

代数系と符号理論 第14回板書プリント

植松友彦 2007.7.3

1 符号の組合せ

今回は、複数の符号を組み合わせることでより強力な符号を作る方法について説明する。

1.1 $|u|u+v|$ 構成

いま、 F_2^n の2つのベクトル

$$u = (u_1, u_2, \dots, u_n), \quad v = (v_1, v_2, \dots, v_n)$$

に対して、 F_2^{2n} のベクトル $|u|u+v|$

$$|u|u+v| = (u_1, u_2, \dots, u_n, u_1+v_1, u_2+v_2, \dots, u_n+v_n)$$

によって定義する。

さて、2元符号 C_1 と C_2 がそれぞれパラメータ (n, k_1, d_1) および (n, k_2, d_2) を有するとする。ここで、 $d_2 > d_1$ であるとする。このとき、長さ $2n$ の線形符号 C を

$$C = |C_1|C_1 + C_2| = \{|u|u+v| : u \in C_1, v \in C_2\}$$

によって定義する。このとき、 C は2元 $(2n, k_1+k_2)$ 符号であり、 C_1, C_2 の生成行列を G_1, G_2 とすれば、 G の生成行列は、

$$G = \begin{bmatrix} G_1 & G_1 \\ 0 & G_2 \end{bmatrix}$$

によって定まる。また、 C の最小距離 $d_{\min}(C)$ は、

$$d_{\min}(C) = \min\{2d_1, d_2\}$$

を満足する。以下では、この最小距離の式を証明する。

$x = |u|u+v|$ と $y = |u'|u'+v'|$ を C の2つの異なる符号語とする。このとき、

$$d_H(x, y) = w_H(u+u') + w_H(u+u'+v+v')$$

が成り立つ。但し、 w_H はハミング重みを表す。ここで場合を分ける。

[$v = v'$ のとき]

$x \neq y$ であるから、 $u \neq u'$ でなければならない、

$$d_H(x, y) = w_H(u+u') + w_H(u+u') = 2w_H(u+u') \geq 2d_1$$

が得られる。但し、最後の不等式は C_1 の最小距離すなわち C_1 の非零の符号語の最小重みが d_1 以上であることを用いた。

[$v \neq v'$ のとき]

三角不等式 $w_H(a+b) \geq w_H(a) - w_H(b)$ を用いて

$$d_H(x, y) \geq w_H(u+u') + w_H(v+v') - w_H(u+u') = w_H(v+v') \geq d_2$$

が得られる。但し、最後の不等式は C_2 の最小距離すなわち C_2 の非零の符号語の最小重みが d_2 以上であることを用いた。

以上をまとめて、

$$d_H(x, y) \geq \min\{2d_1, d_2\}$$

が得られる。ここで、非零の符号語の最小重みは最小距離に等しいから、

$$d_{\min}(C) \geq \min\{2d_1, d_2\}$$

が導かれる。

最後に、この不等式の等号が成り立つことを示す。いま、 u_0 と v_0 をそれぞれ C_1 と C_2 の重み最小の非零の符号語とする。明らかに、 $w_H(u_0) = d_1$ および $w_H(v_0) = d_2$ が成り立つ。このとき、 $|u_0|u_0|$ は C の符号語であり、そのハミング重みは $2d_1$ である。また、 $|0|v_0|$ もまた C の符号語であり、そのハミング重みは d_2 である。従って、 $d_{\min}(C)$ は $2d_1$ か d_2 でなければならず、

$$d_{\min}(C) = \min\{2d_1, d_2\}$$

が成り立つ。

$|u|u+v|$ 構成は、短い符号から長い符号を作るときによく用いられる強力な方法である。

[例 1] C_1 を生成行列

$$G_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

を有する 2 元 (8, 4, 4) 符号とする。また、 C_2 を生成行列

$$G_2 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

を有する 2 元 (8, 1, 1) 符号とする。このとき、 $|u|u+v|$ 構成によつて、2 元 (16, 5) 符号が得られ、その最小距離は 8 である。また、その生成行列は、

$$\begin{aligned} G &= \begin{bmatrix} G_1 & G_1 \\ 0 & G_2 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \end{aligned}$$

である。

1.2 積符号

定義 10.1.1 積符号とは、各行が (n_1, k_1, d_1) 線形符号の符号語であり、各列が (n_2, k_2, d_2) 線形符号の符号語であるような $n_1 \times n_2$ 配列全体のベクトル空間である。

図 1: 積符号

例 2 行符号と列符号に符号長 3 の単一パリティ検査符号 $((3,2,2)$ 符号) を用いた $(9,4,4)$ 符号の符号語は、以下の 16 個である。

0 0 0	0 0 0	0 0 0	0 0 0
0 0 0	0 1 1	1 0 1	1 1 0
0 0 0	0 1 1	1 0 1	1 1 0
0 1 1	0 1 1	0 1 1	0 1 1
0 0 0	0 1 1	1 0 1	1 1 0
0 1 1	0 0 0	1 1 0	1 0 1
1 0 1	1 0 1	1 0 1	1 0 1
0 0 0	0 1 1	1 0 1	1 1 0
1 0 1	1 1 0	0 0 0	0 1 1
1 1 0	1 1 0	1 1 0	1 1 0
0 0 0	0 1 1	1 0 1	1 1 0
1 1 0	1 0 1	0 1 1	0 0 0

定理 10.1.1 積符号のパラメータは $(N, K, D) = (n_1 n_2, k_1 k_2, d_1 d_2)$ である。

積符号の最も簡単な復号法は、次のように行われる。

1. 受信語の各列を独立に復号し、誤り訂正された符号語を各列に並べる。
2. 行に用いた符号の復号アルゴリズムを各行に独立に適用する。

このような復号法を直列的復号 (serial decoding) と呼ぶ。

補題 10.1.1 積符号を直列に復号するとき、重み $(D-1)/4$ 以下の任意の誤りを訂正することができる。

2 接続符号

Reed-Solomon(RS) 符号を構成要素に用いた積符号の一種を「接続符号」という。以下では、接続符号について述べる。まず、RS 符号の 2 元展開について、次の補題が成り立つ。

補題 10.2.1 $q = 2^r$ 個の元からなる体上の $RS(N, K, D)$ 符号の 2 元表現は、2 元 (rN, rK, D') 符号となる。ここで、 $D' \geq D = N - K$ である。

図 2: 接続符号

定義 10.2.1 $q = 2^r$ 個の元からなる体上の $RS(N, K, D)$ 符号を 2 元表現した後、各成分を表す r ビットを更に 2 元 (n, r, d) 符号で符号化することによって得られる 2 元符号を接続符号と呼ぶ。接続符号の符号長は nN であり、次元は kK である。

定理 10.2.1 接続符号の最小距離は Dd 以上である。