The Second Support Weight Distribution of the Kasami Codes

Hans Georg Schaathun, *Member, IEEE,* and Tor Helleseth, *Fellow, IEEE*

***Abstract*—We compute the second support weight distribution of the Kasami codes.**

***Index Terms*—Kasami code, support weight distribution.**

I. Introduction

The support weight distribution (SWD) of linear codes was introduced by Helleseth, Kløve, and Mykkeltveit [1]. From the SWD of a single code, they were able to determine the weight distribution of a corresponding infinite class of codes. After the introduction of the related weight hierarchy in [2], this problem received renewed interest, and in recent years, the SWD's of particular codes [3], [4] and dual codes [5]–[7] have been studied. In this correspondence, we give a short and simple calculation of the second SWD of the Kasami codes.

II. Preliminaries

Let $\mathsf{GF}(q)$ be the finite field of q elements and $\mathsf{GF}(q)^n$ a vector space of dimension n with a fixed coordinate basis. An $[n,k]$ code C over $\mathsf{GF}(q)$ is a k-dimensional subspace of $\mathsf{GF}(q)^n$. For any vector $\boldsymbol{x} \in \mathsf{GF}(q)$, the support $\chi(\boldsymbol{x})$ is defined as the set of coordinate positions where $\boldsymbol{x}$ is nonzero. For a subset $S \subseteq \mathsf{GF}(q)^n$, the support $\chi(S)$ is the union of supports of the members of S. The weight $w(\boldsymbol{x})$ or $w(S)$ of an element or a set is the cardinality of its support.

The weight hierarchy of a code C is the sequence $(d_1, \ldots, d_k)$, where d_r is the smallest weight of any r-dimensional subcode of C. The support weight distribution of C is the array of parameters A_i^r where $0 \leq i \leq n$ and $0 \leq r \leq k$, defined as the number of r-dimensional subcodes of C with weight i.

Let T_m denote the Froebenius trace from $\mathsf{GF}(q^m)$ to $\mathsf{GF}(q)$, defined as

$$T_m(x) = \sum_{i=0}^{m-1} x^{q^i}.$$

It is well known that

$$T_m(x+y) = T_m(x) + T_m(y)$$
$$T_m(x) = T_m(x^q)$$

and if x runs through $\mathsf{GF}(q^m)$, then $T_m(x)$ takes each value in $\mathsf{GF}(q)$ exactly q^{m-1} times. The original Kasami code is a binary code, so throughout the correspondence, we let $q = 2$ and write $Q = 2^m$. Thus,

$$T_m : \mathsf{GF}(Q) \to \mathsf{GF}(2) \quad \text{and} \quad T_{2m} : \mathsf{GF}(Q^2) \to \mathsf{GF}(2).$$

Definition 1 (The Kasami Codes): The Kasami code with parameters $[2^{2m}-1, 3m, 2^{2m-1}-2^{m-1}]$ is the set

$$\mathcal{K}_m = \left\{ \boldsymbol{c}(a,b) : a \in \mathsf{GF}(Q^2), b \in \mathsf{GF}(Q) \right\}$$

where

$$\boldsymbol{c}(a,b) = \left(T_{2m}(ax) + T_m(bx^{Q+1}) : x \in \mathsf{GF}(Q^2)^* \right).$$

The Kasami codes have three different nonzero weights, given by the following lemma.

Lemma 1 ([8]): The weight of a codeword $\boldsymbol{c}(a,b) \in \mathcal{K}_m$ is given by

$$w(\boldsymbol{c}(a,b)) = \begin{cases} d_1 := 2^{2m-1} - 2^{m-1}, & \text{if } b \neq 0 \text{ and } T_m(a^{Q+1}/b) = 1 \\ m_1 := 2^{2m-1} + 2^{m-1}, & \text{if } b \neq 0 \text{ and } T_m(a^{Q+1}/b) = 0 \\ w_1 := 2^{2m-1}, & \text{if } b = 0 \text{ and } a \neq 0 \\ 0, & \text{if } b = 0 \text{ and } a = 0. \end{cases}$$

Remark 1: Given a nonzero $b \in \mathsf{GF}(Q)$, there are 2^{m-1} choices for a^{Q+1} giving $w(\boldsymbol{c}(a,b)) = d_1$ and as many for m_1. For each nonzero value of a^{Q+1}, there are $(2^{2m}-1)/(2^m-1) = 2^m + 1$ choices for a. Hence, the number of codewords $\boldsymbol{c}(a,b)$ for b fixed of minimum and maximum weight are determined by

$$\begin{aligned} \#\{a : T_m(a^{Q+1}) = 1\} &= (2^m+1) \cdot 2^{m-1} \\ \#\{a : T_m(a^{Q+1}) = 0\} &= (2^m+1) \cdot (2^{m-1}-1) + 1 \\ &= 2^{m-1}(2^m - 1). \end{aligned}$$

The weight hierarchy of $\mathcal{K}_m$ was studied in [8], and we will need several lemmas therefrom. Let $\gamma \in \mathsf{GF}(Q^2)$, and define

$$V_\gamma := \{\boldsymbol{c}(\gamma b, b^2) : b \in \mathsf{GF}(Q)\}.$$

Observe that V_γ is a subcode of dimension m.

Lemma 2 ([8]): All the nonzero words of V_γ have the same weight, which is d_1 if $T_m(\gamma^{Q+1}) = 1$ and m_1 if $T_m(\gamma^{Q+1}) = 0$.

Define

$$f(\gamma, a) := \gamma^{2Q} a^2 + \gamma^2 a^{2Q} + a^{Q+1}.$$

Lemma 3: Let $a \in \mathsf{GF}(Q^2)$. If $f(\gamma,a) \neq 0$ and $T_m(\gamma^{Q+1}) = 0$, then the coset $V_\gamma + \boldsymbol{c}(a,0)$ contains $2^{m-1}-1$ words of weight m_1, 2^{m-1} words of weight d_1, and one word of weight w_1.

This lemma is analogous to [8, Lemma 7(ii)], but assuming $T_m(\gamma^{Q+1}) = 0$ instead of equal to one.

Lemma 4: If $T_m(\gamma^{Q+1}) = 0$, then $f(\gamma,a) \neq 0$ for all $a \neq 0$.

Proof: Clearly, the only solution of $f(a,\gamma) = 0$ when $\gamma = 0$ is $a = 0$, so suppose $\gamma \neq 0$ for the rest of the proof. Suppose there is nonzero $a \in \mathsf{GF}(Q^2)$ such that $f(\gamma,a) = 0$. Then

$$\gamma^2 a^{2(Q-1)} + \gamma^{2Q} + a^{Q-1} = 0, \qquad a^{Q^2-1} = 1$$

and writing $z = a^{Q-1}$, z we get that

$$\gamma^2 z^2 + z + \gamma^{2Q} = 0, \qquad z^{Q+1} = 1. \tag{1}$$

Setting $u = \gamma^2 z$ and multiplying by γ^2, we get that (1) is equivalent to

$$u^2 + u + \gamma^{2(Q+1)} = 0, \qquad u^{Q+1} = \gamma^{2(Q+1)}. \tag{2}$$

Manuscript received April 27, 2004; revised December 21, 2004. This work was supported by the Norwegian Research Council (NFR) under Grant 146874/420 and by the Aurora program.

The authors are with the Selmer Centre, Department of Informatics, University of Bergen, PB 7800, N-5020 Bergen, Norway (e-mail: georg@ii.uib.no; tor.helleseth@ii.uib.no).

Communicated by A. E. Ashikhmin, Associate Editor for Coding Theory.
Digital Object Identifier 10.1109/TIT.2005.851770

TABLE I
THE SECOND SWD OF THE KASAMI CODES

A_i^2	i
$\frac{(2^m-1)(2^{m-1}-1)}{3}\left((2^{2m}-1)(2^{2m}-2^{m-1}(7\cdot 2^{m-2}-1))+2^{m-1}(2^m+1)\right)$	$3(2^{2m-2}-2^{m-2})$
$2^{m-2}(2^m-1)(2^m+1)((2^m+1)2^{m-1}-1)$	$3\cdot 2^{2m-2}-2^{m-1}$
$2^{m-1}(2^m-1)(2^{2m}-1)2^{m-1}(2^{m-1}-1)/2$	$3\cdot 2^{2m-2}-2^{m-2}$
$2^{5m-2}-\frac{2^{4m-2}-1}{3}-2^{3m-2}-2^{2m-2}$	$3\cdot 2^{2m-2}$
$2^{m-1}(2^m-1)(2^{2m}-1)2^{m-1}(2^{m-1}-1)/2$	$3\cdot 2^{2m-2}+2^{m-2}$
$2^{m-2}\cdot(2^m-1)^2(2^m+1)(2^{m-1}-1)$	$3\cdot 2^{2m-2}+2^{m-1}$
$\frac{(2^m-1)(2^{m-1}-1)}{3}\left(2^{m-1}(2^{2m}-1)(2^{m-2}-1)+2^{m-1}(2^m-1)\right)$	$3(2^{2m-2}+2^{m-2})$

Set $b=\gamma^{2(Q+1)}$. From (2), we get that $u^2=u+b$, which is, by repeated squaring and multiplication by u, equivalent to

$$u^{2^m+1}=u^2+T_m(b)u$$

which is equal to $\gamma^{2(Q+1)}$ if and only if $T_m(b)=1$ by Lemma 2. This proves the lemma. □

III. SECOND SUPPORT WEIGHT DISTRIBUTION

Consider the two-dimensional subcodes of $\mathcal{K}_m$. There are essentially eight types of such subcodes, which we denote by the weights of the three nonzero words as follows: $w.w.w$, $w.d.d$, $w.d.m$, $w.m.m$, $d.d.d$, $d.d.m$, $d.m.m$, and $m.m.m$. Let $B_{x.x.x}$ denote the number of subcodes of type $x.x.x$, and let A_i^2 be the number of two-dimensional subcodes of weight i. We distinguish four different cases. Let $B_{x.x.x}^y$ denote the number of subcodes of type $x.x.x$ resulting from case y.

Let $D=\langle \boldsymbol{a},\boldsymbol{b}\rangle$ be a two-dimensional subcode, where $\boldsymbol{a}=\boldsymbol{c}(a_1,b_1)$ and $\boldsymbol{b}=\boldsymbol{c}(a_2,b_2)$ and $\boldsymbol{a}+\boldsymbol{b}=\boldsymbol{c}(a_3,b_3)$. Recall that $a_3=a_1+a_2$ and $b_3=b_1+b_2$.

Case 1: $b_1=b_2=b_3=0$.

The words of weight 2^{m-1} are $\boldsymbol{c}(a,0)$ where $a\neq 0$. So if D has three words of weight 2^{m-1} it must be one of the $(2^{2m}-1)(2^{2m-1}-1)/3$ two-dimensional subcodes contained in $\{\boldsymbol{c}(a,0): a\in \mathsf{GF}(2^{2m})\}$

$$B_{w.w.w}^1=(2^{2m}-1)(2^{2m-1}-1)/3.$$

Case 2: $b_1=b_2\neq 0, b_3=0$.

There are 2^m-1 choices for b_1. We have three possibilities, 1) $w(\boldsymbol{a})=w(\boldsymbol{b})=d_1$, 2) $w(\boldsymbol{a})=w(\boldsymbol{b})=m_1$, and 3) $w(\boldsymbol{a})=d_1$ whereas $w(\boldsymbol{b})=m_1$. For 1) and 2), $\boldsymbol{a}$ and $\boldsymbol{b}$ may be interchanged, so each possibility is counted twice. The number of a values giving each weight is found by Remark 1

$$\begin{aligned}B_{w.d.d}^2&=2^{m-2}(2^m-1)(2^m+1)((2^m+1)2^{m-1}-1)\\ B_{w.d.m}^2&=2^{2m-2}(2^{2m}-1)(2^m-1)\\ B_{w.m.m}^2&=2^{m-2}(2^m-1)^2(2^m+1)(2^{m-1}-1).\end{aligned}$$

Cases 3–4: b_1,b_2,b_3 distinct.

Define $\gamma_i=a_i/\sqrt{b_i}$. Observe that $\sqrt{b_3}=\sqrt{b_1}+\sqrt{b_2}$, because $(x+y)^2=x^2+y^2$ in characteristic 2. It follows that if $\gamma_1=\gamma_2$, then

$$a_3=\gamma_3\sqrt{b_3}=\gamma_1(\sqrt{b_1}+\sqrt{b_2})=\gamma_1\sqrt{b_3}$$

so $\gamma_3=\gamma_1$ as well.

Case 3: $\gamma_1=\gamma_2=\gamma_3$.

In this case, $D\subseteq V_{\gamma_1}$. So either D has three words of weight m_1 or three of weight d_1. There are $(2^m-1)(2^{m-1}-1)/3$ possible two-dimensional subcodes for each choice of γ_1; and the number of γ_1 values for each weight is found in Remark 1

$$\begin{aligned}B_{d.d.d}^3&=\frac{(2^m-1)(2^{m-1}-1)}{3}2^{m-1}(2^m+1)\\ B_{m.m.m}^3&=\frac{(2^m-1)(2^{m-1}-1)}{3}2^{m-1}(2^m-1).\end{aligned}$$

Case 4: Distinct $\gamma_1,\gamma_2,\gamma_3$.

In this case, there is an $a'\in\mathsf{GF}(Q^2)$ such that

$$\begin{aligned}\boldsymbol{c}(a_1,b_1)&\in V_{\gamma_3}+\boldsymbol{c}(a',0)\\ \boldsymbol{c}(a_2,b_2)&\in V_{\gamma_3}+\boldsymbol{c}(a',0)\\ \boldsymbol{c}(a_3,b_3)&\in V_{\gamma_3}.\end{aligned}$$

The subcode D is chosen by the following procedure.

1. Choose γ_3. There are 2^{2m} possibilities.
2. Choose $a'\neq 0$. There are $2^{2m}-1$ possibilities.
3. Choose an unordered pair of points $b_1,b_2\in\mathsf{GF}(Q)^*$, which defines uniquely a pair of distinct points in $V_{\gamma_3}+\boldsymbol{c}(a',0)$. There are $(2^m-1)(2^{m-1}-1)$ possibilities.

Consider the case where $T_m(\gamma_3^{Q+1})=0$, which implies that $w(\boldsymbol{c}(a_3,b_3))=m_1$. By Remark 1, there are $(2^m-1)2^{m-1}$ appropriate choices of γ_3. By Lemmas 3 and 4, for any $a'\neq 0, V_{\gamma_3}+\boldsymbol{c}(a',0)$ has $2^{m-1}-1$ words of weight d_1 and 2^{m-1} words of weight m_1. Thus, there are $2^{2m-2}-2^{m-1}$ pairs (b_1,b_2) giving one word of weight d_1 and one of weight m_1. There are $(2^{m-1}-1)(2^{m-2}-1)$ pairs where both words have weight d_1, and $2^{m-2}(2^{m-1}-1)$ where both have weight m_1. Each subcode has been counted once for each maximum weight word it contains, since any such word may be $\boldsymbol{c}(a_3,b_3)$. Thus, we get

$$\begin{aligned}B_{d.d.m}^4&=2^{m-1}(2^m-1)(2^{2m}-1)(2^{m-1}-1)2^{m-2}\\ B_{d.m.m}^4&=2^{m-1}(2^m-1)(2^{2m}-1)2^{m-1}(2^{m-1}-1)/2\\ B_{m.m.m}^4&=\frac{2^{m-1}(2^m-1)(2^{2m}-1)(2^{m-1}-1)(2^{m-2}-1)}{3}.\end{aligned}$$

The number of subcodes with three words of weight d_1 is computed as

$$B_{d.d.d}^4=T-B_{d.d.m}^4-B_{d.m.m}^4-B_{m.m.m}^4$$

where T is the number of words for Case 4, i.e.,

$$T=(2^{4m}-2^{2m})(2^m-1)(2^{m-1}-1)/3.$$

This gives us

$$B_{d.d.d}^4=\frac{(2^{2m}-1)(2^m-1)(2^{m-1}-1)}{3}\cdot(2^{2m}-2^{m-1}(7\cdot 2^{m-2}-1)).$$

To find the weight for each subcode type, and thereby to find the SWD, we need the following lemma.

Lemma 5 ([8]): Let D be an r-dimensional subcode of C. Then

$$w(D)=\frac{1}{2^{r-1}}\sum_{\boldsymbol{c}\in D}w(\boldsymbol{c}).$$

Observe that types $w_1.w_1.w_1$ and $w_1.d_1.m_1$ have the same support weight, whereas the other types have distinct weights. Adding the different cases, we obtain the following theorem.

TABLE II
THE SECOND SWD FOR SOME SMALL KASAMI CODES

$m=2$		$m=3$		$m=4$		$m=5$	
w	A_w	w	A_w	w	A_w	w	A_w
9	70	42	5 544	180	361 760	744	22 915 200
10	135	44	4 410	184	137 700	752	4 312 968
11	90	46	10 584	188	856 800	760	60 888 960
12	215	48	7 707	192	255 595	768	8 292 779
13	90	50	10 584	196	856 800	776	60 888 960
14	45	52	2 646	200	107 100	784	3 805 560
15	6	54	1 960	204	218 400	792	17 836 160

Theorem 1: The second support weight distribution of the $[2^{2m}-1, 3m, 2^{2m-1}-2^{m-1}]$ Kasami code is given by the expressions in Table I.

We have verified the second SWD for some small Kasami codes by computer, and these numbers are shown in Table II.

It appears to be more difficult to determine higher order support weight distributions completely. The most difficult case is probably when all the γ_i are distinct. For instance, studying a three-dimensional subcode, we have one nonzero word in V_{γ_1} and two words in each of three cosets $V_{\gamma_1}+\boldsymbol{c}(a_1,0)$, $V_{\gamma_1}+\boldsymbol{c}(a_2,0)$, and $V_{\gamma_1}+\boldsymbol{c}(a_1+a_2,0)$. Since only three out of the six coset points may be chosen freely, it is not obvious how to divine the weights of the remaining three. Maybe it can be done in combination with other methods.

REFERENCES

[1] T. Helleseth, T. Kløve, and J. Mykkeltveit, "The weight distribution of irreducible cyclic codes with block lengths $n_1((q^l-1)/n)$," *Discr. Math.*, vol. 18, pp. 179–211, 1977.

[2] V. K. Wei, "Generalized Hamming weights for linear codes," *IEEE Trans. Inf. Theory*, vol. 37, no. 5, pp. 1412–1418, Sep. 1991.

[3] O. Milenkovic, S. T. Coffey, and K. J. Compton, "The third support weight enumerators of the doubly-even, self-dual $[32, 16, 8]$ codes," *IEEE Trans. Inf. Theory*, vol. 49, no. 3, pp. 740–746, Mar. 2003.

[4] S. Dougherty, A. Gulliver, and M. Oura, "Higher weights and graded rings for binary self-dual codes," *Discr. Appl. Math.*, vol. 128, pp. 251–261, 2003.

[5] H. G. Schaathun, "Duality and support weight distibutions," *IEEE Trans. Inf. Theory*, vol. 50, no. 5, pp. 862–867, May 2004.

[6] T. Kløve, "Support weight distribution of linear codes," *Discr. Math.*, vol. 106/107, pp. 311–316, 1992.

[7] J. Simonis, "The effective length of subcodes," *Appl. Algebra Engrg. Comm. Comput.*, vol. 5, no. 6, pp. 371–377, 1994.

[8] T. Helleseth and P. V. Kumar, "The weight hierarchy of the Kasami codes," *Discr. Math.*, vol. 145, no. 1–3, pp. 133–143, 1995.

Quasi-Cyclic LDPC Codes for Fast Encoding

Seho Myung, Kyeongcheol Yang, *Member, IEEE*, and Jaeyoel Kim

***Abstract*—In this correspondence we present a special class of quasi-cyclic low-density parity-check (QC-LDPC) codes, called block-type LDPC (B-LDPC) codes, which have an efficient encoding algorithm due to the simple structure of their parity-check matrices. Since the parity-check matrix of a QC-LDPC code consists of circulant permutation matrices or the zero matrix, the required memory for storing it can be significantly reduced, as compared with randomly constructed LDPC codes. We show that the girth of a QC-LDPC code is upper-bounded by a certain number which is determined by the positions of circulant permutation matrices. The B-LDPC codes are constructed as irregular QC-LDPC codes with parity-check matrices of an almost lower triangular form so that they have an efficient encoding algorithm, good noise threshold, and low error floor. Their encoding complexity is linearly scaled regardless of the size of circulant permutation matrices.**

***Index Terms*—Block cycle, circulant permutation matrix, efficient encoding, low-density parity-check (LDPC) codes, quasi-cyclic codes.**

I. INTRODUCTION

Low-density parity-check (LDPC) codes—first discovered by Gallager [7] and rediscovered by Sipser *et al.* [13] and MacKay *et al.* [10], [11]—have created much interest recently since they are shown to have a remarkable performance close to the Shannon limit over additive white Gaussian noise (AWGN) channels [14]. LDPC codes possess many advantages including parallelizable decoding, self-error-detection capability by syndrome check, an asymptotically better performance than turbo codes, etc. Many coding theorists have brought new developments in the construction and decoding schemes of LDPC codes with low complexity for their commercial use in the past few years.

Richardson *et al.* introduced a method to design LDPC codes that perform extremely close to the Shannon capacity for sufficiently large code length under the assumption of no cycles [14]. They computed the threshold of noise level for a large class of binary-input channels by *density evolution*, and presented some simulation results for proving their claims. Here, the threshold of noise level means the maximum noise level to obtain the zero error probability as the block length tends to infinity. To find an ensemble which has larger threshold than that of the conventional ensemble of LDPC codes, Kasai *et al.* introduced *detailedly represented* irregular LDPC codes [8] and Richardson and Urbanke introduced *multi-edge type* LDPC codes [16]. They are obtained by representing the degree distribution according to the type of the edges.

Density evolution is a useful tool to obtain the asymptotical performance of LDPC codes, but not to estimate their performance in the case of finite length. In other words, it is not guaranteed that finite-length LDPC codes with degree distribution suggested by density evolution have good performance. The performance of LDPC codes of

Manuscript received April 27, 2004; revised October 23, 2004. This work was supported in part by the Center for Broadband OFDM Mobile Access (BrOMA) at the Pohang University of Science and Technology (POSTECH) supported by the ITRC program of the Korean Ministry of Information and Communication (MIC) under the supervision of the Institute of Information Technology Assessment (IITA).

S. Myung and K. Yang are with the Department of Electronics and Electrical Engineering, Pohang University of Science and Technology (POSTECH), Pohang, Kyungbuk 790-784, Korea (e-mail: kcyang@postech.ac.kr).

J. Kim is with Samsung Electronics Co., Ltd., Suwon, 416, Maetan-3 dong, Yeongtong-gu, Suwon, Gyeonggi, 442-742, Korea (kimjy@samsung.com).

Communicated by M. P. C. Fossorier, Associate Editor for Coding Techniques.

Digital Object Identifier 10.1109/TIT.2005.851753