Petri Rosendahl

Niho Type Cross-Correlation Functions and Related Equations

Turku Centre *for* Computer Science

TUCS Dissertations
No 53, August 2004

Niho Type Cross-Correlation Functions and Related Equations

by

Petri Rosendahl

To be presented, with the permission of the Faculty of Mathematics and Natural Sciences of the University of Turku, for public criticism in Auditorium XXI of the University on October 1st, 2004, at 12 noon

University of Turku
Department of Mathematics
FIN-20014 Turku, Finland

2004

Supervisor

Docent Iiro Honkala
Department of Mathematics
University of Turku
FIN-20014 Turku
Finland

Reviewers

Professor Pascale Charpin
INRIA-Rocquencourt
Domaine de Voluceau, B.P. 105
78153 Le Chesnay Cedex
France

Principal Lecturer Hannu Tarnanen
Turku Polytechnic
Sepänkatu 3
FIN-20700 Turku
Finland

Opponent

Professor Claude Carlet
INRIA-Rocquencourt, Bat. 10
Domaine de Voluceau, B.P. 105
78153 Le Chesnay Cedex
France

ISBN 952-12-1397-3
ISSN 1239-1883
Painosalama Oy
Turku, Finland
2004

Acknowledgements

First of all I want to thank my supervisor Docent Iiro Honkala. His support has been priceless.

I have had the privilege to work with Professor Tor Helleseth, and I am deeply indebted to him for his help.

I also want to thank my other co-authors Docent Jyrki Lahtonen, Professor Hans Dobbertin and M.Sc. Patrick Felke.

Professor Pascale Charpin and Principal Lecturer Hannu Tarnanen, the reviewers of my thesis, deserve special thanks for their work.

Doctor Kalle Ranto carefully read my manuscript and his help is gratefully acknowledged.

Lastly, I want to thank the staff at the Department of Mathematics at the University of Turku and the Department of Informatics at the University of Bergen.

Turku
September 2004 Petri Rosendahl

Contents

Preface

Cross-correlation functions of maximal period sequences have been studied roughly forty years. The so called Gold sequences were found in 1967, and are still in practical use. In the 1970s Trachtenberg, Niho and Helleseth wrote their very influential theses on the topic. Moreover, cross-correlation functions of maximal period sequences can be interpreted as character sums (or Weil sums) over finite fields and therefore the mathematical theory is actually much older. We can say that the subject is well established and in mathematics a field of its own.

In this thesis, we will study cross-correlation functions corresponding to decimations d which satisfy

$$d \equiv 1 \pmod{2^k - 1},$$

where k is half of the order of the sequences in question, i.e., the period of the sequences is $2^{2k} - 1$. This type of decimations were first studied in the famous thesis by Yoji Niho in 1972. This pioneering work has become one of the most cited works in the theory of m-sequences and coding theory.

Niho's work has been important in essentially two ways. Firstly, because Niho described a method to treat the decimations described above and applied this method to certain special cases. Secondly, and even more importantly, Niho did an extensive computer search for cross-correlation functions with few values. Considering the time this is impressive as this problem is computationally very demanding. In addition, Niho made several conjectures based on his tables and this made his thesis an important source of open problems. Some of these problems have been solved only recently.

In this thesis we have collected essentially all known results about Niho type cross-correlations. Our treatment will be mathematical throughout,

the emphasis being on equations over finite fields. We have made an attempt to give as simple and unified account as possible.

This thesis is organized as follows. In Chapter 1 we give some necessary background on finite fields. This is done mostly in order to fix the notation, and we will assume that the reader has a basic knowledge of the theory of finite fields. In Chapter 2 we recall some basic properties of cross-correlation functions of m-sequences. We also list all decimations for which the cross-correlation function is known. The first two chapters should provide all the tools needed in order to understand the rest of the thesis.

In Chapter 3 we give a simplified proof of the main theorem of Niho, and make some general remarks about Niho type decimations. We will also show how Niho's theorem can be generalized to include also non-binary sequences. At the end of the chapter we generalize Charpin's result on Niho type cross-correlations.

Chapter 4 is devoted to the study of the number of solutions to the third power sum equation in case of Niho type exponents. We develop a technique to treat these equations. Using this technique we will, among other things, solve completely the question when this equation has only trivial solutions.

In Chapter 5 we give the values and their distributions for all known cross-correlations of Niho type. For previously known results we give simplified proofs. The results from Chapter 3 and Chapter 4 play a central role here.

The material of the thesis comes mainly from the articles [25], [22], [35], [23], and [13].

Chapter 1

Preliminaries

We will assume that the reader has a working knowledge of finite fields and algebra in general. Here we give only some basic facts and fix the notation. For additional information and proofs, the reader is referred to the books [31, 37], and the survey [27].

1.1 Basic facts

The finite field with q elements will be denoted by $GF(q)$. It is well known that $q = p^n$ for some prime p and an integer $n \geq 1$. On the other hand, given a prime p and an integer $n \geq 1$, there exists a finite field with p^n elements, and this field is essentially unique. The finite field with $q = p^n$ elements is the splitting field of the polynomial $x^q - x$ over the prime field $GF(p)$, and in fact $GF(q)$ is precisely the set of elements satisfying $x^q = x$.

The multiplicative group of $GF(q)$ will be denoted by $GF(q)^\times$. The group $GF(q)^\times$ is cyclic, and a primitive element of $GF(q)$ is by definition a generator of $GF(q)^\times$. A polynomial $f(x) \in GF(p)[x]$ of degree n is primitive over $GF(p)$ if it is the minimum polynomial of some primitive element of $GF(p^n)$.

Recall that the subfields of $GF(p^n)$ are in one-to-one correspondence with the divisors of n.

Assume that k divides n, so that $GF(p^k)$ is a subfield of $GF(p^n)$, and set $q = p^k$ and $m = n/k$. Then the *trace* function $tr_k^n : GF(p^n) \to GF(p^k)$ is defined by

$$tr_k^n(x) = x + x^q + x^{q^2} + \cdots + x^{q^{m-1}}.$$

The basic properties of the trace are:

(*i*) tr_k^n is linear over $GF(q)$,

(*ii*) tr_k^n is balanced, i.e., every $c \in GF(q)$ occurs exactly q^{m-1} times as an image,

(*iii*) $tr_k^n(x^q) = tr_k^n(x)$, and

(*iv*) the trace function is transitive, that is, $tr_k^n(x) = tr_k^l(tr_l^n(x))$, whenever l divides n and k divides l.

More generally, a polynomial $L(x) \in GF(p^n)[x]$ of the form

$$L(x) = \sum_{i=0}^{n-1} a_i x^{p^i},$$

is called *linearized*.

We will need the following well known and simple fact from linear algebra.

Lemma 1.1. *Let $L(x)$ be a linearized polynomial over $GF(p^n)$ and $\alpha \in GF(p^n)$. Then the equation $L(x) = \alpha$ either has no solutions or it has exactly the same number of solutions in $GF(p^n)$ as the equation $L(x) = 0$.*

Let ζ be a primitive complex p-th root of unity, and let $x \in GF(p^n)$. We set

$$\chi(x) = \zeta^{tr_1^n(x)}.$$

This is the *canonical additive character* of the finite field $GF(p^n)$. The map $\chi : GF(p^n) \to \mathbb{C}^\times$ is indeed a character of the additive group of $GF(p^n)$. It satisfies

(*i*) $\chi(x+y) = \chi(x)\chi(y)$,

(*ii*) $\chi(x^p) = \chi(x)$, and

(*iii*) $\sum_{x \in GF(p^n)} \chi(x) = 0$.

The identity (*iii*) implies that $\sum_{a \in GF(p^n)} \chi(ax) = 0$ if $x \neq 0$. If $x = 0$, then the sum equals p^n, of course.

1.2 Extensions of even degree

In this section we give some definitions and facts that are specific to extensions of even degree.

Let $y \in GF(q^2)$. In analogy with the usual complex conjugation we define

$$\overline{y} = y^q.$$

The usual algebraic properties of conjugation carry over to the finite case. For example, we have

(*i*) $\overline{x+y} = \overline{x} + \overline{y}$ and $\overline{xy} = \overline{x}\,\overline{y}$, for all $x, y \in GF(q^2)$, and

(*ii*) $x + \overline{x} \in GF(q)$ and $x\overline{x} \in GF(q)$, for all $x \in GF(q^2)$.

We define the unit circle of $GF(q^2)$ to be the set

$$S = \left\{x \in GF(q^2) : x\overline{x} = 1\right\}.$$

In other words, S is the group of $(q+1)$-st roots of unity in $GF(q^2)$. We will exploit this group structure in many situations.

A geometric interpretation of Lemma 1.2 gives an analogy with complex numbers. The first parameterization is from [30] and the second one is from [22].

Lemma 1.2. (*i*) *Let $z \in GF(q^2) \setminus GF(q)$ be fixed. Then*

$$S \setminus \{1\} = \left\{\frac{z+u}{\overline{z}+u} : u \in GF(q)\right\}.$$

(*ii*) *Let $\beta \in S \setminus \{\pm 1\}$ be fixed. Then*

$$S \setminus \{\beta\} = \left\{\frac{\alpha\beta+1}{\alpha+\beta} : \alpha \in GF(q)\right\}.$$

Proof. Assume that

$$\frac{z+u}{\overline{z}+u} = \frac{z+v}{\overline{z}+v},$$

for some $u, v \in GF(q)$. Then

$$z\overline{z} + u\overline{z} + zv + uv = z\overline{z} + v\overline{z} + zu + uv,$$

which implies that

$$(\overline{z} - z)\,(u - v) = 0,$$

and therefore $u = v$. Thus the elements $x = (z + u)/(\overline{z} + u)$, where $z \in GF(q^2) \setminus GF(q)$ and $u \in GF(q)$, are distinct. Moreover, they satisfy $\overline{x} = x^{-1}$. Also $x \neq 1$ since $z \neq \overline{z}$. This proves (i), and (ii) is equally simple. □

Assume that q is even. Then $\gcd(q-1, q+1) = 1$, and hence the group $GF(q^2)^\times$ is the direct product of its subgroups $GF(q)^\times$ and S. Thus we have the following lemma, which is analogous to polar representation of complex numbers.

Lemma 1.3. *Assume that q is even. Then every $x \in GF(q^2)^\times$ can be represented uniquely as*

$$x = \alpha\beta,$$

where $\alpha \in GF(q)^\times$ and $\beta \in S$.

For arbitrary x this representation can be found from the following trivial identity

$$x^2 = (x\overline{x}) \left(\frac{x}{\overline{x}}\right). \tag{1.1}$$

We will use this identity indirectly in Chapter 4.

If q is odd, then $\gcd(q-1, q+1) = 2$, and therefore the previous lemma fails to be valid. However, every $x \in GF(q^2)^\times$ has a unique representation as

$$x = \alpha\beta, \tag{1.2}$$

where $\alpha \in GF(q)^\times$, $\beta \in \{1, \gamma, \gamma^2, \ldots, \gamma^q\}$, and γ is a primitive element of $GF(q^2)$. Surprisingly, this completely trivial representation proves to be useful.

1.3 Linear recurring sequences

There are many different approaches, such as matrix theory and the theory of formal power series, to linear recurrences over finite fields. For different aspects the reader should consult [31], [32], and [36]. We are interested in cross-correlation functions, and therefore we will make use of the trace representation.

Let $a_1, \ldots, a_n$, where $a_n \neq 0$, be given elements of the field $GF(p)$. A linear recurring sequence over the field $GF(p)$ is a sequence $u_0, u_1, \ldots$ of elements of $GF(p)$ satisfying a recurrence

$$u_{i+n} + a_1 u_{i+n-1} + a_2 u_{i+n-2} + \cdots + a_n u_i = 0, \tag{1.3}$$

for all i. The sequence u_i is completely determined by the *initial values* $u_0, u_1, \ldots, u_{n-1}$ and the relation (1.3).

The number n is called the *order* (or *degree*) of the recurrence.

Since linear recurring sequences can be generated by shift registers they are also known as *linear feedback shift register sequences*. This is the point of view e.g. in [17].

It is well known that the relation (1.3) produces an ultimately periodic sequence with least period at most $p^n - 1$. It is also clear that a periodic sequence satisfies a linear recurrence relation.

The *characteristic polynomial* of the recurrence (1.3) is by definition

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n. \tag{1.4}$$

Sometimes, e.g. in [31], $f(x)$ is also said to be the characteristic polynomial of the corresponding sequences, but then the reader should note that it is not unique.

It is known that a nonzero sequence generated by (1.3) has the maximum possible period $p^n - 1$ if and only if the characteristic polynomial of the corresponding recurrence is a primitive polynomial over the field $GF(p)$.

Definition 1.4. An *m-sequence (short for maximal period sequence) of order n* is a nonzero sequence which satisfies a recurrence of order n whose characteristic polynomial is a primitive polynomial over the field $GF(p)$.

Due to their randomness properties m-sequences are also known as *pseudo-noise sequences*.

The trace function provides a useful representation of m-sequences.

Theorem 1.5. *Let u_t be an m-sequence of period $p^n - 1$. Then there is an element $y \in GF(p^n)^\times$ such that*

$$u_t = tr_1^n(y\gamma^t), \tag{1.5}$$

for some primitive element γ of the field $GF(p^n)$. Conversely, if γ is a primitive element of $GF(p^n)$ and $y \in GF(p^n)$ is nonzero, then the sequence determined by (1.5) *is an m-sequence.*

In what follows, the following two properties will be fundamental.

Lemma 1.6. *Let u_t and v_t be two m-sequences of period $p^n - 1$. Then*

(*i*) *the sequence u_{dt}, where d is an integer, is an m-sequence if and only if* $\gcd(d, p^n - 1) = 1$*, and*

(*ii*) *there is an integer d and an integer k such that* $\gcd(d, p^n - 1) = 1$ *and $v_{t+k} = u_{dt}$ for all $t = 0, 1, \ldots$.*

For the proof of Theorem 1.5, see [31]. Lemma 1.6 is a straightforward consequence of Theorem 1.5.

If there is an integer k such that $v_{t+k} = u_t$ for all $t = 0, 1, \ldots$, then the sequence v_t is said to be a *cyclic shift* of the sequence u_t. We will make no difference between a sequence and its cyclic shifts.

An integer d satisfying $\gcd(d, p^n - 1)$ is said to be a *decimation*. The previous lemma says that two m-sequences of the same period are connected by a decimation and a cyclic shift.

Chapter 2

Cross-correlation of m-sequences

In this chapter we give the most basic properties of cross-correlation functions of m-sequences. We also list all decimations for which the corresponding cross-correlation function is known.

2.1 Properties of cross-correlation functions

Let u_t and v_t be two periodic sequences of elements from $GF(p)$, and assume that both have the same period ϵ. Furthermore, let ζ be a primitive complex p-th root of unity.

Definition 2.1. The (periodic) *cross-correlation function* $C_{u,v}$ between the sequences u_t and v_t is defined for $\tau = 0, 1, \ldots, \epsilon - 1$ by

$$C_{u,v}(\tau) = \sum_{t=0}^{\epsilon-1} \zeta^{u_t - v_{t+\tau}}. \tag{2.1}$$

Assume for a moment that u_t and v_t are binary, i.e., $p = 2$. Then in the sum (2.1) u_t and a cyclic shift by τ of v_t are compared bit by bit, and then the sum $C_{u,v}(\tau)$ counts the number of agreements and disagreements. In other words, $C_{u,v}$ measures how similar u_t is to v_t. Why this measure is important is explained in detail e.g. in [32].

In the non-binary case the situation is more complex, and from the practical point of view the cross-correlation function is somewhat artificial. However, also non-binary sequences have been used in practice.

Besides the periodic cross-correlation function, there are many other correlation measures, and the reader should consult [21].

An important problem in the theory of sequences is the cross-correlation problem:

> *Find the values and the number of their occurrences of the cross-correlation function $C_{u,v}$.*

Usually, one is not interested in the value $C_{u,v}(\tau)$ for a specific cyclic shift τ, and when one speaks about the cross-correlation function it is actually the multiset of its values in question. Therefore a sequence and its cyclic shifts are considered the same in this context.

From now on we assume that u_t and v_t are, binary or non-binary, m-sequences of period $p^n - 1$. We may, possibly after cyclic shifts, write

$$u_t = tr_1^n(\gamma^t),$$

and $v_t = u_{dt}$, where γ is a primitive element of the field $GF(p^n)$ and d satisfies $\gcd(d, p^n - 1) = 1$. The cross-correlation function between the m-sequences u_t and u_{dt} will be denoted by $C_d(\tau)$.

We have

$$\begin{aligned} C_d(\tau) &= \sum_{t=0}^{p^n-2} \zeta^{tr_1^n(\gamma^t)-tr_1^n(\gamma^{d(t+\tau)})} \\ &= \sum_{t=0}^{p^n-2} \zeta^{tr_1^n(\gamma^t-\gamma^{d(t+\tau)})} \\ &= \sum_{x\in GF(q)^\times} \zeta^{tr_1^n(x-yx^d)} \\ &= \sum_{x\in GF(q)^\times} \chi(x - yx^d), \end{aligned}$$

where χ is the canonical additive character and $y = \gamma^{d\tau}$.

Thus we have an algebraic characterization of the combinatorial cross-correlation problem: we should find the values of certain character sums. We note here that this kind of character sums are strongly connected with the weight distributions of certain cyclic codes and nonlinearity properties of power functions. For these connections, the reader should consult e.g. [4, 5]. For the use of character sums in coding theory, we refer to [27].

It is very common to speak about $C_d(\tau)$ in terms of y without specifying the one-to-one correspondence between τ and y.

Replacing y by $-y$ does not change the values or the number of their occurrences, and therefore (by redefining y) we may write

$$C_d(\tau) = \sum_{x \in GF(q)^\times} \chi(x + yx^d).$$

For the same reason, we may also write

$$C_d(\tau) = \sum_{x \in GF(q)^\times} \chi(yx + x^d).$$

This is combinatorially clear: it does not matter which one of the sequences is shifted cyclically.

When the sequences u_t and v_t are the same[1], e.g. when $d = 1$, one speaks of *autocorrelation*. We have

$$C_1(\tau) = \sum_{x \in GF(q)^\times} \chi(x - yx) = \sum_{x \in GF(q)^\times} \chi((1 - y)x),$$

and therefore

$$C_1(\tau) = \begin{cases} p^n - 1 & , \text{ if } y = 1 \\ -1 & , \text{ otherwise.} \end{cases}$$

This two-level autocorrelation property of m-sequences has many practical applications.

The following simple properties are proved in [39].

Theorem 2.2. (*i*) *The values of* $C_d(\tau)$ *are real.*

(*ii*) *The values and the number of their occurrences do not depend on the choice of* ζ.

Definition 2.3. If two decimations d and d' satisfy $d' \equiv p^i d \pmod{p^n - 1}$ or $dd' \equiv p^i \pmod{p^n - 1}$ for some i, then they are called *equivalent*.

It is straightforward to see that the equivalence of decimations is an equivalence relation.

[1] It is an easy task to prove that u_t and u_{dt} are the same if and only if $d \equiv p^i \pmod{p^n - 1}$.

If d and d' are equivalent, then the values and the number of their occurrences are the same for $C_d(\tau)$ and $C_{d'}(\tau)$, see [39], and we may consider equivalent decimations as the same. On the other hand it is possible that nonequivalent decimations produce the same correlation values with the same distribution.

The following theorem is useful in finding the distributions of values.

Theorem 2.4. *We have*

(i) $\sum_{\tau=0}^{p^n-2}(C_d(\tau)+1) = p^n$

(ii) $\sum_{\tau=0}^{p^n-2}(C_d(\tau)+1)^2 = p^{2n}$

(iii) $\sum_{\tau=0}^{p^n-2}(C_d(\tau)+1)^3 = p^{2n}b$,

where b is the number of $x \in GF(q)$ such that

$$(x+1)^d = x^d + 1. \tag{2.2}$$

Proof. The identities (i) and (ii) are very simple to prove, see e.g. [34].

The identity (iii) is due to Helleseth [18], and was originally derived from more general results. The equation (2.2) will be one of our main interests and to this end we give here a direct proof of (iii).

So denote

$$S_3 = \sum_{\tau=0}^{p^n-2}(C_d(\tau)+1)^3.$$

For notational reasons, we set here that the range of variables u, x, y, and z is $GF(p^n)$, and do not denote this in the sums.

Since $C_d(\tau)+1 = \sum_x \chi\left(x^d + ux\right)$, we have

$$S_3 = \sum_{u\neq 0}\sum_{x,y,z} \chi\left(x^d + y^d + z^d + u(x+y+z)\right).$$

The fact $\gcd(d, p^n-1) = 1$ implies that $x \mapsto x^d$ is one-to-one, and one deduces easily that $\sum_{x,y,z}\chi\left(x^d+y^d+z^d\right) = 0$, and hence

$$\begin{aligned} S_3 &= \sum_{u}\sum_{x,y,z} \chi\left(x^d + y^d + z^d + u(x+y+z)\right) \\ &= \sum_{x,y,z} \chi\left(x^d+y^d+z^d\right)\sum_u \chi(u(x+y+z)). \end{aligned}$$

The inner sum here is zero unless $x + y + z = 0$, and therefore

$$\begin{aligned} S_3 &= p^n \cdot \sum_{x,y} \sum_{z=-x-y} \chi\left(x^d + y^d + z^d\right) \\ &= p^n \cdot \sum_{x,y} \chi\left(x^d + y^d - (x+y)^d\right) \\ &= p^n \left(p^n + \sum_{x \neq 0} \sum_{y} \chi\left(x^d + y^d - (x+y)^d\right) \right). \end{aligned}$$

Here we have used the fact that if p is odd then d is odd. Substituting $y = ax$ and letting a run through $GF(p^n)$, we finally get

$$\begin{aligned} S_3 &= p^n \cdot \left(p^n + \sum_{x \neq 0} \sum_{a} \chi\left(x^d + (ax)^d - (x+ax)^d\right) \right) \\ &= p^n \cdot \left(p^n + \sum_{x \neq 0} \sum_{a} \chi\left(x^d \left(1 + a^d - (1+a)^d\right)\right) \right) \\ &= p^n \cdot \sum_{x} \sum_{a} \chi\left(x^d \left(1 + a^d - (1+a)^d\right)\right) \\ &= p^{2n} \cdot b, \end{aligned}$$

since $x \mapsto x^d$ is one-to-one. □

Similar argumentation leads to expressions for general power sums

$$S_i = \sum_{\tau=0}^{p^n-2} (C_d(\tau) + 1)^i,$$

see [21]. The corresponding equations are unfortunately extremely difficult to handle when $i > 3$.

If $d = p^i$ for some i, then $C_d(\tau)$ is two-valued; the sequences u_t and u_{dt} are in fact the same. Conversely, Helleseth [18] has proved

Theorem 2.5. *If d is not a power of p, then $C_d(\tau)$ has at least three different values.*

Some additional properties, e.g. divisibility results, of cross-correlation can be found in [18], but not very many general results are known about cross-correlation functions of m-sequences. One divisibility result will be given in Theorem 3.5.

2.2 Known cross-correlation functions

The cross-correlation function is completely known for relatively few infinite families of decimations. These are listed in the following.

In addition, there are also some decimations (both binary and non-binary) for which the values are known, but for which the distribution of the values has not been found.

In the following, $p^n - 1$ is always the period of the sequences in question, and k is a parameter which satisfies the given conditions.

2.2.1 Binary cross-correlations

The following decimations produce a three-valued cross-correlation function.

(i) $d = 2^k + 1$, with $n/\gcd(n,k)$ odd,

(ii) $d = 2^{2k} - 2^k + 1$, with $n/\gcd(n,k)$ odd,

(iii) $d = 2^{n/2} + 2^{(n+2)/4} + 1$, with $n \equiv 2 \pmod 4$,

(iv) $d = 2^{n/2+1} + 3$, with $n \equiv 2 \pmod 4$,

(v) $d = 2^{(n-1)/2} + 3$, with n odd,

(vi) $d = 2^{(n-1)/2} + 2^{(n-1)/4} - 1$, with $n \equiv 1 \pmod 4$, and

(vii) $d = 2^{(n-1)/2} + 2^{(3n-1)/4} - 1$, with $n \equiv 3 \pmod 4$.

The case (i) was proved by Gold [16], the case (ii) is due to Kasami [28], and the cases (iii) and (iv) were proved by Cusick and Dobbertin [8]. The case (v) is the famous Welch conjecture and was proved by Canteaut, Charpin and Dobbertin [3]. The cases (vi) and (vii) were conjectured by Niho [34] and proved by Hollmann and Xiang [26] building heavily on results in [3] and [11].

There are only three known four-valued cases:

(*i*) $d = 2^{n/2+1} - 1$, with $n \equiv 0 \pmod 4$,

(*ii*) $d = (2^{n/2} + 1)(2^{n/4} - 1) + 2$, with $n \equiv 0 \pmod 4$, and

(*iii*) $d = \sum_{i=0}^{n/2} 2^{im}$, with $n \equiv 0 \pmod 4$, $0 < m < n$, $\gcd(n, m) = 1$.

The cases (*i*) and (*ii*) are due to Niho [34]. The case (*iii*) is due to Dobbertin [10]. The family (*iii*) includes the decimations in (*i*).

The known five-valued cases are

(*i*) $d = 2^{n/2} + 3$, with n even and $n/2 > 2$, and

(*ii*) $d = 2^{n/2} + 2^{n/4} + 1$, with $n \equiv 0 \pmod 4$ and $n/4$ odd.

The case (*i*) was conjectured by Niho [34] and proved by Helleseth [18]. The family in (*ii*) was found by Dobbertin [10].

The known six-valued cases are

(*i*) $d = \frac{1}{3}(2^n - 1) + 2^s$, with n even, $s < n$, and $\frac{1}{3}2^{-s}(2^n - 1) \not\equiv 2 \pmod 3$, and

(*ii*) $d = 2^{n/2} - 2^{n/4} + 1$, with $n \equiv 0 \pmod 8$.

Both (*i*) and (*ii*) are due to Helleseth [18, 19].

One notable decimation for which the values are known is $d = -1$, see [29]. This is known as the Kloosterman sum. Although there is an apparent connection to the theory of algebraic curves (or algebraic function fields), see [38], this case is the only one which actually has been solved with algebraic-geometric methods.

2.2.2 Non-binary cross-correlations

It seems that in general the (algebraic) cross-correlation problem is more difficult for non-binary than binary sequences. Clearly, one reason is that the computation of non-binary cross-correlation requires exponential amount of time compared to computation of non-binary cross-correlation. The following seven cases have been completely solved:

(*i*) $d = \frac{1}{2}\left(p^{2k} + 1\right)$, with $n/\gcd(n, k)$ odd,

(*ii*) $d = p^{2k} - p^k + 1$, with $n/\gcd(n, k)$ odd,

(*iii*) $d = 2 \cdot 3^{(n-1)/2} + 1$, with $p = 3$ and n odd,

(*iv*) $d = 2 \cdot p^{n/2} - 1$, with n even and $p^{n/2} \not\equiv 2 \pmod 3$,

(*v*) $d = \frac{1}{2}(p^n - 1) + p^i$, with $0 \leq i < n$ and $p^n \equiv 1 \pmod 4$,

(*vi*) $d = \frac{1}{3}(p^n - 1) + p^i$, with $0 \leq i < n$, n even, $p \equiv 2 \pmod 3$ and $\frac{1}{3}p^{-i}(p^n - 1) \not\equiv 2 \pmod 3$, and

(*vii*) $d = p^{n/2} - p^{n/4} + 1$, with $n \equiv 0 \pmod 4$ and $p^{n/4} \not\equiv 2 \pmod 3$.

Cases (*i*) and (*ii*) are three-valued and were found by Trachtenberg [39] for odd n. The generalizations are due to Helleseth [18]. The family (*iii*) was found by Dobbertin et al. [14], and is three-valued as well.

Decimations in (*iv*) were found by Helleseth [18] and they produce four-valued cross-correlations.

The five-valued case (*v*) was found by Helleseth [18].

Cases (*vi*) and (*vii*) are due to Helleseth [18, 20] and are six-valued.

It is interesting to note that apart from (*iii*) and (*vii*) all were found already in the 1970s.

Chapter 3

Decimations of Niho type

In this chapter we review the main theorem in [34] and give a simplified proof. We will also give a generalization of Niho's theorem and show how this implies the original one. Lastly, we give a proof of Charpin's result, which states that Niho type decimations lead to at least four-valued cross-correlation functions.

3.1 Niho's theorem

We begin with a definition.

Definition 3.1. Assume that $n = 2k$ and let $q = p^k$. A decimation d is said to be of Niho type if

$$d \equiv 1 \pmod{q-1}.$$

From now on the length of the sequences in question will always be $p^n - 1$, where $n = 2k$, and the decimations we study will all be of Niho type. In this section $p = 2$.

Theorem 3.2 gives the main technique used in [34]. Niho treated a seemingly more general class of decimations; he assumed only that $d \equiv 2^i \pmod{2^k - 1}$ for some i. However, by Theorem 2.2 the decimation $2^{k-i}d$ produces an equivalent cross-correlation function, and therefore we can assume that $d \equiv 1 \pmod{2^k - 1}$. This simplifies the proof considerably.

When we study cross-correlation functions of m-sequences, we will always assume that $\gcd(d, p^n - 1) = 1$. However, some results make sense

without this condition, and are useful for instance in finding weight distributions of certain cyclic codes.

The following theorem describes the main method used by Niho in his thesis [34]. Recall that

$$S = \{x \in GF(2^n) : x\overline{x} = 1\}.$$

Theorem 3.2. ([34]) *Assume that* $d \equiv 1 \pmod{2^k - 1}$. *Then* $C_d(\tau)$ *assumes exactly the values*

$$-1 + (N(y) - 1) \cdot 2^k,$$

where $N(y)$ *is the number of* $x \in S$ *such that*

$$x^{2d} + yx^{d+1} + \overline{y}x^{d-1} + 1 = 0, \tag{3.1}$$

and y *runs through the nonzero elements of the field* $GF(2^n)$.

Proof. First of all, by Lemma 1.3 every nonzero $x \in GF(2^n)$ can be represented uniquely as $x = \alpha\beta$, where $\alpha \in GF(2^k)$ and $\beta \in S$. Note that $\alpha^d = \alpha$ for $\alpha \in GF(2^k)$ and $\beta^{2^k} = \beta^{-1}$ for $\beta \in S$. Using these together with the linearity and the transitivity of the trace, we get

$$\begin{aligned}
C_d(\tau) &= \sum_{x \neq 0} (-1)^{tr_1^n(yx + x^d)} \\
&= \sum_{\beta} \sum_{\alpha \neq 0} (-1)^{tr_1^n(y\alpha\beta + \alpha^d\beta^d)} \\
&= \sum_{\beta} \sum_{\alpha \neq 0} (-1)^{tr_1^n(\alpha(y\beta + \beta^d))} \\
&= \sum_{\beta} \sum_{\alpha \neq 0} (-1)^{tr_1^k(\alpha(y\beta + \beta^d + \overline{y}\beta^{-1} + \beta^{-d}))} \\
&= -2^k - 1 + \sum_{\beta} \sum_{z \in GF(q)} (-1)^{tr_1^k(z(y\beta + \beta^d + \overline{y}\beta^{-1} + \beta^{-d}))} \\
&= -1 + (N(y) - 1) \cdot 2^k,
\end{aligned}$$

where $N(y)$ is the number of $x \in S$ such that

$$x^d + yx + \overline{y}x^{-1} + x^{-d} = 0.$$

□

Remark 3.3. (*i*) Assume now that for some s, and for some t such that $\gcd(t, 2^k + 1) = 1$, we have $td \equiv s \pmod{2^k + 1}$. Then the mapping $x \mapsto x^t$ is a permutation of S, and substituting x^t for x in (3.1) yields an equivalent equation

$$x^{2s} + yx^{s+t} + \overline{y}x^{s-t} + 1 = 0. \tag{3.2}$$

We could have obtained this equation directly by noting that every $x \in GF(2^n)^\times$ has a unique representation also as $x = \alpha\beta^t$ with $\alpha \in GF(q)^\times$ and $\beta \in S$.

The form (3.2) will occur in Theorem 5.2.

(*ii*) If $\gcd(s, 2^k + 1) = 1$ and $\gcd(t, 2^k + 1) = 1$, then by the Chinese remainder theorem there is a decimation leading to the equation (3.2), i.e., there is a d such that $\gcd(d, 2^n - 1) = 1$ and

$$\begin{cases} d \equiv 1 & \pmod{2^k - 1} \\ td \equiv s & \pmod{2^k + 1}. \end{cases}$$

(*iii*) It is easy to see that replacing s by $-s$ in (3.2) leads to the same equation. Also, the roles of s and t can be changed. These two remarks just reflect the facts that the decimations $2^k d$ and $d^{-1} \pmod{2^n - 1}$ produce equivalent cross-correlation functions.

(*iv*) In (3.2) both s and t are typically odd. In this case the square root can be taken of the equation, since we are interested only in the number of distinct solutions. Replacement of $\sqrt{y}$ by y does not affect the distribution of the number of the solutions, since $\sqrt{y}$ runs through $GF(2^n)$ when y does.

3.2 A generalization of Niho's theorem

In this section p is an arbitrary prime, $n = 2k$ and $q = p^k$.

As we noted, Lemma 1.3 fails to be valid when p is odd. However, using the representation given in the equation (1.2), we can exploit the same ideas as in the proof of Theorem 3.2.

Theorem 3.4. ([*35*]) *Assume that* $d \equiv 1 \pmod{q - 1}$, *and denote* $s = (d - 1)/(q - 1)$. *Then* $C_d(\tau)$ *assumes exactly the values*

$$-1 + (N(y) - 1) \cdot q,$$

where $N(y)$ is the number of common solutions to

$$\begin{cases} z^{2s-1} + \overline{y}z^s + yz^{s-1} + 1 &= 0 \\ z &\in S. \end{cases}$$

Proof. Every nonzero $x \in GF(q^2)$ can be represented uniquely as $x = \alpha^i\beta^j$, where β is a primitive element of $GF(q^2)$, $\alpha = \beta^{q+1}$, $i = 0, 1, \ldots q-2$, and $j = 0, 1, \ldots, q$. Using this

$$\begin{aligned} C_d(\tau) &= \sum_{x\neq 0} \zeta^{tr_1^n(yx-x^d)} \\ &= \sum_j \sum_i \zeta^{tr_1^n(y\alpha^i\beta^j-\alpha^{di}\beta^{dj})} \\ &= \sum_j \sum_i \zeta^{tr_1^n(\alpha^i(y\beta^j-\beta^{dj}))} \\ &= \sum_j \sum_i \zeta^{tr_1^k(\alpha^i(y\beta^j-\beta^{dj}+y^q\beta^{qj}-\beta^{qdj}))} \\ &= -q-1+\sum_j \sum_{z\in GF(q)} \zeta^{tr_1^k(z(y\beta^j-\beta^{dj}+y^q\beta^{qj}-\beta^{qdj}))} \\ &= -1+(N(y)-1)\cdot q, \end{aligned}$$

where $N(y)$ is the number of solutions $x \in \{1, \beta, \ldots, \beta^q\}$ to

$$yx - x^d + y^q x^q - x^{qd} = 0. \tag{3.3}$$

Now divide by x, and denote $z = x^{q-1}$. It is clear that when x runs through $\{1, \beta, \ldots, \beta^q\}$, then z runs through S. Thus replacing y by $-y$ we get an equivalent pair

$$\begin{cases} y + z^{\frac{d-1}{q-1}} + \overline{y}z + z^{\frac{qd-1}{q-1}} &= 0 \\ z &\in S. \end{cases} \tag{3.4}$$

In detail, if $x \in \{1, \beta, \ldots, \beta^q\}$ is a solution to (3.3), then $x^{q-1} = z \in S$ is a solution to (3.4). On the other hand, if $z \in S$ is a solution to (3.4), then there is a unique solution $x \in \{1, \beta, \ldots, \beta^q\}$ to (3.3) such that $x^{q-1} = z$.

The first equation in (3.4) reduces easily to

$$z^{2s-1} + \overline{y}z^s + yz^{s-1} + 1 = 0. \tag{3.5}$$

□

A similar argument leads to the following theorem, which seems to be new.

Theorem 3.5. *Assume that k divides n and that $d \equiv 1 \pmod{p^k-1}$. Then $C_d(\tau)+1$ is divisible by p^k.*

Proof. Note that $x \in GF(p^n)^\times$ has a unique representation as $x = \alpha^i\beta^j$, where β is a primitive element of $GF(p^n)$, $\alpha = \beta^{(p^n-1)/(p^k-1)}$, and $i = 0,1,\ldots,p^k-2$, and $j = 0,1,\ldots,(p^n-1)/(p^k-1)-1$. As $p^{tk} \equiv 1 \pmod{p^k-1}$ for all $t = 0,1,\ldots$, we may proceed as in the proof of Theorem 3.4. □

Remark 3.6. (*i*) Let $p = 2$. The original Niho's theorem can be easily deduced from Theorem 3.4 as follows. Firstly, squaring the equation (3.5) gives an equivalent equation (y^2 may be replaced by y)

$$z^{4s-2} + \overline{y}z^{2s} + yz^{2s-2} + 1 = 0.$$

Secondly, from $s = (d-1)/(q-1)$ we get

$$d = s \cdot (q+1) - 2s + 1, \tag{3.6}$$

and hence

$$2s = s(q+1) + 1 - d,$$

$$2s - 2 = s(q+1) - 1 - d,$$

and

$$4s - 2 = 2s(q+1) - 2d.$$

Since the exponents can be reduced modulo $q+1$, using (3.6) we get the equation (3.1).

(*ii*) The equation (3.3) can sometimes, but not always, be deduced also by combining Theorem 3.8. of [18] and a theorem due to Baumert and McEliece (see [1] and [18]). However, this method leads to lengthy and more detailed calculations, compare the proofs of Theorem 4.13 of [18] and Theorem 5.11.

(*iii*) The condition $z \in S$ is far more convenient than $z \in \{1,\beta,\ldots,\beta^q\}$. Firstly, it usually reduces the degree of the corresponding equation. Secondly, the set S can be parameterized with the elements of $GF(q)$, i.e., the equation can be transformed to an equation over the subfield $GF(q)$, see Lemma 1.2 and Theorem 5.2.

As a quick application of Theorem 3.4 we give a slick proof of the following result.

Theorem 3.7. ([24]) *Let $p = 3$ and $n = 2k$, where $n \not\equiv 2 \pmod 4$. Then for $d = 3 \cdot p^k - 2$, $C_d(\tau)$ is at most five-valued.*

Proof. Since now $d = 3 \cdot \left(p^k - 1\right) + 1$, we may use Theorem 3.4 with $s = 3$. The corresponding equation is then

$$x^5 + \overline{y}x^3 + yx^2 + 1 = 0, \tag{3.7}$$

which is of degree five. Therefore $C_d(\tau)$ is at most six-valued. It suffices to show that (3.7) has never exactly four solutions in S.

It is obvious that if four roots of this equations are in S, then the fifth root is too. Hence (3.7) can have exactly four distinct roots in S if and only if it has a double root and other roots are simple (and of course all roots in S). The usual derivative argument shows that multiple roots in S are possible if and only if $y \in S$. But then (3.7) splits as

$$\left(x^3 + y\right)\left(x^2 + \overline{y}\right) = 0,$$

which has either exactly one or exactly three solutions. □

Computed results in [15] show that this is indeed a five-valued family. Some partial results on the distribution of the values are given in the unpublished manuscript [24].

We will give another application of Theorem 3.4 in the last chapter.

3.3 Charpin's result

Recall that when d is of Niho type, the values of $C_d(\tau)$ are in one-to-one correspondence with the values

$$-1 + (N(y) - 1) \cdot p^k,$$

where $N(y)$ is the number of solutions $x \in S$ to

$$x^{2s-1} + \overline{y}x^s + yx^{s-1} + 1 = 0. \tag{3.8}$$

Let N_i denote the number of times the value $-1 + (i-1) \cdot p^k$ occurs. We have the following equations:

$$\sum_{i=0}^{2s-1} N_i = p^{2k} - 1 \tag{3.9}$$

$$\sum_{i=0}^{2s-1} (i-1) N_i = p^k \tag{3.10}$$

$$\sum_{i=0}^{2s-1} (i-1)^2 N_i = p^{2k}. \tag{3.11}$$

The first equation here is trivial, since there are $p^{2k}-1$ distinct $y \in GF(q^2)^\times$. The second follows easily from the first power sum equation given in Theorem 2.4 and the identity

$$\sum_{\tau=0}^{p^n-2} (C_d(\tau) + 1) = \sum_{i=0}^{2s-1} N_i \left((i-1) \cdot p^k \right)$$

by dividing by p^k. The third equation can be derived similarly from the second power sum equation.

For convenience, we denote

$$r_0 = \gcd(s, q+1)$$

and

$$r_1 = \gcd(s-1, q+1).$$

Furthermore, we denote

$$U_i = S^{r_i} = \{x^{r_i} : x \in S\}$$

for $i = 0, 1$. Note that U_i are subgroups of S.

Let $N(y)$ be the number of solutions to (3.8) corresponding to $y \in GF(q^2)$.

We will need the following lemma.

Lemma 3.8. *If $r_1 > 1$ (resp. $r_0 > 1$) then $U_0 \setminus U_1 \neq \emptyset$ (resp. $U_1 \setminus U_0 \neq \emptyset$).*

Proof. By symmetry, it suffices to prove the first statement. Assume on the contrary that $U_0 \setminus U_1 = \emptyset$, i.e., $U_0 \subseteq U_1$. Then U_0 is a subgroup of U_1, and therefore $(q+1)/r_0$ (the order of U_0) divides $(q+1)/r_1$ (the order of U_1). From this we deduce that r_1 divides r_0. Since clearly $\gcd(r_0, r_1) = 1$, we must have $r_1 = 1$. □

The following result was proved for binary sequences in [7]. The following proof was given in [23], and it applies to non-binary sequences as well. We will implicitly exclude the case of autocorrelation, i.e., we assume that the corresponding sequences are different.[1]

Theorem 3.9. *Assume that d is of Niho type. Then the cross-correlation function $C_d(\tau)$ is at least four-valued.*

Proof. We have to show that $N_i > 0$ for at least four different indices i.

Subtracting (3.9) from (3.11) gives

$$N_1 + 1 = \sum_{i=3}^{2s-1} i(i-2)N_i, \tag{3.12}$$

which is impossible when $N_1 = 0$ or $N_i = 0$ for all $i \geq 3$.

Squaring (3.10) and comparing with (3.11) gives

$$\left(\sum_{i=0}^{2s-1} (i-1)N_i \right)^2 = \sum_{i=0}^{2s-1} (i-1)^2 N_i, \tag{3.13}$$

which implies

$$2 \sum_{i<j} (i-1)(j-1)N_i N_j = \sum_{i=0}^{2s-1} (i-1)^2 \left(N_i - N_i^2 \right). \tag{3.14}$$

Suppose that $N_0 = 0$. If there is only one value $i \geq 2$ such that $N_i > 0$, then (3.10) and (3.11) give $(i-1)N_i = p^k$ and $(i-1)^2 N_i = p^n$. This implies that $i = p^k + 1$ and $N_{p^k+1} = 1$. In this case the correlation value is $-1 + (p^k + 1 - 1)p^k = p^n - 1$, i.e., we have the case of the autocorrelation.

Since the cross-correlation function always takes on at least three values (or from the preceding argument) it follows that $N_i \neq 0$ for two distinct

[1] The decimation $d = 1$ is of Niho type, but produces a two-valued cross-correlation, see page 17.

values $i \geq 2$ and $j \geq 2$. This implies that the left hand side is positive, contradicting the fact that the right hand side is at most 0.

We have now shown that $N_0 > 0$, $N_1 > 0$ and $N_i > 0$ for some $i \geq 3$. Hence, in order to show that cross-correlation function is at least four-valued, we need to show that either $N_2 > 0$ or that N_i and N_j are nonzero for some $i > j > 2$.

In the case $y \in S$ the equation (3.8) splits as

$$\left(x^{s-1} + y\right)(x^s + \overline{y}) = 0, \tag{3.15}$$

and then clearly[2]

(i) $N(y) = r_0$ for $y \in U_0 \setminus U_1$

(ii) $N(y) = r_1$ for $y \in U_1 \setminus U_0$

(iii) $N(y) = r_0 + r_1$ for $y \in U_0 \cap U_1$, $y \neq 1$

(iv) $N(1) = r_0 + r_1 - 1$.

In the case $r_0 = r_1 = 1$ it follows from (iii) that $N(y) = 2$ for any $y \in S \setminus \{1\}$ and therefore $N_2 > 0$ and we have at least four-valued cross-correlation.

In the case when $r_0 > 1$ or $r_1 > 1$, we obtain from (iv) that $N_{r_0+r_1-1} > 0$. Further, (iii) implies that $N_{r_0+r_1} > 0$ except possibly when $U_0 \cap U_1 = \{1\}$. In the exceptional case we have $r_0 > 1$ and $r_1 > 1$, and then Lemma 3.8 implies that at least one of $U_0 \setminus U_1$ or $U_1 \setminus U_0$ is nonempty. From (i) or (ii) we obtain that either $N_{r_0} > 1$ or $N_{r_1} > 1$. Since these indices are ≥ 2 and different from $r_0 + r_1 - 1$, we conclude that the cross-correlation is at least four-valued. □

Note that in the course of the proof we got the fact that -1 is one of the values of $C_d(\tau)$. An old and unproven conjecture of Helleseth states that no matter what d is, -1 is always one of the values of $C_d(\tau)$, see [18]. For Niho type d this is proved in a different way in [13][3].

Corollary 3.10. *If d is of Niho type then both -1 and $-1 - p^k$ occur as values of $C_d(\tau)$.*

[2]It is well known that if the equation $x^m = a$ has a solution in a cyclic group of order $q+1$, then it has exactly $\gcd(q+1, m)$ solutions in this group.

[3]Again this is proved for binary sequences only. However, by Theorem 3.4 the same proof applies to non-binary sequences as well.

The binary case of Corollary 3.10 is also proved in [7].

As a simple consequence of the methods used in the previous proof we get the following result.

Theorem 3.11. *Assume that d is of Niho type and that $C_d(\tau)$ is four-valued. Then $r_0 = 1$ or $r_1 = 1$.*

Proof. Assume on the contrary that both $r_0 > 1$ and $r_1 > 1$. Then $U_0 \setminus U_1 \neq \emptyset$ and $U_1 \setminus U_0 \neq \emptyset$ (this is a simple exercise in group theory; note that $\gcd(r_0, r_1) = 1$), and therefore we know that $N_{r_0} > 0$, $N_{r_1} > 0$, and $N_{r_0+r_1-1} > 0$. Together with $N_0 > 0$ and $N_1 > 0$ we have at least five values. □

Chapter 4

On the third power sum

4.1 Motivation and the idea

Unless otherwise stated, in this chapter p will be an arbitrary prime. As before, we denote $q = p^k$ and d satisfies the Niho condition

$$d \equiv 1 \pmod{q-1}.$$

In what follows, the parameter s is defined by the equation

$$d = (q-1)s + 1.$$

We will now begin our study on the number of solutions $x \in GF(q^2)$ to

$$(x+1)^d = x^d + 1. \tag{4.1}$$

Solving (4.1) gives the value of the third power sum $\sum_{\tau=0}^{p^n-2}(C_d(\tau)+1)^3$, see Theorem 2.4, and is therefore helpful in finding the distribution of the values of $C_d(\tau)$.

The equation (4.1) is interesting in itself. Besides in the theory of m-sequences, it occurs in many other contexts in combinatorics. For instance, it is related to the number of codewords of weight three in certain cyclic codes (see [33]). As another example, (4.1) is related to nonlinearity properties of power functions, (see e.g. [12]); this is of interest in cryptography. The two connections above are also studied in [4] and [5]. Thirdly, in [9] the polynomial $(x+1)^d + x^d + 1$ was used in constructing of difference sets.

Our approach to the equation (4.1) stems from the polar representation described in Lemma 1.3. In the binary case, the representation (1.1) (and

its uniqueness) suggests that comparison of the "α-part" and the "β-part" of both sides of the equation (4.1) may give some information.

In the nonbinary case, the equation (1.1) is still valid. However, it yields two representations for the squares in $GF(q^2)$, and no representation for the non-squares. In spite of this, the representation is still strong enough in many cases. It appears that only minor modifications are needed in order to treat both binary and non-binary cases simultaneously.

Unless otherwise indicated, the results in this chapter are from [23].

4.2 The results

Firstly, we note that every $x \in GF(q)$ is a solution to (4.1). This is a simple consequence of the fact $d \equiv 1 \pmod{q-1}$. Among other things, we will see that under certain conditions there are no other solutions.

We also note that if $d \equiv p^i \pmod{p^j - 1}$ for some i and j, then every $x \in GF(p^j)$ satisfies the equation (4.1).

The following lemma will be crucial.

Lemma 4.1. *Assume that $d = (q-1)s + 1$ and that $x \in GF(q^2)^\times$ is a solution to*

$$(x+1)^d = x^d + 1. \tag{4.2}$$

Then $z = x^{q-1}$ satisfies $z^s = 1$ or $z^{s-1} = 1$.

Proof. Since

$$(x+1)^d = x^d + 1, \tag{4.3}$$

we also have

$$(\overline{x}+1)^d = \overline{x}^d + 1. \tag{4.4}$$

Multiplying these equations gives

$$(x\overline{x} + x + \overline{x} + 1)^d = (x\overline{x})^d + x^d + \overline{x}^d + 1. \tag{4.5}$$

Clearly $x\overline{x}, x+\overline{x} \in GF(q)$ and therefore also $x\overline{x}+x+\overline{x}+1 \in GF(q)$. Since for $a \in GF(q)$ we have $a^d = a$, (4.5) implies

$$x + \overline{x} = x^d + \overline{x}^d.$$

Divided by x this becomes

$$1 + x^{q-1} = x^{d-1} + x^{qd-1}.$$

Let $z = x^{q-1}$. Since $z^{q+1} = 1$, we get

$$1 + z = z^s + z^{1-s},$$

which is equivalent to

$$(z^s - 1)(z^{s-1} - 1) = 0, \tag{4.6}$$

from which the claim follows. □

The key idea here is that z is an element of S, which in turn is a cyclic group; the order of this group is $q + 1$. Therefore (4.6) implies in fact that $z^{\gcd(s,q+1)} = 1$ or $z^{\gcd(s-1,q+1)} = 1$. Very often the greatest common divisors in question are quite small, and the equation (4.1) becomes tractable.

From now on, if x is known from the context, we will denote $z = x^{q-1}$. Note that $z = 1$ if and only if $x \in GF(q)^\times$.

We now give some identities, which will be useful in what follows. Firstly, we have trivially

$$\overline{x} = xz. \tag{4.7}$$

Secondly, we have $x^d = x^{(q-1)s+1} = xz^s$. Therefore, if $z^s = 1$, we have

$$x^d = x. \tag{4.8}$$

On the other hand, if $z^{s-1} = 1$, by (4.7) we have

$$x^d = \overline{x}. \tag{4.9}$$

Since the elements of $GF(q)$ are trivially solutions to (4.1), we may assume $x \neq -1$. Therefore the equations (4.3) and (4.4) imply

$$\left(\frac{x+1}{\overline{x}+1}\right)^d = \frac{x^d+1}{\overline{x}^d+1}.$$

Hence, if $z^s = 1$ we get using (4.8) that

$$\left(\frac{x+1}{\overline{x}+1}\right)^d = \frac{x+1}{\overline{x}+1},$$

i.e.,

$$\left(\frac{x+1}{\overline{x}+1}\right)^{d-1} = 1. \tag{4.10}$$

If $z^{s-1} = 1$ we get using (4.9) that

$$\left(\frac{x+1}{\overline{x}+1}\right)^d = \frac{\overline{x}+1}{x+1},$$

i.e.,

$$\left(\frac{x+1}{\overline{x}+1}\right)^{d+1} = 1. \tag{4.11}$$

Note also that

$$\begin{aligned} \gcd(d+1, q+1) &= \gcd(s(q-1)+2, q+1) \\ &= \gcd(s(q+1)-2s+2, q+1) \\ &= \gcd(2(s-1), q+1), \end{aligned} \tag{4.12}$$

and similarly,

$$\gcd(d-1, q+1) = \gcd(2s, q+1). \tag{4.13}$$

Lemma 4.2. *Assume that q is fixed.*

(*i*) *Let $x \in GF(q^2) \setminus \{0, -1\}$, and denote $z = x^{q-1}$ and $w = (x+1)^{q-1}$. Then x is a solution to* (4.1) *if and only if $z^s = w^s = 1$ or $z^{s-1} = w^{s-1} = 1$.*

(*ii*) *The set of solutions to* (4.1) *depends only on the pair $\{gcd(s, q+1), \gcd(s-1, q+1)\}$, not on the specific choice of s. More precisely, let $e = (q-1)t + 1$ and assume that either*

$$\begin{cases} \gcd(s, q+1) &= \gcd(t, q+1) \\ \gcd(s-1, q+1) &= \gcd(t-1, q+1) \end{cases}$$

or

$$\begin{cases} \gcd(s, q+1) &= \gcd(t-1, q+1) \\ \gcd(s-1, q+1) &= \gcd(t, q+1). \end{cases}$$

Then $x \in GF(q^2)$ is a solution to (4.1) *if and only if x satisfies $(x+1)^e = x^e + 1$.*

Proof. (*i*) If $x \neq 0$ is a solution to (4.1), then by the previous lemma $z^s = 1$ or $z^{s-1} = 1$. If $z^s = 1$, using (4.8) we get from $(x+1)^d = x^d + 1$ that $w^s = 1$. If $z^{s-1} = 1$, then (4.9) implies $w^{s-1} = 1$. If $z^s = w^s = 1$ or $z^{s-1} = w^{s-1} = 1$, then obviously x satisfies (4.1).

(*ii*) This follows easily from (*i*) and the fact that both z and w are elements of S. As an illustration, assume that $\gcd(s, q+1) = \gcd(t, q+1)$ and $\gcd(s-1, q+1) = \gcd(t-1, q+1)$. If $x \neq 0, -1$ satisfies (4.1) then $z^s = w^s = 1$ or $z^{s-1} = w^{s-1} = 1$. We then have $z^t = w^t = 1$ or $z^{t-1} = w^{t-1} = 1$, because of the assumption on the greatest common divisors. From (*i*) we deduce $(x+1)^e = x^e + 1$. The remaining cases are left to the reader.

□

We will now give necessary and sufficient conditions when $GF(q)$ is the exact set of solutions to (4.1). The binary case differs slightly from the non-binary counterpart. The reason for this will become evident.

Theorem 4.3. *Let $q = p^k$ be odd. Assume that $d = (q-1)s + 1$ and that either*

$$\begin{cases} \gcd(s, q+1) &= 1 \\ \gcd(s-1, q+1) &= 2 \end{cases}$$

or

$$\begin{cases} \gcd(s, q+1) &= 2 \\ \gcd(s-1, q+1) &= 1. \end{cases}$$

Then the equation (4.1) *has exactly q solutions in the field $GF(q^2)$, i.e., there are no solutions outside of $GF(q)$.*

Proof. We firstly note that the left hand sides of the equations (4.10) and (4.11) are elements of S. Moreover, from (4.12) (resp. (4.13)) we get that $\gcd(d+1, q+1)$ is 1, 2 or 4 (resp. $\gcd(d-1, q+1)$ is 1, 2 or 4).

In any case, if $x \in GF(q^2) \setminus \{0, -1\}$ is a solution to (4.1), from (4.10) or (4.11) together with (4.12) or (4.13) we have

$$\left(\frac{x+1}{\overline{x}+1}\right)^4 = 1,$$

which we can write as

$$x^4 + 4x^3 + 6x^2 + 4x + 1 = \overline{x}^4 + 4\overline{x}^3 + 6\overline{x}^2 + 4\overline{x} + 1.$$

Again we write $\overline{x} = xz$. By assumption z satisfies $z^2 = 1$. Using this, we get easily

$$x^3 + x = x^3 z + xz,$$

and this implies that $z = 1$, $x = 0$ or $x^2 = -1$. If $z = 1$ or $x = 0$ then $x \in GF(q)$. Furthermore, the solutions of $x^2 = -1$ are in $GF(q)$ if $q \equiv 1 \pmod 4$. We now look closer to the case $q \equiv -1 \pmod 4$. Then k is necessarily odd.

Claim. If $q \equiv -1 \pmod 4$ and $x^2 = -1$, then x is not a solution to (4.1).

Proof of the claim. Note that if $x^2 = -1$, then $x \in GF(p^2)$. Assume on the contrary that $x \notin GF(q)$, i.e., that $x \in GF(p^2) \setminus GF(p)$ satisfies both $x^2 = -1$ and (4.1). Firstly, we note that

$$d = (p^k - 1)s + 1 \equiv (p-1)s + 1 \pmod{p^2 - 1},$$

so

$$(x+1)^{(p-1)s+1} = x^{(p-1)s+1} + 1. \tag{4.14}$$

Case 1. Assume first $x^d = x$. Then we get from (4.14) that $(x + 1)^{(p-1)s} = 1$. Denote $\omega = (x+1)^{p-1}$. Then $\mathrm{ord}(\omega) > 2$, which is seen in the following way:

$$\omega^2 = (x+1)^{2(p-1)} = (x^2 + 2x + 1)^{p-1} = (2x)^{p-1} = x^{p-1} \neq 1,$$

since $x \notin GF(p)$. On the other hand $\mathrm{ord}(\omega)$ divides both $p+1$ and s, since $\omega^{p+1} = (x+1)^{p^2-1} = 1$ and $\omega^s = 1$. Therefore $\mathrm{ord}(\omega) > 2$ is a factor of both $p^k + 1$ (k is odd) and s which is in contradiction with $\gcd(s, q+1) = 1$ or $\gcd(s, q+1) = 2$.

Case 2. Secondly, assume $x^d = \overline{x}$. Since k is odd, we have $\overline{x} = x^p$. Hence (4.14) gives

$$(x+1)^{(p-1)s+1} = x^p + 1 = (x+1)^p,$$

i.e., $(x+1)^{(p-1)(s-1)} = 1$. We may now proceed similarly as in Case 1. □

Because of Lemma 4.2, Case 2 would have followed from Case 1.

The following theorem was given in [22]. We present here the slick proof from [23].

Theorem 4.4. *Assume that* $d \equiv 1 \pmod{2^k - 1}$. *If* $\gcd(d-1, 2^k+1) = \gcd(d+1, 2^k+1) = 1$, *then the equation*

$$(x+1)^d = x^d + 1 \tag{4.15}$$

has exactly 2^k *solutions in* $GF(2^n)$.

Proof. Every $x \in GF(2^k)$ is a solution to (4.15) since $d \equiv 1 \pmod{2^k - 1}$. We now assume that $x \neq 0, 1$ satisfies (4.15).

We know that (at least) one of the equations (4.10) and (4.11) is satisfied. Since $\gcd(d-1, 2^k+1) = \gcd(d+1, 2^k+1) = 1$, we must have

$$\frac{x+1}{\overline{x}+1} = 1,$$

which implies $x = \overline{x}$, i.e., $x \in GF(q)$. □

The converse case to Theorems 4.3 and 4.4 is given by the following. Note that the proof is constructive.

Theorem 4.5. *Assume that* $\gcd(s, q+1) > 2$ *or* $\gcd(s-1, q+1) > 2$. *Then the equation* (4.1) *has a solution outside of* $GF(q)$.

Proof. We will treat the case $\gcd(s, q+1) > 2$. The case $\gcd(s-1, q+1) > 2$ then follows from Lemma 4.2.

The condition $\gcd(s, q+1) > 2$ implies that there are $z_0, z_1 \in S$ such that $z_0, z_1 \neq 1$, $z_0 \neq z_1$, and $z_0^s = z_1^s = 1$. We define

$$x_0 = \frac{z_1 - 1}{z_0 - z_1},$$

and

$$x_1 = x_0 + 1 = \frac{z_0 - 1}{z_0 - z_1}.$$

We then have

$$\begin{aligned}
x_0^{q-1} &= \frac{(z_1-1)^q(z_0-z_1)}{(z_0-z_1)^q(z_1-1)} \\
&= \frac{z_1^q z_0 - z_1^{q+1} - z_0 + z_1}{z_0^q z_1 - z_0^q - z_1^{q+1} + z_1^q} \\
&= \frac{z_1^q z_0 - 1 - z_0 + z_1}{z_0^q z_1 - z_0^q - 1 + z_1^q} \\
&= \frac{z_0 z_1}{z_0 z_1} \cdot \frac{z_1^q z_0 - 1 - z_0 + z_1}{z_0^q z_1 - z_0^q - 1 + z_1^q} \\
&= \frac{z_0^2 - z_0 z_1 - z_0^2 z_1 + z_0 z_1^2}{z_1^2 - z_1 - z_0 z_1 + z_0} \\
&= \frac{z_0(z_1^2 - z_1 - z_0 z_1 + z_0)}{z_1^2 - z_1 - z_0 z_1 + z_0} \\
&= z_0.
\end{aligned}$$

Similarly,

$$\begin{aligned} x_1^{q-1} &= \frac{(z_0-1)^q(z_0-z_1)}{(z_0-z_1)^q(z_0-1)} \\ &= \frac{z_0^{q+1}-z_1z_0^q-z_0+z_1}{z_0^{q+1}-z_0^q-z_1^qz_0+z_1^q} \\ &= \frac{1-z_1z_0^q-z_0+z_1}{1-z_0^q-z_1^qz_0+z_1^q} \\ &= \frac{z_0z_1}{z_0z_1}\cdot\frac{1-z_1z_0^q-z_0+z_1}{1-z_0^q-z_1^qz_0+z_1^q} \\ &= \frac{z_0z_1-z_1^2-z_0^2z_1+z_1^2z_0}{z_0z_1-z_1-z_0^2+z_0} \\ &= z_1. \end{aligned}$$

We claim that x_0 is a solution to (4.1). Note that the conditions $z_0 \neq 1$ and $x_0^{q-1} = z_0$ imply that $x_0 \notin GF(q)$. Since $z_0^s = z_1^s = 1$ we deduce (as earlier) that

$$x_0^d = x_0$$

and

$$x_1^d = x_1.$$

Therefore

$$(x_0+1)^d = x_1^d = x_1 = x_0+1 = x_0^d+1,$$

and the proof is complete. □

Sometimes it is possible to decide whether a specific element $x \in GF(q^2)$ is a solution. As an example, we give the following theorem.

Theorem 4.6. *Let $p = 3$ and $x \in GF(9) \setminus GF(3)$. Then x is a solution to (4.1) if and only if $d \equiv 1$ or $d \equiv 3 \pmod 8$.*

Proof. Firstly, d is odd since $d \equiv 1 \pmod{q-1}$, and therefore $d \equiv 1, 3, 5$ or $7 \pmod 8$. Clearly, if $d \equiv 1$ or $d \equiv 3 \pmod 8$, then x satisfies (4.1). The lemma now follows from the factorizations

$$(x+1)^5 - x^5 - 1 = 2x(x+1)(x-1)^2$$

and

$$(x+1)^7 - x^7 - 1 = x(x+1)(x-1)^4.$$

□

When we consider cross-correlation functions of m-sequences we always assume that $\gcd(d, p^n - 1) = 1$. If $p = 2$ then 3 divides $p^n - 1$ (n is even), and therefore 3 cannot divide d. So 3 divides either $d - 1$ or $d + 1$. Now if k is odd, then 3 divides $2^k + 1$ and we see that Theorem 4.4 does not apply. In fact every $x \in GF(4)$ is a solution to (4.1) since either $d \equiv 1$ or $d \equiv 2 \pmod 3$. The following theorem gives a solution to the cases similar to this.

Theorem 4.7. *Assume that for some $i \geq 1$ either*

$$\begin{cases} \gcd(s, q+1) &= 1 \\ \gcd(s-1, q+1) &= p^i + 1 \end{cases}$$

or

$$\begin{cases} \gcd(s, q+1) &= p^i + 1 \\ \gcd(s-1, q+1) &= 1. \end{cases}$$

Then the set of solutions to (4.1) is $GF(p^k) \cup GF(p^{2i})$, and hence the number of solutions is $p^k + p^{2i} - p^i$.

Proof. We remind the reader that $p^i + 1$ divides $p^k + 1$ if and only if i divides k and k/i is odd. If $p^i + 1$ divides $p^k + 1$, then

$$p^k + 1 = \left(p^i + 1\right)\left(p^{(u-1)i} - p^{(u-2)i} + \cdots - p^i + 1\right),$$

where $u = k/i$.

Assume now that x is a solution outside of $GF(q)$. We will first show that necessarily $x \in GF(p^{2i})$. We note firstly that when $p^i + 1$ divides $p^k + 1$ we never have $q \equiv -1 \pmod{2p^i + 2}$ since k/i is odd. This means (see the equations (4.12) and (4.13)) that $\gcd(d + 1, q + 1) = \gcd(s - 1, q + 1)$ and $\gcd(d - 1, q + 1) = \gcd(s, q + 1)$. Thus we have either from (4.10) or (4.11) that

$$\left(\frac{x+1}{xz+1}\right)^{p^i+1} = 1,$$

where z satisfies $z^{p^i+1} = 1$. From this we deduce

$$x^{p^i+1} + x^{p^i} + x + 1 = x^{p^i+1} z^{p^i+1} + x^{p^i} z^{p^i} + xz + 1,$$

which implies that

$$-(z^{p^i} - 1)x^{p^i} = (z - 1)x$$

or

$$-(z^{p^i-1} + z^{p^i-2} + \cdots + 1)x^{p^i} = x,$$

since now $z \neq 1$.

Since $z \neq 1$ satisfies $z^{p^i+1} = 1$ we have $z^{p^i} = -(z^{p^i-1} + z^{p^i-2} + \cdots + 1)$ and hence

$$z^{p^i} x^{p^i} = x.$$

This is the same as $x^{p^{k+i}} = x$, which in turn is equivalent to $x \in GF(p^{k+i})$.

As noted, k/i must be odd. Thus $\gcd(k+i, 2k) = 2i$ and then $x \in GF(p^{2i})$, which is what we wanted to show. The reader should note here that $GF(p^{2i}) \subseteq GF(p^{2k})$.

Lastly, we have to prove that every $x \in GF(p^{2i})$ satisfies the equation (4.1). Assume firstly that $p^i + 1$ divides s. Since $p^i + 1$ divides $q + 1$ we know that i divides k and therefore $p^i - 1$ divides $q - 1$. Hence $d \equiv 1 \pmod{p^{2i} - 1}$. On the other hand, if $p^i + 1$ divides $s - 1$ we may deduce similarly that $d \equiv p^k \pmod{p^{2i} - 1}$.

The statement on the number of solutions follows easily from the fact $GF(p^k) \cap GF(p^{2i}) = GF(p^i)$. □

Remark 4.8. Let $p = 2$. Theorem 4.4 and Theorem 4.7 cover the cases where the pair of greatest common divisors in question are e.g. $\{1, 1\}$, $\{1, 3\}$, $\{1, 5\}$ or $\{1, 9\}$. Note that for example the pairs $\{1, 7\}$, $\{3, 5\}$, $\{3, 7\}$, and $\{5, 7\}$ are not possible. So the "smallest" unknown case corresponds to the pair $\{1, 11\}$.

Chapter 5

Cross-correlation functions of Niho type

In this chapter we describe all known Niho type cross-correlation functions. Especially, in Section 5.2 we give a large class of decimations which lead to four-valued cross-correlation functions. Another purpose of this chapter is to give a simple and unified treatment for the other cases. A central role is played by the results developed in the preceding two chapters.

5.1 The known cases

The previously known cross-correlation functions of Niho type are

(i) $d = 2^{n/2+1} - 1$, with $n \equiv 0 \pmod 4$,

(ii) $d = (2^{n/2} + 1)(2^{n/4} - 1) + 2$, with $n \equiv 0 \pmod 4$,

(iii) $d = \sum_{i=0}^{n/2} 2^{im}$, with $n \equiv 0 \pmod 4$, $0 < m < n$, $\gcd(n, m) = 1$,

(iv) $d = 2^{n/2} + 3$, with n even and $n/2 > 2$, and

(v) $d = 2 \cdot p^{n/2} - 1$, with n even and $p^{n/2} \not\equiv 2 \pmod 3$.

The first four concern binary sequences only, and the fifth is a p-ary version of the decimations in (i). For the references, see Section 2.2.

In the next section we give a family which properly includes the decimations both in (i) and (ii). In addition we will give simplified treatments

for the other cases, and finally describe a family of decimations, which is connected to Kloosterman sums.

5.2 New four-valued cross-correlations

5.2.1 The fundamental equation

We will see that all *known* four-valued cross-correlation functions (are of Niho type and) lead to a similar equation. These equations are all of the form (5.1), and we are interested in the number of solutions in S. However, according to computed results in [15], there are four-valued cross-correlation functions which are not related to Niho's theorem.

Curiously enough, the equation (5.1) together with the condition $x \in S$ behaves like an affine equation over the subfield. Our treatment is based on this behavior, parameterizations given in Lemma 1.2, properties of linearized polynomials, and the following lemma.

Lemma 5.1. *Let α be a nonzero element in some extension of the field $GF(p)$. If the equation*

$$x^{p^s-1} = \alpha$$

has a solution in $GF(p^k)$, then it has exactly $p^{\gcd(k,s)} - 1$ solutions in the field $GF(p^k)$.

Proof. If x_0 is a solution, then all the solutions are ux_0, where $u \in GF(p^s)^\times$. Of these exactly $p^{\gcd(k,s)} - 1$ belong to the field $GF(p^k)$. □

The binary case of the following theorem was originally proven in [25]. The generalization to all p is from [22].

Theorem 5.2. ([*25, 22*]) *Let $n = 2k$ and $y \in GF(q^2) \setminus \{0\}$. The equation*

$$x^{p^s+1} + yx^{p^s} - \overline{y}x - 1 = 0 \tag{5.1}$$

has either 0, 1, 2 or $p^{\gcd(s,k)} + 1$ solutions $x \in S$.

Proof. The proof is divided into two cases.

Case 1. Assume first that $y \in GF(q)$, i.e., $y = \overline{y}$. In this case $x = 1 \in S$ is a solution to (5.1); in fact $x = 1$ is a solution if and only if $y \in GF(q)$. We apply the parameterization (i) of Lemma 1.2 to the equation (5.1), and then

multiply it by $(\overline{z}+u)^{p^s+1}$. Note that the coefficient of u^{p^s+1} disappears, and we get

$$\begin{aligned}(z-\overline{z}+y\overline{z}-yz)u^{p^s} &+ (z^{p^s}-\overline{z}^{p^s}+yz^{p^s}-y\overline{z}^{p^s})u \\ &= -(z^{p^s+1}-\overline{z}^{p^s+1}+yz^{p^s}\overline{z}-yz\overline{z}^{p^s}).\end{aligned}$$

Every solution $x \in S \setminus \{1\}$ to (5.1) corresponds to a solution $u \in GF(2^k)$ of the previous equation.

If $z-\overline{z}+y\overline{z}-yz=0$, there is nothing to prove. Otherwise we have an affine equation of the form

$$u^{p^s}+\alpha_1 u=\alpha_2, \tag{5.2}$$

where $\alpha_1, \alpha_2 \in GF(q)$. Lemma 5.1 implies that the corresponding linear equation

$$u^{p^s}+\alpha_1 u=0 \tag{5.3}$$

has either exactly one root or exactly $p^{\gcd(k,s)}$ roots in $GF(q)$. From Lemma 1.1 we know that the affine equation (5.2) either has no solutions or it has the same number of solutions as (5.3). Hence, in the case $y \in GF(q)$, the equation (5.1) has either 1, 2 or $p^{\gcd(k,s)}+1$ solutions in S.

Case 2. For the rest of the proof, we assume that $y \notin GF(q)$. If (5.1) has no solution in S, we are through. Suppose now that there is such a solution. We apply the parameterization (ii) of Lemma 1.2 to the equation (5.1). Since $y \notin GF(q)$, the fixed element β can be chosen to be one of the solutions. Multiplied by $(\alpha+\beta)^{p^s+1}$ the equation (5.1) transforms to

$$\begin{aligned}(\beta^{p^s+1}+y\beta^{p^s}-\overline{y}\beta-1)\alpha^{p^s+1} &+ (\beta^{p^s}+y\beta^{p^s+1}-\overline{y}-\beta)\alpha^{p^s} \\ &+ (\beta+y-\overline{y}\beta^{p^s+1}-\beta^{p^s})\alpha \\ &+ (1+y\beta-\overline{y}\beta^{p^s}-\beta^{p^s+1})=0.\end{aligned}$$

By assumption, the leading coefficient here is zero. Now every solution $x \in S \setminus \beta$ to (5.1) corresponds to a solution $\alpha \in GF(q)$ of the previous equation.

If the coefficient of α^{p^s} above is zero, the remaining equation is of degree one and we are through. Otherwise we again have an affine equation of the form

$$\alpha^{p^s}+a_1\alpha=a_2, \tag{5.4}$$

where $a_1, a_2 \in GF(q^2)$ (in fact $a_1, a_2 \in GF(q)$, but this is not needed[1]). To complete the proof, we may now proceed similarly as in the case $y \in GF(p^k)$. □

We will use this theorem only in the case $p = 2$. It is not clear whether it can be applied to non-binary cases or not.

The polynomials of the form $x^{q+1} + ax^q + bx + c$, where q is a power of the characteristic of the field, arise in several other contexts, too. The interested reader should see [2] and references given there.

5.2.2 The decimations

Lemma 5.3. *Let*

$$d = \frac{2^{k-1}}{2^s - 1}(2^{2k} + 2^{s+1} - 2^{k+1} - 1), \tag{5.5}$$

where s is such that $2s$ divides k. Then

(*i*) $\gcd(d, 2^n - 1) = 1$,

(*ii*) $d \equiv 1 \pmod{2^k - 1}$, *and*

(*iii*) $d \equiv \frac{2^k - 2^s}{2^s - 1} \pmod{2^k + 1}$.

Proof. We prove (*ii*) and leave (*iii*) to the reader. Then (*i*) can be proved using (*ii*) and (*iii*) and the well known fact that $\gcd(2^i + 1, 2^j - 1) = 1$ if and only if $j/\gcd(i, j)$ is odd; here it is needed that $2s$ divides k.

We have

$$\begin{aligned} d - 1 &= \frac{2^{3k-1} + 2^{k+s} - 2^{2k} - 2^{k-1} - 2^s + 1}{2^s - 1} \\ &= \frac{2^{k-1}\left(2^{2k} - 1\right) + 2^s\left(2^k - 1\right) - \left(2^{2k} - 1\right)}{2^s - 1} \\ &= \frac{\left(2^k - 1\right)\left(2^{k-1}\left(2^k + 1\right) + 2^s - \left(2^k + 1\right)\right)}{2^s - 1}, \end{aligned}$$

so it suffices to show that $d' = 2^{2k-1} + 2^{k-1} + 2^s - 2^k - 1$ is divisible by $2^s - 1$. But this follows from $d' = 2^{k-1}\left(2^k - 1\right) + (2^s - 1)$, since $2^s - 1$ divides $2^k - 1$. □

[1] An easy computation shows that $\overline{a_i} = a_i$ in (5.4)

Lemma 5.4. *We have* $\gcd(d \pm 1, 2^k + 1) = 1$ *for* d *in* (5.5).

Proof. Since $2^s - 1$ divides $2^k - 1$, we must have $\gcd(2^s - 1, 2^k + 1) = 1$. Hence $\gcd(d \pm 1, 2^k + 1) = \gcd((2^s - 1)(d \pm 1), 2^k + 1)$. The lemma now easily follows from the congruence $(2^s - 1)d \equiv 2^k - 2^s \pmod{2^k + 1}$. □

We now "normalize" d to the equivalent decimation

$$d = \frac{1}{2^s - 1}(2^{2k} + 2^{s+1} - 2^{k+1} - 1).$$

Theorem 5.5. ([25]) *Let* $n = 2k$, *where* $2s$ *divides* k, *and let* $d = (2^{2k} + 2^{s+1} - 2^{k+1} - 1)/(2^s - 1)$. *Then the cross-correlation function* $C_d(\tau)$ *between two* m*-sequences takes on the following values:*

$$\begin{array}{lll} -1 - 2^k & occurs & \frac{2^{2k+s-1} - 2^{k+s-1}}{2^s + 1} \quad times \\ -1 & occurs & \frac{2^{2k} - 2^k - 2^s}{2^s} \quad times \\ -1 + 2^k & occurs & \frac{2^{2k+s-1} - 2^{2k} + 2^{k+s-1}}{2^s - 1} \quad times \\ -1 + 2^{k+s} & occurs & \frac{2^{2k} - 2^k}{2^{3s} - 2^s} \quad times. \end{array}$$

Proof. Since now $(2^s - 1) \cdot d \equiv 2^k - 2^s \pmod{2^k + 1}$ (see Remark 3.3 (i)) Niho's theorem leads to the equation

$$x^{2^s+1} + yx^{2^s} + \overline{y}x + 1 = 0,$$

which is the binary special case of the equation in Theorem 5.2. Therefore $C_d(\tau)$ is four-valued and the values are as claimed. Furthermore, Theorem 4.4 and Lemma 5.4 give that the number b of Theorem 2.4 is 2^k. As usual, we denote by N_i the number of times (5.1) has exactly i solutions in S. We have a system of linear equations

$$\begin{array}{rcl} N_0 + N_1 + N_2 + N_{2^s+1} & = & 2^{2k} - 1 \\ -2^k N_0 + 2^k N_2 + 2^{k+s} N_{2^s+1} & = & 2^{2k} \\ 2^{2k} N_0 + 2^{2k} N_2 + 2^{2k+2s} N_{2^s+1} & = & 2^{4k} \\ -2^{3k} N_0 + 2^{3k} N_2 + 2^{3k+3s} N_{2^s+1} & = & 2^{5k}. \end{array}$$

The first equation comes from the number of equations of the form (5.1), and the other ones are simple consequences of Theorem 2.4. Straightforward calculations give the claimed distribution. □

Remark 5.6. It is a routine matter to verify that $s = 1$ (resp. $s = k/2$) gives a decimation equivalent to the decimation in (i) (resp. (ii)) given at the beginning of this chapter. We note here that Niho's proof of (ii) is somewhat complicated. In fact, it is incomplete: Niho treated only the case $y \in GF(2^k)$ of the corresponding equation and claims that Welch has proven the rest. However, Welch's calculations seem to be unpublished. There is an earlier simple proof of (ii) in [19].

Niho [34] gave tables of binary cross-correlation functions up to $n = 16$, and now all at most four-valued cross-correlation functions of binary m-sequences within this table belong to a known infinite family.

5.3 Other cross-correlation functions

In this section we give the other known cross-correlation functions of Niho type, and present some simplifications of the proofs of the corresponding results.

5.3.1 Dobbertin's family

We have seen that Theorem 5.5 generalizes both of Niho's families. For the first of Niho's families two other generalizations have been found. The following four-valued family, which includes the first of Niho's family, was found by Dobbertin [10].

Consider

$$d = \frac{2^{(k+1)s} - 1}{2^s - 1}. \tag{5.6}$$

It is a routine matter to verify $d \equiv 1 \pmod{2^k - 1}$. Once again Niho's theorem leads to the equation (5.1) (with $p = 2$, of course), and therefore we know the values of $C_d(\tau)$. Using Theorem 4.4 we find that the number b of Theorem 2.4 is 2^k in this case. Solving the corresponding system of equations gives the following distribution of the values.

Theorem 5.7. ([*10*]) *Let $n = 2k$, and assume s satisfies* $\gcd(s, n) = 1$. *Then for d in* (5.6) *the cross-correlation function $C_d(\tau)$ has the following*

values:

$$\begin{array}{lll} -1-2^k & occurs & \frac{2^{2k+s-1}-2^{k+s-1}}{2^s+1} \quad times \\ -1 & occurs & \frac{2^{2k}-2^k-2^s}{2^s} \quad times \\ -1+2^k & occurs & \frac{2^{2k+s-1}-2^{2k}+2^{k+s-1}}{2^s-1} \quad times \\ -1+2^{k+1} & occurs & \frac{2^{2k}-2^k}{2^{3s}-2^s} \quad times. \end{array}$$

The proof presented by Dobbertin is based on Niho's technique but is different otherwise. Dobbertin's treatment of the corresponding equation depends essentially on the restriction $\gcd(s, n) = 1$.

All *known* binary four-valued cross-correlations lead to the equation (5.1). We warn the reader that according to the computed results in [15], there are four-valued cross-correlations which are not of Niho type. However, it may turn out that these are exceptional cases of five-valued cross-correlations where one of the values has "collapsed".

In [13] it is conjectured that all binary four-valued *Niho type* cross-correlation functions arise from the equation (5.1).

5.3.2 Niho-Helleseth family

Niho [34] made several conjectures on cross-correlation functions. The first of these concerned the decimation (5.7), on which Niho gave some partial results himself. The remaining details were done by Helleseth [18]. We give a simplified treatment.

We let

$$d = 2^k + 3, \tag{5.7}$$

and prove that $C_d(\tau)$ is five-valued, and give the distribution of values.

First of all it is easy to show that $\gcd(2^n - 1, d) = 1$. Furthermore, d is equivalent to the decimation

$$d' = 2^{k-2} \cdot d = \left(2^{k-1} - 1\right)\left(2^{k-2} + 1\right) + 1, \tag{5.8}$$

and the corresponding equation is

$$x^4 + yx^3 + \overline{y}x + 1 = 0. \tag{5.9}$$

Thus $C_d(\tau)$ is (at most) five-valued. The following two lemmas are enough to give the distribution of the values. The number of $y \in GF(2^n)^\times$ such that (5.9) has exactly i solutions in S is denoted by N_i.

Lemma 5.8. *We have* $N_3 = 2^{k-1}$ *for* (5.9).

Proof. The equation (5.9) has exactly three distinct solutions in S if and only if it has a solution of multiplicity two and two other solutions. The root of the derivative satisfies $x^2 = \overline{y}/y$. We substitute this into (5.9) to get

$$\left(\frac{\overline{y}}{y}\right)^2 + yx\frac{\overline{y}}{y} + \overline{y}x + 1 = 0.$$

This implies $\overline{y} = y$, i.e., $y \in GF(2^k)$. In this case (5.9) factors as

$$\left(x^2 + 1\right)\left(x^2 + yx + 1\right) = 0.$$

Hence $y = \beta + \beta^{-1}$ for some β. There are three distinct roots if and only if $\beta \in S \setminus \{1\}$. Since $x \mapsto x + x^{-1}$ maps the set $S \setminus \{1\}$ two-to-one, there are exactly 2^{k-1} elements $y \in GF(2^n)^\times$ of the form $y = \beta + \beta^{-1}$ where $\beta \in S$. □

Lemma 5.9. *For* d *in* (5.8)*, the equation*

$$(x+1)^d = x^d + 1 \tag{5.10}$$

has 2^k *solutions if* k *is even, and* $2^k + 2$ *solutions if* k *is odd.*

Proof. Clearly always $\gcd\left(2^{k-2}, 2^k + 1\right) = 1$. It is equally easy to see that $\gcd\left(2^{k-2} + 1, 2^k + 1\right) = 1$ if k is even and $\gcd\left(2^{k-2} + 1, 2^k + 1\right) = 3$ if k is odd. The claim now follows from Theorem 4.4 and Theorem 4.7. □

The previous lemma, as well as Lemma 5.15, follows also from results in [6].

The distribution of the values is as follows.

Theorem 5.10. ([*18*]) *Let* $k > 2$. *Then for* d *in* (5.7) $C_d(\tau)$ *has the following values:*

$-1 - 2^k$	*occurs*	$2^{n-1} - 2^{k-3}\left(2^k + (-1)^{k+1} + 1\right) - 2^{k-1}$	*times*
-1	*occurs*	$\frac{1}{3}\left(2^k\left(2^k + (-1)^{k+1} + 1\right) + 2^{k-1} - 3\right)$	*times*
$-1 + 2^k$	*occurs*	$2^{n-1} - 2^{k-2}\left(2^k + (-1)^{k+1} + 1\right)$	*times*
$-1 + 2^{k+1}$	*occurs*	2^{k-1}	*times*
$-1 + 3 \cdot 2^k$	*occurs*	$\frac{1}{3}\left(2^{k-3}\left(2^k + (-1)^{k+1} + 1\right) - 2^{k-1}\right)$	*times.*

5.3.3 A non-binary family

The only completely known non-binary Niho type cross-correlation function corresponds to the decimation $d = 2p^k - 1$. This is a non-binary counterpart of the first of Niho's families. The case $p > 2$ is due to Helleseth [18]. Using Theorem 3.4 there is no need to separate these cases.

Theorem 5.11. ([*34, 18*]) *Let $n = 2k$, $p^k \not\equiv 2 \pmod 3$, and $d = 2p^k - 1$. Then $C_d(\tau)$ has the following values:*

(i) $-1 - p^k$, *which occurs* $\frac{1}{3}\left(p^{2k} - p^k\right)$ *times,*

(ii) -1, *which occurs* $\frac{1}{2}\left(p^{2k} - p^k - 2\right)$ *times,*

(iii) $-1 + p^k$, *which occurs* p^k *times, and*

(iv) $-1 + 2p^k$, *which occurs* $\frac{1}{6}\left(p^{2k} - p^k\right)$ *times.*

Proof. It is easily seen that $d \equiv 1 \pmod{2^k - 1}$ and $(d-1)/(p^k - 1) = 2$. Therefore (by Theorem 3.4) the corresponding equation is simply

$$x^3 + \overline{y}x^2 + yx + 1,$$

and thus $C_d(\tau)$ is at most four-valued. Using Theorems 4.3 and 4.4 the third power sum is easily found; the number of b of Lemma 2.4 is p^k. Note that, the condition $p^k \not\equiv 2 \pmod 3$ is needed only to guarantee that the decimated sequence is indeed an m-sequence. □

5.3.4 Two other families

To end this chapter we present some results on $C_d(\tau)$ corresponding to the decimation

$$d = 3 \cdot 2^k - 2.$$

Lemma 5.12. *Let $n = 2k$ and $d = 3 \cdot 2^k - 2$. Assume that $k \not\equiv 2 \pmod 4$. Then*

(a) $\gcd(d, 2^n - 1) = 1$,

(b) $d \equiv 1 \pmod{2^k - 1}$, *and*

(c) $d \equiv -5 \pmod{2^k + 1}$.

Proof. Firstly, $d = 3(2^k - 1) + 1$ and $d = 3(2^k + 1) - 5$, and we get (b) and (c). Finally, (a) follows from the following facts. Suppose that a prime $p \neq 2$ divides $2^n - 1$. Then it divides $2^k - 1$ or $2^k + 1$. Using (b) we get that p cannot divide both d and $2^k - 1$. Using (c) we get that if p divides both d and $2^k + 1$, then it divides 5. But this is impossible because of the assumption $k \not\equiv 2 \pmod 4$. □

Theorem 5.13. ([*13*]) *Assume that* $k \not\equiv 2 \pmod 4$, $n = 2k$ *and*

$$d = 3 \cdot 2^k - 2.$$

Then the values of $C_d(\tau)$ *are among*

$$-1 + (N(y) - 1) \cdot 2^k,$$

where $N(y) = 0, 1, \ldots, 5$. *Moreover, if* k *is even, the value* $-1 + 3 \cdot 2^k$ *does not occur.*

Proof. Using Niho's theorem we see that the cross-correlation values are exactly the values

$$-1 + (N(y) - 1) \cdot 2^k,$$

where y runs through the nonzero elements of the field $GF(2^n)$, and $N(y)$ is the number of solutions $x \in S$ to the equation

$$x^5 + yx^3 + \overline{y}x^2 + 1 = 0. \tag{5.11}$$

Since the equation is of degree five, the cross-correlation function is at most six-valued. We have to show that (5.11) cannot have exactly four solutions in S if k is even.

Note that if four solutions of the equation are in S, then the fifth root does too.

Let $f(x) = x^5 + yx^3 + \overline{y}x^2 + 1$. Then $f(x)$ has repeated roots if and only if $y\overline{y} = 1$; this can be seen by forming the derivative. In this case the repeated root is

$$x = y^{2^{2k-1}},$$

and $f(x)$ splits as

$$f(x) = (x^2 + y)(x + \rho)(x + \alpha\rho)(x + \alpha^2\rho), \tag{5.12}$$

where α is a primitive element of $GF(4)$ and ρ is any element such that $\rho^3 = \overline{y}$.

The equation (5.11) can have exactly four solutions in S only if $\rho, \alpha \in S$. But the order of α is 3. Thus 3 has to divide $2^k + 1$ and then necessarily k is odd. □

We have shown the following.

(*i*) Let $n \equiv 0 \pmod 8$, $n = 2k$, and

$$d = 3 \cdot 2^k - 2.$$

Then $C_d(\tau)$ is (at most) five-valued.

(*ii*) Let k be odd, $n = 2k$, and

$$d = 3 \cdot 2^k - 2.$$

Then $C_d(\tau)$ is (at most) six-valued.

Let N_i denote the number of times (5.11) has exactly i solutions in S.

For even k, we know that $N_4 = 0$. The following lemma gives N_4 for odd k.

Lemma 5.14. *Assume that $k > 1$ is odd. Then $N_4 = \frac{1}{3}(2^k - 2)$.*

Proof. If (5.11) has exactly four solutions in S, then $f(x)$ has a root of multiplicity 2 and the other roots are simple. From (5.12) we deduce that this happens if and only if there is $\rho \in S \setminus \{1\}$ such that $\rho^3 = \overline{y}$. Since the mapping $x \mapsto x^3$ is now three-to-one, this happens $(2^k + 1)/3 - 1$ times. □

Lemma 5.15. *Let $n = 2k$, where $k \not\equiv 2 \pmod 4$. Let*

$$d = 2^k + 2^{k-1} - 1.$$

Then

$$(x+1)^d = x^d + 1 \tag{5.13}$$

has exactly

(*i*) *2^k solutions in $GF(2^n)$ if k is even, and*

(*ii*) *$2^k + 2$ solutions in $GF(2^n)$ if k is odd.*

Proof. The equivalent decimation $2 \cdot d = \left(2^k - 1\right) \cdot 3 + 1$ satisfies $d \equiv 1 \pmod{2^k - 1}$ and then the claim follows easily from Theorem 4.4 and Theorem 4.7. □

From the number of equations of the form (5.11) we deduce $\sum_{i=0}^{5} N_i = 2^n - 1$. Thus one more independent equation on the numbers N_i is needed in order to calculate the distribution of the values.

It is shown in [13], that there is a connection between Dickson polynomials and Niho type cross-correlation functions. This connection is then used to calculate the number N_2 in the special case of the equation (5.11). The distribution found is given by the following theorem.

Theorem 5.16. ([13]) *Let $n = 2k$, where k is odd, and let $d = 3 \cdot 2^k - 2$. Then the values of $C_d(\tau)$ are distributed as follows:*

$$\begin{array}{lll}
-1 - 2^k & occurs & \frac{11 \cdot 2^{2k} - 24 \cdot 2^k + R}{30} \quad times \\
-1 & occurs & \frac{9 \cdot 2^{2k} + 22 \cdot 2^k - 3R - 20}{24} \quad times \\
-1 + 2^k & occurs & \frac{2^{2k} - 2 \cdot 2^k + R - 4}{6} \quad times \\
-1 + 2^{k+1} & occurs & \frac{2^{2k} - R + 12}{12} \quad times \\
-1 + 3 \cdot 2^k & occurs & \frac{2^k - 2}{3} \quad times \\
-1 + 2^{k+2} & occurs & \frac{2^{2k} - 14 \cdot 2^k + R + 20}{120} \quad times.
\end{array}$$

Here R is defined as

$$R = \sum_{y \in GF(2^k) \setminus \{0,1\}} \chi\left(\frac{1}{y}\right) K\left(\frac{1}{y^3 + y}\right),$$

where $K(y)$, $y \in GF(2^k)$, denotes the Kloosterman sum

$$K(y) = \sum_{x \in GF(2^k)} \chi\left(\frac{1}{x} + yx\right).$$

In the last sum the convention $1/0 = 0$ is used.

As the proof of Theorem 5.16 involves extensive and very detailed calculations, we do not repeat it here. The reader is referred to the original manuscript.

Of course the above theorem is unsatisfactory in the sense that a closed formula is not given. It is not even clear what is the order of the error term R.

Bibliography

[1] L. Baumert and R. McEliece. Weights of irreducible cyclic codes. *Information and Control*, 20:158–175, 1972.

[2] A. W. Bluher. On $x^{q+1} + ax + b$. *Finite Fields Appl.*, 10(3):285–305, 2004.

[3] A. Canteaut, P. Charpin, and H. Dobbertin. Binary m-sequences with three-valued cross-correlation: a proof of Welch's conjecture. *IEEE Transactions on Information Theory*, 46(1):4–8, 2000.

[4] A. Canteaut, P. Charpin, and H. Dobbertin. Weight divisibility of cyclic codes, highly nonlinear functions on $\mathbf{F}_{2^m}$, and crosscorrelation of maximum-length sequences. *SIAM J. Discrete Math.*, 13(1):105–138, 2000.

[5] C. Carlet, P. Charpin, and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Des. Codes Cryptogr.*, 15(2):125–156, 1998.

[6] P. Chaprin, A. Tietäväinen, and V. A. Zinoviev. On binary cyclic codes with minimum distance three. *Problems of Information Transmission*, 33(4):287–296, 1997.

[7] P. Charpin. Cyclic codes with few weights and Niho exponents. *Journal of Combinatorial Theory A*, to appear.

[8] T. Cusick and H. Dobbertin. Some new three-valued cross-correlation functions for binary m-sequences. *IEEE Transactions on Information Theory*, 42(4):1238–1240, 1996.

[9] J. F. Dillon and H. Dobbertin. New cyclic difference sets with Singer parameters. *Finite Fields Appl.*, 10(3):342–389, 2004.

[10] H. Dobbertin. One-to-one highly nonlinear power functions on $GF(2^n)$. *AAECC Applicable Algebra in Engineering, Communication and Computing*, 9:139–152, 1998.

[11] H. Dobbertin. Almost perfect nonlinear power functions on $GF(2^n)$: the Niho case. *Information and Computation*, 151(1-2):57–72, 1999.

[12] H. Dobbertin. Almost perfect nonlinear power functions on GF(2^n): the Welch case. *IEEE Transactions on Information Theory*, 45(4):1271–1275, 1999.

[13] H. Dobbertin, P. Felke, T. Helleseth, and P. Rosendahl. Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums. Submitted.

[14] H. Dobbertin, T. Helleseth, P. V. Kumar, and H. Martinsen. Ternary m-sequences with three-valued cross-correlation function: new decimations of Welch and Niho type. *IEEE Trans. Inform. Theory*, 47(4):1473–1481, 2001.

[15] H. M. Gjelsvik. Krysskorrelasjon mellom maksimalsekvenser. Master's thesis, University of Bergen, 2002.

[16] R. Gold. Maximal recursive sequences with 3-valued recursive cross-correlation functions. *IEEE Transactions on Information Theory*, 14(1):154–156, 1968.

[17] S. Golomb. *Shift register sequences*. Aegean Park Press, Laguna Hills CA, 1982.

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

[19] T. Helleseth. A note on the cross-correlation function between two binary maximal length linear sequences. *Discrete Mathematics*, 23(3):301–307, 1978.

[20] T. Helleseth. Pairs of m-sequences with a six-valued crosscorrelation. In J.-S. No, H.-Y. Song, T. Helleseth, and P. V. Kumar, editors, *Mathematical Properties of Sequences and Other Combinatorial Structures*, pages 1–6, Boston, 2003. Kluwer Academic Publishers.

[21] T. Helleseth and P. V. Kumar. Sequences with low correlation. In *Handbook of coding theory, Vol. I, II*, pages 1765–1853. North-Holland, Amsterdam, 1998.

[22] T. Helleseth, J. Lahtonen, and P. Rosendahl. On certain equations over finite fields and cross-correlations of m-sequences. In K. Feng, H. Niederreiter, and C. Xing, editors, *Coding, Cryptography and Combinatorics*, volume 23 of *Progress in Computer Science and Applied Logic*, pages 169–176, 2004.

[23] T. Helleseth, J. Lahtonen, and P. Rosendahl. On Niho type cross-correlation functions of m-sequences. Submitted.

[24] T. Helleseth and H. Martinsen. Open problems in sequence design and correlation. Manuscript, University of Bergen.

[25] T. Helleseth and P. Rosendahl. New pairs of m-sequences with four-level cross-correlation. *Finite Fields and Their Applications*, Submitted.

[26] H. Hollmann and Q. Xiang. A proof of Welch and Niho conjectures on cross-correlation of binary m-sequences. *Finite Fields and their applications*, 7(2):253–286, 2001.

[27] I. Honkala and A. Tietäväinen. Codes and number theory. In *Handbook of coding theory, Vol. I, II*, pages 1141–1194. North-Holland, Amsterdam, 1998.

[28] T. Kasami. Weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes. *Information and Control*, 18:369–394, 1971.

[29] G. Lachaud and J. Wolfmann. The weights of the orthogonals of the extended quadratic binary Goppa codes. *IEEE Trans. Inform. Theory*, 36(3):686–692, 1990.

[30] J. Lahtonen. On the odd and the aperiodic correlation properties of the Kasami sequences. *IEEE Transactions on Information Theory*, 41(5):1506–1508, 1995.

[31] R. Lidl and H. Niederreiter. *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and Its Applications*. Addison-Wesley, Reading, 1983.

[32] R. McEliece. *Finite Fields for Computer Scientists and Engineers*. Kluwer Academic Publishers, Boston, 1987.

[33] G. McGuire. On certain 3-weight cyclic codes having symmetric weights and a conjecture of Helleseth. In *Sequences and their applications (Bergen, 2001)*, Discrete Math. Theor. Comput. Sci. (Lond.), pages 281–295. Springer, London, 2002.

[34] Y. Niho. *Multivalued cross-correlation functions between two maximal linear recursive sequences*. PhD thesis, University or Southern California, 1972.

[35] P. Rosendahl. A generalization of Niho's theorem. Submitted to Designs, Codes and Cryptography.

[36] E. Selmer. Linear recurrence relations over finite fields. Lecture notes, University of Bergen, 1966.

[37] C. Small. *Arithmetic of finite fields*, volume 148 of *Monographs and Textbooks in Pure and Applied Mathematics*. Marcel Dekker Inc., New York, 1991.

[38] H. Stichtenoth. Algebraic function fields over finite fields with many rational places. *IEEE Transactions on Information Theory*, 41(6):1548–1563, November 1995.

[39] H. Trachtenberg. *On the cross-correlation functions of maximal linear sequences*. PhD thesis, University or Southern California, 1970.

Turku Centre for Computer Science
TUCS Dissertations

13. **Jukkapekka Hekanaho**, An Evolutionary Approach to Concept Learning
14. **Jouni Järvinen**, Knowledge Representation and Rough Sets
15. **Tomi Pasanen**, In-Place Algorithms for Sorting Problems
16. **Mika Johnsson**, Operational and Tactical Level Optimization in Printed Circuit Board Assembly
17. **Mats Aspnäs**, Multiprocessor Architecture and Programming: The Hathi-2 System
18. **Anna Mikhajlova**, Ensuring Correctness of Object and Component Systems
19. **Vesa Torvinen**, Construction and Evaluation of the Labour Game Method
20. **Jorma Boberg**, Cluster Analysis. A Mathematical Approach with Applications to Protein Structures
21. **Leonid Mikhajlov**, Software Reuse Mechanisms and Techniques: Safety Versus Flexibility
22. **Timo Kaukoranta**, Iterative and Hierarchical Methods for Codebook Generation in Vector Quantization
23. **Gábor Magyar**, On Solution Approaches for Some Industrially Motivated Combinatorial Optimization Problems
24. **Linas Laibinis**, Mechanised Formal Reasoning About Modular Programs
25. **Shuhua Liu**, Improving Executive Support in Strategic Scanning with Software Agent Systems
26. **Jaakko Järvi**, New Techniques in Generic Programming : C++ is More Intentional than Intended
27. **Jan-Christian Lehtinen**, Reproducing Kernel Splines in the Analysis of Medical Data
28. **Martin Büchi**, Safe Language Mechanisms for Modularization and Concurrency
29. **Elena Troubitsyna**, Stepwise Development of Dependable Systems
30. **Janne Näppi**, Computer-Assisted Diagnosis of Breast Calcifications
31. **Jianming Liang**, Dynamic Chest Images Analysis
32. **Tiberiu Seceleanu**, Systematic Design of Synchronous Digital Circuits
33. **Tero Aittokallio**, Characterization and Modelling of the Cardiorespiratory System in Sleep-disordered Breathing
34. **Ivan Porres**, Modeling and Analyzing Software Behavior in UML
35. **Mauno Rönkkö**, Stepwise Development of Hybrid Systems
36. **Jouni Smed**, Production Planning in Printed Circuit Board Assembly
37. **Vesa Halava**, The Post Correspondence Problem for Marked Morphisms
38. **Ion Petre**, Commutation Problems on Sets of Words and Formal Power Series
39. **Vladimir Kvassov**, Information Technology and the Productivity of Managerial Work
40. **Franck Tétard**, Managers, Fragmentation of Working Time, and Information Systems
41. **Jan Manuch**, Defect Theorems and Infinite Words
42. **Kalle Ranto**, Z_4-Goethals Codes, Decoding and Designs
43. **Arto Lepistö**, On Relations between Local and Global Periodicity
44. **Mika Hirvensalo**, Studies on Boolean Functions Related to Quantum Computing
45. **Pentti Virtanen**, Measuring and Improving Component-Based Software Development
46. **Adekunle Okunoye**, Knowledge Management and Global Diversity - A Framework to Support Organisations in Developing Countries
47. **Antonina Kloptchenko**, Text Mining Based on the Prototype Matching Method
48. **Juha Kivijärvi**, Optimization Methods for Clustering
49. **Rimvydas Rukšėnas**, Formal Development of Concurrent Components
50. **Dirk Nowotka**, Periodicity and Unbordered Factors of Words
51. **Attila Gyenesei**, Discovering Frequent Fuzzy Patterns in Relations of Quantitative Attributes
52. **Petteri Kaitovaara**, Packaging of IT Services – Conceptual and Empirical Studies
53. **Petri Rosendahl**, Niho Type Cross-Correlation Functions and Related Equations

Turku
Centre *for*
Computer
Science

Lemminkäisenkatu 14 A, 20520 Turku, Finland | www.tucs.fi

University of Turku

- Department of Information Technology
- Department of Mathematics

Åbo Akademi University

- Department of Computer Science
- Institute for Advanced Management Systems Research

Turku School of Economics and Business Administration

- Institute of Information Systems Sciences

ISBN 952-12-1397-3
ISSN 1239-1883