On Group-Theoretic Codes for Asymmetric Channels

TOR HELLESETH AND TORLEIV KLOVE

Department of Mathematics, University of Bergen,
N-5014 Bergen-U, Norway

We study single error-correcting codes for the asymmetric channel with input and output alphabets being \{0, 1, ..., a - 1\}. From an abelian group \(G\) of order \(N\) with elements \(g_0 = 0, g_1, ..., g_{N-1}\), Constantin and Rao (1979, Inform. Contr. 40, 20–36) define \(V_g = \{(b_1, b_2, ..., b_{N-1}) \in \{0, 1, ..., a - 1\}^{N-1} | \sum_{i=1}^{N-1} b_i g_i = g\}\) and show that \(V_g\) correct single errors. We give explicit expressions for the size and weight distribution of these codes. We further give a short discussion of some constant weight codes obtained by a similar construction.

1. INTRODUCTION

Consider a channel with \{0, 1, ..., a - 1\} as input and output alphabets. We call the channel asymmetric if it has the property that, if symbol \(b\) is transmitted, then only symbols \{0, 1, ..., \(b\)\} can be received. If \((b_1, b_2, ..., b_n)\) is transmitted and \((c_1, c_2, ..., c_n)\) is received we say that an error of weight \(\sum_{i=1}^{n} (b_i - c_i)\) (short: \(\sum_{i=1}^{n} (b_i - c_i)\)-error) has occurred.

Error-correcting codes for symmetric channels with a input and output symbols can be used to correct errors on asymmetric channels. One would expect, however, to find better codes (i.e., codes with more codewords) for the asymmetric channels. The first such codes were found by Kim and Freiman (1959). They are binary \((a = 2)\) 1-error-correcting codes which for most lengths \(n\) are better than the Hamming codes. Varshamov and Tenengol’ts (1965) defined a class of binary 1-error-correcting codes which are better than the Kim–Freiman codes for lengths \(n > 6\). Stanley and Yoder (1973) gave a large class of 1-error-correcting codes which included the Varshamov–Tenengol’ts codes. Constantin and Rao (1979) rediscovered a subclass of these codes. Codes to correct more than one error were given by Varshamov (1973).

In this paper we study the 1-error-correcting codes of Constantin and Rao (1979). Their construction is as follows. Let \(G\) be an abelian group of finite
The group operation is denoted by "\(+\)." Let the group elements be 
$g_0 = 0, g_1, g_2, \ldots, g_{N-1}$. Let $g$ be any element of $G$. The code $V_g$ is defined by

$$V_g = \{(b_1, b_2, \ldots, b_{N-1}) \in \{0, 1, \ldots, a-1\}^{N-1} \mid \sum_{i=1}^{N-1} b_i g_i = g\}$$

and corrects one asymmetric 1-error. The Varshamov–Tenengol'ts codes correspond to $G$ being cyclic. Since $V_{g_0}, V_{g_1}, \ldots, V_{g_{N-1}}$ is a partition of $\{0, 1, \ldots, a-1\}^{N-1}$, the largest of the $V_g$'s contains at least $a^{N-1}/N$ codewords.

The codes of Constantin and Rao have been studied independently by several authors, McEliece and Rodemich (1980), Helleseth and Kløve (1979), Delsarte and Piret (1979).

The size of the Varshamov–Tenengol'ts codes was determined by Ginzburg (1967) and their weight distribution was given by Stanley and Yoder (1973) and also by Mazur (1976). McEliece and Rodemich (1980) gave a formula for the size of the Constantin–Rao codes. Helleseth and Kløve (1979) and Delsarte and Piret (1979) also gave their weight distribution. The formulae of Helleseth and Kløve are more explicit and we shall give them in this paper. We shall use the notations of McEliece and Rodemich. The first part of the paper closely parallels their paper and we make it quite short.

The weight of a code word $(b_1, b_2, \ldots, b_n)$ is $\sum_{i=1}^{n} b_i$. In the binary case this coincides with the Hamming weight and the Constantin–Rao codes can be used to construct good constant weight codes. We give a short discussion of this construction.

### 2. Notations and Preliminaries

As usual $\mathbb{Z}_m$ denotes the (cyclic) additive group of integers modulo $m$.

From the definition of the codes $V_g$ it is clear that isomorphic groups define the same set of codes. Since any finite abelian group is isomorphic to a unique direct sum of cyclic groups of prime power order, it is no restriction to assume that $G$ is so defined, i.e.,

$$G = \sum_{p \in \mathbb{P}} \sum_{j=1}^{s_p} \mathbb{Z}_{p^{\rho_j}},$$

Let

$$E_p = \sum_{j=1}^{s_p} e_{\rho_j},$$
Then the order of $G$ is

$$N = \prod_{p \in \mathcal{P}} p^{e_p}.$$ 

Let

$$S = \sum_{p \in \mathcal{P}} s_p$$

be the total number of elements in the direct sum defining $G$. Then any element $g \in G$ can be represented by an $S$-tuple whose elements are subscripted by $p \in \mathcal{P}$ and $j, 1 \leq j \leq s_p$,

$$g = (g_{pj})_{p \in \mathcal{P}, 1 \leq j \leq s_p},$$

where $0 \leq g_{pj} < p^{e_p}$. For $g \in G$, let

$$V^*_g = \left\{(b_0, b_1, ..., b_{N-1}) \in \{0, 1, ..., a-1\}^N \mid \sum_{i=0}^{N-1} b_i g_i = g \right\}.$$ 

Let $t(g) = t_G(g)$ denote the size of $V^*_g$ and $t^*(g) = t^*_G(g)$ the size of $V^*$. Let $t(g, w)$ be the number of elements of weight $w$ in $V^*_g$ and

$$T_g(y) = \sum_w t(g, w) y^w,$$

and let $t^*(g, w)$ and $T^*_g(y)$ be similarly defined for $V^*_g$. Our aim is to determine $T_g(y)$ and $t(g)$. Note that $T^*_g(y) = \left(1 + y + \cdots + y^{a-1}\right) T_g(y)$, $t^*(g) = at(g)$, and $t^*(g) = T^*_g(1)$. We will determine $T^*_g(y)$; expressions for $T_g(y)$ and $t(g)$ then follow.

3. The Weight Distribution of the Constantin–Rao Codes

Let $G_1, ..., G_s$ be the cyclic groups of prime power order which have $G$ as a direct sum.

For $i = 1, 2, ..., S$, if $G_i = Z_{pe}$, let $\zeta_i = \exp(2\pi i / p^e)$. 

For \( g = (g_1, \ldots, g_s), \ h = (h_1, \ldots, h_s) \in G \), let
\[
\langle g, h \rangle = \prod_{i=1}^{s} \zeta_{s_i}^{g_i h_i}.
\]

Let
\[
\hat{T}_{g}^*(y) = \sum_{g \in G} \langle -h, g \rangle T_{g}^*(y).
\]

Then (McEliece and Rodemich (2.7))
\[
T_{g}^*(y) = \frac{1}{N} \sum_{h \in G} \langle h, g \rangle \hat{T}_{h}^*(y).
\]

Now, if \( A = \{0, 1, \ldots, a-1\}^N \), then
\[
\hat{T}_{g}^*(y) = \sum_{g \in G} \sum_{w} \langle -h, g \rangle y^w
\]
\[
\cdot \# \left\{ (b_0, \ldots, b_{N-1}) \mid \sum_{i=0}^{N-1} b_i g_i = g, \sum_{i=0}^{N-1} b_i = w \right\}
\]
\[
= \sum_{b \in A} \left( \sum_{i=0}^{N-1} b_i g_i \right) y^{\sum b_i}
\]
\[
= \prod_{b \in A} \left( \sum_{i=0}^{N-1} b_i \right) \langle -h, g_i \rangle^{b_i} y^{b_i}
\]
\[
= \prod_{i=0}^{N-1} \frac{1 - \langle -h, g_i \rangle y^a}{1 - \langle -h, g_i \rangle y^a} = \prod_{i=0}^{N-1} \left( 1 - \langle -h, g_i \rangle y^a \right)^{\frac{N-d}{d}}.
\]

Let \( O(h) \) denote the order of \( h \). If \( O(h) = d \), then \( g \mapsto \langle -h, g \rangle \) is a homomorphism from \( G \) onto the complex \( d \)th roots of unity. Hence, if \( \zeta \) is a primitive \( d \)th root of unity, then
\[
\prod_{i=0}^{N-1} \left( 1 - \langle -h, g_i \rangle y^a \right) = \left( \prod_{i=0}^{d-1} \left( 1 - \zeta^i y \right) \right)^{\frac{N-d}{d}} = (1 - y^d)^{\frac{N-d}{d}}.
\]

Since \( O(ah) = d/\gcd(a, d) \) we get similarly
\[
\prod_{i=0}^{N-1} (1 - \langle -ha, g_i \rangle y^a) = (1 - y^{ad/\gcd(a, d)})^{N \cdot \gcd(a, d)/d}.
\]
Hence

\[
T^*_g(y) = \frac{1}{N} \sum_{cd=N} \sum_{h \in G \atop O(h) = d} \langle h, g \rangle \hat{T}^*_h(y)
\]

\[
= \frac{1}{N} \sum_{cd=N} \frac{(1 - y^{Ad \cdot \gcd(a, d)}) \cdots \gcd(a, d)}{(1 - y^d)^c} \sum_{h \in G \atop O(h) = d} \langle h, g \rangle.
\]

Putting \( a = 2 \) and \( y = 1 \) we get Theorem 1 of McEliece and Rodemich (1980). To get a more explicit expression we have to determine the inner sum. For \( G \) a cyclic group this has been done by Ginzburg (1967) and for an elementary abelian group by Constantin and Rao (1979). Delsarte and Piret give a general expression which, however, contains some quantities \( \pi(k, d) \) for which no explicit formulae are given. As an illustration they determine the sum for \( G = \mathbb{Z}_p^2 \oplus \mathbb{Z}_p \). We shall now derive a general and explicit expression for the sum.

Let

\[
S_g(d) = \sum_{h \in G \atop O(h) = d} \langle h, g \rangle.
\]

Further, let

\[
W_k(d) = \sum_{h \in G \atop O(h) = d} \langle h, g \rangle,
\]

\[
W_{k_i}(d) = \sum_{h_i \in G_i \atop O(h_i) = d} \chi_{k_i}(h_i).
\]

First we prove that \( S_g(d) \) is multiplicative. Suppose \( \gcd(d_1, d_2) = 1 \). Then \( O(h) = d_1 d_2 \) if and only if

\[
h = h' + h'', \quad \text{where} \quad O(h') = d_1 \quad \text{and} \quad O(h'') = d_2.
\]

Hence

\[
S_g(d_1 d_2) - \sum_{O(h') = d_1, \atop O(h'') = d_2} \langle h', g \rangle \langle h'', g \rangle = S_g(d_1) S_g(d_2).
\]

Next we note that

\[
W_g(d) = \sum_{mn = d} S_g(n).
\]
Hence \( W_d(d) \) is multiplicative also, further by Moebius’ inversion formula

\[
S_d(d) = \sum_{mn=d} \mu(m) W_d(n).
\]

Since \( O(h) \mid n \) if and only if \( O(h_i) \mid n \) for \( 1 \leq i \leq S \), we get

\[
W_d(n) = \sum_{O(h_i) \mid n} \prod_{i=1}^{S} \zeta_{h_i}^{h_i} = \prod_{i=1}^{S} \sum_{O(h_i) \mid n} \zeta_{h_i}^{h_i} = \prod_{i=1}^{S} W_{h_i}(n).
\]

Let \( p \) be a prime dividing \( N \). We will determine \( W_{g_i}(p^\delta) \) where \( p^\delta \mid N \). If \( G_i = \mathbb{Z}_{q_i} \) where \( q_i \neq p \), then \( O(h_i) \mid p^\delta \) only when \( h_i = 0 \) and so \( W_{g_i}(p^\delta) = 1 \). If \( G_i = \mathbb{Z}_{p_e} \) we shall prove that

\[
W_{g_i}(p^\delta) = p^{\min(\delta, e)} \quad \text{if} \quad \delta \leq \gamma,
\]

\[
= 0 \quad \text{if} \quad \delta > \gamma,
\]

where \( \gamma \) is determined by

\[
\gamma = E_p \quad \text{if} \quad g_i = 0,
\]

\( p^\gamma \) is the exact power of \( p \) dividing \( g_i \)

if \( g_i \neq 0 \).

Note that \( 0 \leq \gamma < e \) or \( \gamma = E_p \).

If \( \delta \geq e \), then \( O(h_i) \mid p^\delta \) for all \( h_i \in \mathbb{Z}_{p^e} \). Hence

\[
W_{g_i}(p^\delta) = \sum_{h_i=1}^{p^e} \zeta_{h_i}^{\frac{p^\delta}{h_i}} = p^\delta \quad \text{if} \quad g_i = 0 \quad \text{(i.e.,} \quad \gamma = E_p),
\]

\[
= 0 \quad \text{if} \quad g_i \neq 0 \quad \text{(i.e.,} \quad \gamma < e).\]

If \( \delta < e \), then \( O(h_i) \mid p^\delta \) if and only if \( p^{\delta - \delta} \mid h_i \). Hence

\[
W_{g_i}(p^\delta) = \sum_{h_i=1}^{p^\delta} \zeta_{h_i}^{p^\delta - h_i} = p^\delta \quad \text{if} \quad g_i = 0 \mod p^\delta \quad \text{(i.e.,} \quad \gamma = \delta),
\]

\[
= 0 \quad \text{if} \quad g_i \neq 0 \mod p^\delta \quad \text{(i.e.,} \quad \gamma < \delta).\]

Therefore, if \( \delta > \gamma \) (in which case \( \gamma < E_p \)), then \( W_{g_i}(p^\delta) = 0 \), and if \( \delta \leq \gamma \), then

\[
W_{g_i}(p^\delta) = p^\delta \quad \text{if} \quad \delta < e,
\]

\[
= p^e \quad \text{if} \quad \delta \geq e.
\]

Collecting our results we see that, if \( g = (g_{p1})_{p \in \mathcal{P}, 1 \leq j \leq s_p} \) and

\[
\Delta(g) = \prod_{p \in \mathcal{P}} \gcd(g_{p1}, g_{p2}, \ldots, g_{ps_p}, p^{E_p}),
\]
then
\[
W_g \left( \prod_{p \in \mathcal{P}} p^{\delta_p} \right) = \prod_{p \in \mathcal{P}} p^{\sum_{j=1}^{\min(\delta_p, e_p)}} \quad \text{if } \prod_{p \in \mathcal{P}} p^{\delta_p} | \Delta(g),
\]
\[
= 0 \quad \text{otherwise}.
\]
Let
\[
W_G \left( \prod_{p \in \mathcal{P}} p^{\delta_p} \right) = \prod_{p \in \mathcal{P}} p^{\sum_{j=1}^{\min(\delta_p, e_p)}}.
\]

**Theorem.** For any \( g \in G \)
\[
T^*_g(y) = \frac{1}{N} \sum_{cd=N} \frac{(1 - yad/gcd(a,d))^c \cdot gcd(a,d)}{(1 - y^d)^c} \sum_{mn=d \atop n | \Delta(g)} \mu(m) W_G(n).
\]

**Corollary 1.**
\[
T_g(y) = \frac{1}{N} \cdot \frac{1 - y}{1 - y^a} \sum_{cd=N} \frac{(1 - yad/gcd(a,d))^c \cdot gcd(a,d)}{(1 - y^d)^c} \sum_{mn=d \atop n | \Delta(g)} \mu(m) W_g(n).
\]

**Corollary 2.**
\[
t(g) = \frac{1}{Na} \sum_{cd=N \atop \gcd(a,d) = 1} \alpha^c \sum_{mn=d \atop n | \Delta(g)} \mu(m) W_G(n)
\]
\[
= \frac{1}{Na} \sum_{mn=N \atop \gcd(a,n) = 1 \atop \gcd(m,a) = 1} W_G(n) \sum_{mc=r \atop \gcd(m,a) = 1} \mu(m) \alpha^c.
\]

**Corollary 3.** If \( \Delta(g) | \Delta(g') \), then \( t(g) \leq t(g') \). In particular \( t(1) \leq t(g) \leq t(0) \), where \( 1 = (1, 1, ..., 1) \), \( 0 = (0, 0, ..., 0) \).

**Corollary 4.** If \( g \in G = \mathbb{Z}_{p_0^{a_0}} \oplus \mathbb{Z}_{p_1^{a_1}} \), \( g' \in G' = \mathbb{Z}_{p_0^{a_0}} \oplus \mathbb{Z}_{p_1^{a_1}} \), and \( \Delta(g) = \Delta(g') \), then \( t_G(g) \leq t_{G'}(g') \).

**Proof.** Corollaries 3 and 4 follows from the fact that
\[
\sum_{mc=r \atop \gcd(m,a) = 1} \mu(m) \alpha^c > 0 \quad \text{for all } r \quad \text{and } \quad W_G(n) \leq W_{G'}(n) \quad \text{for all } n.
\]
COROLLARY 5. The group of order $N$ for which $t_0(0)$ take its maximal value is

$$G = \sum_{p \in \mathcal{P}} \sum_{i=1}^N \mathbb{Z}_p.$$ 

4. Binary Constant Weight Codes

An important application of binary asymmetric error-correcting codes is in the construction of constant weight codes for correction of symmetric errors. Both

$$V_{g,w} = \left\{ (b_1, b_2, \ldots, b_{N-1}) \in \{0, 1\}^{N-1} \left| \sum_{i=1}^{N-1} b_i g_i = g, \sum_{i=1}^{N-1} b_i = w \right. \right\}$$

and

$$V_{g,w}^* = \left\{ (b_1, b_2, \ldots, b_{N-1}) \in \{0, 1\}^N \left| \sum_{i=0}^{N-1} b_i g_i = g, \sum_{i=0}^{N-1} b_i = w \right. \right\}$$

have minimum Hamming distance at least 4. For $V_{g,w}$ this was first noted by Bose and Rao (1978) and for $V_{g,w}^*$ by Graham and Sloane (1980). Graham and Sloane considered only constructions based on cyclic groups. It turns out, however, that other groups in many cases will give larger codes. The size of $V_{g,w}^*$ is $t^*(g, w)$. By the theorem

$$\sum_{w=0}^{N} t^*(g, w) y^w = \frac{1}{N} \sum_{cd=N} (1 - (-y)^d)^c \sum_{\frac{m_n-d}{n|l(g)}} \mu(m) W_g(n).$$

Using the binomial theorem we find an explicit formula for $t^*(g, w)$. In another paper we have shown how to find the largest code $V_{g,w}^*$ for given $N$ and $w$, see Kløve (1979, 1981). For most values of $N$ and $w$ these codes are the largest constant weight codes known.

Received: September 6, 1979; revised: May 13, 1981

References


