The second support weight distribution of the Kasami codes

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

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

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

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], [6], [7] have been studied. In this paper we give a short and simple calculation of the second SWD of the Kasami codes.

I. 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 $\mathbf{x} \in \mathsf{GF}(q)$, the support $\chi(\mathbf{x})$ is defined as the set of coordinate positions where $\mathbf{x}$ is non-zero. 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 $w(\mathbf{x})$ 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 $0 \le i \le n$ and $0 \le r \le k$, 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 paper, we let $q = 2$ and write $Q = 2^m$. Thus $T_m : \mathsf{GF}(Q) \to \mathsf{GF}(2)$ and $T_{2m} : \mathsf{GF}(Q^2) \to \mathsf{GF}(2)$.

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

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

where

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

The Kasami codes have three different non-zero weights, given by the following lemma.

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

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

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

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

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

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

Observe that V_γ is a subcode of dimension m.

Lemma 2 ([8]) *All the non-zero 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* $V_\gamma + \mathbf{c}(a,0)$ *contains* $2^{m-1}-1$ *words of weight* m_1*,* 2^{m-1} *words of weight* d_1*, and 1 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 non-zero $a \in \mathsf{GF}(Q^2)$ such that $f(\gamma,a) = 0$. Then

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

T. Helleseth and H. G. Schaathun are at The Selmer Centre, Department of Informatics, University of Bergen, PB 7800, N-5020 Bergen, Norway (emails: georg@ii.uib.no and tor.helleseth@ii.uib.no)

The work has been supported by NFR under grant No. 146874/420 and the Aurora programme.

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

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

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

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

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. ■

II. 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 non-zero 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 $D = \langle \mathbf{a}, \mathbf{b} \rangle$ be a two-dimensional subcode, where $\mathbf{a} = \mathbf{c}(a_1, b_1)$ and $\mathbf{b} = \mathbf{c}(a_2, b_2)$ and $\mathbf{a}+\mathbf{b} = \mathbf{c}(a_3, b_3)$. 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 $\mathbf{c}(a, 0)$ where $a \neq 0$. So if D has three words of weight 2^{m-1} it must be one of the $(2^{2m}-1)(2^{2m-1}-1)/3$ 2-dimensional subcodes contained in $\{\mathbf{c}(a,0) : a \in \mathsf{GF}(2^{2m})\}$.

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

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) $w(\mathbf{a}) = w(\mathbf{b}) = d_1$, (2) $w(\mathbf{a}) = w(\mathbf{b}) = m_1$, and (3) $w(\mathbf{a}) = d_1$ whereas $w(\mathbf{b}) = m_1$. For (1) and (2), $\mathbf{a}$ and $\mathbf{b}$ may be interchanged, so each possibility is counted twice. The number of a values giving each weight is found by Remark 1.

$$B_{w.d.d}^2 = 2^{m-2}(2^m - 1)(2^m + 1)((2^m + 1)2^{m-1} - 1),$$
$$B_{w.d.m}^2 = 2^{2m-2}(2^{2m} - 1)(2^m - 1),$$
$$B_{w.m.m}^2 = 2^{m-2}(2^m - 1)^2(2^m + 1)(2^{m-1} - 1).$$

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.

$$B_{d.d.d}^3 = \frac{(2^m - 1)(2^{m-1} - 1)}{3}2^{m-1}(2^m + 1),$$
$$B_{m.m.m}^3 = \frac{(2^m - 1)(2^{m-1} - 1)}{3}2^{m-1}(2^m - 1).$$

Case 4 Distinct γ_1, γ_2, γ_3.

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

$$\mathbf{c}(a_1, b_1) \in V_{\gamma_3} + \mathbf{c}(a', 0),$$
$$\mathbf{c}(a_2, b_2) \in V_{\gamma_3} + \mathbf{c}(a', 0),$$
$$\mathbf{c}(a_3, b_3) \in V_{\gamma_3}.$$

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 $V_{\gamma_3} + \mathbf{c}(a', 0)$. There are $(2^m - 1)(2^{m-1} - 1)$ possibilities.

Consider the case where $T_m(\gamma_3^{Q+1}) = 0$, which implies that $w(\mathbf{c}(a_3, b_3)) = m_1$. By Remark 1, there are $(2^m - 1)2^{m-1}$ appropriate choices of γ_3. By Lemmata 3 and 4, for any $a' \neq 0$, $V_{\gamma_3} + \mathbf{c}(a', 0)$ 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 $\mathbf{c}(a_3, b_3)$. Thus we get

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

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*

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

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 1 about here.]

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.*

[Table 2 about here.]

We have verified the 2nd 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 non-zero word in V_{γ_1} and two words in each of three cosets $V_{\gamma_1}+\mathbf{c}(a_1,0)$, $V_{\gamma_1}+\mathbf{c}(a_2,0)$, and $V_{\gamma_1}+\mathbf{c}(a_1+a_2,0)$. 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] Tor Helleseth, Torleiv Kløve, and Johannes Mykkeltveit, "The weight distribution of irreducible cyclic codes with block lengths $n_1((q^l-1)/n)$," *Discrete Math.*, vol. 18, pp. 179–211, 1977.

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

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

[4] Steven Dougherty, Aaron Gulliver, and Manabu Oura, "Higher weights and graded rings for binary self-dual codes," *Discrete Applied Mathematics*, vol. 128, pp. 251–261, 2003, Special issue for WCC 2001.

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

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

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

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

Tor Helleseth (M'89-SM'96-F'97) received the Cand. Real. and Dr. Philos. degrees in mathematics from the University of Bergen, Bergen, Norway, in 1971 and 1979, respectively.

From 1973 to 1980 he was a Research Assistant at the Department of Mathematics, University of Bergen. From 1981 to 1984 he was at the Chief Headquarters of Defense in Norway. Since 1984 he has been a Professor at the Department of Informatics at the University of Bergen. During the academic years 1977-1978 and 1992-1993 he was on sabbatical leave at the University of Southern California, Los Angeles, and during 1979-1980 he was a Research fellow at the Eindhoven University of Technology, The Netherlands. His research interests include coding theory and cryptology.

From 1991 to 1993 he served as an Associate Editor for Coding Theory for IEEE TRANSACTIONS ON INFORMATION THEORY. He was Program Chairman for Eurocrypt'93 and for the Information Theory Workshop in 1997 in Longyearbyen, Norway. He will also be the Program Chairman for SETA04. In 1997 he was elected an IEEE Fellow for his contributions to coding theory and cryptography.

Hans Georg Schaathun was born in Bergen, Norway, in 1975. He received a Cand.Mag. degree with mathematics from the University of Bergen in 1996. He is Cand.Scient. 1999 and Dr.Scient 2002 from the Department of Informatics at the University of Bergen. During 2002 he was a lecturer, and from 2003 he is a post-doctoral researcher at this university. He has been at research stays at ENST in Paris 2000/2001 and at the Royal Holloway, University of London 2003/2004.

His research interest include codes for digital fingerprinting and higher weights of linear codes.

LIST OF TABLES

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

TABLE I

THE SECOND SWD OF THE 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

TABLE II

THE 2ND SWD FOR SOME SMALL KASAMI CODES.