = \theta_1(y)$,
2. if $x \in (p) \setminus \{0\}$, writing $x = pj$ ($1 \leq j \leq p-1$), then, because $w_2^p = w_1$, we have $\theta_2(x) = w_2^{pj} = w_1^j$, an element of $\mathbb{Q}(w_1)$. After taking traces of both sides, we get $Tr_2(\theta_2(x)) = \theta_1(y)$,
3. if $x \in \mathbb{Z}_{p^2} \setminus (p)$, then $n_{pj}(x) = 0$, for $0 \leq j \leq p-1$, hence $Tr_2(\theta_2(x)) = 0$. Now all $n_i(y)$ are the same, therefore $\theta_1(y) = 0$. $\square$

3.2 Arithmetic Geometry Estimates

Like in [3], we build on the deep results of [8].

Proposition 3.3

$$\theta_{\max} \leq (p-1)p^{m/2+1}.$$

Proof. We apply Theorem 3.1. We know from [8] that

$$|\theta_2(x)| \leq (p-1)p^{m/2}.$$

Since conjugation by the p elements of the Galois Group $\mathbb{Q}(w_2)/\mathbb{Q}(w_1)$ acts as a multiplier on the powers of w_2 that occur in $\theta_2(x)$ we can apply the same upper bound to each of the p conjugates of $\theta_2(x)$, which are also exponential sums of the same type, namely

$$\sum_{t \in T_m^*} w_2^{(y \text{Tr}(At))}.$$

The result follows by the triangle inequality. $\square$

4 Nonlinearity

We provide a parametrization of the p -adic expansion of the entries of the words of the smaller Kerdock code by nonlinear functions. We assume that $\xi \equiv \theta \pmod{p}$, say, where $\overline{h_m}(\theta) = 0$. Denote by tr the standard trace from $\mathbb{F}_{p^m}$ down to $\mathbb{F}_p$. Let $Q_p(\cdot)$ be the polynomial of $\mathbb{F}_p[T]/(T^{p^m} - T)$ given by

$$\frac{-1}{p} \sum \binom{p}{i_0, i_1, \dots, i_{m-1}} T^{p^{i_0} + \dots + p^{i_{m-1}}}.$$

The sum is taken over all m -tuples $i_0 \leq \dots \leq i_{m-1} < p$ such that $i_0 + \dots + i_{m-1} = p$. The symbol $\binom{p}{i_0, \dots, i_{m-1}}$ is the multinomial coefficient $p!/(i_0! \dots i_{m-1}!)$. Observe that this quantity is divisible by p by Fermat's little theorem.

Theorem 4.1 *Let c be a generic word of $k_{p^2, m}$ and let t run over T_m^* . If $c_t = \text{Tr}((A_0 + pA_1)\xi^t)$ with $A_0, A_1 \in T_m$, then its p -adic expansion $a_t + pb_t$ with $a_t, b_t \in T_m$ is given by*

$$a_t = \text{tr}(\pi\theta^t)$$

$$b_t = Q_p(\pi\theta^t) + \text{tr}(\eta\theta^t),$$

where

$$\pi = \mu(A_0)$$

$$\eta = \mu(A_1).$$

Proof. The expression for a_t is immediate because of the commutation relation

$$\mu \circ Tr = tr \circ \mu.$$

Since $a_t \in T_m$ we have that $a_t^p = a_t$. From there we get $pb_t = c_t - c_t^p$. Further

$$pb_t = Tr(A_0 \xi^t) - (Tr(A_0 \xi^t))^p + pTr(A_1 \xi^t).$$

Now by definition of the trace function

$$Tr(A_0 \xi^t) = \sum_{j=0}^{m-1} (A_0 \xi^t)^{p^j}.$$

The expression for b_t follows after expanding the p^{th} power of the preceding quantity by the multinomial theorem. $\square$

We proceed to show that the Gray image of the smaller Kerdock code is indeed nonlinear. First, we require a lemma on its residue and torsion codes. Every $\mathbb{Z}_{p^2}$ -linear code C has two associated p -ary codes, the residue code C_R and the torsion code C_T , such that $C_R = \mu(C)$ and C_T is the largest p -ary code D with the property that $pD \subseteq C$.

Lemma 4.2 *The residue and torsion codes of $k_{p^2,m}$ are the p -ary cyclic code $M_{p,m}$ of parity-check polynomial $\overline{h_m}$ and of parameters $[p^m - 1, m, (p - 1)p^{m-1}]$. Furthermore each nonzero codeword of $M_{p,m}$ contains each digit of $\mathbb{F}_p^\times$ exactly p^{m-1} times.*

Proof. It can be seen that both residue and torsion codes coincide with the cyclic code of parity-check polynomial $\overline{h_m}$. From the irreducibility and primitiveness of $\overline{h_m}$, we infer that $M_{p,m}$ is a maximum length code (in the sense of [7, p.1777]). The statement on the complete weight distribution follows then by the “run” property of m -sequences [7, Lemma 3.6]. $\square$

Let S be the set of ordered pairs (a, b) such that $a, b \in \mathbb{Z}_p$ and $a + b \geq p$. (We identify $\mathbb{Z}_p$ with $\{0, 1, \dots, p - 1\}$.) Let $f \in \mathbb{Z}_p[x, y]$ be defined as

$$f(x, y) = \left[(x^p - x)(y^p - y) \sum_{i=1}^{p-1} \frac{1}{x - i} \prod_{(i,j) \in S} \frac{1}{y - j} \right]^{p-1}.$$

It is easy to check that f is the characteristic function of S , i.e., $f(a, b) = 1$ for every $(a, b) \in S$ and is zero otherwise. For $c = (c_0, \dots, c_{n-1}) \in \mathbb{Z}_p^n$ and $d = (d_0, \dots, d_{n-1}) \in \mathbb{Z}_p^n$, we define

$$f(c, d) = (f(c_0, d_0), \dots, f(c_{n-1}, d_{n-1})).$$

For $A, B \in \mathbb{Z}_{p^2}^n$, write $A = A_0 + pA_1$ and $B = B_0 + pB_1$, where $A_0, A_1, B_0, B_1 \in \mathbb{Z}_p^n$.

Lemma 4.3 [11, Theorem 4.6] *If C is a $\mathbb{Z}_{p^2}$ -linear code of length n , then $\Phi(C)$ is a linear code over $\mathbb{Z}_p$ if and only if, for all $A, B \in C$, we have $pf(A_0, B_0) \in C$.*

Theorem 4.4 *The Gray image of the smaller Kerdock code is not $\mathbb{F}_p$ -linear.*

Proof. For a codeword x of $k_{p^2, m}$, we say that the coordinate place r is light (resp. heavy) if $(x_r, x_r) \notin S$ (resp. $(x_r, x_r) \in S$). Since the residue and torsion codes coincide, a necessary condition for the Gray image of $k_{p^2, m}$ to be non-linear (by Lemma 4.3) is that all coordinate places of x are heavy. In view of the complete weight distribution of $M_{p, m}$, this is impossible. In particular, for $p \geq 3$, all r with $x_r = 1$ are light. $\square$

5 Examples

The examples below were obtained in the following way. The complete weight enumerator of the Kerdock code was computed in Magma. Then the correlation was derived in Maple. It seems that the bound on the correlation can be improved by a factor p .

For $p = 3, m = 2$, we used $h_2 = x^2 + 4x + 8$, and found $\theta_{\max} = 4.41 \dots < 2\sqrt{3^2} = 6$.

$ \theta_2 ^2$	3.185	4.227	1.411	1	0.185	1.227	4.411
frequency	8	8	8	8	16	16	16

For $p = 3, m = 3$ we used $h_3 = x^3 + 3x^2 + 2x + 1$, and found $\theta_{\max} = 7.99 \dots < 2\sqrt{3^3} \simeq 10.39$.

$ \theta_2 ^2$	1	1	7.638	.958	2.596	3.596	.0418	6.638	6.234	4	7.99	7.034
frequency	26	78	78	78	78	78	78	78	26	78	26	26

For $m = 4, 5$, the relevant complete weight enumerators contain respectively 22 and 36 terms. Therefore, an analytic derivation of the correlation values (as in e.g. [4]) seems difficult.

Acknowledgments. The authors thank the referees for their helpful suggestions.

References

1. Barg, A.: Two families of low-correlated binary sequences. *AAECC* **7**, 433–437 (1996)
2. Berlekamp, E.: *Algebraic Coding Theory*, McGraw-Hill, 1968
3. van Asch, B., van Tilborg, H.C.A.: Two dual families of nearly-linear codes over $\mathbb{Z}_p$, p odd. *AAECC* **11**, 313–329 (2001)
4. Boztas, S., Hammons, R., Kumar, P.V.: 4-phase sequences with near-optimum correlation properties, *IEEE Trans. on Inform. Theory*, vol. IT-**38**, May 1992, pp. 1101–1113
5. Carlet, C.: $\mathbb{Z}_{2^k}$ -linear codes, *IEEE Trans. on Inform. Theory*, vol. IT-**44**, July 1998, pp. 1543–1547
6. Hammons, A.R., Kumar, P.V. Jr, Calderbank, A.R., Sloane, N.J.A., Solé, P.: The $\mathbb{Z}_4$ -linearity of Kerdock, Preparata, Goethals and related codes, *IEEE Trans. on Inform. Theory* vol. IT-**40**, March 1994, pp. 301–319
7. Helleseht, T., Kumar, P.V.: Sequences with low correlation, *Handbook of Coding Theory*, edited by V. Pless and C. Huffman, Elsevier Science Publishers, 1998
8. Kumar, P.V., Helleseht, T., Calderbank, A.R.: An upper bound for Weil exponential sums over Galois rings and applications, *IEEE Trans. on Inform. Theory*, vol. IT-**41**, March 1995, pp. 456–468
9. Kuz'min, A.S., Nechaev, A.A.: Linear recurrence sequences over Galois rings (in Russian), *Uspekhi Mat. Nauk* **48** 1(289) 167–168 (1993); translation in *Russian Math. Surveys* **48**(1), 171–172 (1993)
10. Kuz'min, A.S., Nechaev, A.A.: Linearly representable codes and the Kerdock code over an arbitrary Galois field of characteristic 2 (in Russian), *Uspekhi Mat. Nauk* **49** 5(299), 165–166 (1994); translation in *Russian Math. Surveys* **49**(5), 183–184 (1994)
11. Ling, S., Blackford, J.T.: $\mathbb{Z}_{p^{k+1}}$ -linear codes, *IEEE Trans. on Inform. Theory*, vol. IT-**48**, September 2002, pp. 2592–2605
12. Marcus, D.A.: *Number Fields*, Springer Universitext, 1977
13. Solé, P.: A quaternary cyclic code and a family of quadriphase sequences with low correlation properties. *Springer Lecture Notes in Comp. Sc.* **388**, 193–201 (1989)