〈一般研究課題〉　マトロイド理論を用いた誤り訂正符号の研究
助 成 研 究 者　　愛知県立大学　城本　啓介

マトロイド理論を用いた誤り訂正符号の研究

城本　啓介
（愛知県立大学）

1. はじめに

符号理論とは、デジタル情報を伝送または記録する際に生じる誤りを検出あるいは訂正するための符号の理論であり、その符号を実際に構成して実用化を図るのが、符号理論の主要な目的である。現代の情報通信・情報システムのいたるところで実用化（身近な所では、コンピュータ・携帯電話等）されている最先端の情報理論であり、数学や数理物理学等の他の様々な分野と大きく関わりを持つ分野である。特に、この符号理論に関して、代数的構造に着目して研究を行うのが代数的符号理論である。

有限体上の線形符号とは、有限体上のベクトル空間の部分空間である。その符号の特徴を表す重要なパラメータである最小重みとは、符号の各元（符号語）に対して取り得る値（重み）を定め（例えば、ハミング重みとは、ベクトルにおける０でない成分の個数）、その中での最小値のことであり、符号の誤り訂正能力の限界を表現したり、通信路における雑音の抑制に有効なパラメータである。符号理論における研究テーマの一つに、この最小重みに関する限界式の作成、さらにその限界式の等号を満たす線形符号の構成・解析がある（有名な例では、シングレトン限界式やグリスマー限界式がある。）。特に、有限体上の自己双対符号に関しては、N. Sloane や H. Ward らによって様々な限界式が証明され、そのことで極値的な自己双対符号（最小ハミング重みが限界値である符号）に関する存在・非存在問題がクローズアップされた。また、線形符号の各部分符号に対して値（重み）を定め、その最小値を一般化重みと言う。特に、1990年に V. Wei が一般化ハミング重みを導入し、情報セキュリティの分野への応用の可能性が指摘されたことに始まり、色々な符号に対してその重みを決定することが重要な研究であるとされている。

また、符号理論は組み合わせデザイン理論や整数論等の様々な研究分野と大きく関わっており、他の分野の手法を用いて符号を考察することも一つの重要な研究分野である。

2. 定義と基礎概念

まずは、本研究で重要となるマトロイドについて定義を行う。マトロイドとは、有限な集合EとEの部分集合族Iで次の性質をみたすものの順序対$M=(E, I)$である。

(1) $\phi \in I$

(2) $R \in I$であり、$R' \subseteq R$ならば$R' \in I$が成立する。

(3) $R, R' \in I$であり、$|R'| < |R|$ならば、元$e \in R-R'$で$R' \cup e \in I$を満たすものが存在する。

ここで、Iの元を独立集合と呼び、Iの元でないものを従属集合と言う。また、極小の従属集合をサーキットといい、極大な独立集合を基底と言う。任意の部分集合Xに対して、Xの階数を次のように定める。

$$r(X)=\max\{|Y| : Y \subseteq X, Y \in I\}$$

マトロイドMの双対マトロイドM^*を次のような集合を基底とするマトロイドとする。

$$\{E-B : B \text{は} M \text{の基底}\}$$

特に、双対マトロイドの階数については、次の事実が知られている。

$$r^*(X)=|X|-r(M)+r(E-X)$$

$M=M^*$のとき、マトロイドMを自己双対マトロイドと言う。

マトロイド$M=(E, I)$と任意の部分集合$T \subseteq E$に対して、$M \setminus T = (E-T, \{R \subseteq E-T : R \in I\})$がマトロイドの構造を持つことが明白であり、このマトロイドをMのTによるdeletionと、言いMのTによるcontractionを次のマトロイドで定義する。

$$M/T=(M^* \setminus T)^*$$

ここで、deletionとcontractionの組み合わせ$M/T \setminus S$をMのマイナーと言う。

$GF(2)=\{0,1\}$を成分とする$m \times n$行列Aに対して、EがAの列番号の集合であり、IがAの一次独立な列番号の集合族のとき、$M[A]=(E, I)$はマトロイドの構造を持ち、このマトロイドを、2元マトロイドと言う。

$GF(2)$上のベクトル$\mathbf{x}=(x_1, \ldots, x_n)$と部分集合に対して、それぞれのサポートを次のように定義する。

$$\mathrm{supp}(\mathbf{x})=\{i : x_i \neq 0\}$$

$$\mathrm{Supp}(D)=\bigcup_{x \in D} \mathrm{supp}(\mathbf{x})$$

Cを$GF(2)$上の$[n,k]$符号とする、つまり、$GF(2)$上のn次元ベクトル空間のk次元部分空間とする。ここで、$1 \leq r \leq k$の各rに対して、r番目の一般化ハミング重みを次のように定義する。

$$d_r(C)=\min\{|\mathrm{Supp}(D)| : D \text{は} C \text{の} [n,r] \text{部分符号}\}$$

このパラメータは、V. Weiにより最初に導入され、以後暗号等の情報セキュリティ分野への応用も含めて符号における新たな重要なパラメータとして多くの研究者によって研究がなされている。本研究の目的は、この値に関してマトロイド理論を適用することで、新たな限界式を証明することである。

3.2 元マトロイドに関する限界式

以下、本章では、Mを2元マトロイドとする。ここで、Mのgirthを次のように定義する。

$$g(M)=\min\{|F| : F \text{は} M \text{のサーキット}\}$$

ここで、次の命題が知られている。

命題1. Fを一様マトロイド$U_{k,k+2}$と同型なマイナーを持たないマトロイドのサーキットとし、eをE-Fの要素とする。このとき、FはM/eにおいて、サーキットになるか、または、$F-X_1,\ldots,F-X_n$がサーキットであるようなFの分割$X_1,\ldots,X_n$が存在するかのどちらかである。

ここで、上記の命題を用いると次の定理が証明できる。

定理2. Mを階数がrであるような2元マトロイドとする。もしMが位数が $i(r\leq i\leq r+4)$であるような従属集合を持ち、さらに、Fがサーキットか互いに共通部分を持たないいくつかのサーキットの和集合ならば、次の不等式が成立する。

$$2g(M)-4\leq r$$

証明：Fが互いに共通部分を持たないいくつかのサーキットの和集合ならば、少なくとも２つの互いに共通部分を持たないサーキットでFに含まれるものが存在し、それらをF_1,F_2とする。このとき、次の不等式が成立する。

$$r+4\geq|F|\geq|F_1|+|F_2|\geq 2g(M)$$

ここで、もしFの位数が$r+2$以上ならば、Fはサーキットでない。従って、Fは位数がrか$r+1$のサーキットであると仮定する。

(1) 位数が$r+1$のとき

E-Fの要素eに対して、M/eの階数は$r-1$であるから、FはM/eのサーキットではない。従って、命題1よりM/eの2つの互いに共通部分を持たないサーキットF_1, F_2を用いて$F=F_1\cup F_2$とかける。このとき、以下の不等式が成立する。

$$r+1\geq|F_1|+|F_2|\geq(g(M)-1)+(g(M)-1)=2g(M)-2$$

(2) 位数がrのとき

E-Fの要素e_1に対して、FがM/e_1のサーキットではないならば、上記の(1)の場合と同様に定理を証明することが出来る。従って、FがM/e_1のサーキットであると仮定する。e_1と異なるE-Fの要素e_2に対して、$M/e_1/e_2$の階数は$r-2$であるから、Fが$M/e_1/e_2$のサーキットではなく、よって、$M/e_1/e_2$の２つの互いに共通部分を持たないサーキットF_1,F_2を用いて$F=F_1\cup F_2$とかける。このとき、以下の不等式が成立する。

$$r\geq|F_1|+|F_2|\geq(g(M)-2)+(g(M)-2)=2g(M)-4$$

(1),(2) より、定理における不等式が成立することが示せた。 ■

2元マトロイドMに対して、$L(M)=(T(M))^*$とする。ここで、$T(M)$はMのtruncationを表す。このとき、$L(M)$のサーキットはMの異なる2つのサーキットの極小な和集合であることが知られている。また、命題1より以下の補題が直ちに証明できる。

補題3. Mを階数がrであるような2元マトロイドとする。もし、Mが位数が $i(r\leq i\leq r+4)$であるような従属集合Fを持ち、さらに、Fがサーキットか互いに共通部分を持たないいくつかのサーキットの

和集合ならば、次の不等式が成立する。

$$2g(L(M))+g(M)-8 \leq 2r$$

また、条件を少し変更しても以下の補題が成立する。

補題4. Mを階数がrであるような2元マトロイドで$r^*(M) \geq 4$とする。もし、Mが位数がrか$r+1$であるようなサーキットFを持つならば、次の不等式が成立する。

$$2g(L(M))+g(M)-8 \leq 2r$$

証明： BをMの基底とし、Fのある元eに対して、$B \supseteq F-e$とする。このとき、Bに対する2つの基本サーキットとして、$F_1=F(e_1,B)$と$F_2=F(e_2,B)$を考える。ここで、$e_1,e_2 \in E-B-e$とし、$e_1 \neq e_2$とする。

(1) Fの位数$r+1$がのとき

一般性を失うことなく、$|F_1| \leq (r+3)/2$かつ$|F_2| \leq (r+3)/2$であると仮定することができるので、次の不等式が成立する。

$$g(L(M)) \leq |F_1 \cup F_2| = |F_1|+|F_2|-|F_1 \cap F_2| \leq r+3-|F_1 \cap F_2|$$

ここで、F_1とF_2の対称差$F_1 \Delta F_2$は、Fと等しくなく、従って、$F \Delta F_1 \Delta F_2$は空集合でなくMのサーキットを含む。よって、以下の不等式が成立する。

$$g(M) \leq |F \Delta F_1 \Delta F_2| = |F|+|F_1 \Delta F_2|-2(F \cap (F_1 \Delta F_2)) \leq 2r+8-2g(L(M))$$

mを1か2をあらわす数とする。$r^*(M) \geq 4$より、$|F_j-F|=m$であるような2つのサーキットF_1とF_2を考えることが出来る。上記と同様の議論により、$|F_1|+|F_2| \leq r+2m$と仮定することが出来る。従って以下の不等式を得る。

$$g(L(M)) \leq r+2m-|F_1 \cup F_2|$$

よって、次の不等式を導くことが出来る。

$$g(M) \leq |F \Delta F_1 \Delta F_2| = |F|+|F_1 \Delta F_2|-2|F_1 \Delta F_2-\{e_1,e_2\}| \leq 2r+8-2g(L(M))$$

■

補題3と補題4を組み合わせて考えることで、次の定理を得る。

定理5. Mを階数がrであるような2元マトロイドで$r^*(M) \geq 4$とする。もし、Mが位数がi($r \leq i \leq r+4$)であるような従属集合Fを持ち、さらに、Fがサーキットか互いに共通部分を持たないいくつかのサーキットの和集合ならば、次の不等式が成立する。

$$2g(L(M))+g(M)-8 \leq 2r$$

4.2 元符号に関する限界式

Mを2元符号の生成行列から構成される2元マトロイドとしたとき、Mのコサーキットはその符号の極小サポートに対応し、$L(M)$のコサーキットは2次元部分符号の極小サポートに対応することが知られている。ここで、A_iを重みがiである符号語の個数とすると、定理2と定理5を符号理論へ適用することで以下の結果を得る。

系6. Cを$GF(2)$上の$[n,k,d]$符号とする。もし、$n-k \le i \le n-k+4$であるiに対して、$A_i \neq 0$であるならば、$2d-4 \le n-k$が成立する。

系7. Cを$GF(2)$上の$[n,k,d]$符号で$k \le 4$とする。もし、$n-k \le i \le n-k+4$であるiに対して、$A_i \neq 0$であるならば、$2d_2+d-8 \le 2(n-k)$が成立する。

任意の自然数nに対して、2元Krawtchouk多項式を以下のように定義する。

$$\mathrm{P}_m(x)=\sum_{j=0}^{m}(-1)^n\binom{x}{j}\binom{n-x}{m-j}$$

ここで、$m=0,1,\ldots,n$である。この多項式を用いると、$GF(2)$上の$[n,k]$符号Cとその双対符号$\mathrm{C}^{\perp}$に関して、マックウィリアムズ恒等式から以下の等式が成立する。

$$2^k A_m^{\perp}=\sum_{i=0}^{n} A_i P_m(i)$$

さらに、2元Krawtchouk多項式については、以下の等式が証明されている。

$$\mathrm{P}_{n/2}(i)=(-1)^{i/2}\binom{n}{n/2}\binom{n/2}{i/2}/\binom{n}{i}$$

ここで、nとiは偶数とする。以上の結果より、次の命題が成立することが分かる。

命題8. Cを$GF(2)$上の$[n,k,d]$符号で$n/2 \le k \le n/2+4$とし、nを偶数とする。もし、双対符号$C^{\perp}$のすべての符号語の重みが4で割り切れるならば、$2d-4 \le n-k$かつ$2d_2+d-8 \le 2(n-k)$が成立する。

5. デザイン理論によるアプローチ

Cを$GF(2)$上の重偶自己双対符号とする。つまり、$C=C^{\perp}$であり、すべての符号語の重みが4で割り切れるような符号であるとき、$k=n/2$であり、nは8の倍数であることが知られている。また、最小重みdに関しては、次の限界式が知られている。

$$d \le 4\left\lfloor \frac{n}{24} \right\rfloor+4$$

特に、$d=4\lfloor n/24 \rfloor+4$が成立する場合、極値的であると言う。

有限集合Pとその部分集合族Bに対して、次の条件を満たすとき、それらの組(P,B)をt-(ν,k,λ)デザインと言う。

(1) $|\mathrm{P}|=\nu$

(2)任意の部分集合$B \in \mathrm{B}$（ブロックと言う）に対して、$|\mathrm{B}|=k$

(3)任意のt個の要素をからなるPの部分集合に対して、それを含むブロックの個数はλ個

ここで、極値的な重偶自己双対符号とデザインの間にはAssmus-Mattsonの定理と呼ばれる以下の関係が成立する。

定理 Cを$GF(2)$上の極値的な$[n,n/2,d=4\lfloor n/24 \rfloor+4]$重偶自己双対符号とする。ここで、$\mathrm{P}=\{1,2,\ldots n\}$とし、$\mathrm{B}_i$を重みが$i$であるようなすべての符号語のサポートの集合とすると、$(\mathrm{P},\mathrm{B}_i)$は$t$-$(n,i,A_i\binom{i}{t}/\binom{n}{t})$デザインになる。

この定理を用いて構成されたデザインとその構造を考察し、極値的な重偶自己双対符号の２番目の一般化ハミング重みに関しては、前章の限界式とあわせて考えることでそれほど大がかりな計算を行うことなく、以下の定理を証明できる。

定理9. もし、$GF(2)$上の極値的な$[n,n/2,d=4\lfloor n/24 \rfloor+4]$重偶自己双対符号$C$が$8 \leq n \leq 144$において存在するならば、$C$の2番目の一般化ハミング重み以下の表のように求めることが出来る。

n	$t-(v,k,\lambda)$ デザイン	d	d_2
8	3－(8,4,1)	4	6
16	1－(16,4,7)	4	6
24	5－(24,8,1)	8	12
32	3－(32,8,7)	8	12
40	1－(40,8,57)	8	12
48	5－(48,12,8)	12	18
56	3－(56,12,65)	12	18
64	1－(64,12,558)	12	18 か 20
72	5－(72,16,78)	16	24
80	3－(80,16,665)	16	24 か 26
88	1－(88,16,5848)	16	24 か 26
96	5－(96,20,816)	20	30
104	3－(104,20,7125)	20	30 か 32
112	1－(112,20, 63525)	20	30,32 か 34
120	5－(120,24,8855)	24	36 か 38
128	3－(128,24,78430)	24	36,38 か 40
144	5－(144,28,98280)	28	42 か 44

6. まとめ

本研究においては、誤り訂正符号理論へマトロイド理論を適用することで、符号の構造の特徴を考察することであった。まず、マトロイドにおける限界式を証明し、それを符号へ適用することで符号の一般化ハミング重みに関する限界式を作成した。さらに、Assmus-Mattsonの定理から極値的な重偶自己双対符号から得られるデザインを考察し、限界式を用いることで符号長が144以下の符号に関しては、2番目の一般化ハミング重みの値もしくは限界式を証明することが出来た。

今後の課題としては、3番目以降の一般化ハミング重みに関しても、本研究と同様の結果を得ることと、それらを用いて存在の知られていない符号に関する存在・非存在の証明にもアプローチすることが考えられる。

謝辞：本研究は、日比科学技術振興財団の研究助成によって行われた研究である。

参考文献：

[1] K. Shiromoto, Bounds for binary matroids, 第21回代数的組合せ論シンポジウム報告集,p.95～101, 2004

[2] K. Shiromoto, Second generalized Hamming weights for extremal self-dual codes, Proceedings of the International Workshop on Coding and Cryptography, p.11～19, 2005