有限剰余環上の誤り訂正符号

西村, 滋人 / HIRAMATSU, Toyokazu / NISHIMURA, Shigeto / 平松, 豊一

(出版者 / Publisher)
法政大学工学部
(雑誌名 / Journal or Publication Title)
法政大学工学部研究集報 / 法政大学工学部研究集報
(巻 / Volume)
37
(開始ページ / Start Page)
11
(終了ページ / End Page)
16
(発行年 / Year)
2001-03
(URL)
https://doi.org/10.15002/00003783

有限剰余環上の誤り訂正符号

ERROR CORRECTING CODES OVER FINITE RESIDUE RINGS

西村滋人*, 平松豊一**

Shigeto NISHIMURA and Toyokazu HIRAMATSU

This article is the brief review of basic general properties of the error-correcting codes over finite residue rings. We study the algebraic structure of the codes and then the parameters and properties of the codes are easily known by it.

Key Words:Error Correcting Codes, Finite Residue Ring, p-adic Error Correcting Codes.

1 序

誤り訂正符号の理論は、通信の信頼性の向上を目的とする理論である。デジタル通信システムにおける最初の手続きは、情報を、有限種類の記号を有限個並べた記号列に置き換えて再現性の高いデータを確保することであり、こうして得られた記号列を本論文では情報系列と呼ぶ。情報系列は通信路を介して送信・受信されるが、通信媒体における雑音の混入を考慮にいれるならば、受信した記号列が、送信された記号列と確実に同じものであるという保証はない。こうした通信の誤りに対処するために、送信者側は情報系列をそのまま通信路に流すのではなく、符号器を介して情報系列を符号語と呼ばれる記号列に変換し、これを通信路に送り出す。途中で誤りが生じるかもしれないが、受信者側では受信した記号列を復号器で処理して通信路で生じたかもしれない誤りを推定し、必要なら受信した記号列の誤りを訂正して正しい情報を取り出す。通常、情報系列ならびに符号語は、たんなる記号列ではなく、有限体上のベクトルとされるが、本論文の目的は、これらを有限剰余環の要素を並べた系列に置き換えた、有限剰余環上の誤り訂正符号について論じることである。すでにハミング符号やBCH符号といった符号族については構成方法の直接的な拡張が、有限体上のみならず有限剰余環上でも試みられており([2],[7])、とくに $\mathbf{Z}/4\mathbf{Z}$ 上の符号理論については研究も多い([8])。しかし有限体上での成果を押し広げようとするあまりに直接的な拡張の試みは、しばしば零因子の扱いをめぐって回りくどい操作を必要としたり、一般性に乏しかったりすることがある。法が相異なる素数べきの積である場合には、それぞれの素数べきを法とする剰余環上の符号に分けて調べればよく、本論文では素数べきを法とする有限剰余環上の符号を扱うが、代数的な構造を明確に述べさえすれば、符号長、次元、最小ハミング重さという符号の基本的パラメータや、生成行列及び検査行列といった符号器や復号器を構成するうえで基本的な道具は、有限体上の符号理論を基礎としておのずと明らかになる。また、以下の議論の延長線上に、p-進整数環上の符号が自然に現れる。これは1995年にA.R.CalderbankとN.J.A.Sloane [1]においていささか実験的に試みられたものであるが、ここでは射影的極限を用いた基礎づけを与える。

*大学院システム工学専攻
**システム制御工学科

2 $\mathbf{Z}/p^m\mathbf{Z}$ 上の誤り訂正符号

p を素数とし p^m を法とする剰余環 $\mathbf{Z}/p^m\mathbf{Z}$ を以下 $\mathbf{Z}_{p^m}$ と記す。便宜上 $m=\infty$ となることを許し p-進整数環を表すことにする。

$\mathbf{Z}_{p^m}^n$ の加法部分群 C を $\mathbf{Z}_{p^m}$ 上の符号長 n の符号と呼ぶ。最初の目的は C の生成行列が、本質的には、有限体上の符号の生成行列を並べて得られることを、m にかんする帰納法で示すことである。まず、

$$\phi_{m-1}:\mathbf{Z}_{p^m}^n \longrightarrow \mathbf{Z}_{p^{m-1}}^n$$

を $\bmod p^{m-1}$ の射影とし $C_0=C\cap\ker\phi_{m-1}$ とおく。C_0 は $\mathbf{Z}_p$ 上の符号と見なせるから生成行列を有する。その生成行列を G_0 とおく。一方 $C_{m-1}=\mathrm{Im}\,\phi_{m-1}$ とおくと C_{m-1} は $\mathbf{Z}_{p^{m-1}}$ 上の符号である。x が $\mathbf{Z}_{p^m}$ の単数なら $x+ap^{m-1}$ $(a=0,1\cdots,p-1)$ も $\mathbf{Z}_{p^m}$ の単数で、したがって符号語における単数の個数は C/C_0 の各剰余類ごとに一定である。また ap^{m-1} 以外の零因子は bp^y $(b=1,\cdots,p-1, 1\le y\le m-2)$ と書けるが、$bp^y+ap^{m-1}\equiv 0 \bmod p$ かつ $bp^y+ap^{m-1}\not\equiv 0 \bmod p^{m-1}$ だから ap^{m-1} 以外の零因子の個数もまた C/C_0 の各剰余類ごとに一定である。これらの個数の和が C_{m-1} の各符号語のハミング重さとなる。

C/C_0 は加法群として C_{m-1} と同型であり、したがって $\mathbf{Z}_{p^m}$ 上の符号と見なせるが、成分に ap^{m-1} $(a=1,\cdots,p-1)$ なるかたちの零因子が現れることを許しているため対応する符号語のハミング重さは必ずしも等しくない。

さて、生成行列であるが、$m=2$ のとき C_1 は有限体 $\mathbf{Z}_p$ 上の符号であるから生成行列を有する。それを G_1 で表す。簡単のため G_1 の ϕ による C 上への引き戻しも G_1

で表すことにする。ただし G_1 の C 上への ϕ による引き戻しとは、G_1 の行に並べられた C_{m-1} の各符号語 c を、$\phi(c')=c$ となる C/C_0 の代表元 c' (任意に選んだものでよい)に各々置き換えたものである。

補題 2.1 $\mathbf{Z}_{p^2}$ 上の符号は $G=\begin{pmatrix} pG_0 \\ G_1 \end{pmatrix}$ なる生成行列を有する。情報系列は $\mathbf{Z}_p$ 上のベクトルである。

この補題 2.1 は、$\mathbf{Z}_{p^2}$ 上の符号は必ず、$\mathbf{Z}_p$ 上の符号 C_0 に $pc\in C_0$ となるような $c\in\mathbf{Z}_{p^2}^n$ を適当につけ加えて構成できることを意味している。

例 2.1 次の $\mathbf{Z}_4$ 上の符号について生成行列を求める。

$$C=\left\{\begin{array}{l}(0000),\ (2202),\ (2222),\ (0020),\\ (1323),\ (3121),\ (3101),\ (1303),\\ (1111),\ (3313),\ (3333),\ (1131),\\ (2030),\ (0232),\ (0212),\ (2010).\end{array}\right\}$$

C_0 は mod 2 の射影をとると (0000) となるような符号語を抜き出したものだから、

$$C_0=\{(0000),(2202),(2222),(0020)\}$$

である。C_0 は生成行列が

$$G_0=\begin{pmatrix}1&1&0&1\\1&1&1&1\end{pmatrix}$$

で与えられるような $\mathbf{Z}_2$ 上の符号と見なせる。C/C_0 の代表系 $\{(0000),(1323),(1111),(2030)\}$ を mod 2 で考えた $\{(0000),(1101),(1111),(0010)\}$ は生成行列が $G_1=\begin{pmatrix}1&1&0&1\\1&1&1&1\end{pmatrix}$ であるような $\mathbf{Z}_2$ 上の符号と見なせる。G_1 の ϕ による引き戻し $G_1=\begin{pmatrix}1&3&2&3\\1&1&1&1\end{pmatrix}$ 及び $2G_0=\begin{pmatrix}2&2&0&2\\2&2&2&2\end{pmatrix}$ を並べることにより次のように生成行列が求められる。

$$G=\begin{pmatrix}2&2&0&2\\2&2&2&2\\1&3&2&3\\1&1&1&1\end{pmatrix}.$$

生成行列の構成は、符号器の設計という観点からすると、情報系列と符号語が一意的に対応するように行われるべきである。補題 2.1 で情報系列は $\mathbf{Z}_p$ 上のベクトルからとったが、いまの例では $2(1111)=(2222)$, $2(1323)=(2202)$ となることから、

$$G=\begin{pmatrix}1&3&2&3\\1&1&1&1\end{pmatrix}$$

とすれば $\mathbf{Z}_4$ の要素を並べたものを情報系列としても符号化の一意性は保たれる。しかし、有限体上の場合と違って $\mathbf{Z}_{p^2}$ 上の符号 C については、任意の符号語 $c\in C$ について $pc'=c$ となる符号語 $c'\in C$ がつねに存在するとは限らないため、このようなことはいつでもできるわけではない。いま C/C_0 の基底 $c_1,\cdots,c_{k_1}$ $(k_1=\dim_{\mathbf{Z}_p}C_1)$ を選んだとする。詳しくいえば、C/C_0 の代表系を任意に固定し、mod p で射影をとったとき Z_p 上の基底となっているものを選んだとする。$p\phi_1(c_1)$, $p\phi_1(c_{k_1})$ は C_0 の 0 でない符号語であり、

$$a_1p\phi_1(c_1)+\cdots+a_{k_1}p\phi_1(c_{k_1})\equiv 0\pmod{p^2}$$

ならば

$$a_1\phi_1(c_1)+\cdots+a_{k_1}\phi_1(c_{k_1})\equiv 0\pmod{p}$$

であるから、$a_1\equiv\cdots\equiv a_{k_1}\equiv 0 \bmod p$ でなければならない。ここで一般に $\mathbf{Z}_{p^2}^n\ni x=(x_1\ \cdots\ x_n)$ について $x_i\equiv a_i \bmod p$, $a_i\in\{0,1\cdots,p-1\}$ とすれば

$$p\phi_1(x)=p(a_1\ \cdots\ a_n)=(px_1\ \cdots\ px_n)=px$$

だから $pc_1,\cdots,pc_{k_1}$ は C_0 の独立な部分集合であり、したがって C_0 の基底は $pc_1,\cdots,pc_{k_1}$ を含むようにとることができる。一般には $k_1\le k_0$ $(k_0=\dim_{\mathbf{Z}_2}C_0)$ である。符号語数は $p^{k_1}p^{k_0}$ であり、$k_1<k_0$ のときには、$\mathbf{Z}_{p^2}$ の要素を並べて情報系列を作ろうとしても、それを一意的に符号語に変換するような生成行列を得ることができない。

例 2.1 のように、与えられた符号語から生成行列を見出そうとする場合、C_0 による剰余類分解を実行する必要はなく、まず成分が全て p で割れているような符号語を全て抜き出せば C_0 が得られるから、その基底 $c_1,\cdots,c_{k_0}$ $(k_0=\dim_{\mathbf{Z}_2}C_0)$ を生成行列の行にまず並べ、次に、各 c_i に対し $pc_i'=c_i$ となる符号語 c_i' があるかどうかを調べて、あればそれを生成行列の行に追加すればよい。

$m>2$ の場合にうつる。すでに述べたように $\mathbf{Z}_{p^m}$ 上の符号を ϕ_{m-1} で射影をとって C_0 と C/C_0 に分解すると、任意の符号語は C_0 に属する符号語と C/C_0 に属する符号語との和に一意的に書くことができる。C_0 は $\mathbf{Z}_p$ 上の符号と見てよく、また $C_{m-1}\cong C/C_0$ は $\mathbf{Z}_{p^{m-1}}$ 上の符号と見てよい。$\mathbf{Z}_{p^{m-1}}$ 上の符号 C_{m-1} はさらに、ϕ_{m-2} で射影をとることによって $\mathbf{Z}_p$ 上の符号と $\mathbf{Z}_{p^{m-2}}$ 上の符号とに分解されるから、C_{m-1} の符号語は $\mathbf{Z}_p$ 上の符号の符号語と $\mathbf{Z}_{p^{m-2}}$ 上の符号の符号語との和に一意的に書かれる。m についての帰納法を使うと補題 2.1 から、$\mathbf{Z}_{p^m}$ 上の符号の生成行列が、本質的には、有限体上の符号の生成行列を並べて得られることがわかる。情報系列は $\mathbf{Z}_p$ のベクトルである。

定理 2.1 $\mathbf{Z}_{p^m}$ 上の符号は $G=\begin{pmatrix} p^{m-1}G_0 \\ G_{m-1} \end{pmatrix}$ なる生成行列を有する。情報系列は $\mathbf{Z}_p$ 上のベクトルである。

さらに著しい結果として次の主張が成り立つ。

定理 2.2 C の最小ハミング重さを d_H, C_0 のそれを d_H^* とすると $d_H=d_H^*$.

(証明) $C_0=C\cap\ker\phi_{m-1}$ より、C_0 に属する符号語の成分は 0 もしくは $ap^{m-1},(a=1,\cdots,p-1)$ である。符号語 $c=(c_1\ \cdots\ c_n)$ に p^{m-1} を乗じるとき

$$w_H(c)\geq w_H(p^{m-1}c)=\#\{i:(c_i,p)=1\}$$

一方 $p^{m-1}c\in C_0$ だから、最小重さを与える符号語は C_0 に属している。

■

有限体上の符号の基本的性能は符号長 n, 次元 k, それに最小重さ d で決まる。したがって、自然数 n,k,d を与えたとき、それらを符号長、次元、最小重さとして持つ符号を具体的に構成できるかという問題が生ずる。これを(有限体上での)符号の構成問題という。定理 2.2 によれば、$\mathbf{Z}_{p^m}$ での符号構成問題は、最小重さのみに着目するならば、有限体 $\mathbf{Z}_p$ 上のそれに帰着してしまう。別の見方をすると、定理 2.2 から、任意に与えられた $C_0\subset\mathbf{Z}_p^n$ をもとにして $\mathbf{Z}_{p^m}$ 上の符号を構成することができ、そのとき符号長 n, 最小ハミング重さ d_H を固定したままアルファベットだけを増やせる、したがって符号語数だけを増やせることになる。

例 2.2 次の $\mathbf{Z}_8$ 上の符号について生成行列を求める。

$$C=\left\{\begin{array}{l}(0000),\ (1234),\ (2460),\ (3614),\ (4040),\\ (5274),\ (6420),\ (7654),\ (3650),\ (1270),\\ (7610),\ (5230),\ (3672),\ (1256),\ (7632),\\ (5216),\ (4062),\ (0044),\ (4026),\ (0022),\\ (0066),\ (2446),\ (4004),\ (6442),\ (1212),\\ (2424),\ (3636),\ (5252),\ (6464),\ (7676),\\ (6406),\ (2402).\end{array}\right\}$$

C_0 は mod 4 で射影をとると (0000) となるような符号語を抜き出したものだから、

$$C_0=\{(0000),(4040),(4004),(0044)\}$$

である。C_0 は生成行列が

$$G_0=\begin{pmatrix}1&0&1&0\\1&0&0&1\end{pmatrix}$$

で与えられるような $\mathbf{Z}_2$ 上の符号と見なせる。代表系は

$$C/C_0=\left\{\begin{array}{l}(0000),\ (1234),\ (2460),\ (3614),\\ (2446),\ (4062),\ (1212),\ (3636).\end{array}\right\}$$

と取ることができる。符号語の成分に現れる 4 以外の零因子の個数、単数の個数はそれぞれ各剰余類ごとに一定である。代表系を mod 4 で射影をとった

$$\left\{\begin{array}{l}(0000),\ (1230),\ (2020),\ (3210),\\ (2002),\ (0022),\ (1212),\ (3232).\end{array}\right\}$$

は生成行列が $G_2=\begin{pmatrix}2&0&2&0\\2&0&0&2\\1&2&3&0\end{pmatrix}$ であるような $\mathbf{Z}_4$ 上の符号と見なすことができ、この生成行列を ϕ_2 で C 上へ引き戻した行列、及び $4G_0$ を並べることにより、次のように生成行列が求められる。

$$G=\begin{pmatrix}4&0&4&0\\4&0&0&4\\2&4&6&0\\2&4&4&6\\1&2&3&4\end{pmatrix}$$

次に双対符号を考察する。まず $\mathbf{Z}_{p^2}$ 上の符号について考えてみると、$C^\perp$ についても mod p での射影をとり、$(C^\perp)_0=C^\perp\cap\ker\phi_1$ と $(C^\perp)_1=C^\perp/(C^\perp)_0$ とにわければ $(C^\perp)_0=p(C_1)^\perp$ である。これは $\mathbf{Z}_{p^m}$ 上の符号について一般化したかたちで証明することができる。そのために記号を準備する。$\mathbf{Z}_{p^m}^n$ から $\mathbf{Z}_{p^l}^n$ への mod p^l $(1\leq l\leq m-1)$ での射影を、記号を流用して ϕ_l で表し、$C\subset\mathbf{Z}_{p^m}^n$ に対して $C_0^{(l)}=C\cap\ker\phi_l$, $C_1^{(l)}=C/C_0^{(l)}$ と記すことにする。$C_0^{(l)}$ は $\mathbf{Z}_{p^{m-l}}$ 上の符号と見なすことができ、$C_1^{(l)}$ は $\mathbf{Z}_{p^l}$ 上の符号と見なすことができる。

$\mathbf{Z}_{p^m}$ 上の符号の双対性にかんして、以上の準備のもとに述べられる次の定理は基本的である。

定理 2.3

(1) C を $\mathbf{Z}_{p^2}$ 上の符号とするとき $\mathbf{Z}_p$ 上の符号として

$$(C^\perp)_0\cong(C_1)^\perp,\quad(C^\perp)_1\cong(C_0)^\perp$$

(2) C を $\mathbf{Z}_{p^m}$ 上の符号とするとき $\mathbf{Z}_{p^{m-l}}$ 上の符号として

$$(C^\perp)_0^{(l)}\cong(C_1^{(m-l)})^\perp,\quad(C^\perp)_1^{(m-l)}\cong(C_0^{(l)})^\perp\qquad(1\leq l\leq m-1).$$

系 1 $\mathbf{Z}_{p^m}$ 上の符号長 n の符号 C について $\#C=p^k$ ならば $\#C^\perp=p^{mn-k}$

(証明) (1)は(2)の特別な場合である。(2)を示す。
$x\in(C^\perp)_0^{(l)}$ なら $x=p^lx_0$, $x_0\in\mathbf{Z}_{p^{m-l}}^n$ と書けている。x は C の双対符号の符号語だから $y\in C$ とすれば

$$x\cdot y\equiv 0\bmod p^m\quad\text{すなわち}\quad x_0\cdot y\equiv 0\bmod p^{m-l}$$

が満たされる。y を mod p^{m-l} で考えたものは $\phi_{m-l}(C) = C_1^{(m-l)}$ に属し、いま $y \in C$は任意でよいから、$x_0 \in \mathbf{Z}_{p^{m-l}}^n$ は $C_1^{(m-l)}$ の全ての符号語と直交する。すなわち $x_0 \in (C_1^{(m-l)})^\perp$ である。逆に $x \in (C_1^{(m-l)})^\perp$ なら $p^l x \in (C^\perp)_0^{(l)}$ だから、その意味で $(C_1^{(m-l)})^\perp \subset (C^\perp)_0^{(l)}$ も成り立つ。よって両辺を各々の仕方で $\mathbf{Z}_{p^{m-l}}$ 上の符号と見なせば $(C^\perp)_0^{(l)} \cong (C_1^{(m-l)})^\perp$ である。さらに C の代わりに $C^\perp$ をとれば $(C^\perp)_1^{(l)} = (C_0^{(m-l)})^\perp$ が成り立つ。

■

以下では定理 2.3 を足がかりにして検査行列の計算方法を考える。符号アルファベットが $\mathbf{Z}_{p^2}$ の場合からとりかかることにする。$\mathbf{Z}_p$ 上の符号については、I_k を k 次の単位行列、P を $n-k$ 次の正方行列として生成行列が $(P\ I_k)$ で与えられているならば、検査行列は、I_{n-k} を $n-k$ 次の単位行列として $\left(I_{n-k}\ -{}^t P\right)$ である。いま C_1 は $\mathbf{Z}_p$ 上の符号だから、C_1 の検査行列は計算することができ、$(C^\perp)_0 \cong (C_1)^\perp$ だから、定理 2.3 の証明から判るように $(C^\perp)_0 = p(C_1)^\perp$ として $(C^\perp)_0$ が知れる。さらに $(C^\perp)_1$ を決定しなければならないが、$(C^\perp)_1 \cong (C_0)^\perp$ だから $c_i' \in (C^\perp)_1$ を

$$c_i' = (c_{i1}' \cdots c_{in}') + p(x_{i1}' \cdots x_{in}'),$$
$$(c_{i1}' \cdots c_{in}'), (x_{i1}' \cdots x_{in}') \in \mathbf{Z}_p^n$$

と書いてみれば、定理 2.3 の証明からわかるように

$$(c_{i1}' \cdots c_{in}') = \phi_1(c_i') \in (C_0)^\perp$$

である。C_0 は $\mathbf{Z}_p$ 上の符号であり C_0 の検査行列を計算すれば $(C^\perp)_1$ の基底の mod p での射影が求まる。あとは各 $(c_{i1}' \cdots c_{in}')$ について、C_1 と直交するように、$(x_{i1}', \cdots, x_{in}')$ を決めればよい。C_1 の基底を $c_j = (c_{j1} \cdots c_{jn}) + p(x_{j1} \cdots x_{jn})$ $(1 \le j \le k_1)$ とすれば、$x_{i1}, \cdots, x_{in}$ は $c_i' \cdot c_j \equiv 0 \bmod p^2$ すなわち一次合同式系

$$c_{j1}x_{i1}' + \cdots + c_{jn}x_{in}' \equiv -\frac{1}{p}(c_{i1}' \cdots c_{in}') \cdot (c_{j1} \cdots c_{jn}) - (c_{i1}' \cdots c_{in}')(x_{j1} \cdots x_{jn}) \bmod p$$

から定まる。

一般の場合も、まず定理 2.3 (2) で $l = 1$ とおくと

$$(C^\perp)_0^{(1)} \cong (C_1^{(m-1)})^\perp$$

となることから、$C^\perp$ の基底のうち、成分が全て p で割れているような部分符号の基底を求める計算は、C を mod p^{m-1} で射影して得られる $\mathbf{Z}_{p^{m-1}}$ 上の符号の双対符号の計算に帰着する。のこる問題は $(C^\perp)_1^{(1)}$ を計算することである。$c_i' \in (C^\perp)_1^{(1)}$ を

$$c_i' = (c_{i1}' \cdots c_{in}') + p^{m-1}(x_{i1}' \cdots x_{in}'),$$
$$(c_{i1}' \cdots c_{in}') \in \mathbf{Z}_{p^{m-1}}^n,\ (x_{i1}' \cdots x_{in}') \in \mathbf{Z}_p^n$$

と書く。$\phi_{m-1}(c_i') = (c_{i1}' \cdots c_{in}')$ である。まず定理 2.3 (2) で $l = 1$ とおいたとき

$$(C^\perp)_1^{(m-1)} \cong (C_0^{(1)})^\perp$$

となることから、$(C^\perp)_1^{(m-1)}$ の基底の mod p^{m-1} での射影が $\mathbf{Z}_{p^{m-1}}$ 上の符号 $C_0^{(1)}$ の検査行列を計算すれば求められ、$(c_{i1}' \cdots c_{in}')$ はここでさらに mod p での射影をとって零とならないものである。あとは $C_1^{(1)}$ と直交するように、$(x_{i1}', \cdots, x_{in}')$ を決めればよく、$C_1^{(1)}$ の基底を $c_j = (c_{j1} \cdots c_{jn}) + p(x_{j1} \cdots x_{jn})$ $(1 \le j \le k_1)$ とすれば、$x_{i1}', \cdots, x_{in}'$ は $c_i' \cdot c_j \equiv 0 \bmod p^m$ $(j = 1, 2, \cdots)$ すなわち一次合同式系

$$c_{j1}x_{i1}' + \cdots + c_{jn}x_{in}' \equiv -\frac{1}{p^{m-1}}(c_{i1}' \cdots c_{in}') \cdot (c_{j1} \cdots c_{jn}) - (c_{i1}' \cdots c_{in}')(x_{j1} \cdots x_{jn}) \bmod p$$

から定まる。

例 2.3 例 2.2 の符号の双対符号を計算する。$C_k^{(l)}$ の生成行列を $G_k^{(l)}$ と書く。まず、

$$G_1^{(2)} = \begin{pmatrix} 2 & 0 & 2 & 0 \\ 2 & 0 & 0 & 2 \\ 1 & 2 & 3 & 0 \end{pmatrix}$$

を生成行列とする $\mathbf{Z}_4$ 上の符号の検査行列を計算する。$C_0 = \{(0000), (1010), (1001), (0011)\}$ 及び $C_1 = \{(0000), (1010)\}$ の検査行列は各々

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

である。ここで (1230) との直交条件を (1011) + $2(x_{11}x_{12}x_{13}x_{14})$, (0100) + $2(x_{21}x_{22}x_{23}x_{24})$ とおいて調べると

$$(1011)(1230) + 2(x_{11}x_{12}x_{13}x_{14})(1230) \equiv 0 \pmod 4$$
すなわち $x_{11} + x_{13} \equiv 0 \pmod 2$
$$(0100)(1230) + 2(x_{21}x_{22}x_{23}x_{24})(1230) \equiv 0 \pmod 4$$
すなわち $x_{21} + x_{23} \equiv 1 \pmod 2$

だから $(x_{11}x_{12}x_{13}x_{14}) = (0000)$, $(x_{21}x_{22}x_{23}x_{24}) = (1000)$ ととり (1011) 及び (2100) を得る。これらと $2\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 2 & 0 & 0 \\ 2 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$ を並べたものが求める検査行列 $H_1^{(2)} = \begin{pmatrix} 0 & 2 & 0 & 0 \\ 2 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \\ 1 & 0 & 1 & 1 \\ 2 & 1 & 0 & 0 \end{pmatrix}$ である。$G_0^{(1)} =$

$\begin{pmatrix} 2&0&2&0\\ 2&0&0&2\\ 1&2&3&0\\ 1&2&2&3 \end{pmatrix}$ の検査行列 $H_0^{(1)} = \begin{pmatrix} 2&0&2&2\\ 0&2&0&0\\ 1&0&1&3\\ 0&1&2&2 \end{pmatrix}$ も同様に計算できる。mod 2 で射影をとって零とならない (1013) と (0122) について各々 $(1013)+4(x_{11}x_{12}x_{13}x_{14})$, $(0122)+4(x_{21}x_{22}x_{23}x_{24})$ とおいて (1234) との直交条件を調べれば

$$(1013)(1234)+4(x_{11}x_{12}x_{13}x_{14})(1234)\equiv 0 \pmod 8$$
すなわち $x_{11}+x_{13}\equiv 0 \pmod 2$
$$(0122)(1234)+4(x_{21}x_{22}x_{23}x_{24})(1234)\equiv 0 \pmod 8$$
すなわち $x_{21}+x_{23}\equiv 0 \pmod 2$

したがって $(x_{11}x_{12}x_{13}x_{14})=(x_{21}x_{23}x_{23}x_{24})=(0000)$ でよい。$2H_1^{(2)}$ と (1013), (0122) を並べると、検査行列が次のように求められる。

$$H=\begin{pmatrix} 0&4&0&0\\ 4&0&4&0\\ 0&0&0&4\\ 2&0&2&2\\ 4&2&0&0\\ 1&0&1&3\\ 0&1&2&2 \end{pmatrix}$$

とくに C が $\mathbf{Z}_{p^2}$ 上の自己双対符号のとき、定理 2.3 から $(C_1)^\perp=(C^\perp)_0=C_0$ であり、また $C_1\subset C_0$ だから C_1 は自己直交である。したがってまた、任意の符号語について $c\cdot c'=0 \bmod p^2$ が満たされるような $\mathbf{Z}_p$ 上の自己直交符号があれば、それから直ちに $\mathbf{Z}_{p^2}$ 上の自己双対符号が作られる (ただし逆は成り立たない)。

定理 2.4 G_0 を任意の符号語 c_1, c_2 について $c_1\cdot c_2=0 \bmod p^2$ が満たされるような $\mathbf{Z}_p$ 上の自己直交符号の生成行列、H_0 をその検査行列とすれば $G=\begin{pmatrix} pH_0\\ G_0 \end{pmatrix}$ は $\mathbf{Z}_{p^2}$ 上の自己双対符号の生成行列となる。

例 2.4 C_1 を $\mathbf{Z}_p$ 上の符号長 p^2m の繰り返し符号とすれば、次のような $\mathbf{Z}_{p^2}$ 上の自己双対符号が構成される。

$$G=\begin{pmatrix} -p&p&0&\cdots&0\\ -p&0&p&\cdots&0\\ \vdots&\vdots&\vdots&\ddots&\vdots\\ -p&0&0&\cdots&p\\ p&p&p&\cdots&p\\ 1&1&1&\cdots&1 \end{pmatrix}$$

$p=2$ のとき、この符号は Klemm が与えた ([5])。C_0 は C_1 の双対符号だから、C_1 の完全重さ分布多項式

$$W_{C_1}(X_a;a\in\mathbf{Z}_p)=X_0^{p^2m}+X_1^{p^2m}+\cdots+X_{p-1}^{p^2m}$$

にマックウイリアムスの恒等式を使い、変数 X_a を X_{ap} に置き換えれば C_0 の完全重さ分布多項式が求まるが、一般に C_0 を $\mathbf{Z}_p$ 上の符号とするとき pC_0 と $(11\cdots1)$ で生成される $\mathbf{Z}_{p^2}$ 上の符号 C の完全重さ分布多項式は

$C_0\ni(11\cdots1)$ ならば
$$W_C(X_a;a\in\mathbf{Z}_{p^2})=\sum_{i=0}^{p-1}W_{C_0}(X_{0+i},X_{p+i},\cdots,X_{(p-1)p+i})$$
$C_0\not\ni(11\cdots1)$ ならば
$$W_C(X_a;a\in\mathbf{Z}_{p^2})=\sum_{i=0}^{p}W_{C_0}(X_{0+i},X_{p+i},\cdots,X_{(p-1)p+i})$$

(添字は mod p^2 でみる) であるから、この符号の完全重さ分布多項式は $\zeta=e^{\frac{2\pi\sqrt{-1}}{p}}$ として次式で与えられる。

$$W_C(X_a;a\in\mathbf{Z}_{p^2})=\frac{1}{p}\sum_{i=0}^{p-1}\left\{(\sum_{j=0}^{p-1}X_{i+j})^{p^2m}+(\sum_{j=0}^{p-1}\zeta^jX_{i+j})^{p^2m}+\cdots+(\sum_{j=0}^{p-1}\zeta^{(p-1)j}X_{i+j})^{p^2m}\right\}$$

例 2.5 $G_1=\begin{pmatrix} 1&1&1&1&0&0\\ 0&0&1&1&1&1 \end{pmatrix}$ は $\mathbf{Z}_2$ 上の自己直交符号だが定理 2.4 の条件を満たさない。ただし mod 2 で twist すれば $G_1=\begin{pmatrix} 1&1&1&1&0&0\\ 0&0&3&1&1&1 \end{pmatrix}$ とその双対から次のような $\mathbf{Z}_4$ 上の自己双対符号が作られる。

$$G=\begin{pmatrix} 2&0&2&0&2&0\\ 2&2&0&0&0&0\\ 0&0&2&2&0&0\\ 0&0&0&0&2&2\\ 1&1&1&1&0&0\\ 0&0&3&1&1&1 \end{pmatrix}$$

この符号は一般に $\mathbf{Z}_{p^2}$ 上で定義することができ、

$$G_1=\begin{pmatrix} \overbrace{1\cdots1}^{p^2m-2n\text{ 個}} & 1 & \cdots & 1 & \overbrace{1\cdots1}^{n\text{ 個}} & 0\cdots0\\ 0\cdots0 & \underbrace{p^2-1\cdots p^2-1}_{n\text{ 個}} & & & 1\cdots1 & \underbrace{1\cdots1}_{p^2m-2n\text{ 個}} \end{pmatrix}$$

から自己双対符号を作ることができる。

Remark. p を奇素数とするとき $\mathbf{Z}/p^m\mathbf{Z}$ の乗法群は位数 $(p-1)p^{m-1}$ の巡回群である。生成元を β とし、$2l|(p-1)$ を満たす l をとって $\alpha=\beta^{\frac{(p-1)p^{m-1}}{2l}}$ とおく。$\mathbf{Z}/p^m\mathbf{Z}$ の l 次元リー距離 ([6]) を

$$\varphi(e_i)=\alpha^{i-1}\quad(1\le i\le l)$$

によって定めれば、成分の 1 箇所だけが α^{i-1} $(1\le i\le l)$ で他は 0 であるような系列が、重さが 1 であるような誤りパターンの全てとなることから

$$H=\begin{pmatrix} 1&\beta&\beta^2&\cdots&\beta^{n-1} \end{pmatrix}\quad\left(n=\frac{p^{m-1}(p-1)}{2l}\right)$$

を検査行列とする $\mathbf{Z}/p^m\mathbf{Z}$ 上の符号は φ が定める l 次元リー距離のもとで 1 誤り訂正可能であることがわかる。

3　p-進整数環上の符号

$\mathbf{Z}_{p^m}$ 上の符号 C は mod p^{m-1} の射影をとることで $\mathbf{Z}_{p^{m-1}}$ 上の符号となったが、mod p^{m-2} での射影をとれば $\mathbf{Z}_{p^{m-2}}$ 上の符号になる等々も帰納的にわかる。そこで射影的極限を考えることによって、p-進整数環上の符号を定義することができる。

定義 3.1 $\mathbf{Z}_{p^\infty}$ 上の符号長 n の符号とは、$\mathbf{Z}_{p^m}$ 上の符号長 n の符号 $C^{(m)}$ と ϕ_{m-1} によって与えられる射影系の射影的極限 $C^{(\infty)} = \varprojlim(C^{(m)}, \phi_{m-1})$ である。

定義から p-進整数環上の符号とは $\mathbf{Z}_{p^m}$ 上の符号 $C^{(m)}$ の列 $(\cdots, C^{(m)}, \cdots, C^{(1)})$ で $\phi_{m-1}(C^{(m)}) = C^{(m-1)}$ を満たすものである。したがってまた p-進整数環上の符号 $C^{(\infty)}$ の符号語とは、$C^{(m)}$ の符号語 $c^{(m)}$ の列 $(\cdots, c^{(m)}, \cdots, c^{(1)})$ で $\phi_{m-1}(c^{(m)}) = c^{(m-1)}$ を満たすものである。いま $c^{(m)} = (\, c_1^{(m)} \;\; c_2^{(m)} \;\; \cdots \;\; c_n^{(m)})$ として成分ごとにみれば $\phi_{m-1}(c_i^{(m)}) = c_i^{(m-1)}$ だから、

$$c^{(\infty)} \in \mathbf{Z}_{p^\infty}^n.$$

次に p-進整数環上の符号の生成行列を考察する。

$$C^{(\infty)} = (\cdots, C^{(m)}, \cdots, C^{(1)}), \quad \phi_{m-1}(C^{(m)}) = C^{(m-1)}$$

について $C^{(m)}$ の生成行列を

$$G^{(m)} = \begin{pmatrix} \mathcal{G}_1^{(m)} \\ \mathcal{G}_2^{(m)} \\ \vdots \\ \mathcal{G}_{k_m}^{(m)} \end{pmatrix}$$

とする。ここで $\mathcal{G}_i^{(m)}$ $(1 \le i \le k_m)$ は $C^{(m)}$ の符号語であり、したがって各 $\mathcal{G}_i^{(m)}$ について $\phi_{m-1}(\mathcal{G}_i^{(m)}) = \mathcal{G}_i^{(m-1)}$ となる $C^{(m-1)}$ の符号語 $\mathcal{G}_i^{(m-1)}$ が存在する。生成行列 $G^{(m)}$ は定理 2.1 にならって構成してあるものとすれば、零でない $\mathcal{G}_i^{(m-1)}$ たちを並べたものが $C^{(m)}/(C^{(m)})_0^{(m-1)} = (C^{(m)})_1^{(m-1)} = C^{(m-1)}$ の生成行列である。要するに、$G^{(m)}$ の各行ベクトル毎に ϕ_{m-1} での射影をとり、零となる行は除いて得られる行列が $C^{(m-1)}$ の生成行列である。その意味で

$$G^{(\infty)} = (\cdots, G^{(m)}, \cdots, G^{(1)}), \quad \phi_{m-1}(G^{(m)}) = G^{(m-1)}$$

と記す。$G^{(\infty)}$ は $\mathbf{Z}_{p^\infty}$ を成分とする行列とみてよい。また $C^{(m)}$ の双対符号を簡略に $C^{(m)}$ と記せば $c \in C^{(m)}$, $c' \in C^{(m)}$ は $c \cdot c' \equiv 0 \bmod p^m$ を満たさねばならないが、それぞれ

$$c = a + p^{m-1}x, \quad c' = b + p^{m-1}y,$$
$$(\phi_{m-1}(c) = a,\ \phi_{m-1}(c') = b,\ a, b \in \mathbf{Z}_{p^{m-1}}^n)$$

とおけば $\phi_{m-1}(c) \cdot \phi_{m-1}(c') = a \cdot b \equiv 0 \bmod p^{m-1}$ でなければならず、$\phi_{m-1}(c) \in C^{(m-1)}$ だから $\phi_{m-1}(c') \in C^{(m-1)}$ である。すなわち

定義 3.2 $C^{(\infty)}$ の双対符号とは、$C^{(m)}$ の双対符号 $C^{(m)}$ の射影的極限 $C^{(\infty)} = \varprojlim(C^{(m)}, \phi_{m-1})$ のことである。

定義から $C^{(m)}$ は $C^{(m)}$ の双対符号 $C^{(m)}$ の列

$$C^{(\infty)} = (\cdots, C^{(m)}, \cdots, C^{(1)}), \quad \phi_{m-1}(C^{(m)}) = C^{(m-1)},$$

である。$C^{(\infty)}$ の検査行列は $C^{(m)}$ の検査行列 $H^{(m)}$ から

$$H^{(\infty)} = (\cdots, H^{(m)}, \cdots, H^{(1)}), \quad \phi_{m-1}(H^{(m)}) = H^{(m-1)}$$

と定義できる。

例 2.6 $G^{(\infty)} = \begin{pmatrix} 1 & \lambda & -1 & 0 \\ 0 & 1 & \lambda & -1 \end{pmatrix}$

ここで λ は $\lambda^2 + 2 = 0$ を満たす3-進数で、3 進展開の最初の 5 項は $\lambda = 21022\cdots$ (したがってもうひとつの解は $11200\cdots$) である。$G^{(1)}$ は λ の 3-進展開の第 1 項をとり $\lambda \equiv 2 \bmod 3$ とおくことによって得られ、また $G^{(2)}$ は 3-進展開の第 2 項までとって $\lambda \equiv 2 + 1 \cdot 3 = 5 \bmod 9$ とおいて得られる。

$$G^{(1)} = \begin{pmatrix} 1 & 2 & -1 & 0 \\ 0 & 1 & 2 & -1 \end{pmatrix} \equiv \begin{pmatrix} 1 & 2 & 2 & 0 \\ 0 & 1 & 2 & 2 \end{pmatrix} \bmod 3,$$

$$G^{(2)} = \begin{pmatrix} 1 & 5 & 8 & 0 \\ 0 & 1 & 5 & 8 \end{pmatrix},$$

$$\vdots$$

$G^{(1)}$ が定義する $\mathbf{Z}_3$ 上の符号は [4,2] 3 元ハミング (Ternary Hamming) 符号である。

参考文献

[1] A.R.Calderbank, N.J.A.Sloane, Modular and p-adic cyclic codes, Designs,Codes and Cryptogr.6(1995), p21-35.

[2] I.F.Blake, Codes over certain rings, Inform.Control, 20(1972), p396-404.

[3] I.F.Blake, Codes over integer residue rings, Inform.Control, 29(1975), p295-300.

[4] 金子尚史, 有限剰余環上の線形符号の生成行列について, 法政大学大学院工学研究科修士論文, 1999.

[5] M.Klemn,Selbstduale Codes über dem Ring der ganzen Zahlen modulo 4,Arch.Math 53,p201-207.

[6] S.Nishimura,T.Hiramatsu,Generalized Lee distance and error-correcting codes,*preprint*.

[7] E.Spiegel, Codes over $\mathbf{Z}_m$, Inform.Control, 35(1977), p48-51.

[8] Zhe-Xian Wan, Quatenary Codes, World Scientific, 1998.