法政大学学術機関リポジトリ
HOSEI UNIVERSITY REPOSITORY

PDF issue: 2024-06-13

Duadic符号の復号誤り率

疋田, 祐士 / HIKITA, Yuji

(発行年 / Year)
2006-03-24
(学位授与年月日 / Date of Granted)
2006-03-24
(学位名 / Degree Name)
修士(工学)
(学位授与機関 / Degree Grantor)
法政大学 (Hosei University)

修士論文

Duadic 符号の復号誤り率

Decoding error rate of duadic code

法政大学大学院工学研究科
システム工学専攻修士課程

04R6118
疋田祐士

指導教員　平松豊一教授

2005 年度

Abstract

In this paper, we treat Duadic Code and cyclotomic duadic codes. Quadratic residue Codes have idempotent generator. We propose a method of Construction of Duadic Codes by orbit decomposition. We compute weight distributions for decoding error rate, and comparison code rate with decoding error rate.

Key Words : duadic codes, weight distributions, orbit decomposition, decoding error rate

目次

１　はじめに……4
　１．１　符合理論とは……4
　１．２　通信系のモデル……4
　１．３　符号の種類……5

２　目的……7

３　基本事項……8
　３．１　ハミング符号とハミング重み……8
　３．２　誤り訂正・検出の原理……10
　３．３　線形符号……12
　３．４　巡回符号……15
　３．５　ハミング符号……17
　３．６　その他の数学的基礎……19

４　Duadic 符号……21
　４．１　冪等生成元……21
　４．２　平方剰余符号……22
　４．３　Duadic 符号……26

５　軌道分解……27
　５．１　軌道分解……27
　５．２　分割の構成……29

６　Duadic 符号の復号誤り率……32
　６．１　重さ分布……32
　６．２　復号誤り率……33
　６．３　Duadic 符号の復号誤り率……35

７　考察……42

８　結論……43

１．　はじめに

１．１　符合理論とは

符号理論とは，広い意味での情報理論の一分野である．広義の情報理論の最も主要なテーマは符号化である．符号化とは，広く言えば，情報の形態を変換することである．符号化はさまざまな目的で行われるが，情報理論の主な対象は，情報伝達の記録の効率向上のための符号化，信頼向上のための符号化，セキュリティ向上のための符号化の三つである．

効率向上のための符号化は情報源符号化，高能率符号化などと呼ばれ，情報の冗長性を除去し，圧縮して伝達または記録するために行われる．信頼性向上のための符号化は通信路符号化と呼ばれることもあるが，誤り訂正符号への符号化が中心である．セキュリティ向上のための符号化は，秘密を守ること，情報の偽造や不正や改変を防ぐことなどを目的として行われ，暗号が主役を演じる．

１．２　通信系のモデル

符号理論で取り扱うには，ディジタル化された情報である．これらの情報の発生源や，それをディジタル化する部分を含めて情報源という．

<情報源>
送りたい情報を 0,1 のビット列として発生させる．

<符号器>
符号器は情報ビット列をｋビットごとのブロックに区切って扱う．これを通報といい，$i=(i_1\cdots i_k)$で表す．符合器では，通報ｉに対応したnビットのビット列$w=(x_1\cdots x_n)$を出力する符号器で$m=n-k$ビットの余分なビットが付加されることになる．このnを符号長，ｋを情報ビット数という．また，wを符号語，この操作を符号化という．通報の種類が全部で$M=2^k$個あるので符号語もM種類ある．この符号語の全体$C=\{w_1\cdots w_M\}$を符号と呼ぶ．符号長n，情報ビット数ｋの符号を(n,k)符号といい，$R=\frac{k}{n}$を符号化率という．Ｒは符号の能率を表す量の１つであり，高いほど，望ましい．

<通信路>

通信路は, 送信語 $w=(x_1\cdots x_n)$ が入力されると, n ビットの受信語 $y=(y_1\cdots y_n)$ を出力する．伝送媒体に雑音等の影響がなければ送信語 $w=(x_1\cdots x_n)$ と同じものが出力されるが，実際にはある確率で異なったものが受信される．各ビットの誤りを e_i とし， $e=(e_1\cdots e_n)$ で表すとき，

$$y=w+e \tag{1}$$

ここで， e を誤りパターンという．

<復号器>

復号器では，y をもとにいずれの符号語が送信されたかを推測し，送信語 w の推定値 $\tilde{w}$ を得る．誤りパターン e に関する(1)式の計算はビットごとに mod 2 で行う．例えば，送信語 $w=(0110)$ を送ったとする．通信路で１ビット目が誤り，$y=(1110)$ を受信したとする．これは(1)式の誤りパターンが $e=(1000)$ であるに場合に相当する．

いままでは，符号語は 0,1 よりなるビット列であり，２元符号という．一般には，q 種類の記号からなる記号列でよい．この場合，q元符号という．このｑ種類を数字で表せば，０, １, …, ｑ-1 となる．

１．３　符号の種類

通信路で生じた誤りを訂正することを目的とした，いままでに述べた符号を誤り訂正符号という．他に，誤りの検出を目的とする誤り検出符号がある．両者をまとめて誤り制御符号と呼ぶこともある．２つの符号に本質的な差はなく，使われ方に違いがあるのみである．したがって，符号の種類は，

（１）受信語でまず誤りを検出し，その後その誤りを符号の能力によって訂正する．
（２）検出だけに止めておき，送信側にデータの再送を要求する．
（３）検出の後，データの性質を利用し他の正常なデータから誤ったデータから誤ったデータの正しい値を推測する．

さて, ランダム誤り訂正符号の能力は, 訂正可能な誤りの個数 t で評価される．

tが大きい符号が良い符号である．一般に，誤り訂正能力が高いと符号化率Rは低い．また，Rを一定にしたとき，符号長nが長いほど復号誤り率はちいさくなる．

符号がブロック単位で独立に通報と符号語を対応させているとき，ブロック符号といい，過去のブロックに関わって現時点の符号語が決まる逐次的な対応であるとき，畳み込み符号という．ブロック符号は，それが線形の方程式に基づいて定義されるとき，線形符号という．これはまた，巡回符号と非巡回符号に分類される．後者の中には，代数幾何符号が含まれる．

2　目的

符号長nの巡回符号を構成する際，多項式x^n-1を有限体上で因数分解することにより生成多項式を求める．しかし，巡回符号は$e(x)=e(x)^2$を満たす冪等生成元を持つ性質から，冪等の多項式を決定することが可能である．その代表的な例として平方剰余符号が挙げられ，その拡張として Cyclotomic Duadic 符号がある．

Cyclotomic Duadic 符号は 2 を冪剰余に持つ素数 p に対し，軌道分解し，条件に合う様に軌道を組み合わせることで構成される符号である．

本論分では軌道分解とその組み合わせ方の違いによる符号の具体的な構成法についての定理とプログラムを使い重み分布を調べ，復号誤り率を計算し符号化率と比較，検証する．

3　基本事項

3．1　ハミング距離とハミング重み

二つの記号uとvの間のハミング距離は

$$d_H(u,v)=\begin{cases}0, u=v\\ 1, u\neq v\end{cases}$$

で定義され，長さnの二つの系列$u=u_1u_2\cdots u_n$と$v=v_1v_2\cdots v_n$の間のハミング距離は,

$$d_H(u,v)=\sum_{i=1}^{n}d_H(u_i,v_i)$$

で定義される．ただし，この和は通常の整数の和である．すなわち，uとvの対応する位置にある成分の対のうち異なる対の数がuとvとのハミング距離である．

同じ長さの任意の系列u, v, wに対し，ハミング距離が三つの性質を持つことから容易に確かめられる．

非　負　性：$d_H(u,v)\geq 0$であり，＝0になるのは，$u=v$の場合に限る．

対　称　性：$d_H(u,v)=d_H(v,u)$

三角不等式：$d_H(u,v)\leq d_H(u,w)+d_H(w,v)$

この三つの性質は距離の三公理と呼ばれ，数学的にこれを満たすものを距離と呼ぶ．従って，ハミング距離は数学的な意味でも距離となっている．

長さがnの系列$u=u_1u_2\cdots u_n$の0でない成分の数をuのハミング重みと呼び,

$w_H(u)$で表す.

ハミング重みはハミング距離を用いて,

$$w_H(u)=d_H(u,0)$$

と書くことができる.

最小距離

ブロック符号の任意の二つの異なる符号語間のハミング距離の最小値をこの

符号の最小ハミング距離または最小距離と呼び，$d_{\min}$ で表す．これは，ランダム誤り通信路におけるこの符号の誤り訂正や誤り検出の能力を決める重要なパラメータである．なお，最小距離 $d_{\min}$ の (n,k) 符号を $(n,k,d_{\min})$ 符号と書くことがある．

３．２　誤り訂正・検出の原理

（１）誤り訂正の原理

符号語 w_1，符号Ｃが $C = w_1, w_2, \cdots, w_m$ とする．限界距離 t とＣの最小距離 $d_{\min}$ の関係が

$$d_{\min} \geq 2t+1$$

をみたすとき．送信語として w_1 を送り t 箇所以下の誤りを生じた y が受信されたとする．このとき，受信側で y に最も近い符号語 w_1 に訂正される．

w_1 を送信し，t 箇所以下の誤りが生じた y を受信したとする．このとき t が $d_{\min} \geq 2t+1$ を満たしていれば，各符号語間の距離に対して送信語 w_1 と受信語 y の距離が十分小さい．十分小さいとはつまり，受信語 y から最も近い符号語は w_1 ただ一つとなるということである．そこで，受信側で，送られてきた送信語は y から距離がもっとも近い w_1 であると判断し，y を w_1 に訂正する．

t 箇所以下の誤りのみ訂正対象とする復号法を限界距離復号法という．

（２）誤り検出の原理

送信語 w_1 に対し，r 個箇所以下の誤りが加わり受信語 y になったとする．y は w_1 を中心とする半径 r の小球内にある．そこで，

$$d \geq r+1$$

ならば，その小球の中に他の符号語はなく，y が他の符号語と一致することはない．したがって，誤りとして検出できる．しかし，訂正は必ずしもできない．また，r を超える個数の誤りが生じて，他の符号語と一致してしまった場合は誤りの検出もできず，見逃し誤りとなる．通信の分野では，誤り検出符号は古くから使われている．電話のように双方向に通信路がある場合は，誤りを検出できさえすれば，もう一度送るように頼むことができる．したがって，複雑な装置を要する誤り訂正符号を用いる必要はなくなる．

（３）誤り訂正同時検出の原理

少ない誤りに対しては訂正を，多い誤りに対しては検出する場合を考える．すなわち，t 重誤りまでは訂正し，それ以上 $t+1$ 重までは検出する場合を考える．

各符号語 w_i を中心とする半径 t の小球内の受信語は，中心の符号語に復号される．

この小球の訂正領域という．

$t+r$重誤りまでの誤りが加わり受信語yを得たとき, その検出されるためにはyが他の符号語の訂正領域になければよい. すなわち, 各符号語を中心とする半径$t+r$の小球が他の符号語を中心とする半径tの小球と重複部を持たなければよい.

$$d \geq 2t+r+1$$

をみたすt，rに対し，t重誤りを訂正し，同時に$t+r$重の誤りを検出することができる.

（例）
最小距離d=5の符号は，次の３通りの使い方がある.
（１）２重誤り訂正　(t=2,r=0)
（２）１誤り訂正かつ２重誤り検出　(t=1,r=2)
（３）４重誤り検出　(t=0,r=4)

これからもわかるように, 最小距離dを訂正能力と検出能力にいかに配分するかによって使い方が決まる.

３．３　線形符号

線形符号の定義

ガロア体GF(q)上のn次元ベクトル空間V_nとする．すなわち，V_nはGF(q)の元を成分とする長さnの系列（n次元ベクトル）すべての集合であり，ベクトル間の加算は成分ごとのGF(q)上の加算として行われ，ベクトルとGF(q)の元cとの乗算は，cをベクトルの各成分にGF(q)上で乗算することにより行われる．

ガロア体GF(q)を符号アルファベットとする符号長nの符号Cが，n次元ベクトル空間の部分空間をすなわち，この符号CはGF(q)上の線形符号(linear Code)であるという．言い換えれば，Cの任意の符号語w_1とw_2およびGF(q)の任意の元c_1とc_2に対し，

$$c_1 w_1 + c_2 w_2$$

がCの符号語となっているなら，Cを線形符号と呼ぶ．

ガロア体がGF(2)である場合には，c_1，c_2としては，0,1しかないから，２元符号Cが0=(0,0,…,0)を符号語として持ち，さらに任意の（異なる）二つの符号語w_1とw_2に対し$w_1 + w_2$が符号語となれば，Cは線形符号となる．

線形符号の基底

ガロア体GF(q)上の線形符号Cのｋ個の符号語$w_1, w_2, \cdots, w_k$を用いて，GF(q)の元を係数とする一次結合，

$$w = c_1 w_1 + c_2 w_2 + \cdots + c_k w_k$$

$$c_1, c_2, \cdots, c_k \in GF(q)$$

を作れば，線形符号の定義から，wは明らかにCの符号語である．

ここで，$w_1, w_2, \cdots, w_k$がGF(q)上で一次独立であるとしよう．すなわち，GF(q)の元$a_1, a_2, \cdots, a_k$に対し，

$$a_1 w_1 + a_2 w_2 + \cdots + a_k w_k = 0$$

となるのが$a_1 = a_2 = \cdots = a_k = 0$のときに限るとするのである．このとき，Cの任

意の符号語wが上式で表すことができるなら，$\{w_1, w_2, \cdots, w_k\}$はこの線形符号の基底をなすという．また，基底に含まれる符号語のｋをこの線形符号Ｃの次元と呼び，dim(C)で表す．線形符号Cの基底は一般にいくつもの選び方があるが，dim(C)は線形符号Ｃに対し一意的に定まる．

生成行列

生成行列の定義と基本行操作

GF(q)上の符号長nの線形符号Cの基底$\{w_1, w_2, \cdots, w_k\}$に含まれる各符号語を行として並べた$k \times n$行列をCの生成行列と呼ぶ．線形符号$w$は基底を用いて次の定理が得られる．

定理

GF(q)上の符号長nの線形符号Cの生成行列をGとすれば，GF(q)上のn次元ベクトルwがCの符号語となる必要十分条件は，

$$w = (c_1, c_2, \cdots, c_k)G$$

と書けることである．ここに，$c_1, c_2, \cdots, c_k$はGF(q)の元である．

基底は一般に複数個存在するから，Cの生成行列も一般に複数個存在する．実際，線形符号Cの任意の生成行列に対し，次の基本操作を施したものはまたCの生成行列になっている．

〔基本操作〕

(1)　任意の二つの行を交差する．

(2)　任意の行に，他の任意の行にGF(q)の元を乗じたものを加える．

(3)　任意の行にGF(q)の0でない元を乗じる．

２元符号の場合には(3)の操作は意味がないし，(2)の操作で意味があるのは，(2’)任意の行に他の任意の行を加える，という操作である．

基本行操作は，結局，$k \times n$生成行列に左からk次正則行列を掛ける操作の手順を与えるものと言ってもよい．線形符号Cの一つの生成行列から，基本行操作によって，Cのすべての生成行列を導くことができる．

３．４　巡回符号

GF(q)上の(n,k)線形符号Ｃの任意の符号語を，

$$w=\left(w_{n-1},w_{n-2},\cdots,w_{1,}w_0\right)$$

とする．この符号語を巡回置換した

$$w=\left(w_{n-2},\cdots,w_{1,}w_0,w_{n-1}\right)$$

が常にＣの符号語になるなら，Cを巡回符号という．

巡回符号を扱うには，GF(q)上のn次元ベクトル$w=\{w_{n-1},\cdots,w_1,w_0\}$をGF(q)上の多項式

$$w=w_{n-1}x^{n-1}+\cdots+w_1x+w_0$$

で表せる．特に符号語をこのような多項式で表現したものを符号多項式(Code-polynomial)と呼ぶ.

このような多項式表現を用いると，wの巡回置換は次式のように表せる．

$$\begin{aligned}&w_{n-2}x^{n-1}+\cdots+w_1x^2+w_0x+w_{n-1}\\&=\left[xW(x)\right]\mathrm{mod}\left(x^n-1\right)\end{aligned}$$

ここで，この剰余をとるという演算が線形であることに注意しておく．すなわち，任意の多項式$A_1(X)$，$A_2(X)$に対し，次式が成立する．

$$\begin{aligned}&\left[A_1(x)+A_2(x)\right]\mathrm{mod}\,B(x)\\&=\left[A_1(x)\right]\mathrm{mod}\,B(x)+\left[A_2(x)\right]\mathrm{mod}\,B(x)\end{aligned}$$

さて，巡回符号の定理から，任意の符号語wに対し，それをi回巡回置換したものも符号語となる．従って，$W(x)$が符号多項式であれば，

$$\left[x^iW(x)\right]\mathrm{mod}\left(x^n-1\right)$$

も符号多項式になる．また，巡回符号は線形符号であるから，このような符号多項式の任意の一次結合もまた符号多項式となる．従って，任意の正整数mとGF(q)の任意の元

$$\sum_{i=1}^{m} a_i \left[x^i W(x)\right] \bmod \left(x^n - 1\right)$$
$$= \left[A(x) W(x)\right] \bmod \left(x^n - 1\right)$$

もまた符号多項式となる．すなわち，符号多項式$W(x)$に任意の多項式$A(x)$を乗じ，$x^n - 1$で割った剰余をとれば，その結果はまた符号多項式となるのである．

巡回符号Ｃの0を除く符号多項式で次数が最小で最高次の係数が１である多項式を生成多項式という．

符号多項式$W(x)$は

$$W(x) = A(x)G(x)$$

$W(x)$：符号多項式，$A(x)$：通報多項式，$G(x)$：生成多項式

で表せる．

q元(n,k)巡回符号Ｃの生成多項式$G(x)$とするとき

$$H(x) = \frac{x^n - 1}{G(x)}$$

をＣの検査多項式という．

３．５　ハミング符号

１個の誤りを訂正する２元線形符号（単一誤り訂正２元線形符号）の構成法を考えよう．単一誤りを訂正するには，それの対するシンドロームがすべて異なり，しかも 0 でなければよい.

ここで，２元(n,k)線形符号Ｃの検査符号 $H=\left[h_1 h_2 \cdots h_n\right]$ とする．$h_i (i=1,\cdots,n)$ は GF(2)上の $n-k$ 次元列ベクトルである．また，第 i 番目の位置に生じた単一誤り語を e_i とする．すなわち，

$$e_i = (00\cdots010\cdots00)$$

このような誤りに対するシンドロームは,

$$s = e_i H^T = h_i^T$$

となる．ここで h_i^T は h_i を転置した行ベクトルを表す．従って，このような単一誤りに対しシンドロームがすべて異なり, 0 とならないためには, $h_i (i=1,\cdots,n)$ がすべて異なり，しかもどれも 0 でなければよい.

任意の正整数mに対し，GF(2)上の 0 でないm次元ベクトルで異なるものの数は 2^m-1，情報ビット $k=n-m$ の符号は単一誤り訂正符号となる．この符号をハミング符号と呼ぶ.

ハミング符号の検査行列が

$$H=\left[P^T I_m\right]$$

という規約標準形で与えられていたとしよう．ここで，P は検査記号生成行列であり，この場合 GF(2)上の $k\times m$ 行列である．ただし，$k=n-m$ である．P を用いれば，k 個の情報ビット $m_{1,}\cdots,m_k$ から m 個の検査ビット $p_{1,}\cdots,p_m$ を

$$(p_{1,}\cdots,p_m)=(m_1,\cdots,m_k)P$$

により計算できる. ここで, Ｐの(i,j)の要素を $p_{i,j}\left(i=1,\cdots,k;\ j=1,\cdots,m\right)$ とすると,

この式は,

$$p_j = p_{1j}m_1 + p_{2j}m_2 + \cdots + p_{kj}m_j, j = 1, \cdots, m$$

と書ける．この加算を排他的論理和を用いて実行すれば，ハミング符号の符号化が行える．

受信語からのシンドロームの生成は上で述べた方法で行えばよい．シンドロームから誤り語を推定するには，シンドロームと単一誤りの誤り語との対応表を用いてもよいし，シンドロームを入力するとそれに対応する単一誤り語を出力するような理論回路を構成してもよい．これらの表や回路は，第i列（の転置）になることから，容易に作ることができる．

３．６　その他の数学的基礎

位数

GF$\left(p^m\right)$の任意の元$\delta(\neq 0)$に対し

$$\delta^n = 1$$

となる最小の正整数ｎをδの位数という.

（例）

$\delta = \alpha^3$とすると,

$$\left(\alpha^3\right)^2 = \alpha^6 \qquad \left(\alpha^3\right)^3 = \alpha^9 \qquad \left(\alpha^3\right)^4 = \alpha^{12} \qquad \left(\alpha^3\right)^5 = \alpha^{15} = 1$$

$$\therefore \alpha^3\text{の位数は}5$$

$\delta = \alpha$とすると,

αは，原始元であるからαの位数は$2^4 - 1 = 15$

共役根

GF(2)上では,

$$\left(F(x)\right)^2 = F\left(x\right)^2$$

である.

従って，GF(2)上において，δが$F(x)$の根であれば，$F(\delta) = 0$より,

$$\left(F(x)\right)^2 = F\left(\delta^2\right) = 0$$

であるから，δ^2も$F(x)$の根となる.

GF(q)上では,

$$\left(F(x)\right)^q = F\left(x\right)^q$$

であり，共役根は$\delta, \delta^q, \delta^{q^2}, \cdots, \delta^{q^{d-1}}$である.

$d : \delta^{2^{d'}} = \delta$となる$d'$の最小の正整数

（例）

GF(2^4)において,

α の共役根 $\{\alpha, \alpha^2, \alpha^4, \alpha^8\}$ $\quad (\alpha^{16} = \alpha)$

α^3 の共役根 $\{\alpha^3, \alpha^6, \alpha^{16}, \alpha^9\}$ $\quad (\alpha^{24} = \alpha^9, \alpha^{18} = \alpha^3)$

（例）

α^3 の最小多項式 $M_3(x)$ を求める.

α^3 の共役根は $\{\alpha^3, \alpha^6, \alpha^{16}, \alpha^9\}$

$$M_3(x) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9)$$

$$= x^4 + x^3 + x^2 + x + 1$$

α は原始多項式の根だから α の最小多項式 $M_1(x)$ は原始多項式

$$M_1(x) = x^4 + x + 1$$

４　Duadic符号

４.1　冪等生成元（idempotent）

ある多項式を２乗したものが元に戻る多項式のことを冪等元という.

（例）

$$e(x) = x^4 + x^2 + x + 1$$

このとき

$$\begin{aligned} e(x)^2 &= \left(x^4 + x^2 + x + 1\right)^2 \quad \bmod x^7 - 1 \\ &= x^8 + x^4 + x^2 + 1 \\ &\equiv x^4 + x^2 + x + 1 = e(x) \end{aligned}$$

したがって，この e(x)は冪等元になる.

巡回符号においては，生成多項式の代わりに同じ符号内の符号多項式を用いても，同等の符号が得られる．ここで，生成多項式の代わりに用いる冪等元を冪等生成元という．冪等生成元を集合Ｅを用いて

$$e(x) = \sum_{i=0}^{n-1} e_i x^i = \sum_{i \in E} x^i \in F_2[x]$$

とおくとき，$e(x)^2 = \sum_{i=0}^{n-1} e_i x^{2i}$ だから $e(x) = e(x)^2$ であるためには,

$$2\mathrm{E} = \mathrm{E}$$

でならなければならない.

４．２　平方剰余符号（Quadratic Residue Codes）

冪等生成元により構成される典型的な符号が平方剰余符号である．

p を奇素数とし，a と p が互いに素であるとき

$$x^2 \equiv a \pmod{p}$$

が解を持つとき，a と p を法として平方剰余であるといい，

$$\left(\frac{a}{p}\right) = 1$$

と書く．そうでないとき，平方非剰余といい

$$\left(\frac{a}{p}\right) = -1$$

と書く．

この記号$\left(\frac{a}{p}\right)$をルジャンドルの平方剰余記号という．

オイラーの基準

p を奇素数とし，a を p と互いに素な有理整数とする．そのとき

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

が成立する．

（証明）

$A = \{1,2,\cdots, p-1\}$ とおく．$r \in A$ に対し，

$$1\cdot r, 2\cdot r, \cdots, (p-1)\cdot r$$

も法 p に関する既約類の代表系になる．このとき，$(a, p) = 1$ だから，$sr \equiv a \pmod{p}$ となるＡの元 r がただ一つである．そして，対応 $r \to s$ は単射である．この s と r を互いの同伴数という．

(1)

$\left(\frac{a}{p}\right) = 1$ のとき．$X^2 \equiv a \pmod{p}$ は解 $X = r$ をもつ．このことは，r がそれ自身同伴であることを示す．$(p-r)^2 \equiv a \pmod{p}$ だから，$p-r$ も自分自身と同伴である．

r と $p-r$ は p を法として合同でないから，２次方程式

$$X^2 \equiv a \pmod{p}$$

の解 r と $p-r$ の２個のみである．したがって，Ａの元の残りｐ - ３個は互いに同伴なものの組に分かれる．ゆえに

$$1\cdot 2\cdots(p-1) = (p-1)! \equiv r(p-r)a^{\frac{p-3}{2}} \pmod{p}$$

$$\equiv -a^{\frac{p-1}{2}} \pmod{p}$$

となる．よって

$$(p-1)! \equiv -a^{\frac{p-1}{2}} \pmod{p}$$

(2)

$\left(\frac{a}{p}\right) = -1$ のとき． $X^2 \equiv a \pmod{p}$ は解を持たないから，(1) と同様にして

$$(p-1)! \equiv a^{\frac{p-1}{2}} \pmod{p}$$

さて， $a = 1$ のときは， $\left(\frac{1}{p}\right) = 1$ だから (1) より

$$(p-1)! \equiv -1 \pmod{p}$$

したがって， $\left(\frac{a}{p}\right) = 1$ ならば $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$， $\left(\frac{a}{p}\right) = -1$ ならば $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ と

なる．よって，

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

（オイラー）

ｐを奇素数とするとき，

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

が成立する．

（証明）

$a=-1$とする．$(-1,p)=1$だから，

$$\left(\frac{-1}{p}\right)\equiv(-1)^{\frac{p-1}{2}}(\mathrm{mod}\ p)$$

pは奇素数だから等号が成立する．

（フェルマーの小定理）

pを任意の素数として，$(a,p)=1$とする．そのとき，$a^{p-1}\equiv 1(\mathrm{mod}\ p)$が成立する．

（証明）

$p=2$のときは明らかである． $p\neq 2$のとき， $a^{\frac{p-1}{2}}\equiv\pm 1(\mathrm{mod}\ p)$の両辺を証明すればよい．

系． pを奇素数とし， $(a,p)=(b,p)=1$とする．そのとき，

(1) $a\equiv b(\mathrm{mod}\ p)$ならば$\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$．

(2)$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$，つまり$(l,p)=1$のとき，$\left(\frac{l}{p}\right)$は$l$について乗法的である．

（証明）

$$\left(\frac{ab}{p}\right)\equiv(ab)^{\frac{p-1}{2}}=a^{\frac{p-1}{2}}b^{\frac{p-1}{2}}=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)(\mathrm{mod}\ p)$$

ここでpは奇数だから

$$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

を得る．

２元の平方剰余符号では, 2 が平方剰余となるような素数を符号長にとる必要がある.

$$p \equiv \pm 1 \pmod 8$$
$$E = \{ i^2 ; i \in \mathrm{F}_p \}$$
$$e(x) = \sum_{i \in E} x^i$$

このような多項式は冪等元となっている．このようにしてできた冪等生成元により構成される符号が平方剰余符号である.

（例）

符号長 n=7 の平方剰余符号

$$\text{平方剰余} \mathrm{E} = \{1,2,4\},$$
$$\text{平方非剰余} \mathrm{E}^{\perp} = \{3,5,6\}$$

これらによって生成される冪等生成元はそれぞれ

$$e(x) = x^4 + x^2 + x$$
$$e(x) + 1 = x^4 + x^2 + x + 1$$
$$e^{\perp}(x) = x^6 + x^5 + x^3$$
$$e^{\perp}(x) + 1 = x^6 + x^5 + x^3 + 1$$

となる.

４．３　Duadic 符号

集合Ｅにより構成される次の多項式の中の一つを冪等生成元として用いることで Duadic 符号を定義することが出来る.

Z/nZ の分割

$$E \cup E^{\perp} = (Z/nZ)^{\times}$$

$$E \cap E^{\perp} = \phi$$

$$\mu E = E^{\perp}$$

$$\mu E^{\perp} = E$$

$$\left(|E| = |E^{\perp}| = \frac{n-1}{2}, \mu \in (Z/nZ)^{\times} \right)$$

と分割したとき,

$$e(x) = \sum_{i \in E} x^i, e(x)^{\perp} = \sum_{i \in E^{\perp}} x^i$$

$$1 + e(x) = \sum_{i \in E \cup \{0\}} x^i, 1 + e(x)^{\perp} = \sum_{i \in E^{\perp} \cup \{0\}} x^i$$

が冪等になる.

５ 軌道分解

５．１軌道分解

$e(x)=\sum_{i\in E}x^i$ が冪等であるためには，Z/nZ を 2 の乗法による作用で軌道分解したとき，Ｅが軌道の和集合になっていればよい；$(Z/nZ)^{\times}$ の乗法部分群をＧとするとき，

$$C_a=\{ag:g\in G\}(a\in Z/nZ)$$

を a の軌道という．このとき $(Z/nZ)^{\times}$ は互いに交わらない軌道の和集合に表せる．Ｇとしてとくに $g\in(Z/nZ)^{\times}$ の生成する部分群を取ったとき

$$Z/nZ=\bigcup_a C_a,\quad a\neq a'\text{ならば}C_a\cap C_{a'}=\phi$$

をｇの乗法による作用での軌道分解という．

$p=2ef+1$ を奇素数とする．F_p の原始元をｇとし，$F_p^{\times}$ を g^{2e} の乗法による作用で軌道分解したときの軌道分解したときの軌道を，

$$C_i=\left\{g^{2ex+i}:0\le x\le\frac{p-1}{2e}-1\right\}\quad(0\le i\le 2e-1)$$

と記す．一般化した式は

$$\begin{aligned}C_0&=\{g^0,2^1g^0,2^2g^0,\cdots\}\\C_1&=\{g^1,2^1g^1,2^2g^1,\cdots\}\\C_2&=\{g^2,2^1g^2,2^2g^2,\cdots\}\\\vdots&\qquad\vdots\end{aligned}$$

と表すことができる．

分割Ｅ，$E^{\perp}$ がこれらの軌道の輪集合であるとき，２元 Duadic 符号のを位数 2e の Cyclotomic Duadic 符号という．

定理

（１）４乗剰余

pが以下の条件を満たすとき位数 2e=4 の平方剰余符号と異なる Cyclotomic Duadic 符号が存在する.

$$\left\{p \equiv 1(\mathrm{mod}\ 8) p = a^2 + 64b^2\right\}$$

（２）６乗剰余

pが以下の条件を満たすとき位数 2e=6 の平方剰余符号と異なる Cyclotomic Duadic 符号が存在する.

$$\left\{p \equiv 1,7(\mathrm{mod}\ 24) p = x^2 + 27y^2\right\}$$

一般に，2 が mod p で 2e 乗剰余，すなわち

$$p \equiv 1 \bmod 2e \text{かつ} 2^{\frac{p-1}{2e}} \equiv 1 \bmod p$$

のとき，分割の具体的な構成法を与えることができる.

５．２　分割の構成

定理

l を，$2e/l$ が偶数となる様な，$2e$ の約数としたとき，
次の様に分割を構成することができる．

$$\mathrm{E}_{\mathrm{l,m}} = \bigcup_{a\equiv m,\cdots m+l-1 \pmod{2l}} C_a,$$

$$\mathrm{E}^{\perp}{}_{\mathrm{l,m}} = \bigcup_{a\equiv m,\cdots m+2l-1 \pmod{2l}} C_a$$

とくに $l=1$ のとき $\mathrm{E}_{1,0}$, $\mathrm{E}^{\perp}{}_{1,0}$ は平方剰余と平方非剰余への分割となり，得られる符号は平方剰余符号となる．また，分割の総数は

$$\sum_{l|e} l$$

となる．

（例）$F_{73}^{\times}$ の軌道分解は以下の通りである．

p=73，g=5，l=1,2,4

$C_0 = \{1, 2, 4, 8, 16, 32, 64, 55, 37\}$
$C_1 = \{5, 10, 20, 40, 7, 14, 28, 56, 39\}$
$C_2 = \{25, 50, 27, 54, 35, 70, 67, 61, 49\}$
$C_3 = \{52, 31, 62, 51, 29, 58, 43, 13, 26\}$
$C_4 = \{41, 9, 18, 36, 72, 71, 69, 65, 57\}$
$C_5 = \{59, 45, 17, 34, 68, 63, , 53, 33, 66\}$
$C_6 = \{3, 6, 12, 24, 48, 23, 46, 19, 38\}$
$C_7 = \{15, 30, 60, 47, 21, 42, 11, 22, 44\}$

これらの８つの軌道から，以下の７つの分割が得られる．

$$\left(\mathrm{E}_{1,0},\mathrm{E}^{\perp}{}_{1,0}\right)=\left(\mathrm{C}_0\cup\mathrm{C}_2\cup\mathrm{C}_4\cup\mathrm{C}_6,\mathrm{C}_1\cup\mathrm{C}_3\cup\mathrm{C}_5\cup\mathrm{C}_7\right)$$
$$\left(\mathrm{E}_{2,0},\mathrm{E}^{\perp}{}_{2,0}\right)=\left(\mathrm{C}_0\cup\mathrm{C}_1\cup\mathrm{C}_4\cup\mathrm{C}_5,\mathrm{C}_2\cup\mathrm{C}_3\cup\mathrm{C}_6\cup\mathrm{C}_7\right)$$
$$\left(\mathrm{E}_{2,1},\mathrm{E}^{\perp}{}_{2,1}\right)=\left(\mathrm{C}_0\cup\mathrm{C}_3\cup\mathrm{C}_4\cup\mathrm{C}_7,\mathrm{C}_1\cup\mathrm{C}_2\cup\mathrm{C}_5\cup\mathrm{C}_6\right)$$
$$\left(\mathrm{E}_{4,0},\mathrm{E}^{\perp}{}_{4,0}\right)=\left(\mathrm{C}_0\cup\mathrm{C}_1\cup\mathrm{C}_2\cup\mathrm{C}_3,\mathrm{C}_4\cup\mathrm{C}_5\cup\mathrm{C}_6\cup\mathrm{C}_7\right)$$
$$\left(\mathrm{E}_{4,1},\mathrm{E}^{\perp}{}_{4,1}\right)=\left(\mathrm{C}_0\cup\mathrm{C}_5\cup\mathrm{C}_6\cup\mathrm{C}_7,\mathrm{C}_1\cup\mathrm{C}_2\cup\mathrm{C}_3\cup\mathrm{C}_4\right)$$
$$\left(\mathrm{E}_{4,2},\mathrm{E}^{\perp}{}_{4,2}\right)=\left(\mathrm{C}_0\cup\mathrm{C}_1\cup\mathrm{C}_6\cup\mathrm{C}_7,\mathrm{C}_2\cup\mathrm{C}_3\cup\mathrm{C}_4\cup\mathrm{C}_5\right)$$
$$\left(\mathrm{E}_{4,3},\mathrm{E}^{\perp}{}_{4,3}\right)=\left(\mathrm{C}_0\cup\mathrm{C}_1\cup\mathrm{C}_2\cup\mathrm{C}_7,\mathrm{C}_3\cup\mathrm{C}_4\cup\mathrm{C}_5\cup\mathrm{C}_6\right)$$

分割の総数
l=1,2,4 より７つ
最初の分割からは平方剰余符号を得られるが,
残りは平方剰余符号と同値ではない.

（例） $F_{31}^{\times}$ の軌道分解は以下の通りである.

p=31，g=3，l=1,3

$$C_0=\{1,2,4,8,16\}$$
$$C_1=\{3,6,12,24,17\}$$
$$C_2=\{9,18,5,10,20\}$$
$$C_3=\{27,23,15,30,29\}$$
$$C_4=\{19,7,14,28,27\}$$
$$C_5=\{26,21,11,22,13\}$$

これらの４つの軌道から，以下の３つの分割が得られる.

$$\left(\mathrm{E}_{1,0},\mathrm{E}^{\perp}{}_{1,0}\right)=\left(\mathrm{C}_0\cup\mathrm{C}_2\cup\mathrm{C}_4,\mathrm{C}_1\cup\mathrm{C}_3\cup\mathrm{C}_5\right)$$
$$\left(\mathrm{E}_{3,0},\mathrm{E}^{\perp}{}_{3,0}\right)=\left(\mathrm{C}_0\cup\mathrm{C}_1\cup\mathrm{C}_2,\mathrm{C}_3\cup\mathrm{C}_4\cup\mathrm{C}_5\right)$$
$$\left(\mathrm{E}_{3,1},\mathrm{E}^{\perp}{}_{3,1}\right)=\left(\mathrm{C}_0\cup\mathrm{C}_4\cup\mathrm{C}_5,\mathrm{C}_1\cup\mathrm{C}_2\cup\mathrm{C}_3\right)$$
$$\left(\mathrm{E}_{3,2},\mathrm{E}^{\perp}{}_{3,2}\right)=\left(\mathrm{C}_0\cup\mathrm{C}_1\cup\mathrm{C}_5,\mathrm{C}_2\cup\mathrm{C}_3\cup\mathrm{C}_4\right)$$

分割の総数
l=1,3 より４つ
最初の分割からは平方剰余符号を得られるが,
残りは平方剰余符号と同値ではない.

Duadic 符号を構成することができた.

６　Duadic 符号の復号誤り率

６．１　重さ分布

q 元(n,k)線形符号 C の重さが i の符号語の数をA_iとするとき

$$(A_0, A_1, \cdots, A_n)$$

を C の重さ分布という．また

$$A(x) = \sum_{i=1}^{n} A_i x^i$$

を C の重さ分布多項式という．

（例）

n=7,k=4

$$W(x) = \begin{pmatrix} 1101010 \\ 0111001 \\ 0011100 \end{pmatrix}$$

$$(1223201)$$

$$A(x) = 1 + 2x + 2x^2 + 3x^3 + 2x^4 + x^6$$

マクウィリアムスの恒等式

　重み分布を求める上で非常に重要なものに２元線形符号とその双対符号の重さ分布の関係がある．

$$A^{\perp}(x) = 2^{-k}(1+x)^n A\left(\frac{1-x}{1+x}\right)$$

６．２復号誤り率

２元(n, k)線形符号Ｃを用いた場合に，正復号率P_C，復号誤り率P_E，復号不能確率P_Dとする．

$$P_C + P_E + P_D = 1$$

（１）正復号率P_C

正復号率P_Cは長さ n の受信語において，その符号語に正確に復号される確率であるから，

$$P_C = \sum_{i=0}^{t} {}_nC_i p^i (1-p)^{n-i} = \sum_{i=0}^{e} \binom{n}{i} p^i (1-p)^{n-i}$$

$e = \left\lfloor \frac{d-1}{2} \right\rfloor$であり，$\binom{n}{i}$は二項係数である．

で表すことができる．

二項展開の一般項 $x^k y^{n-k}$ の係数を二項係数と呼び，

$$\binom{n}{i}$$

で与えられる．

ここで${}_nC_i$は

$$\binom{n}{i} = {}_nC_i = \frac{n(n-1)\cdots(n-i+1)}{i(i-1)\cdots 1}, \quad i = 1, \cdots, n$$

（２）復号誤り率P_E

復号誤り率P_Eは受信語が送信語とは異なる符号語の復号領域に入る確率である．線形符号 Ｃ の任意の符号語wを Ｃ の個々の符号語に加えて作った集合は再び Ｃ となる．このことは，線形符号ではどの符号語から見ても他の符号語の位置の分布は全く同じであることを意味する．したがって送信語が何であっても復号誤り率は変わらない．そこで，送信語は 0 とする．このとき，復号誤り率P_Eは，

$$P_E = \sum_{i=0}^{t} A_w \sum_{t=0}^{2e} \sum_{s=e-t}^{\left\lfloor e-\frac{t}{2} \right\rfloor} \binom{w}{s} \binom{n-w}{s-e+t} p^{w-e+t} (1-p)^{n-w+e-t}$$

$$e = \left\lfloor \frac{d-1}{2} \right\rfloor, \quad \text{k<0 のとき} \binom{n}{i} = 0 \text{ とする}$$

により計算できる.

よって線形符号の重み分布$(A_0, A_1, \cdots, A_n)$により復号誤り確率が決まる.

（例）

$(15,4)$符号をビット誤り率 p=0.1 の２元対称通信路に用いるものとする．この符号の最小距離は 8 であるので，t=3 個まで誤りを訂正できる．このとき，正復号率は,

$P_C = 0.9^{15} + 15 \cdot 0.1 \cdot 0.9^{14} + 105 \cdot 0.1^2 \cdot 0.9^{13} + 455 \cdot 0.1^3 \cdot 0.9^{12}$ 約 94 パーセントの確率で受信語が
$= 0.94444$

送信語に対応する領域

に入り，送信語が正しく推定される

例）

$C = \{(0,0,0),(1,1,1)\}$ とすると $(0,0,0)$ を送信したときに, 誤って $(1,1,1)$ に復号される確率は,

$$P_E = p^3 + 3p^2(1-p)$$

（３）復号不能率

$P_D = 1 - P_C - P_E$

より求められる.

６．３　Duadic 符号の復号誤り率

重さ分布と復号誤り率 P_E の式のプログラムを作成し, 任意のｐを与え，n＝7, 17，23，31，41 の重さ分布，復号誤り率を計算した.

結果

n=7，2e=2，l=1，m=0

重み分布 A_w

0 = 1
3 = 7
4 = 7
7 = 1

最小距離 = 3

復号誤り率

p=0.1……0.00064633
p=0.01……0.00000066939
p=0.001……0.00000000067173
p=0.0001……0.00000000000067197
p=0.00001……0.0000000000000067199
p=0.000001……0.000000000000000067199

p=17，2e=2，l=1，m=0

重み分布 A_w

0 = 1
6 = 68
8 = 85
10 = 68
12 = 34

最小距離 = 6

復号誤り率

p=0.1……0.0000023971
p=0.01……0.000000000026617
p=0.0001……0.00000000000000026896
p=0.00001……0.0000000000000000000026924
p=0.000001……0.000000000000000000000000026927
p=0.0000001……0.00000000000000000000000000000026927

n=23, 2e=2, l=1, m=0

重み分布 A_w

0 = 1
7 = 253
8 = 506
11 = 1288
12 = 1288
15 = 506
16 = 253
23 = 1

最小距離 = 7

復号誤り率

p=0.1……0.052463
p=0.01……0.00000061414
p=0.001……0.0000000000062384
p=0.0001……0.000000000000000062482
p=0.00001……0.00000000000000000000062492
p=0.000001……0.0000000000000000000000000062493

p=31, 2e=6, l=1, m=0

重み分布 A_w

0 = 1
7 = 155
8 = 465
11 = 5208
12 = 8680
15 = 18259
16 = 18259
19 = 8680
20 = 5208
23 = 465
24 = 155
31 = 1

復号誤り率

p=0.1……0.090843
p=0.01……0.0000011453
p=0.001……0.000000000011720
p=0.0001……0.00000000000000011747
p=0.00001……0.0000000000000000000011750
p=0.000001……0.000000000000000000000000011750

p=41, 2e=2, l=1, m=0

重み分布 A_w

0 = 1
10 = 1312
12 = 7585
14 = 33210
16 = 97539
18 = 195160
20 = 255266
22 = 232060
24 = 146370
26 = 60024
28 = 16605
30 = 3034
32 = 410

最小距離 = 10

復号誤り率-推移

p=0.1……0.0000034216
p=0.01……0.00000000000046259
p=0.001……0.000000000000000000047670
p=0.0001……0.00000000000000000000000047814
p=0.00001……0.0000000000000000000000000000047828
p=0.000001……0.000000000000000000000000000000000047830

以上の復号誤り率とビット誤り率を表にまとめた.

Teble1. n＝7, 17, 23, 31, 41 の復号誤り率

p	7	17	23	31	41
0.000001	6.7199×10^{-16}	2.6728×10^{-26}	6.2492×10^{-22}	1.175×10^{-21}	4.78×10^{-34}
0.00001	6.7197×10^{-13}	2.6925×10^{-21}	6.2482×10^{-17}	1.1747×10^{-16}	4.78×10^{-27}
0.0001	6.7173×10^{-10}	2.6897×10^{-16}	6.2384×10^{-12}	1.172×10^{-11}	4.7670×10^{-20}
0.001	6.6939×10^{-7}	2.6618×10^{-11}	6.1414×10^{-7}	1.1453×10^{-6}	4.6259×10^{-13}
0.01	6.4633×10^{-4}	2.3972×10^{-6}	5.2463×10^{-2}	9.0843×10^{-2}	3.0421×10^{-6}

復号誤り率とビット誤り率の関係を対数グラフに示した.

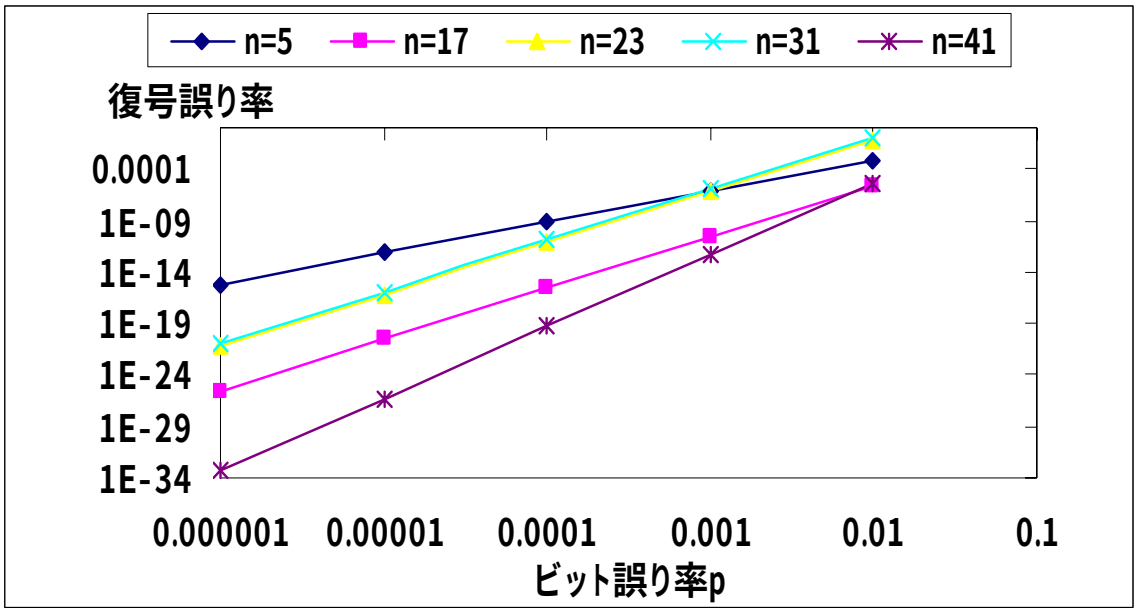

図１．復号誤り率とビット誤り率の関係

次に符号化率を計算した.

符号化率(Code rate)

$$R = \frac{k}{n}$$

符号化率を計算すると,
n＝７の場合，0．5714
n＝17 の場合，0．4705
n＝23 の場合，0．5217
n＝31 の場合，0．5161
n＝41 の場合，0．4878
となる.

７　考察

図より，

まず，n=7 と n=23，31 を比較してみる．p=0.001 を境に n=7 と n=23，31 が交差していることから，p>0.001 のときは n=7，p<0.001 のときは n=23，31 の方が復号誤り率は小さい．

n=17，41 のときは復号誤り率が極端に小さいが，符号化率が悪い．両者を比較した場合 n=41 の方が復号誤り率が小さい上に符号化率が高いことから，よい符号ということがわかる．

８　結論

Duadic 符号の具体的な構成法を証明することができた．　プログラムにより Duadic 符号の重さ分布を調べ，復号誤り率を計算することができた．これにより，Duadic 符号はビット誤り率により復号誤り率が変化するが，任意で符号長を選ぶことによって復号誤り率，符号化率も変化する．復号誤り率と符号化率を比較し，n=41 の符号が実験した中では比較的よい符号であることがわかった．

謝辞

本研究を進めるにあたり，様々な方にお世話になりました．この場を借りて厚くお礼申し上げます．特に，本研究を進めるにあたっていろいろとご指導，ご助言いただいた平松豊一教授，また様々な面でご指導いただいた多田秀樹氏，斎藤正顕氏，共同研究者の原山康昌氏には紙面上ではございますが，感謝の意を申し上げたいと思います．

参考文献

(1)J. S. Leon, J. M. Maseley and V. Pless;Duadic codes , IEEE trans. IT. , **30**(1984), 709-714

(2)C. Ding and V. Pless;Cyslotomic and duadic codes of prime lengths, IEEE trans. IT. , **45**(1999), 453-466

(3)Philippe Gaborit, Carmen-Simona Nedeloaia, and AlfredWassermann; On the weight enumerators of duadic and quadratic residue codes, IEEE trans. IT. , **51**(2005), 402-407

(4)平松豊一；数論を学ぶための相互法則入門，牧野書店，1988

(5)今井秀樹；符号理論入門，社団法人電子情報通信学会，1990

(6)藤原良，神保雅一；符号と暗号の数理，共立出版株式会社，1993

(7)嵩忠雄；情報と符号の理論入門，昭晃堂，1989