Analysis of Kasami-Welch Functions in Odd Dimension using Stickelberger's Theorem

Philippe Langevin
GRIM-USTV
University of Toulon
France

Gregor Leander[*]
DTU Mathematics
Technical University of Denmark
Denmark

Gary McGuire[†]
School of Mathematical Sciences
University College Dublin
Ireland

Eugen Zălinescu[‡]
MSR-INRIA Joint Center
Orsay
France

August 25, 2009

Abstract

In this article we apply some number theoretical techniques to derive results on Boolean functions. We apply Stickelberger's theorem on 2-adic valuations of Gauss sums to the Kasami-Welch functions $\mathrm{tr}_L(x^{4^k-2^k+1})$ on $\mathbb{F}_{2^n}$, where n is odd and $(k,n)=1$. We obtain information on the Fourier spectrum, including a characterization of the support of the Fourier transform. One interesting feature is that the behaviour is different for different values of k. We also apply the Gross-Koblitz formula to the Gold functions $\mathrm{tr}_L(x^{2^k+1})$.

Keywords: Kasami-Welch; Fourier transform; Walsh-Hadamard transform; finite field; Stickelberger; Gross-Koblitz.
AMS Classification: 05C38, 11T24, 94B15.

1 Introduction

Let $L=\mathbb{F}_q$, the finite field with $q=2^n$ elements. Let tr_L denote the trace map from L to $\mathbb{F}_2$. The *Fourier transform* of any real-valued function F defined on L is the function $\widehat{F}$ defined by

$$\widehat{F}(a)=\sum_{x\in L}F(x)(-1)^{\mathrm{tr}_L(ax)}$$

[*] Supported by a DAAD postdoc fellowship

[†] Supported by a visitors grant from the University of Toulon, and the Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006.

[‡] Supported by GRIM

for $a \in L$. The *Fourier spectrum* of F is the set of values of $\widehat{F}$, that is the set

$$\{\widehat{F}(a) : a \in L\}.$$

To a Boolean function $f : L \longrightarrow \mathbb{F}_2$ we associate the real-valued function $F = (-1)^f$. When we say the Fourier spectrum of f, we mean the Fourier spectrum of the associated function $F = (-1)^f$. For a general f it is difficult to find the Fourier spectrum.

When the Fourier spectrum of a Boolean function is known, further information can be obtained using Stickelberger's theorem on 2-adic valuations of Gauss sums, but often the information is difficult to extract. Studying Boolean functions using Stickelberger's theorem leads to the study of a set which we call the J-set. We will give the definition in section 2. It is this J-set that is often hard to find explicitly, but when found it reaps rich rewards. Finding the J-set leads to finer information about the Fourier spectrum, and its support. For example, in section 5 we easily determine the degree of the characteristic function of the support using our results.

A Boolean function is said to be *bent* if its Fourier spectrum consists of the two values $\pm 2^{n/2}$, and thus n is necessarily even. An analysis of the J-set of Kasami-Welch bent functions, functions of the form $\mathrm{tr}_L(x^{4^k-2^k+1})$, was carried out in Langevin-Leander [7]. In this article we undertake an analysis of the J-set of $\mathrm{tr}_L(x^{4^k-2^k+1})$ for n odd. This is different from the n even case, and the complete result depends on paths in a certain graph (see sections 3 and 4).

One motivation for this article is a question of Hans Dobbertin, who asked for a trace description of the support of the Fourier transform of the Kasami-Welch functions. Dillon gives a description in [2], answering Dobbertin's question, although the description is not a trace description. In particular, he proves the No-Chung-Yun conjecture for n odd, which concerns one particular k, when $3k \equiv \pm 1 \pmod{n}$, and does give a trace description in that case. In the Dillon-Dobbertin [1] paper the n even case is proved. Our description is by its nature a trace description, which coincides with that of [2] in the $3k \equiv \pm 1 \pmod{n}$ case (see section 6).

We were also motivated by a desire to explain the data in Langevin-Veron [8]. As part of that research they searched on a computer for examples of the simplest possible J-set. It was observed that a single Kasami exponent has a J-set of this simple form. We are able to prove this result (see section 6).

Viewing the Kasami-Welch exponent as the $t = 3$ case of the family $(2^{tk} + 1)/(2^k + 1)$, we also consider in detail the next case, when $t = 5$. We are able to determine the J-set in terms of paths in two graphs (see section 7). The family of exponents $(2^{tk} + 1)/(2^k + 1)$ is of great interest because most known cases of a Fourier spectrum with five or fewer values belong to this family. The $t = 5$ case is known by results of Kasami to have 5-valued spectrum.

Finally, we discuss the Gross-Koblitz formula in our context in section 8, and apply this to the Gold functions in section 9. This allows us to determine the sign of the Fourier coefficient at 1, showing yet again how finer information can be deduced using these techniques. Besides Stickelberger's theorem and Gross-

Koblitz formula, all our analyses make heavy use of the fundamental formula in [4] on modular multiplication.

2 Stickelberger's Theorem and the J-Set

Let n be odd. Let $\mu(y) = (-1)^{\mathrm{tr}_L(y)}$, so μ is the canonical additive character of L. We let $L^\times = L\backslash\{0\}$.

Let $\mathbf{Q}_2$ denote the field of 2-adic (or dyadic) numbers, and let $\overline{\mathbf{Q}_2}$ denote its algebraic closure. As usual $\mathbf{Z}_2$ denotes the ring of 2-adic integers. We consider characters of $L^\times$ taking values in $\overline{\mathbf{Q}_2}$. In fact, the character values will lie in the unramified algebraic extension of $\mathbf{Q}_2$ of degree n.

Let $\widehat{L^\times}$ denote the group of characters of $L^\times$ taking values in $\overline{\mathbf{Q}_2}$. Elements of $\widehat{L^\times}$ are sometimes called multiplicative characters of L. The group $\widehat{L^\times}$ is a cyclic group of order $2^n - 1$, generated by the *Teichmüller character.* In order to define the Teichmüller character, let i be any primitive (2^n-1)-th root of unity in $\overline{\mathbf{Q}_2}$. The ring of integers of the extension $\mathbf{Q}_2(i)$ is $\mathbf{Z}_2[i]$, and this local ring has a unique maximal ideal generated by 2. The quotient $\mathbf{Z}_2[i]/(2)$ is a finite field of order 2^n, and is therefore isomorphic to L. We use this representation of L for the definition.

The Teichmüller character $\omega : L \longrightarrow \mathbf{Q}_2(i)$ is defined by the relation

$$\omega(i^j \mod 2) = i^j, \quad j = 0, 1, \ldots, 2^n - 2. \tag{1}$$

Using the convention $\omega(0) = 0$, the above relation is equivalent to saying that

$$\forall a \in L, \quad \omega(a) \mod 2 = a. \tag{2}$$

Next we recall Gauss sums. The Gauss sum associated to $\chi \in \widehat{L^\times}$ is

$$\tau(\chi) = -\sum_{x \in L^\times} \chi(x)\mu(x). \tag{3}$$

There are good justifications to introduce the minus sign in the definition of Gauss sums. The reader who is not familiar with the above definitions will find the basic material (characters and Gauss sums) in the book of Lidl and Niederreiter [9], and in the course of Koblitz [5] for the p-adic approach.

The following theorem can be found in [7].

Theorem 1 *Continuing the above notation, if $f(x) = \mu(x^d)$ then*

$$\widehat{f}(a) \equiv -\sum_{j=1}^{2^n-1} \tau(\overline{\omega}^j)\ \tau(\omega^{jd})\ \overline{\omega}^{jd}(a) \pmod{2^n}. \tag{4}$$

For any integer m, let $\mathrm{wt}_2(m)$ denote the 2-weight of m, namely $\sum_i m_i$ where $m \mod (2^n-1) = \sum_i m_i 2^i$ is the base 2 expansion of $m \mod (2^n-1)$.

A well known result of Stickelberger shows that for all integers $0 \leq j < 2^n - 1$, the following congruence holds:

$$\tau(\bar{\omega}^j) \equiv 2^{\mathrm{wt}_2(j)} \pmod{2^{1+\mathrm{wt}_2(j)}} \tag{5}$$

and so this gives us the 2-adic valuation of the Gauss sums in equation (4). It follows that the 2-adic valuation of each term in the sum (4) for $\widehat{f}(a)$ is $\mathrm{wt}_2(j) + \mathrm{wt}_2(-jd)$, and the overall 2-adic valuation of $\widehat{f}(a)$ is not less than the minimum of the numbers $\mathrm{wt}_2(j) + \mathrm{wt}_2(-jd)$ over all $j = 1, 2, \ldots, 2^n - 2$.

Definition 1 *Continuing the above notation, if $f(x) = \mu(x^d)$ let*

$$M_d = \min_{j \in \{1,2,\ldots,2^n-2\}} [\mathrm{wt}_2(j) + \mathrm{wt}_2(-jd)].$$

Definition 2 *Continuing the above notation, if $f(x) = \mu(x^d)$ let*

$$J_d = \big\{ j \in \{1, 2, \ldots, 2^n - 2\} : \mathrm{wt}_2(j) + \mathrm{wt}_2(-jd) = M_d \big\}.$$

We refer to this set J_d as the J-set. Its importance is summarized in the following Lemma.

Lemma 1 *Continuing the above notation, if $f(x) = \mu(x^d)$ it holds that*

$$2^{M_d+1} | \widehat{f}(a) \;\Leftrightarrow \sum_{j \in J_d} a^{-jd} = 0.$$

Proof. Using the definition of J_d and Theorem 1,

$$\widehat{f}(a) \equiv 2^{M_d} \sum_{j \in J} \overline{\omega}^{jd}(a) \pmod{2^{M_d+1}}$$

by definition of the Teichmüller character $a \equiv \omega(a) \mod 2$. Thus the valuation of $\widehat{f}(a)$ is greater than M_d if and only if $\sum_{j \in J_d} a^{-jd} = 0$.

□

Note that the J-set is closed under multiplication by 2, and so is a union of cyclotomic cosets. Let $\tilde{J}_d$ denote a set of cyclotomic representatives of J_d. Then, since n is odd,

$$\sum_{j \in J_d} a^{-jd} = \mathrm{tr}_L\Big(\sum_{j \in \tilde{J}_d} a^{-jd}\Big).$$

As the reader will see, determining the J-set leads to information about the Fourier spectrum. For the Kasami exponent $d = 4^k - 2^k + 1$, where n is odd and $(k, n) = 1$, we use the well-known fact (see [3] for example) that the Fourier spectrum is $\{0, \pm 2^{(n+1)/2}\}$.

Corollary 1 *Continuing the above notation, if the Fourier spectrum of $f(x) = \mu(x^d)$ is $\{0, \pm 2^{(n+1)/2}\}$ then $M_d = (n+1)/2$, and the support of the Fourier transform is $\{a \in L : \mathrm{tr}_L(\sum_{j \in \tilde{J}_d} a^{-jd}) = 1\}$.*

3 J-Sets for All Kasami Exponents

Let n be odd. Let $d = 4^k - 2^k + 1$ be a Kasami exponent, with $k > 1$ relatively prime to n. In this section we shall collect some results about the J-set.

We assume that j is an element of the J-set, with binary expansion

$$j = \sum_{i=0}^{n-1} j_i 2^i.$$

Let $s = jd \mod (2^n - 1)$. Then

$$s = \sum_{i=0}^{n-1} (j_{i-2k} - j_{i-k} + j_i) 2^i \mod (2^n - 1).$$

As usual, all subscripts are considered modulo n. First we recall the fundamental relation derived in [4]:

$$2c_i + s_i = j_{i-2k} - j_{i-k} + j_i + c_{i-1}, \quad i = 0, 1, \ldots, n-1, \tag{6}$$

where the *i-th carry* c_i is an integer in the set $\{-1, 0, 1\}$ and $\sum_i s_i 2^i$ is the binary expansion of s. Let c be the sequence $c_0, c_1, \ldots, c_{n-1}$. Overloading the notation, we write $\mathrm{wt}_2(c)$ for $\sum_i c_i$.

Lemma 2 $\mathrm{wt}_2(c) = -\frac{n-1}{2}$.

Proof. Summing equation (6) over all i gives

$$2\sum c_i + \sum s_i = \sum j_i - \sum j_i + \sum j_i + \sum c_i$$

or

$$\begin{aligned} \mathrm{wt}_2(c) &= \mathrm{wt}_2(j) - \mathrm{wt}_2(s) \\ &= \mathrm{wt}_2(j) - (n - \mathrm{wt}_2(-s)) \\ &= \mathrm{wt}_2(j) + \mathrm{wt}_2(-jd) - n \\ &= \frac{n+1}{2} - n \\ &= -\frac{n-1}{2}. \end{aligned}$$

□

Lemma 3 ([4]) *For all i, $c_i + c_{i-k} \in \{-1, 0, 1\}$.*

Corollary 2 *c has exactly $(n-1)/2$ entries equal to -1. The remaining $(n+1)/2$ entries are equal to 0.*

Proof. By Lemma 3, c_i and c_{i-k} cannot both be -1. This means that c has at most $(n-1)/2$ entries equal to -1. But combining Lemma 2 with the fact that $c_i \in \{-1, 0, 1\}$, gives that c has at most $(n-1)/2$ entries equal to -1. This shows the result.

□

As $(k, n) = 1$ we may re-order the sequence c_i as

$$c_0, c_{-k}, c_{-2k}, c_{-3k}, \ldots, c_{-(n-1)k}. \tag{7}$$

In this ordering no two consecutive entries can be -1 by Lemma 3. We may assume $c_0 = c_1 = 0$ up to cyclotomic equivalence, and then in this re-ordering the sequence c_i is

$$0, 0, -1, 0, -1, 0, -1, 0, \ldots, 0, -1. \tag{8}$$

In other words, if we change the subscript variable to r where $i = -rk$, then $c_r = 0$ if $r \in \{0, 1, 3, 5, \ldots, n-2\}$, and $c_r = -1$ if $r \in \{2, 4, 6, \ldots, n-1\}$. In this new ordering, the fundamental relation (6) becomes

$$2c_r + s_r = j_{r+2} - j_{r+1} + j_r + c_{r+e} \tag{9}$$

where $ek \equiv 1 \pmod{n}$. We will assume wlog that e is odd (if e is even then replace k by $n-k$).

Note that if $r + e < n$ then the subscript $r + e$ has the opposite parity to r, whereas if $r + e \geq n$ then $r + e$ (reduced modulo n) has the same parity as r.

Let $\ell = n - e$, which we note is even. We now show that exactly $\ell + 3$ bits in j are uniquely determined. These bits are:

$$j_2, j_3, \ldots, j_{\ell+2}, j_{\ell+3}, j_{\ell+4}.$$

These are determined because for $0 < r \leq \ell$ and r even, the relation (9) becomes

$$-2 + s_r = j_{r+2} - j_{r+1} + j_r + 0 \tag{10}$$

and there is a unique solution $s_r = 1$, $j_{r+2} = 0$, $j_{r+1} = 1$, $j_r = 0$. The $r = \ell + 1$ equation is

$$s_{\ell+1} = j_{\ell+3} - j_{\ell+2} + j_{\ell+1}$$

which determines $j_{\ell+3} = 0$. Then the $r = \ell + 2$ equation is

$$-1 + s_{\ell+2} = j_{\ell+4} - j_{\ell+3} + j_{\ell+2}$$

which implies $j_{\ell+4} = 0$.

The remaining $n - \ell - 3 = e - 3$ bits of j are not determined uniquely, in general. The number of solutions is equal to the number of paths of length $(e-3)/2$ starting at a certain vertex in a certain directed graph, as we will explain in the next section. If $e = 3$ then j is completely determined and the J-set has one element (in this case $j_{\ell+3} = j_0$ and $j_{\ell+4} = j_1$). We will discuss particular values of e later.

4 The Graph describing the J-Sets

First we note that the equations for $r > \ell + 2$ are

$$-2 + s_r = j_{r+2} - j_{r+1} + j_r - 1, \ r \text{ even},$$

and

$$0 + s_r = j_{r+2} - j_{r+1} + j_r + 0, \ r \text{ odd},$$

which do not have a unique solution. For example, although $j_{\ell+3} = 0$, $j_{\ell+4} = 0$, the $r = \ell + 3$ equation is

$$s_{\ell+3} = j_{\ell+5} - j_{\ell+4} + j_{\ell+3}$$

which does not determine $j_{\ell+5}$ (assuming $e > 3$).

Equations for r between 2 and $\ell + 2$ have already been used. We will take the equations for $r > \ell + 2$ in pairs; the first corresponds to an odd r, the second to an even r. If r is odd, and $x = j_r$, $y = j_{r+1}$, $z = j_{r+2}$, $t = j_{r+3}$, the fact that the r-th equation has a solution is equivalent to

$$x - y + z \in \{0, 1\} \tag{11}$$

and the fact that the next equation for $r + 1$ has a solution is equivalent to

$$y - z + t + 1 \in \{0, 1\}. \tag{12}$$

We consider (11) and (12) as the restrictions in moving from one odd-even pair of bits (x, y) to the next odd-even pair (z, t). We note that these are the only restrictions on (z, t), and we further note that when (z, t) are chosen, they in turn will use (11) and (12) to determine the next odd-even pair. The next odd-even pair will not depend on x and y at all, only on z and t.

In this way, we can track how ordered pairs (j_r, j_{r+1}) (with r odd) of undetermined bits give rise to possibilities for the next pair of undetermined bits. We can express this situation very concisely in the form of the directed graph G given in Figure 1.

It is now evident that solutions for the undetermined bits correspond to paths in this graph G that start at 00. The length of the path should be one half the number of undetermined bits, i.e., $(e - 3)/2$. The last vertex in the path is the final pair of undetermined bits (j_0, j_1). We have proved:

Theorem 2 *There is a one-to-one correspondence between paths in G of length $(e - 3)/2$ that start at 00, and representatives from cyclotomic cosets in the J-set.*

5 The Degree of The Support Function

The support of the Fourier transform is described by the function

$$a \mapsto \mathrm{tr}_L\Big(\sum_{j \in \tilde{J}_d} a^{-jd}\Big),$$

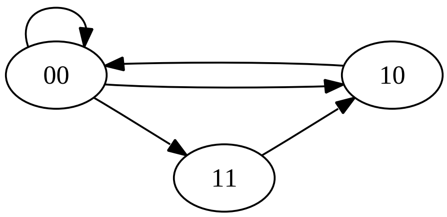

Figure 1: Graph G of Transitions $(j_r, j_{r+1}) \to (j_{r+2}, j_{r+3})$

called the *support function*. An application of our results is that we can determine the degree of this function for any Kasami exponent.

Theorem 3 *Let n be odd. Let $d = 4^k - 2^k + 1$ be the Kasami exponent, with $ek \equiv 1 \pmod{n}$, e odd. Then the degree of the support function $a \mapsto \mathrm{tr}_L(\sum_{j \in \tilde{J}_d} a^{-jd})$ is $(e+1)/2$.*

Proof. The degree of the support function is determined by the maximum value of $\mathrm{wt}_2(-jd)$ where j is in the J-set. As

$$\mathrm{wt}_2(j) + \mathrm{wt}_2(-jd) = \frac{n+1}{2}$$

this maximum is achieved by minimising $\mathrm{wt}_2(j)$. By Theorem 2, elements of the J-set correspond to paths in the graph G. This minimum is achieved by choosing a path in G of smallest weight. It is clear that a path of weight 0 can always be chosen, simply by choosing the loop from 00 to itself for each edge. The resulting element of the J-set has weight $\ell/2$, so

$$\max_{j \in J_d} \mathrm{wt}_2(-jd) = \frac{n+1}{2} - \frac{\ell}{2} = \frac{n+1-(n-e)}{2} = \frac{e+1}{2}.$$

□

6 J-Sets for Particular Kasami Exponents

Experimental results in Langevin-Veron [8] showed that for $n < 39$ and not divisible by 3, there is exactly one Kasami exponent that has a J-set consisting of one cyclotomic coset. We are now able to prove this, and identify the exponent. It turns out that Dillon [2] and Dillon-Dobbertin [1] discussed this particular Kasami exponent before, and gave the trace description of the support of the Fourier transform. We give a different proof of this trace description as a simple corollary of our description of the J-set.

Theorem 4 *Let n be odd and not divisible by 3. Let $d = 4^k - 2^k + 1$ be the Kasami exponent with $3k \equiv 1 \pmod{n}$.*

(1) *There is exactly one element in the J-set up to cyclotomy, which is $1/(2^{-2k} - 1)$, i.e.,*

$$J_d = \Big\{\frac{2^i}{2^{-2k} - 1} : i = 0, 1, 2, \ldots, n-1\Big\}.$$

(2) *This is the only Kasami exponent whose J-set consists of a single cyclotomic coset.*

(3) *The support of the Fourier transform is $\{a \in L : \mathrm{tr}_L(a^{2^k+1}) = 1\}$.*

Proof. (1) Here $e = 3$ and $\ell = n - e = n - 3$. By Theorem 2 the J-set has one element j up to cyclotomic equivalence. The element is completely determined as we explained in section 4. The bits of j in the re-ordering are

$$j_2 = 0, j_3 = 1, j_4 = 0, j_5 = 1, \ldots,$$

$$j_{\ell+1} = 1, j_{\ell+2} = 0, j_{\ell+3} = j_0 = 0, j_{\ell+4} = j_1 = 0.$$

Upon reverting to the original ordering, this gives j as

$$j = \sum_{s=1}^{(n-3)/2} 2^{-k(2s+1)} = 2^{-3k} \sum_{s=0}^{(n-5)/2} 2^{-2sk} = 2^{-3k} \frac{2^{-2k(n-3)/2} - 1}{2^{-2k} - 1} = \frac{1}{2^{-2k} - 1}.$$

(2) We assume $k \neq 1$, and thus $e \neq 1$ because $k = 1$ is the Gold case $d = 3$. As e is odd, any other value of e is at least 5 and there are at least three paths in G of the required type, and therefore the J-set contains at least three cyclotomic cosets.

(3) As we showed in section 2 the support of the Fourier transform is given by

$$\{a : \mathrm{tr}_L(\sum_{j \in \tilde{J}_d} a^{-jd}) = 1\}.$$

In this case $d = 2^{2k} - 2^k + 1 = (2^k + 1)(2^{2k} - 1)$ so $jd = -(2^k + 1)$.

□

Theorem 5 *Let n be odd and not divisible by 5. Let $d = 4^k - 2^k + 1$ be the Kasami exponent with $5k \equiv 1 \pmod{n}$.*

(1) *There are exactly three elements in the J-set up to cyclotomy, which are*

$$\frac{1}{2^{-2k} - 1}, 1 + \frac{2^{2k-1}}{2^{-2k} - 1}, 1 + 2^{-k} + \frac{2^{2k-1}}{2^{-2k} - 1}.$$

(2) *This is the only Kasami exponent whose J-set consists of three cyclotomic cosets.*

(3) *The support of the Fourier transform is the set of $a \in L$ such that*

$$\mathrm{tr}_L(a^{2^{3k}+2^k+1} + a^{2^{2k}+1} + a) = 1.$$

Proof. (1) Here $e = 5$ and $\ell = n - e = n - 5$. By Theorem 2 the J-set has three elements up to cyclotomic equivalence. All bits except two are completely determined. The bits of j in the re-ordering are

$$j_2 = 0, j_3 = 1, j_4 = 0, j_5 = 1, \ldots,$$

$$j_{\ell+1}=1, j_{\ell+2}=0, j_{\ell+3}=0, j_{\ell+4}=0.$$

Here $j_{\ell+5}=j_0$, $j_{\ell+6}=j_1$ are undetermined, the possibilities are determined by length one paths in the graph G starting at 00. There are three such paths, so the possibilities for (j_0, j_1) are 00, 10, and 11. Call the corresponding elements of the J-set $j^{(0)}, j^{(1)}, j^{(2)}$ respectively. Upon reverting to the original ordering, this gives $j^{(0)}$ as

$$j^{(0)}=\sum_{s=1}^{(n-5)/2} 2^{-k(2s+1)}=2^{-3k}\sum_{s=0}^{(n-7)/2} 2^{-2sk}=2^{-3k}\frac{2^{-2k(n-5)/2}-1}{2^{-2k}-1}=\frac{2^{2k-1}}{2^{-2k}-1}.$$

Then $j^{(1)}=j^{(0)}+1$ and $j^{(2)}=j^{(0)}+1+2^{-k}$, by adding the appropriate powers of 2 according to the path.

(2) We assume $k \neq 1$, and thus $e \neq 1$, because $k=1$ is the Gold case $d=3$. We showed that the $e=3$ case has one element in the J-set. As e is odd, any other value of e is at least 7 and there are more than three paths in G of the required type, and therefore the J-set contains more than three cyclotomic cosets.

(3) As we showed in section 2 the support of the Fourier transform is given by

$$\{a : \mathrm{tr}_L(\sum_{j\in \tilde{J}_d} a^{-jd}) = 1\}.$$

By part (1) this gives the support as the a such that

$$\mathrm{tr}_L(a^{-d[\frac{1}{2^{-2k}-1}]}+a^{-d[1+\frac{2^{2k-1}}{2^{-2k}-1}]}+a^{-d[1+2^{-k}+\frac{2^{2k-1}}{2^{-2k}-1}]})=1.$$

Note that, in this case, $d=(2^{3k}+2^k+1)(2^{2k}-1)$ and thus

$$-d\left(\frac{1}{2^{-2k}-1}\right)=(2^{3k}+2^k+1)2^{2k}$$

which is cyclotomic equivalent to $2^{3k}+2^k+1$. Furthermore,

$$-d\left(1+\frac{2^{2k-1}}{2^{-2k}-1}\right)=2^{-k}(2^{2k}+1)$$

which is cyclotomic equivalent to $2^{2k}+1$ and finally

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

Therefore, the support is given by

$$\mathrm{tr}_L(a^{2^{3k}+2^k+1}+a^{2^{2k}+1}+a)=1$$

as claimed.

□

Theorem 6 *Let n be odd. For any $k > 1$ with $(k, n) = 1$, the J-set (for $d = 4^k - 2^k + 1$) contains the element*

$$\frac{1}{2^{-2k} - 1}.$$

Proof. This element is derived as in the proof of Theorem 5, by choosing the path in the graph G with all vertices 00.

□

7 The Case $d = \frac{2^{5k}+1}{2^k+1}$

In this section we shall extend the methods used to determine the J-set for the Kasami-Welch exponent $d = \frac{2^{3k}+1}{2^k+1} = 4^k - 2^k + 1$ to the exponent $d = \frac{2^{5k}+1}{2^k+1} = 16^k - 8^k + 4^k - 2^k + 1$. For this exponent it is known that the Fourier spectrum is 5-valued, and that the values are $\{0, \pm 2^{(n+1)/2}, \pm 2^{(n+3)/2}\}$. Thus we know that $M_d = (n+1)/2$ here, the same as for the Kasami-Welch case. However the analysis of the J-set is more complicated here. There are two graphs instead of one graph, and the number of solutions corresponds to paths in both graphs that link up correctly.

Using the same notations as in section 3, the fundamental relation of [4] becomes

$$2c_i + s_i = j_{i-4k} - j_{i-3k} + j_{i-2k} - j_{i-k} + j_i + c_{i-1}, \tag{13}$$

where $c_i \in \{-2, -1, 0, 1, 2\}$.

Lemma 4 $\mathrm{wt}_2(c) = -\frac{n-1}{2}$.

Proof. Same as for the Kasami-Welch case (Lemma 2).

□

Lemma 5 ([4]) *For all i, $c_i + c_{i-k} \in \{-1, 0, 1\}$.*

Corollary 3 *c has at least $(n-1)/2$ entries equal to -1.*

Proof. Applying the previous lemma gives the following information.

$$\begin{aligned}
c_i = 2 &\implies c_{i+k} \in \{-2, -1\} \\
c_i = 1 &\implies c_{i+k} \in \{-2, -1, 0\} \\
c_i = 0 &\implies c_{i+k} \in \{-1, 0, 1\} \\
c_i = -1 &\implies c_{i+k} \in \{0, 1, 2\} \\
c_i = -2 &\implies c_{i+k} \in \{1, 2\}.
\end{aligned}$$

¿From this it follows that if $c_i = -2$ then both c_{i-k} and c_{i+k} are $+1$ or $+2$. Therefore any c_i that is -2 cannot contribute anything towards $\mathrm{wt}_2(c)$. Since the 2-weight must reach $-(n-1)/2$, and any -2 entries contribute nothing, the only contribution can come from -1 entries.

□

Corollary 4 *c has exactly $(n-1)/2$ entries equal to -1. The remaining $(n+1)/2$ entries are equal to 0.*

Proof. By Lemma 5, c_i and c_{i+k} cannot both be -1. This means that c has at most $(n-1)/2$ entries equal to -1. Combining this with Corollary 3 gives the first statement.

If any c_i is positive, there are at least $(n+1)/2$ c_i's equal to -1 because of the 2-weight. This would imply there is an i with c_i and c_{i+k} both -1.

□

As we did in the Kasami-Welch case, we may re-order the sequence c_i as

$$c_0, c_{-k}, c_{-2k}, c_{-3k}, \ldots, c_{-(n-1)k} \tag{14}$$

which again wlog is

$$0, 0, -1, 0, -1, 0, -1, 0, \ldots, 0, -1. \tag{15}$$

In other words, if we change to the "r-ordering" where $i = -rk$, then $c_r = 0$ if $r \in \{0, 1, 3, 5, \ldots, n-2\}$, and $c_r = -1$ if $r \in \{2, 4, 6, \ldots, n-1\}$. In this new ordering, the fundamental relation (13) becomes

$$2c_r + s_r = j_{r+4} - j_{r+3} + j_{r+2} - j_{r+1} + j_r + c_{r+e} \tag{16}$$

where $ek \equiv 1 \pmod{n}$. We will assume wlog that e is odd (if e is even then replace k by $n-k$).

As before we let $\ell = n - e$, which is even. In the Kasami-Welch case, for some values of r the equation (16) had a unique solution. This does not happen here. There are four cases, depending on the parity of r and $r+e$:

$$\begin{aligned}
r \in \{1, 2, \ldots \ell\}, &\quad r \text{ odd}, \quad (c_r, c_{r+e}) = (0, -1) && (17)\\
r \in \{1, 2, \ldots \ell\}, &\quad r \text{ even}, \quad (c_r, c_{r+e}) = (-1, 0) && (18)\\
r \in \{\ell+1, \ell+2, \ldots n-1\}, &\quad r \text{ odd}, \quad (c_r, c_{r+e}) = (0, 0) && (19)\\
r \in \{\ell+1, \ell+2, \ldots n-1\}, &\quad r \text{ even}, \quad (c_r, c_{r+e}) = (-1, -1). && (20)
\end{aligned}$$

The $r = n = 0$ equation also has $(c_r, c_{r+e}) = (0, 0)$.

We consider the bits of j in fours, starting at $r = 1$ although this is arbitrary. For any four bits $(j_r, j_{r+1}, j_{r+2}, j_{r+3})$, the transition to the next four bits $(j_{r+4}, j_{r+5}, j_{r+6}, j_{r+7})$ is determined by the four equations (16) for $r, r+1, r+2, r+3$. These four equations completely determine the transition. Therefore, we define two graphs. We consider the case $n \equiv 1 \pmod{4}$ and $\ell \equiv 0 \pmod{4}$, the other cases being similar but slightly different.

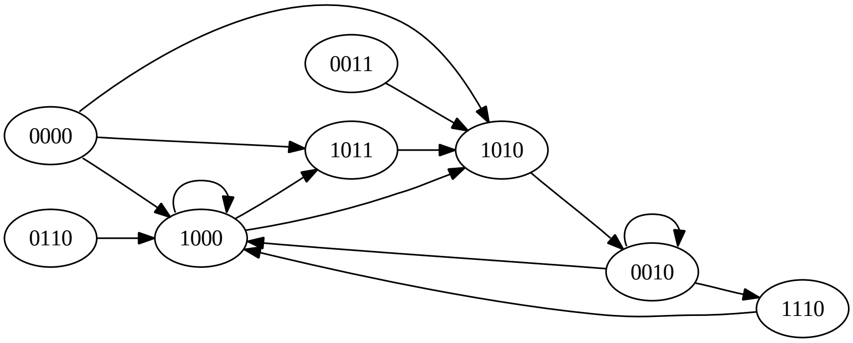

Figure 2: Graph G_1 of Transitions $(j_r, j_{r+1}, j_{r+2}, j_{r+3}) \rightarrow (j_{r+4}, j_{r+5}, j_{r+6}, j_{r+7})$ for $r \in \{1, 2, \ldots \ell\}$.

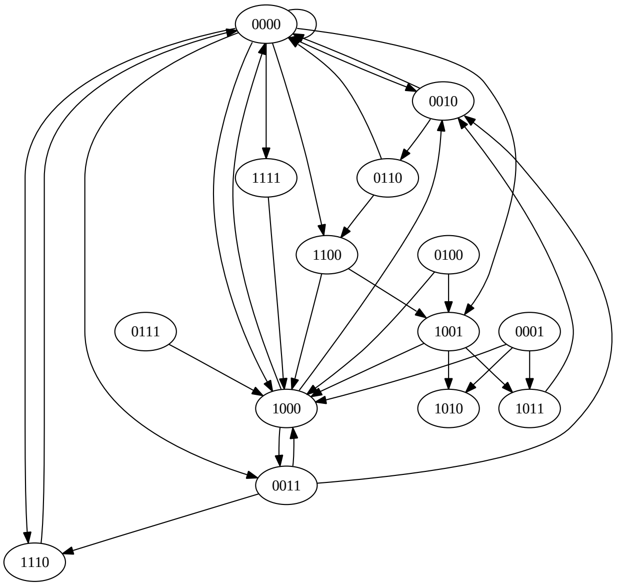

Figure 3: Graph G_2 of Transitions

The first graph G_1 is for $r \in \{1, 2, \ldots \ell\}$. The four equations governing the transition will alternate between (17) and (18). The graph G_1 (Figure 2) shows all allowable transitions, and paths give us all possible solutions for $j_1, \ldots, j_{\ell+4}$.

The graph G_2 (Figure 3) does the same job for determining all solutions for $j_{\ell+5}, \ldots j_{n-1}$. The start vertex in G_2 must be the ending vertex of the path in G_1.

Finally, the ending vertex of the path in G_2 must link back to the starting vertex in G_1, satisfying the equations for $r = n-4, n-3, n-2, n-1, 0$. These are all the equations involving j_0.

Let $v_s(P)$ denote the first vertex of a path P, and let $v_e(P)$ denote the last vertex.

Theorem 7 *Let $n \equiv 1 \pmod 4$ and $\ell = n - e \equiv 0 \pmod 4$. There is a one-to-one correspondence between representatives from cyclotomic cosets in the J-set, and pairs (P_1, P_2), where P_1 is a path in G_1 of length $\ell/4 - 1$ and P_2 is a path* *in G_2 of length $(n-1-\ell)/4$, such that*

1. $v_e(P_1) = v_s(P_2)$
2. *there exists a path from $v_e(P_2)$ to $v_s(P_1)$ consistent with the $r = n-4, n-3, n-2, n-1, 0$ equations.*

Example Take $n = 13$, $e = k = 1$, and $d = 11$. Here $\ell = n-1$ so we are only interested in paths of length 2 in G_1 and G_2 is not involved at all. There are three paths satisfying Theorem 7:

$$\begin{array}{ll} 0000 \longrightarrow 1000 \longrightarrow 1000 & (j_0 = 1) \\ 0000 \longrightarrow 1010 \longrightarrow 0010 & (j_0 = 1) \\ 0110 \longrightarrow 1000 \longrightarrow 1000 & (j_0 = 1). \end{array}$$

yielding three elements in the J-set, which up to cyclotomy are $\{273, 325, 557\}$.

8 Gross-Koblitz's Formula and the K-Set

Let us denote by ν the minimal dyadic valuation of the Fourier coefficient of the power mapping x^d. By section 2, we know that $\nu = M_d$. The goal of this section is to study the dyadic expansion of the Fourier coefficients, and thus to describe the Boolean functions f_0 and f_1 such that :

$$\widehat{f}(a) = 2^{\nu}\big(f_0(a) + f_1(a)2^1 + \cdots\big) \tag{21}$$

As we saw, ν and f_0 are connected to the J-set of d. The determination of f_1 will depend on the *K-set* of d :

$$K_d = \{j \mid \mathrm{wt}_2(j) + \mathrm{wt}_2(-jd) = M_d + 1\}.$$

The Gross-Koblitz formula [5, 10] claims that, for any residue j modulo $2^n - 1$, the following equality holds:

$$\tau(\bar{\omega}^j) = (-2)^{\mathrm{wt}_2(j)} \prod_{i=0}^{n-1} \Gamma\big(1 - \langle \frac{2^i j}{2^n - 1} \rangle\big) \tag{22}$$

where $\langle x \rangle$ is the fractional part of x, and Γ the dyadic Gamma function. The dyadic Gamma function is defined over $\mathbf{N}$ the set of positive integers by

$$\forall k \in \mathbf{N}, \quad \Gamma(k) = (-1)^k \prod_{\substack{j < k \\ j \text{ odd}}} j. \tag{23}$$

If x and y are two positive integers such that $x \equiv y \pmod{2^k}$ then $\Gamma(x) \equiv \Gamma(y) \pmod{2^k}$. The dyadic Γ function is extended by continuity over the ring of dyadic numbers i.e.

$$\forall s \in \mathbf{Z}_2, \quad \Gamma(s) = \lim_{\mathbf{N} \ni k \to s} \Gamma(k).$$

In particular,

$$\Gamma((1-\langle\frac{j}{2^n-1}\rangle)) \equiv \Gamma(1+j_0+2j_1) \pmod 4, \tag{24}$$

where $j_0+2j_1+\dots$ in the dyadic expansion of j. Note that an empty product in (23) is equal to 1. The first values of the dyadic Gamma function are: $\Gamma(0)=1$, $\Gamma(1)=-1$, $\Gamma(2)=+1$, $\Gamma(3)=-1$, and $\Gamma(4)=3\equiv -1 \pmod 4$. In other words, for all bits $u,v\in\{0,1\}$, we have $\Gamma(1+u+2v)\equiv(-1)^{1+u+uv} \pmod 4$ and the following congruence holds

$$\Gamma((1-\langle\frac{j}{2^n-1}\rangle)) \equiv \Gamma(1+j_0+2j_1) \equiv (-1)^{1+j_0+j_0j_1} \pmod 4. \tag{25}$$

It follows that

$$\begin{aligned}\tau(\bar\omega^j) &\equiv (-2)^{\mathrm{wt}_2(j)}(-1)^n(-1)^{\mathrm{wt}_2(j)}(-1)^{Q(j)}\\ &\equiv (-1)^n 2^{\mathrm{wt}_2(j)}(-1)^{Q(j)} \pmod{2^{\mathrm{wt}_2(j)+2}}\end{aligned}$$

where $Q(j)=j_0j_1+j_1j_2+\cdots+j_{n-1}j_0$ is the number of consecutive pairs of ones in the dyadic expansion of j.

Let us denote by g the Boolean function defined by

$$\sum_{j\in J_d}\bar\omega(a)^{jd} \equiv f_0(a)+2g(a) \pmod 4. \tag{26}$$

Then

$$g(a) \equiv \sum_{\substack{j<k\\ j,k\in J_d}} \bar\omega(a)^{(j+k)d} \pmod 2. \tag{27}$$

Indeed, squaring (26) we obtain:

$$2\sum_{\substack{j<k\\ j,k\in J_d}} \bar\omega(a)^{(j+k)d} + \sum_{j\in J_d}\bar\omega(a)^{jd} \equiv f_0(a) \pmod 4 \tag{28}$$

and so

$$2\sum_{\substack{j<k\\ j,k\in J_d}} \bar\omega(a)^{(j+k)d} + 2g(a) \equiv 0 \pmod 4. \tag{29}$$

Now, if we introduce the set $J'_d=\{j\in J_d \mid Q(j)=1\}$, we obtain the complete description of $f_1(a)$ as :

$$f_1(a)=\sum_{j\in K}\bar\omega^{jd}(a)+\sum_{j\in J'_d}\bar\omega^{jd}(a)+\sum_{\substack{j<k\\ j,k\in J_d}}\bar\omega^{(j+k)d}(a).$$

As a first consequence, the degree of f_0 is less than ν, and the degree of f_1 is less than $2\nu-1$.

9 An Application to Gold Exponents

Now, we propose to use the theory developed in the preceding section to re-find a recent result of Lahtonen, McGuire and Ward [6] concerning the sign of the Fourier coefficient at 1 of the Gold exponent (the result for the Kasami-Welch exponent is also proved). This result for the Gold exponent is also stated in the appendix of [1].

Let n be odd, k be an integer coprime to n, and $d = 2^k + 1$. Let us denote by f the Gold mapping $f(x) = \mu(x^{2^k+1})$. The Fourier coefficient at one of f satisfies

$$\widehat{f}(1) = \begin{cases} +2^{(n+1)/2}, & n \equiv \pm 1 \pmod{8}, \\ -2^{(n+1)/2}, & n \equiv \pm 3 \pmod{8}. \end{cases} \tag{30}$$

Note that

$$\widehat{f}(1) > 0 \Longleftrightarrow \sharp K_d \equiv \sharp J'_d \pmod{2}.$$

Indeed, the sign of $\widehat{f}(a)$ is completely determined by the value of $f_0(a) + 2f_1(a)$. In the case of $a = 1$, we get :

$$f_0(1) + 2f_1(1) \equiv (\sharp J_d)^2 + 2\sharp K_d + 2\sharp J'_d \pmod{4}.$$

9.1 J-Set

For the computation of the J-set and K-set in the Gold case we restricted ourselves without loss of generality to the case where the inverse e of k modulo n is even.

The fundamental equation for the Gold exponent $d = 2^k + 1$ is

$$2c_i + s_i = j_i + j_{i-k} + c_{i-1}$$

where in this case the carries are usual bits, i.e. $c_i \in \{0, 1\}$. In particular we have the following relation

$$\mathrm{wt}_2(c) + \mathrm{wt}_2((2^k + 1)j) = 2\mathrm{wt}_2(j). \tag{31}$$

As it has been shown in [4] for the Gold case we get $M_d = (n+1)/2$ and therefore the J-set is characterized by

$$j \in J_d \quad \Leftrightarrow \quad \mathrm{wt}_2(j) + \mathrm{wt}_2(-dj) = (n + 1)/2.$$

In particular we have $\mathrm{wt}_2(j) < (n + 1)/2$. From equation (31) it follows that $\mathrm{wt}_2(dj) \leq 2\mathrm{wt}_2(j)$ with equality iff all carry bits are zero. Thus we get

$$(n + 1)/2 = \mathrm{wt}_2(j) + \mathrm{wt}_2(-dj) = \mathrm{wt}_2(j) + n - \mathrm{wt}_2(dj) \geq n - \mathrm{wt}_2(j).$$

This implies $\mathrm{wt}_2(j) \geq (n-1)/2$, and therefore $\mathrm{wt}_2(j) = (n-1)/2$. But this means nothing else than $\mathrm{wt}_2(-dj) = 1$. Thus in the Gold case the J-set consists of a single cyclotomic coset, or more precisely,

$$J_d = \left\{ -\frac{2^i}{2^k+1} \ : \ i \in \{0, \dots, n-1\} \right\}.$$

In order to use the ideas developed in the previous section, we have to compute

$$\sharp J'_d = Q\left(-\frac{1}{2^k+1}\right) \bmod 2.$$

For this note that, as we do not get any non-zero carry, in the k-ordering of the bits j_i we do not have any consecutive ones. Furthermore, due to cyclotomic equivalence, we can assume that in the k-ordering we have

$$j_0, j_k, j_{2k}, \dots, j_{(n-1)k} = 0, 0, 1, 0, 1, 0, \dots, 1, 0, 1.$$

In other words, we can assume that $j_i = 1$ if and only if there exist $t \in \{1, \dots, (n-1)/2\}$ such that $i = 2kt$.

To compute $Q(j)$ we have to compute the number of consecutive ones in the normal ordering, i.e. the number of indices i such that $j_i = 1$ and $j_{i+1} = 1$. This corresponds to the number of solutions $t, t' \in \{1, \dots, (n-1)/2\}$ such that

$$2kt \equiv 2kt' + 1 \pmod{n},$$

which implies

$$t - t' \equiv \frac{e}{2} \pmod{n}.$$

Due to the restriction $t, t' \in \{1, \dots, (n-1)/2\}$ and the assumption that e is even, this number can easily be computed to be $(n-1)/2 - e/2$. The following lemma summarizes these results.

Lemma 6 *Let $d = 2^k + 1$ with $ke \equiv 1 \pmod{n}$ and e even. The J-set corresponds to the cyclotomic class of*

$$\tilde{j} = -\frac{1}{d}$$

and we have

$$Q(\tilde{j}) = ((n-1)/2 - e/2) \bmod 2.$$

9.2 K-Set

Using the same arguments as for the J-set, it is easy to see that elements in the set

$$K = \left\{ j \ : \ \mathrm{wt}_2(j) + \mathrm{wt}_2(-(2^k+1)j) = \frac{n+3}{2} \right\}$$

can only have two possible weights and we split the set accordingly into two subsets $K = K_1 \cup K_2$ where

$$K_1 = \left\{ j \in K \ : \ \mathrm{wt}_2(j) = \frac{n-3}{2} \right\}$$

and

$$K_2 = \left\{ j \in K \ : \ \mathrm{wt}_2(j) = \frac{n-1}{2} \right\}$$

which we treat separately.

Size of K_1 Elements of K_1 have weight $\frac{n-3}{2}$ and therefore we have $n-3 = \mathrm{wt}_2((2^k+1)j) = 2\mathrm{wt}_2(j)$, which implies that all carries c_i are zero (see equation (31)). Thus, in the k-ordering, we have to count the number of bit-strings of length n and weight $\frac{n-3}{2}$ with no consecutive ones. Using elementary combinatorics the size of K_1 can be shown to be

$$\sharp K_1 = \binom{\frac{n+1}{2}}{3} + \binom{\frac{n+3}{2}}{3}.$$

Size of K_2 Elements of K_2 have weight $\frac{n-1}{2}$, which implies that all but one carries c_i are zero and exactly one carry equals one. Again considering the k-ordering, we have exactly two consecutive bits. Due to cyclotomic equivalence we can assume that $j_0 = j_r = 1$. In this case having exactly one non-zero carry implies that $j_1 = j_{r+1} = 0$ and $j_{k(n-1)} = j_{2k} = 0$. The remaining positions have to be filled with $\frac{n-5}{2}$ ones and $\frac{n-7}{2}$ zeros with the restriction that there are no additional consecutive ones. This gives $\frac{n-e-3}{2}$ possibilities and therefore, including cyclotomic equivalent elements we get

$$\sharp K_2 = \frac{n-e-3}{2} n$$

Computing $(\sharp J'_d + \sharp K) \bmod 2$ we get

$$\begin{aligned}
\sharp J'_d + \sharp K &= Q(\widetilde{j}) + \sharp K \pmod 2 \\
&= Q(\widetilde{j}) + \sharp K_1 + \sharp K_2 \pmod 2 \\
&\equiv \frac{n-1-e}{2} + \sharp K_1 + \frac{n-e-3}{2} n \pmod 2 \\
&\equiv \sharp K_1 \pmod 2 \\
&= \binom{\frac{n+1}{2}}{3} + \binom{\frac{n+3}{2}}{3} \pmod 2 \\
&\equiv \begin{cases} 0, & n \equiv \pm 1 \pmod 8 \\ 1, & n \equiv \pm 3 \pmod 8 \end{cases}
\end{aligned}$$

and this is equivalent to (30).

References

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

[2] J. F. Dillon. Multiplicative difference sets via additive characters. *Designs, Codes and Cryptography*, 17:225–235, 1999.

[3] H. Dobbertin. Another proof of Kasami's theorem. *Designs, Codes and Cryptography*, 17(1–3), 1999.

[4] H. D. L. Hollmann and Q. Xiang. A proof of the Welch and Niho conjectures on crosscorrelations of binary m-sequences. *Finite Fields and their Applications*, 7(2):253–286, 2001.

[5] N. Koblitz. *p-adic Analysis: a Short Course on Recent Work.* Number 46 in London Mathematical Society Lecture Note Series. Cambridge University Press, 1980.

[6] J. Lahtonen, G. McGuire, and H. N. Ward. Gold and Kasami-Welch functions, quadratic forms and bent functions. *Advances in Mathematics of Communications*, 1(2):243–250, 2007.

[7] P. Langevin and G. Leander. Monomial bent functions and Stickelberger's theorem. *Finite Fields and their Applications*, 14(3):727–742, 2008.

[8] P. Langevin and P. Véron. On the non-linearity of power functions. *Designs, Codes and Cryptography*, 37(1):31–43, 2005.

[9] R. Lidl and H. Niederreiter. *Finite Fields.* Addison-Wesley, 1983.

[10] A. Robert. The Gross-Koblitz formula revisited. *Rendiconti del Seminario Matematico della Universit di Padova*, 105:157–170, 2001.