On the Existence of Hermitian Self-Dual Extended Abelian Group Codes

Lilibeth Dicuangco*, Pieter Moree**, Patrick Solé§

Abstract

Split group codes are a class of group algebra codes over an abelian group. They were introduced by Ding, Kohel and Ling in [3] as a generalization of the cyclic duadic codes. For a prime power q and an abelian group G of order n such that $\gcd(n, q) = 1$, consider the group algebra $\mathbb{F}_{q^2}[G^*]$ of $\mathbb{F}_{q^2}$ over the dual group G^* of G. We prove that every ideal code in $\mathbb{F}_{q^2}[G^*]$ whose extended code is Hermitian self-dual is a split group code. We characterize the orders of finite abelian groups G for which an ideal code of $\mathbb{F}_{q^2}[G^*]$ whose extension is Hermitian self-dual exists and derive asymptotic estimates for the number of non-isomorphic abelian groups with this property.

Keywords: counting function, extended group codes, group algebra codes, Hermitian self-dual codes, non-isomorphic abelian groups, split group codes, splittings.
Mathematics Subject Classification: 11N64, 94B05, 11N37

1 Introduction

Binary duadic codes were first introduced in 1984 by Leon, Masley and Pless [11] as a generalization of quadratic residue codes. Smid [28] generalized these results further by defining duadic codes over arbitrary finite fields in terms of a *splitting* of the length of the code. The Q-codes of Pless [20] are then duadic codes over $\mathbb{F}_4$ in this setting.

Quadratic residue codes have also been generalized in a different direction (i.e., see [29]). In this approach, quadratic residue codes are defined as ideals of abelian group algebras, which is a generalization of cyclic codes. Rushanan [24] proceeded to define duadic codes in this setting.

*Mathematics Department, University of the Philippines, Diliman, Quezon City, 1101 Philippines, ldicuangco@math.upd.edu.ph

**Max-Planck-Institut, Vivatsgasse 7, D-53111 Bonn, Germany, moree@mpim-bonn.mpg.de

§CNRS, I3S ESSI, BP 145, Route des Colles, 06 903 Sophia Antipolis, France, sole@essi.fr

In [3], Ding, Kohel and Ling defined split group codes as ideals of abelian group algebras. Their construction makes use of a *splitting* of the abelian group. Under this definition, split group codes are seen as a generalization of duadic codes.

In this paper, we consider the finite field $F = \mathbb{F}_{q^2}$ and an abelian group G of order n such that $\gcd(n, q) = 1$. Following the treatment in [3], we work with the dual group G^* of G and consider the group algebra $F[G^*]$. We prove that every ideal code in $F[G^*]$ whose extension by a suitable parity-check is Hermitian self-dual is a split group code (Corollary 3.7). We then give sufficient and necessary conditions on the order of the group G for the existence of Hermitian self-dual extended ideal codes (Theorem 3.11). We conclude the paper by deriving asymptotic estimates on $HSD(x)$, the number of non-isomorphic abelian groups of order less than x for which a Hermitian self-dual extended ideal code exists (Theorem 4.3).

2 Preliminaries

All of the results in this section are taken from [3]. In general, these results work for any finite field but since we will be dealing with Hermitian duality, we restrict our study to finite fields of square order.

Let R be a finite commutative ring with unity. Let G be its underlying finite abelian group written additively. Denote the order and exponent of G by n and m, respectively. Let q be a power of a prime p_1 such that $\gcd(n, q) = 1$ or equivalently, $\gcd(m, q) = 1$. Let $F = \mathbb{F}_{q^2}$. Let K be the smallest extension of F containing all the m-th roots of unity.

Let G^* be the set of all characters of G into K. The groups G and G^* are isomorphic. Let $K[G^*]$ be the group algebra of K over G^*. The elements of $K[G^*]$ are the sums $\sum_{\psi \in G^*} a_\psi \psi$ where the a_ψ's are elements of K. An ideal I of $K[G^*]$ is called an *ideal code*.

The dimension of the commutative group algebra $K[G^*]$ over K is n. This group algebra $K[G^*]$ contains a subgroup isomorphic to G^*. For any character ψ in G^*, we also denote by ψ the corresponding element in $K[G^*]$.

If $x \in G$ and $f = \sum_{\psi \in G^*} a_\psi \psi \in K[G^*]$, define $f(x) = \sum_{\psi \in G^*} a_\psi \psi(x)$. Thus we can view the elements of $K[G^*]$ as functions from G to K.

2.1 Ideal codes and Idempotent Generators

An element e of a ring is called an idempotent if $e^2 = e$. An idempotent is called primitive if for every other idempotent f, either $ef = e$ or $ef = 0$.

Proposition 2.1 ([3].) *The primitive idempotents of $K[G^*]$ are the elements*

$$e_x = \frac{1}{n} \sum_{\psi \in G^*} \psi(x)^{-1} \psi,$$

for each element x of G.

Proposition 2.2 ([3].) *The ring $K[G^*]$ decomposes as a direct sum $\oplus_{x\in G} K e_x$. If $f \in K[G^*]$, then f has the form*

$$f = \sum_{x\in G} f(x)e_x.$$

Every idempotent e in $K[G^*]$ can be uniquely written in the form

$$e = \sum_{x\in X} e_x,$$

for some non-empty subset X of G.

Let X be a non-empty subset of G and define the ideal

$$I_X = \{f \in K[G^*] \mid f(x) = 0 \text{ for all } x \in X\}.$$

Corollary 2.3 ([3].) *For every ideal I in $K[G^*]$, there is a unique proper subset X of G such that $I = I_X$ and I is generated by the idempotent $e = \sum_{x\notin X} e_x$.*

2.2 Split Group Codes

Let s be an element of R. Consider the endomorphism of G given by $\tau_s : x \longrightarrow sx$. This induces a map μ_s on G^* given by $\mu_s(\psi) = \psi \circ \tau_s$ for each element ψ of G^*. This extends to a map on $K[G^*]$, also denoted by μ_s, defined by $\mu_s(f) = f \circ \tau_s$ for all $f \in K[G^*]$. That is, for $f \in K[G^*]$, $\mu_s(f)(x) = f(sx)$ for every $x \in G$.

A *splitting* of G over Z is a triple (Z, X_0, X_1) which gives a partition $G = Z \cup X_0 \cup X_1$ such that there exists an invertible element s of R with $\tau_s(X_0) = X_1$ and $\tau_s(X_1) = X_0$. Under these conditions, s is said to *split* the triple (Z, X_0, X_1). In addition, an invertible element r of R is said to *stabilize* the splitting if $\tau_r(X_0) = X_0$ and $\tau_r(X_1) = X_1$.

Given a splitting (Z, X_0, X_1), let $C_0(K)$ be the ideal I_{X_0} over K and let $C_1(K)$ be the ideal I_{X_1} over K. The ideal $C_0(K)$ is defined as the *split group code* associated to the splitting, and the ideal $C_1(K)$ is called the *conjugate split group code*. The following notations are used to denote some special subcodes: $C_0^Z(K) = I_{Z\cup X_0}$, $C_1^Z(K) = I_{Z\cup X_1}$ and $C_Z(K) = I_{X_0\cup X_1}$.

Let s be an invertible element of R. The element s is said to *split* the group code $C_0(K)$ if $\mu_s(C_0(K)) = C_1(K)$ and $\mu_s(C_1(K)) = C_0(K)$, while s is said to *stabilize* the code $C_0(K)$ if $\mu_s(C_0(K)) = C_0(K)$ and $\mu_s(C_1(K)) = C_1(K)$.

Proposition 2.4 ([3].) *Let s be a unit in R. A split group code $C_0(K)$ is split or stabilized by s if and only if s splits or stabilizes (Z, X_0, X_1), respectively.*

Theorem 2.5 ([3].) *Let (Z, X_0, X_1) be a splitting. Let $C_0(K)$ be the split group code associated to this splitting. Then the following hold:*

1. *The codes $C_0(K)$ and $C_1(K)$ are generated by the idempotents*

$$e = \sum_{x \notin X_0} e_x \quad \text{and} \quad f = \sum_{x \notin X_1} e_x.$$

The codes $C_0^Z(K)$, $C_1^Z(K)$ and $C_Z(K)$ are generated by

$$\sum_{x \in X_1} e_x, \quad \sum_{x \in X_0} e_x, \quad \text{and} \quad \sum_{z \in Z} e_z.$$

2. *If the splitting is given by s, then μ_s induces an equivalence of $C_0(K)$ with its conjugate $C_1(K)$, and of the subcode $C_0^Z(K)$ with $C_1^Z(K)$.*

3. *$K[G^*]$ decomposes as a direct sum $C_Z(K) \oplus C_0^Z(K) \oplus C_1^Z(K)$.*

Corollary 2.6 ([3].) *The codes $C_0(K)$ and $C_1(K)$ have dimension $(n+|Z|)/2$. The subcodes $C_0^Z(K)$ and $C_1^Z(K)$ have dimension $(n-|Z|)/2$. The subcode $C_Z(K)$ has dimension $|Z|$.*

2.3 Split Group Codes Over $\mathbb{F}_{q^2}$

In the previous section, the split group codes are defined over the field K which is assumed to contain all the m-th roots of unity. In this paper, we want our split group codes to be defined over the subfield $F = \mathbb{F}_{q^2}$ without requiring $\mathbb{F}_{q^2}$ to contain any m-th roots of unity. In this section, we present sufficient and necessary conditions given in [3] for split group codes to be defined over a subfield of K.

Let $V = V(K)$ be a vector subspace of $K^n = K[G^*]$. Define $V(F) = V(K) \cap F^n$. Clearly, $\dim_F(V(F)) \leq \dim_K(V(K))$. If equality holds then we say that V is *defined over the field F*.

If the vector subspace $C_0(K)$ of $K^n = K[G^*]$ is defined over F, we simply write C_0 for the subcode $C_0(F) = C_0(K) \cap F^n$ in $F^n = F[G^*]$. In this case, we call C_0 *the split group code over F*. Similarly, we write C_1, C_0^Z, C_1^Z and C_Z for the other codes defined over F.

Note that $(m, q) = 1$ by assumption, so the integer $-q$ as an element of the finite ring R is invertible and τ_{q^2} is a well-defined automorphism of G. The action of the group generated by τ_{q^2} on the elements of G partitions G into disjoint orbits. These $\langle \tau_{q^2} \rangle$-orbits play the same role as the cyclotomic cosets for the cyclic codes.

Proposition 2.7 ([3].) *The idempotents of $F[G^*]$ are those e in $K[G^*]$ of the form*

$$e = \sum_{x \in Y} e_x,$$

where Y is a union of $\langle \tau_{q^2} \rangle$-orbits in G. An idempotent e in $F[G^*]$ is primitive if and only if $Y = \langle \tau_{q^2} \rangle x$ for some $x \in G$.

Corollary 2.8 ([3].) *Let $\{e_1, e_2, \ldots, e_r\}$ be the set of all primitive idempotents of $F[G^*]$. Then every nonzero ideal I of $F[G^*]$ is generated by $e = \sum_{i \in T} e_i$ where T is a non-empty subset of $\{1, 2, \ldots, r\}$.*

Theorem 2.9 ([3].) *Let I be an ideal in $K[G^*]$. Then the following conditions are equivalent.*

1. *The ideal I is defined over F.*
2. *The set $X = \{x \in G \mid f(x) = 0 \text{ for all } f \in I\}$ is a union of $\langle \tau_{q^2} \rangle$-orbits.*
3. *The idempotent generator of I lies in $F[G^*]$.*

Corollary 2.10 ([3].) *If $C_0(K)$ is defined over F then so is $C_1(K)$. Moreover $F[G^*]$ has the decomposition*

$$F[G^*] = C_Z(F) \oplus C_0^Z(F) \oplus C_1^Z(F).$$

If s gives the splitting, then μ_s gives an equivalence of C_0 and C_1 and of C_0^Z and C_1^Z.

Theorem 2.11 ([3].) *Let C be a code in $K[G^*]$. The block length, dimension, and minimum distance are well-defined invariants of C, independent of the field over which C is defined.*

3 Hermitian Duality and Extended Ideal Codes in $F[G^*]$

In this section, we present results concerning the Hermitian orthogonality of ideal codes in $F[G^*]$. We prove that every Hermitian self-orthogonal ideal code in $F[G^*]$ is a subcode of a split group code for some splitting of G given by $-q$. We then proceed to define an extension of ideal codes and determine conditions for the extended code to be Hermitian self-dual. We also give necessary and sufficient conditions on the order of the abelian group G for the existence of Hermitian self-dual extended ideal codes.

3.1 Hermitian Orthogonality of Ideal Codes in $F[G^*]$

Let $f = \sum_{\psi \in G^*} a_\psi \psi$ and $g = \sum_{\psi \in G^*} b_\psi \psi$ be elements of $F[G^*]$. The *Hermitian inner product* between f and g is defined as $\langle f, g \rangle_H = \sum_{\psi \in G^*} a_\psi b_\psi^q$.

Let C be a code in $F[G^*]$. The Hermitian dual of C is the ideal $C^{\perp_H} = \{f \in F[G^*] \mid \langle f, g \rangle_H = 0 \text{ for all } g \in C\}$. The code C is said to be *Hermitian self-orthogonal* if $C \subseteq C^{\perp_H}$ and is *Hermitian self-dual* if $C = C^{\perp_H}$.

Theorem 3.5 states the main result of this section. It is a generalization of Proposition 4.4 in [2] to split group codes. We first prove some basic results concerning the Hermitian duals of split group codes.

Proposition 3.1 *Let $f = \sum_{\psi \in G^*} a_\psi \psi$ and $g = \sum_{\psi \in G^*} b_\psi \psi$ be elements of $F[G^*]$. Then the Hermitian inner product of f and g is*

$$\langle f,\, g \rangle_H = \frac{1}{n} \sum_{x \in G} f(x) g(-q^{-1}x)^q$$

Proof. Note that $\mu_{-q^{-1}}(g)(x) = g(-q^{-1}x) = \sum_{\psi \in G^*} b_\psi \psi(-q^{-1}x) = \sum_{\psi \in G^*} b_\psi \psi(q^{-1}x)^{-1}$. Thus $(\mu_{-q^{-1}}(g)(x))^q = \sum_{\psi \in G^*} b_\psi^q \psi(q^{-1}x)^{-q} = \sum_{\psi \in G^*} b_\psi^q \psi(x)^{-1}$, or equivalently, $(\mu_{-q^{-1}}(g))^q = \sum_{\psi \in G^*} b_\psi^q \psi^{-1}$.

Define $f * g = f(\mu_{-q^{-1}}(g))^q$. Then the coefficient of the trivial character of $f * g$ is $\sum_{\psi \in G^*} a_\psi b_\psi^q$, which is $\langle f, g \rangle_H$. Expanding $f * g$ in terms of its idempotent decomposition, we get

$$\begin{aligned} f * g &= \sum_{x \in G} (f(\mu_{-q^{-1}}(g))^q)(x) e_x \\ &= \sum_{x \in G} f(x)(\mu_{-q^{-1}}(g)(x))^q e_x \\ &= \sum_{x \in G} f(x)(g(-q^{-1}x))^q e_x \\ &= \frac{1}{n} \sum_{\psi \in G^*} \sum_{x \in G} f(x)(g(-q^{-1}x))^q \psi^{-1}(x) \psi. \end{aligned}$$

Using this expansion, the coefficient of the trivial character of $f*g$ is $\frac{1}{n} \sum_{x \in G} f(x)(g(-q^{-1}x))^q$. The result follows. $\square$

Proposition 3.2 *Let C be an ideal in $K[G^*]$ which is defined over F. Suppose $C = I_X$ for some non-empty subset X of G. Then $C^{\perp_H} = I_{X'}$ where $X' = G \setminus \tau_{-q}(X)$.*

Proof. From Theorem 2.9, X is a union of $\langle \tau_{q^2} \rangle$-orbits. Let $X' = G \setminus \tau_{-q}(X)$. Let $f \in I_{X'}$ and $g \in C = I_X$. By Proposition 3.1, $\langle f, g \rangle_H = \frac{1}{n} \sum_{x \in G} f(x)(g(-q^{-1}x))^q$. Since X and $\tau_{-q}(X)$ are unions of $\langle \tau_{q^2} \rangle$-orbits and clearly x and $q^2 x$ belong to the same τ_{q^2}-orbit, it follows that $-q^{-1}x \in X$ if and only if $(-q)^2(-q^{-1})x \in X$ if and only if $-qx \in X$ if and only if $(-q)(-q)x \in \tau_{-q}(X)$ if and only if $x \in \tau_{-q}(X)$. Thus $g(-q^{-1}x) = 0$ for all $x \in \tau_{-q}(X)$. Since $f \in I_{X'}$, $f(x) = 0$ for every $x \in X' = G \setminus \tau_{-q}(X)$. Therefore $\sum_{x \in G} f(x)(g(-q^{-1}x))^q = 0$, implying that $\langle f, g \rangle_H = 0$. Thus $I_{X'} \subseteq C^{\perp_H}$. Comparing dimensions, we get $C^{\perp_H} = I_{X'}$. $\square$

`Remark`. We note that for any subset X of G which is a union of $\langle \tau_{q^2} \rangle$-orbits of G, we have $\tau_{-q^{-1}}(X) = \tau_{(-q)^2}(\tau_{-q^{-1}}(X)) = \tau_{-q}(X)$.

Proposition 3.3 *Let (Z, X_0, X_1) be a splitting of G over Z where Z, X_0 and X_1 are unions of $\langle \tau_{q^2} \rangle$-orbits. The ring element $-q$ splits or stabilizes C_0 if and only if $-q^{-1}$ splits or stabilizes C_0, respectively.*

Proof. Using Proposition 2.4, we need only show that $-q$ splits or stabilizes (Z, X_0, X_1) if and only if $-q^{-1}$ splits or stabilizes (Z, X_0, X_1), respectively. From the remark above, $\tau_{-q^{-1}}(X_0) = \tau_{-q}(X_0)$ and $\tau_{-q^{-1}}(X_1) = \tau_{-q}(X_1)$. The result follows. $\square$

Proposition 3.4 *Let (Z, X_0, X_1) be a splitting of G over Z. Assume that Z, X_0 and X_1 are unions of $\langle \tau_{q^2} \rangle$-orbits. Suppose Z is stabilized by τ_{-q}. Then $C_Z^{\perp_H} = C_0^Z \oplus C_1^Z$. If $-q$ splits C_0, then $C_0^{\perp_H} = C_0^Z$. If $-q$ stabilizes C_0, then $C_0^{\perp_H} = C_1^Z$.*

Proof. Note that $\tau_{-q^{-1}}(Z) = \tau_{(-q)^2}(\tau_{-q^{-1}}(Z)) = \tau_{-q}(Z)$ and by assumption, $\tau_{-q}(Z) = Z$. Let $f \in C_Z = I_{X_0 \cup X_1}$ and let $g \in C_0^Z \oplus C_1^Z$. Then

$$\langle f, g \rangle_H = \frac{1}{n} \sum_{x \in G} f(x)(g(-q^{-1}x))^q = 0,$$

since $f(x) = 0$ for all $x \in X_0 \cup X_1$ and $g(-q^{-1}x) = 0$ for all $x \in Z$. Thus $C_0^Z \oplus C_1^Z \subseteq C_Z^{\perp_H}$. Comparing dimensions, we have $C_Z^{\perp_H} = C_0^Z \oplus C_1^Z$.

Suppose $-q$ splits C_0. Let $f \in C_0$ and $g \in C_1^Z$. Note that $\tau_{-q^{-1}}(Z) = Z$. By assumption, $\tau_{-q}(X_1) = X_0$, or equivalently, $\tau_{-q^{-1}}(X_1) = X_0$. Clearly $f(x) = 0$ for all $x \in X_0$ and $g(-q^{-1}x) = 0$ for all $x \in Z \cup X_1$. Thus

$$\langle f, g \rangle_H = \frac{1}{n} \sum_{x \in G} f(x)(g(-q^{-1}x))^q = 0,$$

implying that $C_0^Z \subseteq C_0^{\perp_H}$. Comparing dimensions, we have $C_0^{\perp_H} = C_0^Z$.

Suppose $-q$ stabilizes C_0. Then $\tau_{-q^{-1}}(X_1) = \tau_{-q}(X_1) = X_1$. Let $f \in C_0$ and $g \in C_1^Z$. Clearly $f(x) = 0$ for all $x \in X_0$ and $g(-q^{-1}x) = 0$ for all $x \in Z \cup X_1$. Thus

$$\langle f, g \rangle_H = \frac{1}{n} \sum_{x \in G} f(x)(g(-q^{-1}x))^q = 0,$$

implying that $C_1^Z \subseteq C_0^{\perp_H}$. Comparing dimensions, we have $C_1^{\perp_H} = C_0^Z$. $\square$

We now prove the main result of this section.

Theorem 3.5 *Let $C = I_X$ be an ideal in $F[G^*]$. Then C is Hermitian self-orthogonal if and only if $C = C_0^Z$ for some splitting (Z, X_0, X_1) of G which is split by $-q$ (that is, C is a subcode of a split group code which is split by $-q$).*

Proof.
($\Longleftarrow$) Suppose (Z, X_0, X_1) is a splitting of G which is split by $-q$. Let $C = C_0^Z$. By Proposition 3.4, $C^{\perp_H} = (C_0^Z)^{\perp_H} = C_0 \supseteq C_0^Z = C$.
($\Longrightarrow$) Let $C^{\perp_H} = I_{X'}$. By Proposition 3.2, $X' = G \setminus \tau_{-q}(X)$. By assumption, $C \subseteq C^{\perp_H}$. Thus $X' \subseteq X$, or $G \setminus \tau_{-q}(X) \subseteq X$. Note that both X and X' are unions of $\langle \tau_{q^2} \rangle$-orbits.

Write $X = Z \cup X_0$ with $\tau_{-q}(Z) = Z$ and $Z \cap X_0 = \emptyset$. Since τ_{-q} either fixes a $\langle \tau_{q^2} \rangle$-orbit or it sends it to another $\langle \tau_{q^2} \rangle$-orbit, we are actually choosing Z as the union of $\langle \tau_{q^2} \rangle$-orbits contained in X which are fixed by τ_{-q} and X_0 as the complement of Z in X, so that clearly $\tau_{-q}(X_0) \cap X_0 = \emptyset$.

We first show that neither Z nor X_0 is empty. If $0 \notin X$ then $0 \notin \tau_{-q}(X)$, which implies that $0 \in G \setminus \tau_{-q}X$. But $G \setminus \tau_{-q}(X) \subseteq X$, implying that $0 \in X$, a contradiction. Thus $0 \in X$, and so by our choice of partition of X, $0 \in Z$ proving that $Z \neq \emptyset$. If $X_0 = \emptyset$ then $X = Z$ and $\tau_{-q}(X) = X$. Thus $X' = G \setminus \tau_{-q}(X) = G \setminus X$ which implies that $X' \cap X = \emptyset$, a contradiction since $X' \subseteq X$. Thus $X_0 \neq \emptyset$.

Note that $X' = G \setminus \tau_{-q}(X) = G \setminus Z \cup \tau_{-q}(X_0)$. Since $X_0 \cap Z = X_0 \cap \tau_{-q}(X_0) = \emptyset$, we have $X_0 \subseteq X'$. Consider $\tau_{-q}(X') = G \setminus X$. Since $X' \subseteq X$, it follows that $\tau_{-q}(X') \cap X' = \emptyset$ and τ_{-q} does not fix any $\langle \tau_{q^2} \rangle$-orbit contained in X', implying that $X' \subseteq X_0$. Hence $X' = X_0$. Let $X_1 = \tau_{-q}(X')$. Then (Z, X_0, X_1) gives a splitting of G such that $\tau_{-q}(Z) = Z$, $\tau_{-q}(X_0) = X_1$ and $\tau_{-q}(X_1) = X_0$ and $C = I_X = I_{Z \cup X_0} = C_0^Z$. □

3.2 Extensions of Ideal Codes in $F[G^*]$

Using the terminology of split group codes, duadic codes are easily seen to be split group codes for splittings of G over $Z = \{0\}$ where G is cyclic (see Example III.1 of [3]). In [2], we defined an extension for an odd-like duadic code and gave a sufficient condition for the extended code to be Hermitian self-dual. In this section, we consider split group codes for the abelian group G with splittings over $Z = \{0\}$ and derive analogous results regarding Hermitian self-duality of the extended split group codes.

Let the order n of the abelian group G be odd. Consider the equation

$$\frac{1}{n} + \gamma^{q+1} = 0, \tag{1}$$

which is solvable in $\mathbb{F}_{q^2}$. Let γ be a solution to (1). For each $f \in F[G^*]$, define $\widetilde{f} = (f, -\gamma f(0)) \in F[G^*] \times F$. If C is a code in $F[G^*]$ then the extended code $\widetilde{C}$ is defined as the subspace

$$\widetilde{C} = \{\widetilde{f} = (f, -\gamma f(0)) \mid f \in C\} \subseteq F[G^*] \times F.$$

Proposition 3.6 *Let $(Z = \{0\}, X_0, X_1)$ be a splitting of G where Z, X_0 and X_1 are unions of $\langle \tau_{q^2} \rangle$-orbits. Let C_0 be the corresponding split group code defined over $F = \mathbb{F}_{q^2}$.*

1. *The extended codes $\widetilde{C_0}$ and $\widetilde{C_1}$ are equivalent.*

2. *If $-q$ splits C_0, then $\widetilde{C_0}^{\perp_H} = \widetilde{C_0}$ and $\widetilde{C_1}^{\perp_H} = \widetilde{C_1}$.*

3. *If $-q$ stabilizes C_0, then $\widetilde{C_0}^{\perp_H} = \widetilde{C_1}$ and $\widetilde{C_1}^{\perp_H} = \widetilde{C_0}$.*

Proof. The equivalence of $\widetilde{C_0}$ and $\widetilde{C_1}$ is an immediate consequence of Theorem 2.5.

Suppose $-q$ splits C_0. Let f, g be elements of C_0. From Proposition 3.3, $-q^{-1}$ also splits C_0. Thus $\mu_{-q^{-1}}(g) \in C_1$. Note that $-q^{-1}x \in X_0 \iff x \in \tau_{-q^{-1}}(X_0) = X_1$. It follows that $f(x) = 0$ for all $x \in X_0$ and $g(-q^{-1}x) = 0$ for all $x \in X_1$. Hence using Proposition 3.1, we get

$$\langle f, g\rangle_H \;=\; \frac{1}{n} f(0)g(0)^q = -\gamma^{q+1} f(0)g(0)^q.$$

Thus $\langle \widetilde{f}, \widetilde{g}\rangle_H = 0$ and $\widetilde{C_0}^{\perp_H} = \widetilde{C_0}$. By a similar argument, it can be shown that $\widetilde{C_1}^{\perp_H} = \widetilde{C_1}$.

Suppose $-q$ stabilizes C_0. Let $f \in C_0$ and let $g \in C_1$. The element $-q^{-1}$ also stabilizes C_0 and $\mu_{-q^{-1}}(g) \in C_0$. Again, $-q^{-1}x \in X_1 \iff x \in \tau_{-q^{-1}}(X_1) = X_1$. So $f(x) = 0$ for all $x \in X_0$ and $g(-q^{-1}x) = 0$ for all $x \in X_1$. Thus

$$\langle f, g\rangle_H \;=\; \frac{1}{n} f(0)g(0)^q = -\gamma^{q+1} f(0)g(0)^q,$$

and so $\langle \widetilde{f}, \widetilde{g}\rangle_H = 0$ and $\widetilde{C_0}^{\perp_H} = \widetilde{C_1}$. Similarly, $\widetilde{C_1}^{\perp_H} = \widetilde{C_0}$. □

Corollary 3.7 *Let $C = I_X$ be a group code defined over F. The extended code $\widetilde{C}^{\perp_H}$ is Hermitian self-dual if and only if C is a split group code for some splitting $(Z = \{0\}, X_0, X_1)$ of G by $-q$.*

Proof.
($\Longleftarrow$) This follows directly from the previous theorem.
($\Longrightarrow$) Since $\widetilde{C}^{\perp_H}$ is Hermitian self-dual, the dimension of C is $\frac{n+1}{2}$ and so C cannot be Hermitian self-orthogonal. This fact combined with the assumption that $\widetilde{C}^{\perp_H}$ is Hermitian self-dual implies that $0 \notin X$. Let $C_e = I_{X\cup\{0\}}$. This subcode C_e is Hermitian self-orthogonal and has dimension $\frac{n-1}{2}$. By Theorem 3.5, C_e is a subcode of a split group code which is split by $-q$, that is, $C_e = C_0^Z$ for some splitting (Z, X_0, X_1) of G by $-q$. Since $\dim C_e = \frac{n-1}{2}$ and $\dim C_0^Z = \frac{n-|Z|}{2}$, it follows that $Z = \{0\}$. Hence $X = X_0$ and C is a split group code of G which is split by $-q$. □

3.3 Existence of Hermitian Self-dual Extended Ideal Codes

In view of Theorem 3.5 and Corollary 3.7, it is natural to ask under what conditions we obtain splittings over $Z = \{0\}$ of an abelian group G by $-q$. Such conditions would guarantee existence of Hermitian self-orthogonal codes and Hermitian self-dual extended codes in $F[G^*]$. We remark that the results in this section are generalizations of results on extended duadic codes in [2].

Define $ord_r(q)$ to be the smallest positive integer t such that $q^t \equiv 1 \pmod r$. If l is a positive odd integer relatively prime to q then l is said to be split by $-q$ over $\mathbb{F}_{q^2}$ if and only if the set $X = \{1, 2, \ldots, l\}$ has a partition $X = X_0 \cup X_1$ such that $(-q)X_0 = X_1$ and $(-q)X_1 = X_0$, where the multiplication is read modulo l.

Proposition 3.8 ([2].) *Let l be a positive odd integer which is relatively prime to q. The integer l has a splitting by $-q$ if and only if $ord_r(q) \not\equiv 2 \pmod 4$ for every prime r dividing l.*

Theorem 3.9 *Let G be an abelian group of order n. The group G has a splitting over $Z = \{0\}$ given by $-q$ if and only if $ord_r(q) \not\equiv 2 \pmod 4$ for every prime r dividing n.*

Proof. The abelian group G is isomorphic to a unique product of cyclic groups of the form

$$\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_s},$$

where m_i divides m_{i+1} for $i = 1, 2, \ldots, s-1$, and $m_s = m$ where m denotes the exponent of G.

If each summand $\mathbb{Z}_{m_i}$ has a splitting over $Z = \{0\}$ given by $-q$ then G also has a splitting over $Z = \{0\}$ given by $-q$. Indeed if $(\{0\}, X_0^{(i)}, X_1^{(i)})$ is a splitting by $-q$ of $\mathbb{Z}_{m_i}$ for each $i = 1, 2, \ldots, s$ then letting

$$\begin{aligned} X_t \quad = \quad & X_t^{(1)} \times \mathbb{Z}_{m_2} \times \mathbb{Z}_{m_3} \times \cdots \times \mathbb{Z}_{m_s} \\ & \cup \{0\} \times X_t^{(2)} \times \mathbb{Z}_{m_3} \times \cdots \times \mathbb{Z}_{m_s} \\ & \cup \{0\} \times \{0\} \times X_t^{(3)} \times \mathbb{Z}_{m_4} \times \cdots \times \mathbb{Z}_{m_s} \\ & \qquad \vdots \\ & \cup \{0\} \times \{0\} \times \{0\} \times \cdots \times \{0\} \times X_t^{(s)} \end{aligned}$$

for $t = 0, 1$, $(\{0\}, X_0, X_1)$ gives a splitting of G by $-q$. Conversely, suppose that G has a splitting over $Z = \{0\}$ given by $-q$. Let $\mathbb{Z}_i = \{0\} \times \{0\} \times \ldots \times \mathbb{Z}_{m_i} \times \{0\} \times \ldots \{0\}$ be the subgroup of G isomorphic to $\mathbb{Z}_{m_i}$. If $(Z = \{0\}, X_0, X_1)$ gives a splitting for G by $-q$, then $(Z = \{0\}, \mathbb{Z}_i \cap X_0, \mathbb{Z}_i \cap X_1)$ gives a splitting for $\mathbb{Z}_i$ given by $-q$. Hence using Proposition 3.8, G has a splitting over $Z = \{0\}$ given by $-q$ if and only if each summand $\mathbb{Z}_{m_i}$ has a splitting over $Z = \{0\}$ given by $-q$ if and only if m_i is split by $-q$ for all $i = 1, 2, \ldots, m$ if and only if $ord_r(q) \not\equiv 2 \pmod 4$ for every prime r dividing m_i for all $i = 1, 2, \ldots, s$ if and only if $ord_r(q) \not\equiv 2 \pmod 4$ for every prime r dividing m. But the primes dividing m are precisely the primes dividing n. Thus G has a splitting over $Z = \{0\}$ given by $-q$ if and only if $ord_r(q) \not\equiv 2 \pmod 4$ for every prime r dividing n. $\square$

Example: Let $G = \mathbb{Z}_3 \times \mathbb{Z}_9$ and $\mathbb{F}_{4^2} = \mathbb{F}_{16}$. Note that $ord_3(4) = 1$ and by Theorem 3.9 the abelian group G has a partition which is split by -4. The cyclic groups $\mathbb{Z}_3$ and $\mathbb{Z}_9$ have splittings by the multiplier μ_{-4} given by $(\{0\}, A_1, A_2)$ and $(\{0\}, B_1 \cup B_3, B_2 \cup B_6)$, respectively, where A_i is the 16-cyclotomic coset modulo 3 containing i and B_j is the 16-cyclotomic coset modulo 9 which contains j. Define $C_{(i,j)}$ as the orbit of τ_{16} in G containing (i, j). Letting $X_0 = C_{(1,0)} \cup C_{(1,1)} \cup C_{(1,2)} \cup C_{(1,3)} \cup C_{(1,6)} \cup C_{(0,1)} \cup C_{(0,3)}$ and $X_1 = C_{(2,0)} \cup C_{(2,1)} \cup C_{(2,2)} \cup C_{(2,3)} \cup C_{(2,6)} \cup C_{(0,2)} \cup C_{(0,6)}$, the set $(\{(0,0)\}, X_0, X_1)$ gives a splitting of G by

-4. Notice that this partition can be obtained from the splittings of $\mathbb{Z}_3$ and $\mathbb{Z}_9$ as described in the proof. $\square$

We remark that $ord_r(q) \not\equiv 2 \pmod 4$ means that either $ord_r(q)$ is odd or $ord_r(q)$ is doubly even. It can easily be verified that $ord_r(q)$ is doubly even if and only if $ord_r(q^2)$ is even. Thus Theorem 3.9 can be restated as:

Theorem 3.10 *Let G be an abelian group of order n. The group G has a splitting over $Z = \{0\}$ given by $-q$ if and only if for every prime r dividing n, either $ord_r(q)$ is odd or $ord_r(q^2)$ is even.*

Thus we get the following condition for the existence of extended ideal codes of $F[G^*]$ which are Hermitian self-dual.

Theorem 3.11 *Let G be an abelian group of order n. An ideal code of $F[G^*]$ whose extension is Hermitian self-dual exists if and only if for every prime r dividing n, either $ord_r(q)$ is odd or $ord_r(q^2)$ is even.*

Proof. This is a direct consequence of Corollary 3.7 and Theorem 3.10. $\square$

We note that the same result as the preceding theorem was obtained by Martínez-Pérez and Willems in [14] for ideal codes in a group algebra over any finite group.

4 Counting Hermitian self-dual extended abelian group codes

Theorem 3.11 raises the question of counting the number of non-isomorphic abelian groups of order $\leq x$ for which an ideal code of $F[G^*]$ whose extension is Hermitian self-dual exists. An estimate for this quantity is provided by Theorem 4.3.

Let $q = p_1^t$ be a prime power and let $\mathcal{P}_q$ be the set of primes $r \neq p_1$ for which $\mathrm{ord}_r(q)$ is odd or $\mathrm{ord}_r(q^2)$ is even. Let $\mathcal{P}_q(x)$ be the associated counting function. The primes r not counted, that is the primes r such that $\mathrm{ord}_r(q) \equiv 2 (\mathrm{mod}\ 4)$ or the prime $r = p_1$ can be shown, see [2], to have a natural density $\delta(q)$ that is given by the following formula (with λ the exponent of 2 in the factorisation of t):

$$\delta(q) = \delta(p_1^t) = \begin{cases} 7/24 & \text{if } p_1 = 2 \text{ and } \lambda = 0; \\ 1/3 & \text{if } p_1 = 2 \text{ and } \lambda = 1; \\ 2^{-\lambda-1}/3 & \text{if } p_1 = 2 \text{ and } \lambda \geq 2; \\ 2^{-\lambda}/3 & \text{if } p_1 \neq 2. \end{cases}$$

It can be proved, see [2, Lemma A.3], that

$$\mathcal{P}_q(x) = (1 - \delta(q))\mathrm{Li}(x) + O_q\left(\frac{x(\log\log x)^4}{\log^3 x}\right), \tag{2}$$

where the subscript q indicates that the implied constant may depend on q and $Li(x) = \int_2^x dt/\log t$ denotes the logarithmic integral.

Let $\mathcal{G}_q$ be the subsemigroup of the natural numbers generated by the primes in $\mathcal{P}_q$. Let $HSD(x)$ count the number of non-isomorphic abelian groups of order n with $(n,q)=1$ and $n \leq x$ for which an ideal code of $F[G^*]$ whose extension is Hermitian self-dual exists. Then by Theorem 3.11 we have that

$$HSD(x) = \sum_{n \leq x,\ n \in \mathcal{G}_q} a(n),$$

where $a(n)$ denotes the number of non-isomorphic abelian groups having n elements.

Thus we are naturally led to study the behaviour of $a(n)$ on subsemigroups $\mathcal{G}$ of the natural numbers. For our purposes it is enough to restrict to subsemigroups $\mathcal{G}$ that are generated by a set $\mathcal{P}$ of primes satisfying

$$\mathcal{P}(x) = \tau \mathrm{Li}(x) + E_{\mathcal{P}}(x), \tag{3}$$

where $0 < \tau < 1$ and the error term $E_{\mathcal{P}}(x)$ is small enough.

Although the literature on $a(n)$ is quite extensive, the latter problem does not seem to have been studied before. Before delving into it, we recall some relevant facts on the behaviour of $a(n)$.

4.1 Counting non-isomorphic abelian groups

It is easy to see that $a(n)$ is a multiplicative function with the property that $a(p^k) = P(k)$ for every prime p and every integer $k \geq 1$, where $P(k)$ denotes the number of unrestricted partitions of k. Thus $a(p^k)$ does not depend on p but only on k, so that $a(n)$ is a "prime independent" multiplicative function.

An analytic approach to $a(n)$ is based on the fact that the Dirichlet series associated with this function may be written as products of the Riemann zeta function, which is defined for $\Re(s) > 1$ as $\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_p (1-p^{-s})^{-1}$ and otherwise by analytic continuation. Using the well-known identity

$$\sum_{k=0}^{\infty} P(k)x^k = \prod_{m=1}^{\infty} \frac{1}{1-x^m},\ |x| < 1,$$

one finds that, for $\Re(s) > 1$,

$$\sum_{k=0}^{\infty} \frac{a(p^k)}{p^{ks}} = \sum_{k=0}^{\infty} \frac{P(k)}{p^{ks}} = \prod_{m=1}^{\infty} \frac{1}{1-\frac{1}{p^{ms}}},$$

and thus, using the multiplicativity of $a(n)$,

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s} = \prod_p \sum_{k=0}^{\infty} \frac{a(p^k)}{p^{ks}} = \prod_p \prod_{m=1}^{\infty} \frac{1}{1-\frac{1}{p^{ms}}} = \prod_{m=1}^{\infty} \zeta(ms).$$

Using the standard results from tauberian theory, one obtains

$$\sum_{n\le x} a(n) \sim x \prod_{m=2}^{\infty} \zeta(m),\ x \to \infty,$$

from this. By much more refined methods, it can be shown that

$$\sum_{n\le x} a(n) = \sum_{m=1}^{3} c_m x^{1/m} + E(x),\ c_m = \prod_{\substack{k=1\\ k\ne m}}^{\infty} \zeta\left(\frac{k}{m}\right),$$

where the estimates for the error term $E(x)$ have a long history of improvements, with the best result to date being due to Robert and Sargos [25], who proved that $|E(x)| \ll x^{1/4+\epsilon}$. Furthermore one has, see [4, p. 274], $c_1 = 2.2948565916\cdots$, $c_2 = -14.6475663016\cdots$ and $c_3 = 118.6924619727\cdots$.

Thus on average $a(n)$ is constant (namely about 2.29). Individual values, however, might get large. In this direction Krätzel [10] proved that

$$\lim_{n\to\infty} \sup \log(a(n))\frac{\log\log n}{\log n} = \frac{\log 5}{4}, \tag{4}$$

which implies that $a(n) \ll n^{\epsilon}$ for every $\epsilon > 0$.

Ivić [9] has pointed out that $C(x)$, the number of *distinct* values assumed by $a(n)$ for $n \le x$, satisfies the bound

$$C(x) \le \exp((1+o(1))2\pi\sqrt{\log x/3\log\log x}). \tag{5}$$

The reason for this (see [9, pp. 130-131]) is that there are

$$\exp((1+o(1))2\pi\sqrt{\log x/3\log\log x})$$

integers $n \le x$ of the form

$$n = 2^{a_2}3^{a_3}\cdots p^{a_p},\ a_2 \ge a_3 \ge \cdots \ge a_p \ge 1, \tag{6}$$

which is a classical result of Hardy and Ramanujan [23, pp. 245-261]. Suppose that $a(n)$ is counted by $C(x)$, and let

$$n = p_{1,1}^{b_1}\cdots p_{1,k}^{b_k},\ b_1 \ge b_2 \ge \cdots \ge b_k \ge 1,$$

be the canonical decomposition of n. Then if $m = 2^{b_1}3^{b_2}\cdots p_k^{b_k}$, we have $m \le n$ and $a(m) = P(b_1)\cdots P(b_k) = a(n)$. Therefore $C(x)$ does not exceed the number of $n \le x$ having the form (6) and hence inequality (5) holds.

Note that if f is *any* prime independent function, then the number of distinct values assumed by it for $n \le x$ satisfies the same upperbound as in (5).

4.2 Summing $a(n)$ over $\mathcal{G}$

Let $\chi_{\mathcal{G}}$ be the characteristic function of $\mathcal{G}$, i.e.,

$$\chi_{\mathcal{G}}(n) = \begin{cases} 1 & \text{if } n \text{ is in } \mathcal{G}; \\ 0 & \text{otherwise.} \end{cases}$$

We consider

$$\sum_{n \le x,\ n \in \mathcal{G}} a(n) = \sum_{n \le x} \chi_{\mathcal{G}}(n) a(n).$$

Note that $\chi_{\mathcal{G}}(n)a(n)$ is multiplicative in n.

Theorem 4.1 *If* (3) *is satisfied with* $E_{\mathcal{P}}(x) = O(x \log^{-1-\gamma} x)$ *and* $0 < \gamma < 1$*, then*

$$\sum_{n \le x,\ n \in \mathcal{G}} a(n) = x b_0 \log^{\tau - 1} x + O_{\mathcal{G}}(x \log^{\tau - 1 - \gamma/2} x).$$

If (3) *is satisfied with* $E_{\mathcal{P}}(x) = O(x \log^{-2-\gamma} x)$ *and* $\gamma > 0$*. Then*

$$\sum_{n \le x,\ n \in \mathcal{G}} a(n) = x \sum_{0 \le \nu < \gamma} b_\nu \log^{\tau - 1 - \nu} x + O_{\mathcal{G}}(x \log^{\tau - 1 - \gamma + \epsilon} x), \tag{7}$$

where $b_0, b_1, \ldots$ *are constants possibly depending on* $\mathcal{G}$ *and*

$$b_0 = \frac{1}{\Gamma(\tau)} \lim_{s \downarrow 1} (s-1)^\tau \sum_{n \in \mathcal{G}} \frac{a(n)}{n^s} > 0.$$

The proof uses the following lemma, which except for the formula for b_0 is taken from [17]. The formula for b_0 is well-known.

Lemma 4.2 [17]. *Let* $f : \mathbb{N}_{\ge 0} \to \mathbb{R}_{\ge 0}$ *be a multiplicative function satisfying*

$$0 \le f(p^r) \le c_1 c_2^r,\ c_1 \ge 1,\ 1 \le c_2 < 2, \tag{8}$$

and

$$\sum_{p \le x} f(p) = \tau \mathrm{Li}(x) + O(x \log^{-2-\gamma} x), \tag{9}$$

where $\tau > 0$ *and* $\gamma > 0$ *are fixed, then, for* $\epsilon > 0$,

$$\sum_{n \le x} f(n) = x \sum_{0 \le \nu < \gamma} b_\nu \log^{\tau - 1 - \nu} x + O(x \log^{\tau - 1 - \gamma + \epsilon} x),$$

where $b_0 = \frac{1}{\Gamma(\tau)} \lim_{s \downarrow 1} (s-1)^\tau \sum_{n=1}^\infty f(n) n^{-s}$.

Proof of Theorem 4.1. The first assertion has been proved by Odoni [19] using a tauberian remainder theorem due to Subhankulov. □

In order to prove the second assertion we apply Lemma 4.2 with $f(n) = a(n)\chi_{\mathcal{G}}(n)$. The fact that condition (8) is satisfied follows from the classical result of Hardy and Ramanujan (see [23, p. 240]), that $a(p^r) = P(r) = (1 + o(1))(4\sqrt{3}r)^{-1}e^{\pi\sqrt{2r/3}}$ as r tends to infinity. However, the much more easily proved upperbound $P(r) \le 5^{r/4}$, see [10], is already sufficient in order to show that (8) is satisfied. The assumption on $E_{\mathcal{P}}(x)$ ensures that condition (9) is satisfied. On invoking Lemma 4.2 the proof is then completed.

For our problem at hand we the find the following estimate:

Theorem 4.3 *Let $HSD(x)$ count the number of non-isomorphic abelian groups of order n with $(n, q) = 1$ and $n \le x$ for which an ideal code of $F[G^*]$ whose extension is Hermitian self-dual exists. Then*

$$HSD(x) = b_0 \frac{x}{\log^{\delta(q)} x} + O_{\epsilon,q}\left(\frac{x}{\log^{\delta(q)+1-\epsilon} x}\right),$$

where

$$b_0 = \frac{1}{\Gamma(1-\delta(q))} \lim_{s\downarrow 1}(s-1)^{1-\delta(q)} \sum_{n\in\mathcal{G}} \frac{a(n)}{n^s}.$$

4.3 The connection with free arithmetical semigroups

A much weaker form of Theorem 4.3 is obtained as a straightforward consequence of Bredikhin's Theorem, which is a basic result in the theory of *free arithmetical semigroups*.

Let G be a commutative semigroup with identity element 1, relative to a multplication operation denoted by juxtaposition. Suppose that G has a finite or countably infinite subset P of generators and that G is *free*. This means that every element n in G has a unique factorisation of the form $n = \omega_1^{a_1} \cdot \omega_2^{a_2} \cdots \omega_r^{a_r}$, where the ω_r are distinct elements of P, the a_i are possible integers, and uniqueness is up to order of factors. A free semigroup will be called a free arithmetical semigroup if in addition there exists a homomorphism of G into some multiplicative semigroup $\overline{G}$ consisting of real numbers such that for every $x > 0$, G contains only finitely many elements n with $|n| \le x$, where $|n|$ denotes the image (or norm) of the element n of G under the homomorphism $|.|$. (In the older literature the generators of $\overline{G}$ are called Beurling's generalized primes.) Bredikhin's theorem, for a proof see e.g. [22, pp. 92-99], then reads as follows:

Theorem 4.4 *(Bredikhin.) If G is a free arithmetical semigroup such that*

$$\sum_{|\omega|\le x,\ \omega\in G} 1 = \tau \frac{x}{\log x} + O\left(\frac{x}{\log^{1+\gamma} x}\right), \tag{10}$$

where $\tau > 0$ *and* $\gamma > 0$ *are fixed, then*

$$\sum_{\substack{|n|\leq x\\ n\in G}} 1 = C_G x \log^{\tau-1} x + O(x\log^{\tau-1} x(\log\log x)^{-\gamma_1}),$$

where $\gamma_1 = \min(1,\gamma)$ *and* $C_G = \Gamma(\tau)^{-1}\lim_{s\downarrow 1}(s-1)^\tau \sum_{n\in G}|n|^{-s}$.

Now consider the free arithmetical semigroup G of all non-isomorphic finite abelian groups with as composition the usual direct product operation and as norm function $|A| = \mathrm{card}(A)$. By the fundamental theorem on finite abelian groups, G is a free arithmetical semigroup having $C(p)$, $C(p^2)$, $C(p^3), \cdots$ as generators, where p runs over all the primes and $C(n)$ is the cyclic group of order n. Since the number of cyclic groups of prime power order whose norm is not prime having norm $\leq x$ is $O(\sqrt{x}\log x)$, by the prime number theorem in the form $\pi(x) = x/\log x + O(x/\log^2 x)$, (10) is satisfied with $\tau = 1$ and $\gamma = 1$. It then follows from Bredikhin's theorem that

$$\sum_{\substack{|n|\leq x\\ n\in G}} 1 = \sum_{n\leq x} a(n) = x\prod_{m=2}^{\infty}\zeta(m) + O\left(\frac{x}{\log\log x}\right),$$

where we have used the observations that $\sum_{n\in G}|n|^{-s} = \sum_n a(n)n^{-s} = \prod_{m=1}^{\infty}\zeta(ms)$ and $\lim_{s\downarrow 1}(s-1)\zeta(s) = 1$.

Now let G_q be the free arithmetical semigroup generated by all cyclic groups of the form $C(p), C(p^2), C(p^3), \ldots$, with $\mathrm{ord}_p(q)$ is odd or $\mathrm{ord}_p(q^2)$ is even. Then similarly using Bredikhin's theorem we obtain the result in Theorem 4.3 with the much weaker error term $O_q(x\log^{-\delta(q)} x(\log\log x)^{-1})$.

4.4 The maximal order of $a(n)$ on $\mathcal{G}$

In this section we indicate what Krätzel's result (4) looks like when one considers the maximal order of $a(n)$ on the subsemigroup $\mathcal{G}$.

Theorem 4.5 *Let* $A = A(n)$ *be the smallest integer such that*

$$\sum_{p\in\mathcal{P},\ p\leq A} \log p \geq (\log n)/4.$$

Then as n *tends to infinity and runs through the elements of* $\mathcal{G}$*, the estimate*

$$\log a(n) \leq \mathcal{P}(A)\log 5 + O(\mathcal{P}(A^\theta)\log A),$$

holds with $\theta = \log(121)/\log(125) < 0.994$*, and there are infinitely many integers* n*,* $n \in G$*, for which one has* $\log a(n) = \mathcal{P}(A)\log 5$.

Proof. Completely similar to that of the (only) theorem in Schwarz and Wirsing [26], who proved this result in case $\mathcal{P}$ is the full set of primes. In their proof one merely intersects every range of primes that occurs with $\mathcal{P}$. □

`Remark`. The implicit constant in the order term can taken to be

$$\frac{2\pi^2}{3\log 5\cdot\log 2} = 5.898\cdots$$

Theorem 4.6 *If $\mathcal{P}(x)\sim\tau x/\log x$ as x tends to infinity, then*

$$\lim_{n\to\infty}\sup_{n\in\mathcal{G}}\log(a(n))\frac{\log\log n}{\log n} = \frac{\log 5}{4}.$$

Proof. By a standard argument in elementary number theory it follows that if $\mathcal{P}(x)\sim\tau x/\log x$, then $\sum_{p\in\mathcal{P},\ p\le x}\log p\sim\tau x$, $A(n)\sim(\log n)/(4\tau)$ and $\mathcal{P}(A)\sim\log n/(4\log\log n)$. On invoking Theorem 4.5 the result then follows. □

`Remark`. Let $p_1, p_2, \cdots$ denote the consecutive primes in $\mathcal{P}$. Let $n_r=\prod_{i=1}^r p_i^4$. Suppose that $\mathcal{P}(x)\sim\tau x/\log x$ as x tends to infinity. We leave it as an exercise to the reader to show that

$$\lim_{r\to\infty}\log(a(n_r))\frac{\log\log n_r}{\log n_r} = \frac{\log 5}{4}.$$

`Remark`. It is rather surprising that in Theorem 4.6 the estimate does not depend on τ. A similar situation arises if one compares the maximal order of $\log d(n)$ with that of $\log r(n)$, where $d(n)$ denotes the number of divisors of n and $r(n)$ the number of way n can be written as a sum of two squares. Jacobi proved that $r(n)=4\{d_1(n)-d_3(n)\}$, where $d_1(n)$ and $d_3(n)$ denote the number of the divisor of n of the form $4k+1$ and $4k+3$, respectively. Thus $r(n)$ counts (crudely) the divisors of n made up of prime $\equiv 1(\text{mod } 4)$. These primes have density $1/2$ amongst all primes, but nevertheless the maximal orders of $\log d(n)$ and $\log r(n)$ are the same. Namely, we have

$$\lim_{n\to\infty}\sup\log(d(n))\frac{\log\log n}{\log n} = \log 2,\quad \lim_{n\to\infty}\sup\log(r(n))\frac{\log\log n}{\log n} = \log 2.$$

For further details see e.g. Nicolas [18]. The maximal order for $\log d(n)$ was first determined by S. Wigert in 1907. Hardy and Wright [5, Theorem 338] erroneously give $(\log 2)/2$ instead of $\log 2$ in the result for $\log r(n)$.

4.5 Counting distinct values assumed by $a(n)$ on $\mathcal{G}$

Let $C_{\mathcal{G}}(x)$ denote the number of distinct values assumed by $a(n)$ with $n\in\mathcal{G}$ and $n\le x$.

Theorem 4.7 *Let p_0 be the smallest prime in $\mathcal{P}$. Suppose that there are positive constants c_3 and c_4 such that, for $x\ge p_0$,*

$$c_3x < \sum_{p\in\mathcal{P},\ p\le x}\log p < c_4x,$$

then

$$\log C_{\mathcal{G}}(x) \sim \log C(x) \sim (1+o(1))2\pi\sqrt{\log x/3\log\log x},$$

as x tends to infinity.

Proof. Very similar to that given in [23, pp. 245-261]. Instead of defining l_n to be the product of the first n consecutive primes, we define it to be the product of the first n consecutive primes in $\mathcal{P}$. Then instead of (3.23) we find $\phi(s) > c_1 \int_{p_0}^{\infty} e^{-c_1 sx}dx/\log x + O(1)$ and instead of (3.24) we find $\phi(s) < c_2 \int_{p_0}^{\infty} e^{-c_2 sx}dx/\log x + O(1)$. This, through Lemma 3.4, then leads to the same asymptotic for $\phi(s)$ as in the paper of Hardy and Ramanujan. This then results in the same asymptotic for $C_{\mathcal{G}}(x)$ as that for $C(x)$. □

Acknowledgements. The first author gratefully acknowledges financial support from the University of the Philippines and from the Philippine Council for Advanced Science and Technology Research and Development through the Department of Science and Technology.

The second author would like to thank Alexander Ivić for pointing out reference [25] to him.

References

[1] R.A. Brualdi, W.C. Huffman, V.S. Pless, *An Introduction to Algebraic Codes*, in *Handbook of Coding Theory*, V.S. Pless & W.C. Huffman (Editors), Elsevier Science, Amsterdam (1998), pp. 3-139.

[2] L. Dicuangco, P. Moree, P. Solé, *The Lengths of Hermitian Self-dual Extended Duadic Codes*. Preprint (2005), arXiv:math.CO/0511295, submitted.

[3] C. Ding, D.R. Kohel, S. Ling, *Split Group Codes*. IEEE Transactions on Information Theory, Vol. **IT-46** (2000), pp. 485-495.

[4] S.R. Finch, *Mathematical constants*. Encyclopedia of Mathematics and its Applications **94**, Cambridge University Press, Cambridge, 2003.

[5] G.H. Hardy, E.M. Wright, *An introduction to the theory of numbers*. Fifth edition. The Clarendon Press, Oxford University Press, New York, 1979

[6] W.C. Huffman, V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 2003.

[7] T.W. Hungerford, *Algebra*. Springer-Verlag, New York, 1974.

[8] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory (Second Edition)*. Graduate Texts in Mathematics **84**, Springer-Verlag, New York, 1990.

[9] A. Ivić, *On the number of abelian groups of a given order and on certain related multiplicative functions*. J. Number Theory, **16** (1983), pp. 119-137.

[10] E. Krätzel, *Die maximale Ordnung der Anzahl der wesentlich verschiedenen abelschen Gruppen n-ter Ordnung*. Quart. J. Math. Oxford Ser, **21** (1970), pp. 273-275.

[11] J.S. Leon, J.M. Masley, V. Pless, *Duadic Codes*. IEEE Transactions on Information Theory, Vol. **IT-30**, No. 5 (1984), pp. 709-714.

[12] F.J. MacWilliams, A.M. Odlyzko, N.J.A. Sloane, H.N. Ward, *Self-Dual Codes over GF(4)*. Journal of Combinatorial Theory, Series **A 25** (1978), pp. 288-318.

[13] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*. North Holland Publishing Company, Amsterdam (1983).

[14] C. Martínez-Pérez, W. Willems, *Self-Dual Extended Cyclic Codes*. Preprint (2004), http://www.math.uni-magdeburg.de/preprints/shadows/04-30report.html.

[15] P. Moree, *On the divisors of* $a^k + b^k$. Acta Arithmetica **80**, No. 3 (1997), pp. 197-212.

[16] P. Moree, *On primes* p *for which* d *divides* $ord_p(g)$. Funct. Approx. Comment. Math. **33** (2005), pp. 85-95.

[17] P. Moree and J. Cazaran, *On a claim of Ramanujan in his first letter to Hardy*. Exposition. Math., **17** (1999), pp. 289-311.

[18] J.-L. Nicolas, *On highly composite numbers*, in *Ramanujan revisited* (Urbana-Champaign, Ill., 1987), Academic Press, Boston, MA, 1988, pp. 215–244.

[19] R.W.K. Odoni, *A problem of Rankin on sums of powers of cusp-form coefficients*. J. London Math. Soc. (2), **44** (1991), pp. 203-217.

[20] V. Pless, *Q-Codes*. Journal of Combinatorial Theory, Series **A 43** (1986), pp. 258-276.

[21] V. Pless, J.M. Masley, J.S. Leon, *On Weights in Duadic Codes*. Journal of Combinatorial Theory, Series **A 44** (1987).

[22] A.G. Postnikov, *Introduction to analytic number theory*. Translations of Mathematical Monographs **68**, AMS, Providence, RI, 1988.

[23] S. Ramanujan, *Collected papers*. Chelsea, New York, 1962.

[24] J.J. Rushanan, *Duadic Codes and Difference Sets*. Journal of Combinatorial Theory, Series **A 57** (1991), pp. 254-261.

[25] O. Robert and P. Sargos, *Three-dimensional exponential sums with monomials*. J. Reine Angew. Math. **591** (2006), pp. 1-20.

[26] W. Schwarz and E. Wirsing, *The maximal number of non-isomorphic abelian groups of order* n. Arch. Math. (Basel), **24** (1973), pp. 59-62.

[27] M. Smid, *Duadic Codes*. IEEE Transactions on Information Theory, Vol. **IT-33** No. 3 (1987), pp. 432-433.

[28] M. Smid, *On Duadic Codes*. Master's Thesis, Eindhoven University of Technology, The Netherlands, 1986.

[29] H.N. Ward, *Quadratic Residue Codes and Divisibility*, in *Handbook of Coding Theory*, V.S. Pless & W.C. Huffman (Editors), Elsevier Science, Amsterdam (1998), pp. 827-870.

[30] H.N. Ward, L. Zhu, *Existence of Abelian Group Code Partitions*. Journal of Combinatorial Theory Series **A 67** (1994), pp. 276-281.