

**MACWILLIAMS TYPE IDENTITIES FOR SOME NEW
WEIGHT ENUMERATORS AND THEIR APPLICATIONS**

AMIT KUMAR SHARMA



**DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY DELHI
OCTOBER 2016**

© Indian Institute of Technology Delhi (IITD), New Delhi, 2016.

MACWILLIAMS TYPE IDENTITIES FOR SOME NEW
WEIGHT ENUMERATORS AND THEIR APPLICATIONS

by

AMIT KUMAR SHARMA

Department of Mathematics

Submitted

in fulfillment of the requirements of the degree of

Doctor of Philosophy

to the



Indian Institute of Technology Delhi
October 2016

Dedicated to
My Family

Certificate

This is to certify that the thesis entitled “**MacWilliams type identities for some new weight enumerators and their applications**” submitted by “**Mr. Amit Kumar Sharma**” to the Indian Institute of Technology Delhi, for the award of the Degree of Doctor of Philosophy, is a record of the original bona fide research work carried out by him under our supervision and guidance. The thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.

The results contained in this thesis have not been submitted in part or full to any other university or institute for the award of any degree or diploma.

New Delhi
October 2016

Dr. Anuradha Sharma
Assistant Professor
Department of Mathematics
IIT Delhi

Prof. R. K. Sharma
Professor
Department of Mathematics
IIT Delhi

Acknowledgements

First of all, I would like to express my sincere gratitude to my supervisor, Dr. Anuradha Sharma, for her expert supervision and research insight. Above all and the most needed, she provided me unflinching encouragement and support in various ways. I am privileged to have the opportunity to work under her. With her valuable suggestions, understanding, patience, enthusiasm, vivid discussions and above all with her friendly nature, she helped me in successfully completing my Ph.D. work. I would also like to thank my co-supervisor, Prof. R.K. Sharma, for his constant support throughout my research work.

I am thankful to IIT Delhi authorities for providing me the necessary facilities and teaching assistantship for smooth completion of my research work. I express my regards to Dr. Aparna Mehra, DRC Chairperson, for her love and support. Special thanks to my SRC (Student Research Committee) Members: Dr. Shravan Kumar (Department of Mathematics) and Prof. S.K. Gupta (Department of Computer Science) for generously sharing their time and knowledge. I'm grateful to all faculty members of Department of Mathematics, IIT Delhi, for their co-operation and support.

Words cannot completely express my love and gratitude to my family who have supported and encouraged me through this journey. I would like to thank my parents for their life-long support, and sacrifices, which sustained my interest in research and motivated me towards the successful completion of this study. My heartiest thanks to my brother and sisters who have supported me through my difficult times with their inspiration and continued encouragement. I would also like to heartily thank my dearest wife Ritunjali for her unconditional support and love. I also acknowledge all the members

of my extended family for their love and support.

I will always remember the true friends who have walked with me on my path. There are too many to mention by name, yet, too few to ever lose room for in my heart. Many thanks to my dear friends, especially of Alok, Subhabrata, Sunil, Ratikant, Sudhakar, Sarvesh, Shailesh, Dipti and Swati for times of laughter when I needed a reprieve from the intensity of research. I also enjoyed the company of my senior colleagues; Dr. Dinabandhu, Dr. Balchand, Dr. Pushparaj, and Dr. Sunil.

Finally, I thank the almighty God for the passion, strength, perseverance, and the resources to complete this study.

New Delhi

October 2016

Amit Kumar Sharma

Abstract

Computer memory systems using high-density RAM chips are vulnerable to m-spotty byte errors when they are exposed to high-energy particles. These errors can be effectively detected or corrected using (m-spotty) byte error-control codes. In order to study the properties of these codes and to measure their error-detection and error-correction performance, m-spotty weight enumerators are introduced and studied with respect to various weights such as m-spotty Hamming weight, m-spotty Lee weight, RT weight. For a large code \mathcal{C} , it is in general very hard to obtain the m-spotty weight enumerator. However, when the code has a large size, its dual code is of comparatively smaller size. MacWilliams [*Bell System Tech. J.*, 1963] proved an identity for linear codes relating the weight enumerator of a linear code with that of its dual code. This identity enables one to obtain the weight enumerator of a large code from the weight enumerator of its dual code.

Based on this, we introduced and studied m-spotty weight enumerator, split m-spotty weight enumerator, g -fold joint m-spotty weight enumerator, complete m-spotty weight enumerator, with respect to both m-spotty Hamming weight and m-spotty Lee weight, of codes over the ring \mathbb{Z}_ℓ of integers modulo ℓ or a finite field \mathbb{F}_ℓ or the finite chain ring $\mathbb{R}_q = \mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q + \cdots + u^{e-1}\mathbb{F}_q$ ($u^e = 0$) or the ring $\mathfrak{R}_q = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$ ($u^2 = 0, v^2 = 0, uv = vu$). We have discussed some of their applications and derived MacWilliams type identities for each of the

enumerators. We have also defined and studied the split ρ weight enumerator of a linear code in $M_{n \times s}(R)$, where R is any finite Frobenius commutative ring and derive MacWilliams type identity for the same. Further, we defined the Lee complete ρ weight enumerator of a linear code in $M_{n \times s}(\mathbb{Z}_k)$ and obtain the MacWilliams identity for it.

As an application of MacWilliams identity, one can determine several modular forms from weight enumerators of self-dual codes over certain finite rings. In this thesis, we obtained Jacobi forms (or Siegel modular forms) of genus g from byte weight enumerators (or symmetrized byte weight enumerators) in genus g of Type I and Type II codes over either the ring \mathbb{Z}_{2m} of integers modulo $2m$ or the quaternionic ring $\Sigma_{2m} = \mathbb{Z}_{2m} + \alpha\mathbb{Z}_{2m} + \beta\mathbb{Z}_{2m} + \gamma\mathbb{Z}_{2m}$ with $\alpha = 1 + \hat{i}$, $\beta = 1 + \hat{j}$ and $\gamma = 1 + \hat{k}$, where $\hat{i}, \hat{j}, \hat{k}$ are elements of the ring \mathbb{H} of real quaternions satisfying $\hat{i}^2 = \hat{j}^2 = \hat{k}^2 = -1$, $\hat{i}\hat{j} = -\hat{j}\hat{i} = \hat{k}$, $\hat{j}\hat{k} = -\hat{k}\hat{j} = \hat{i}$ and $\hat{k}\hat{i} = -\hat{i}\hat{k} = \hat{j}$. We also obtained Jacobi forms over the totally real field $k_p = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ with $\zeta_p = e^{2\pi i/p}$ from byte weight enumerators of self-dual codes over \mathbb{F}_p . We also determined Siegel modular forms of genus g ($g \geq 1$ is an integer) over k_p by substituting certain theta series into byte weight enumerators in genus g of self-dual codes over \mathbb{F}_p for all $p \in \mathfrak{P}$, where the set \mathfrak{P} consists of all those odd primes p for which the ring \mathcal{O}_{k_p} of algebraic integers of k_p is a Euclidean domain. Further, we defined some partial Epstein zeta functions and derive their functional equation using the Mellin transform of the theta series in each case.

Self-dual codes (Type I and Type II codes) play an important role in the construction of even unimodular lattices, and hence in the determination of Jacobi forms. In this thesis, we constructed Type I and Type II codes (of higher lengths) over the ring \mathbb{Z}_{2^m} of integers modulo 2^m from shadows of Type I codes over \mathbb{Z}_{2^m} , and obtain their complete weight enumerators. As an application, we determined some Jacobi forms on the modular group $\Gamma(1) = SL(2, \mathbb{Z})$. Besides this, we constructed

self-dual codes (of higher lengths) over \mathbb{Z}_{2^m} from the generalized shadow of a self-dual code \mathcal{C} of length n over \mathbb{Z}_{2^m} with respect to a vector $s \in \mathbb{Z}_{2^m}^n \setminus \mathcal{C}$ satisfying either $\langle s, s \rangle \equiv 0 \pmod{2^m}$ or $\langle s, s \rangle \equiv 2^{m-1} \pmod{2^m}$.

Contents

Certificate	i
Acknowledgements	iii
Abstract	v
List of Figures	xv
List of Tables	xvii
List of Symbols	xix
1 Introduction	1
1.1 MacWilliams Type Identities for Weight Enumerators	2
1.2 Construction of Modular Forms from Byte Weight Enumerators	8
1.3 Construction of Self-dual Codes of Higher Lengths from Type II Codes	11
2 MacWilliams Type Identities for Weight Enumerators with respect	

to m-spotty Hamming Weight	15
2.1 Introduction	15
2.2 Some Preliminaries	16
2.3 Split m-spotty Hamming Weight Enumerator	19
2.3.1 A MacWilliams Type Identity	20
2.3.2 An Example	26
2.3.3 Some Applications	28
2.4 Joint m-spotty Hamming Weight Enumerator	38
2.4.1 MacWilliams Type Identities	43
2.4.2 An Example	56
3 MacWilliams Type Identities for g-fold Joint m-spotty Hamming Weight Enumerators	59
3.1 Introduction	59
3.2 The g -fold Joint m-spotty Hamming Weight Enumerator	60
3.2.1 MacWilliams Type Identities	66
3.2.2 An Example	73
4 MacWilliams Type identities for Weight Enumerators with respect to m-spotty Hamming Weight of Codes over Rings	77
4.1 Introduction	77
4.2 Some Preliminaries	78
4.3 The m-spotty Hamming Weight Enumerator	81
4.3.1 An Application	83
4.4 Split m-spotty Hamming Weight Enumerator	84
4.4.1 Some Applications	88
4.5 The g -fold Joint m-spotty Hamming Weight Enumerator	91
4.6 Complete m-spotty Hamming Weight Enumerator	98

5	MacWilliams Type Identities for Weight Enumerators with respect to m-spotty Lee Weight	101
5.1	Introduction	101
5.2	The m-spotty Lee Weight Enumerator	102
5.2.1	A MacWilliams Type Identity	104
5.2.2	An Example	108
5.2.3	An Application	110
5.3	Split m-spotty Lee Weight Enumerator	115
5.3.1	A MacWilliams Type Identity	118
5.3.2	An Example	120
5.3.3	An Application	121
5.4	Joint m-spotty Lee Weight Enumerator	125
5.4.1	MacWilliams Type Identities	131
5.4.2	An Example	143
6	MacWilliams Type Identities for a g-fold Joint m-spotty Lee Weight Enumerator	147
6.1	Introduction	147
6.2	The g -fold Joint m-spotty Lee Weight Enumerator	148
6.2.1	MacWilliams Type Identities	153
6.2.2	An Example	160
7	MacWilliams Type Identities for Weight Enumerators with respect to m-spotty Lee Weight of Codes over Rings	165
7.1	Introduction	165
7.2	Some Preliminaries	166
7.3	The m-spotty Lee Weight Enumerator	167
7.3.1	An Application	170
7.4	Split m-spotty Lee Weight Enumerator	171

7.4.1	An Application	174
7.5	The g -fold Joint m -spotty Lee Weight Enumerator	175
7.6	Complete m -spotty Lee Weight Enumerator	182
8	Byte Weight Enumerators and Modular Forms of Genus g	185
8.1	Introduction	185
8.2	Some Preliminaries	186
8.2.1	Byte Weight Enumerators in Genus g of Byte Error-Control Codes over R	187
8.2.2	Jacobi Forms of Genus g	190
8.3	Lattices and Byte Weight Enumerators in Genus g	192
8.4	Invariant Space containing Byte Weight Enumerators in Genus g of Type II Codes over R	195
8.5	Determination of Jacobi and Siegel Modular Forms of Genus g from Type II Codes	198
8.6	Determination of Jacobi Forms and Siegel Modular Forms of Genus g from Type I Codes over R	206
8.7	Partial Epstein Zeta Functions	213
9	Byte Weight Enumerators of Codes over \mathbb{F}_p and Modular Forms over a Totally Real Field	219
9.1	Introduction	219
9.2	Some Preliminaries	220
9.2.1	Byte Weight Enumerators in Genus g	220
9.2.2	Jacobi Form over a Totally Real Field	222
9.2.3	Lattices Induced by Codes over \mathbb{F}_p	224
9.3	Theta Series for a Lattice and Byte Weight Enumerator of a Code over \mathbb{F}_p	225

9.4	Invariant Spaces and Jacobi Forms over k_p	227
9.5	Siegel Modular Forms of Genus g over k_p	230
9.5.1	Determination of Siegel Modular Forms over k_p	232
9.6	Invariant Space and Siegel Modular Forms of Genus g over k_p	238
9.7	Partial Epstein Zeta Functions	242
10	Construction of Self-dual Codes over \mathbb{Z}_{2^m}	249
10.1	Introduction	249
10.2	Some Preliminaries	250
10.2.1	Shadow of a Type I Code	252
10.2.2	Generalized Shadow of a Self-dual Code	255
10.3	Construction of Type I and Type II Codes from Shadows of Type I Codes	257
10.4	Construction of Self-dual Codes from Generalized Shadows of Self- dual Codes	270
10.5	Some Examples	272
11	MacWilliams Type Identities for Weight Enumerators with respect to ρ Metric	277
11.1	Introduction	277
11.2	Some Preliminaries	278
11.3	Split ρ Weight Enumerator	280
11.3.1	An Application	283
11.4	Lee Complete ρ Weight Enumerator	285
	Bibliography	293
	Bio-Data	301

List of Figures

2.1	An instance of u and v (the shaded region represents non-zero bits). .	22
2.2	The i th bytes: r_i and c_i	37
2.3	An instance of v, g and u (the shaded region represents non-zero bits).	48
2.4	An instance of u, g, h and v (the shaded region represents non-zero bits).	50
3.1	$\sigma_{q+1}(a)$ and $\mu_{q+1}(a)$	71

List of Tables

2.1	Distribution vectors of codewords of \mathcal{C}^\perp	27
2.2	Contributing polynomials of the codewords	28
2.3	Distribution vectors of codewords of \mathcal{D}	57
2.4	Contributing Polynomials	57
3.1	Contributing Polynomials	75
5.1	Codewords, Composition vectors and Contributing polynomials . . .	110
5.2	Codewords, Composition vectors and Contributing polynomials . . .	121
5.3	The composition vectors $j_u(v) = k = (k_1, k_2, k_3)$ and the contributing polynomials $G_k = G_{k_1}G_{k_2}G_{k_3}$ for each pair $v \in \mathcal{D}_1$ and $u \in \mathcal{C}_1^\perp$	145
6.1	Contributing Polynomials	162
8.1	Values of δ	208
8.2	Values of ν	209

List of Symbols

Symbol	Meaning
$\lceil \cdot \rceil$	The Ceiling function
$\lfloor \cdot \rfloor$	The Floor function
w_H	The Hamming weight
w_L	The Lee weight
w_M	The m-spotty Hamming weight
w_{ML}	The m-spotty Lee weight
w_ρ	The ρ -weight
$\langle \cdot, \cdot \rangle$	The standard inner product
d_H	The Hamming distance
d_L	The Lee distance
d_M	The m-spotty Hamming distance
d_{ML}	The m-spotty Lee distance
d_ρ	The ρ distance
\mathbb{Z}_ℓ	The residue class ring of integers modulo ℓ , $\ell \geq 2$
\mathbb{F}_ℓ	The finite field of order ℓ , ℓ a prime power

$M_{n \times s}(R)$	the R -module of all $n \times s$ matrices over the ring R
ζ_p	A primitive p th root of unity
\mathcal{C}	Linear code
\mathcal{C}^\perp	The dual code of \mathcal{C}
$ A $	cardinality of the set A
$\binom{n}{r}$	The Binomial coefficient
\mathbb{R}	The set of Real numbers
\mathbb{C}	The set of Complex numbers