■1 群（信号・システム）- 2 編（符号理論）

4 章 符号の構成

（執筆者：西島利尚）［2012 年 3 月 受領］

■概要■

本章では，符号の構成について述べる．

誤り訂正符号を実際に装置化する際に，装置の仕様として要求される信頼性を保障したうえで，符号語のビット数あるいは情報記号のビット数などに制約がある場合がある．こうした制約を解消するために，何らかの方法で構成された線形符号に対して簡単な変更を加えて用いる．この簡単な変更により得られる符号を修正符号と呼んでいる．実際に，重要な修正符号には，パリティ検査ビットを付加することにより得られる拡大線形符号，一部の情報ビットを 0 に固定することで得られる短縮符号，符号語の一部を除去することで得られるパンクチャ符号などがある．

また，情報ビット数及び検査ビット数を適当に大きくすることで，訂正能力のより高い符号化を行えば，一般に復号器の装置化がかなり複雑になる．更に実際の通信路は，ランダム誤り，バースト誤り，あるいは両者の誤りが混在するなど，様々である．これらの様々な制約を解消するために，適当な二つ以上の符号を組み合わせて使用する場合がある．これは，比較的装置化が簡単でかつ，比較的誤り訂正能力の高い符号，そして実際の通信路に適した構造をもつ符号を構成することができる．更に，適当な符号の組合せにより理論的にも興味深い符号を構成できることがある．符号の組合せ方法として，基本的な積符号と連接符号の二つの方法について述べる．

【本章の構成】

本章は，符号の修正（4-1 節），積符号（4-2 節），連接符号（4-3 節），からなる．

■1 群 - 2 編 - 4 章

4-1 符号の修正

（執筆者：西島利尚）[2012 年 3 月 受領]

本節では 2 元線形符号に対する各種の符号の修正法について述べる

2 元 $(n, k, d_{\min})$ 線形符号 C のすべての符号語に対して，パリティ検査ビットを付加して得られる 2 元 $(n+1, k, d'_{\min})$ 線形符号 C' を拡大線形符号とする[1, 2]．一般に，$(n, k, d_{\min})$ 線形符号 C のパリティ検査行列 H が与えられたとき，$(n+1, k, d'_{\min})$ 拡大線形符号 C' のパリティ検査行列 H' は，

$$H' = \left[\begin{array}{ccc|c} & H & & \begin{matrix}0\\0\\\vdots\\0\end{matrix} \\ \hline 1 & 1 \quad \cdots \quad 1 & & 1 \end{array}\right] \tag{4·1}$$

で与えられる．ただし，$d_{\min}$ が奇数のときは $d'_{\min} = d_{\min} + 1$，偶数のときは $d'_{\min} = d_{\min}$ である．$(7, 4, 3)$ ハミング符号 C のパリティ検査行列 H と $(8, 4, 4)$ 拡大ハミング符号 C' のパリティ検査行列 H' はそれぞれ，

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}, \tag{4·2}$$

$$H' = \left[\begin{array}{ccccccc|c} 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ \hline 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right], \tag{4·3}$$

で与えられる．$(7, 4, 3)$ ハミング符号 C の符号語と，それに対応する $(8, 4, 4)$ 拡大ハミング符号 C' の符号語を表 4·1 に示す．

次に，2 元 $(n, k, d_{\min})$ 線形符号 C のすべての符号語に対して，符号語の一部 s ビットを除去して得られる 2 元 $(n-s, k, d'_{\min})$ 線形符号 C' をパンクチャ符号とする[1, 2]．ここで，$d'_{\min} \geq d_{\min} - s$，$s < n - k$ である．$(7, 4, 3)$ ハミング符号 C の生成行列 G と $(6, 4, 2)$ パンクチャ符号 C' の生成行列 G' はそれぞれ，

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}, \tag{4·4}$$

表 4･1　$(7,4,3)$ **ハミング符号** C **と** $(8,4,4)$ **拡大ハミング符号** C'

ハミング符号	拡大ハミング符号	ハミング符号	拡大ハミング符号
0000000	00000000	0001011	00010111
1110100	11101000	1000101	10001011
0111010	01110100	1100010	11000101
0011101	00111010	0110001	01100011
1001110	10011100	1011000	10110001
0100111	01001110	0101100	01011001
1010011	10100110	0010110	00101101
1101001	11010010	1111111	11111111

$$G' = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}, \tag{4･5}$$

で与えられる．G' は，G の最後の 7 列目を除去したもので，ハミング符号 C のすべての符号語の検査ビットから最後尾の 1 ビットを除去している．$(7,4,3)$ ハミング符号 C の符号語と，それに対応する $(6,4,2)$ パンクチャ符号 C' の符号語を表 4･2 に示す．

表 4･2　$(7,4,3)$ **ハミング符号** C **と** $(6,4,2)$ **パンクチャ符号** C'

ハミング符号	パンクチャ符号	ハミング符号	パンクチャ符号
0000000	000000	0001011	000101
1110100	111010	1000101	100010
0111010	011101	1100010	110001
0011101	001110	0110001	011000
1001110	100111	1011000	101100
0100111	010011	0101100	010110
1010011	101001	0010110	001011
1101001	110100	1111111	111111

最後に，2 元 $(n,k,d_{\min})$ 線形符号 C のすべての符号語に対して，s ビットの情報ビットを 0 に固定して得られる 2 元 $(n-s,k-s,d'_{\min})$ 線形符号 C' を短縮線形符号とする[1, 2)．ここで，$d'_{\min} \geq d_{\min}$ である．$(7,4,3)$ ハミング符号 C の 4 ビットの情報ビットのうち，最初の 2 ビットをあらかじめ 0 とおき，$(7,4,3)$ ハミング符号 C の生成行列 G で符号化する．得られた符号語の最初の 2 ビットの 0 を除去することで $(5,2,3)$ 短縮ハミング符号 C' を得る．$(7,4,3)$ ハミング符号 C の符号語と，それに対応する $(5,2,3)$ 短縮ハミング符号 C' の符号語を表 4･3 に示す．

表 4·3　(7, 4, 3) ハミング符号 C と (5, 2, 3) 短縮ハミング符号 C'

情報記号系列	ハミング符号	短縮ハミング符号
0000	0000000	00000
0001	0001111	01111
0010	0010110	10110
0011	0011001	11001

■1 群 - 2 編 - 4 章

4-2 積符号

（執筆者：西島利尚）[2012 年 3 月 受領]

積符号では，第 1 段の符号として，q 元 $(n_1, k_1, d_{1\min})$ 線形符号 C_1 を与え，第 2 段の符号として，q 元 $(n_2, k_2, d_{2\min})$ 線形符号 C_2 を与える．

長さ k_1k_2 の q 元情報シンボルが与えられたとき，まず，k_1 個の長さ k_2 の q 元情報シンボルを，符号 C_2 の符号語として，第 2 段の符号化を行う．そして，得られた k_1 個の符号語を並べ，$k_1 \times n_2$ の 2 次元配列をつくる．次に，n_2 個の長さ k_1 の q 元情報シンボルを，符号 C_1 の符号語として，第 1 段の符号化を行う．この結果得られた，長さ n_1n_2 の q 元系列の集合を，q 元 $(\mathcal{N}, \mathcal{K}, \mathcal{D}_{\min})$ 積符号 C という[1, 2]．したがって，積符号 C は，$C = C_1 \otimes C_2$，と表される．ここで，$\otimes$ は直積を表す．積符号 C の符号パラメータは，$\mathcal{N} = n_1n_2$，$\mathcal{K} = k_1k_2$，$\mathcal{D}_{\min} = d_{1\min}d_{2\min}$，である．

積符号は，レディ‐ロビンソン復号法により，$t = \lfloor \frac{\mathcal{D}_{\min}-1}{2} \rfloor$ 個以下のすべての誤りを訂正することが可能である[3]．ここで，レディ‐ロビンソン復号法とは，限界距離復号法を一般化した，一般化最小距離復号法を積符号の復号に適用したものである[4]．ただし現在は，ターボ復号を行うことで，積符号はそれ以前の復号法を用いるよりも優れた誤り率を達成できることが知られている [6 章 6-1 節 参照]．更に，2 次元構造の符号語を行方向，あるいは列方向に逐次通信路に入力して行くと仮定し，通信路においてバースト誤りが生起した場合を考える．このとき積符号 C は，インタリーブを施していると考えることができるので，バースト長 $b = \max[n_1t_2, n_2t_1]$ 以下のバースト誤りを訂正することが可能である[5]．ただし，$t_1 = \lfloor \frac{d_{1\min}-1}{2} \rfloor$，$t_2 = \lfloor \frac{d_{2\min}-1}{2} \rfloor$ である．

積符号 C の符号化・復号の過程を図 4･1 に示す．

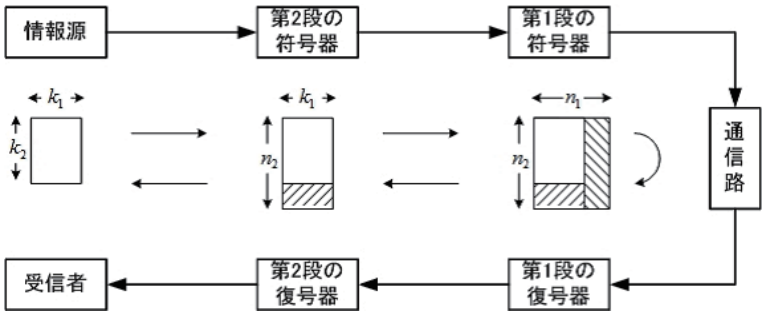

図 4･1　積符号 C の符号化・復号の過程

2 次元の積符号を s 次元に拡張することにより構成される q 元 $(\mathcal{N}, \mathcal{K}, \mathcal{D}_{\min})$ 繰り返し積符号 C は，$C = C_1 \otimes C_2 \otimes \cdots \otimes C_s$，と表される．繰り返し積符号 C の符号パラメータは，$\mathcal{N} = \prod_{i=1}^{s} n_i$，$\mathcal{K} = \prod_{i=1}^{s} k_i$，$\mathcal{D}_{\min} = \prod_{i=1}^{s} d_{i\min}$，である．

エライアスは，2 元対称通信路を対象として，繰り返し積符号 C の第 i 段の $(n_i, k_i, d_{i\min})$

符号 C_i に，2 元 $(2^{m+i-1}, 2^{m+i-1}-(m+i), 4)$ 拡大ハミング符号 C_i を適用して，符号長を十分大，すなわち，$s \to \infty$ とし，符号化率が非ゼロで，かつ復号後のビット誤り率が 0 に収束する繰り返し積符号 C を構成した．すなわち，復号後のビット誤り率 $p_s \leq (2^{m+1}p)^{2^s}$，そして符号化率 $\mathcal{R} = \prod_{i=1}^{s} \frac{k_i}{n_i} = \prod_{i=1}^{s}(1 - \frac{m+i}{2^{m+i-1}}) > 1 - \frac{m+2}{2^{m-1}}$ である繰り返し積符号を構成した[6]．ここで，p は 2 元対称通信路の誤り率，$m \geq 4$ の整数である．符号化率は，m の値に従属した離散値でしか実現することができない．しかし，符号化比率が非ゼロで符号長を十分大としたとき，複合語の誤り率が 0 に収束することを非ランダムな符号化によって証明された最初の線形符号である．

最後に，積符号の一般化について述べる．すなわち，第 1 段の q 元 $(n_1, k_1, d_{1\min})$ 線形符号 C_1 を，k_1 個の部分符号 $C_1 = C_1^{(1)} \supseteq C_1^{(2)} \supseteq \cdots \supseteq C_1^{(i)} \supseteq \cdots \supseteq C_1^{(k_1)}$ をもつ，非組織符号で与え，第 2 段の符号を，k_1 個の q 元 $(n_2, k_2^{(i)}, d_{2\min}^{(i)})$ 線形符号 $C_2^{(i)}$，$i = 1, 2, \ldots, k_1$，$k_2^{(1)} \leq k_2^{(2)} \leq \cdots \leq k_2^{(i)} \leq \cdots \leq k_2^{(k_1)}$，で与える．

長さ $\prod_{i=1}^{k_1} k_2^{(i)}$ の q 元情報シンボルが与えられたとき，第 1 番目の長さ $k_2^{(1)}$ の q 元情報シンボルを，符号 $C_2^{(1)}$ の符号語として，符号化する．次いで，第 2 番目の長さ $k_2^{(2)}$ の q 元情報シンボルを，符号 $C_2^{(2)}$ の符号語として，符号化する．以下同様にして，第 k_1 番目の長さ $k_2^{(k_1)}$ の q 元情報シンボルを，符号 $C_2^{(k_1)}$ の符号語として，順次符号化する．そして，得られた k_1 個の符号語を並べ，$k_1 \times n_2$ の 2 次元配列をつくり，第 2 段の符号化を終了する．次に，n_2 個の長さ k_1 の q 元情報シンボルを，符号 C_1 の符号語として，第 1 段の符号化を行う．この結果得られた，長さ $n_1 n_2$ の q 元系列の集合を，q 元 $(\mathcal{N}, \mathcal{K}, \mathcal{D}_{\min})$ 修正積符号 C という[7]．したがって，修正積符号 C は，$C = C_1 \otimes [C_2^{(1)}, C_2^{(2)}, \ldots, C_2^{(K_1)}]$，と表される．修正積符号 C の符号パラメータは，$\mathcal{N} = n_1 n_2$，$\mathcal{K} = \prod_{i=1}^{k_1} k_2^{(i)}$，$\mathcal{D}_{\min} = \min_{1 \leq i \leq k_1}[d_{1\min}^{(i)} d_{2\min}^{(i)}]$，である．ここで，$d_{1\min}^{(i)}$ は符号 C_1 の部分符号 $C_1^{(i)}$ の最小距離である．

修正積符号は，積符号と同様，レディ‐ロビンソン復号法により，$t = \lfloor \frac{\mathcal{D}_{\min}-1}{2} \rfloor$ 個以下のすべての誤りを訂正することが可能である．

■1 群 - 2 編 - 4 章

4-3 連接符号

（執筆者：西島 利尚）[2012 年 3 月 受領]

長さ kK の q 元情報シンボルが与えられたとき，まず，長さ K の系列を一組として GF(q^K) 上の元とみなし，長さ k の q^K 元情報シンボルを，q^K 元 $(n, k, d_{\min})$ 線形符号 C_{Outer} の符号語として，符号化する．ここで，符号 C_{Outer} を外部符号（外符号とも呼ばれる）といい，この符号化を外部符号化という．次に，得られた n 個の GF(q^K) 上の元，すなわち外部符号の符号語シンボルを，それぞれ長さ K の q 元情報シンボルとみなし，それを，q 元 $(N, K, D_{\min})$ 符号 C_{Inner} の符号語として，符号化する．ここで，符号 C_{Inner} を内部符号（内符号とも呼ばれる）といい，この符号化を内部符号化という．得られた内部符号の符号語を連接して得られる長さ nN の q 元系列の集合を，q 元 $(\mathcal{N}, \mathcal{K}, \mathcal{D}_{\min})$ 連接符号 C という[4]．連接符号 C の符号パラメータは，$\mathcal{N} = nN$，$\mathcal{K} = kK$，$\mathcal{D}_{\min} \geq d_{\min} D_{\min}$，である．

連接符号は，積符号と同様，レディ－ロビンソン復号法により，$t = \lfloor \frac{\mathcal{D}_{\min}-1}{2} \rfloor$ 個以下のすべての誤りを訂正することが可能である．

連接符号 C の符号化・復号の過程とその符号語を図 4･2 に示す．内部符号器・復号器に対して本来の通信路を内部通信路，外部符号器・復号器に対して内部符号器・通信路・内部復号器をまとめて通信路とみなすことで，外部通信路と呼ぶこともある．

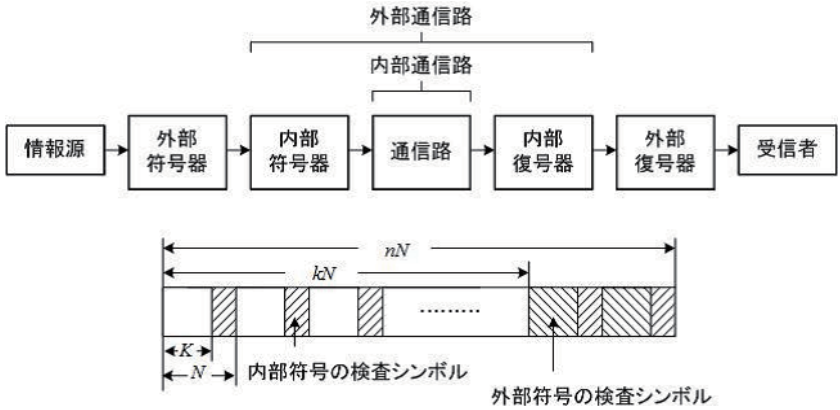

図 4･2　連接符号 C の符号化・復号の過程とその符号語

q 元 $(n, k, d_{\min})$ 線形符号 C の符号化率を $R = \frac{k}{n}$，そして，固定された値 R をもつ符号の集合族のなかで，符号のもつ最小距離の最大値を $d_{\min}(n, R)$ で表せば，符号 C の漸近的距離比は，

$$\delta(R) = \lim_{n\to\infty} \sup \frac{1}{n} d_{\min}(n, R) \tag{4･6}$$

と定義される．

GF(2^K) 上の原始リード‐ソロモン符号で外部符号化し，ギルバート‐バルシャモフ限界を満たす 2 元線形符号で内部符号化すれば，次の漸近的距離比をもつ 2 元連接符号 C が存在する．

$$\delta(\mathcal{R}) \geq \max_{0\leq R\leq 1}\Big[(1-\frac{\mathcal{R}}{R})H^{-1}(1-R)\Big]. \tag{4･7}$$

式 (4･7) が，ジアブロフ限界と呼ばれている[8]．ここで，$H^{-1}(x)$ は 2 元エントロピー関数 $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$ の逆関数である．

上記 2 元連接符号と同様，まず，GF(2^K) 上の原始リード‐ソロモン符号で外部符号化する．そして，原始リード‐ソロモン符号の符号語の $n(= 2^K - 1)$ 個のシンボル $a_i \in$GF(2^K), $i = 0, 1, \cdots, 2^K - 2$ を順次，生成行列 $[1, \alpha^i]$ で内部符号化する．$[1, \alpha^i]$ は GF(2^K) 上の，ボーゼンクラフトのランダムシフト $(2, 1)$ 符号 $C^{(i)}$ の生成行列である．ただし，α，$1 \in$GF(2^K) はそれぞれ，原始元と単位元を表す．この符号化方法を，n 個の異なる符号で内部符号化を行うという意味で，可変内部符号化という．この 2 元連接符号 C が，漸近的距離比が 0 に収束しない構成的に与えられる最初の代数的符号である[9]．ユーステセン符号と呼ばれる．ユーステセン符号 C の漸近的距離比は，

$$\delta(\mathcal{R}) \geq \max_{\frac{1}{2}\leq R\leq 1}\Big[(1-\frac{\mathcal{R}}{R})H^{-1}(1-R)\Big] \tag{4･8}$$

で与えられる．式 (4･8) は，高符号化率の範囲で，式 (4･7) に一致する．ユーステセン符号は，漸近的距離比が非ゼロの値をもつものの，ギルバート‐バルシャモフ限界にはかなりの隔たりがある．そこで，ユーステセン符号には様々な改良が加えられている[10, 12, 13, 11]．しかし一方では，原始リード－ソロモン符号で外部符号化し，かつ可変内部符号化によって構成される 2 元連接符号のクラスには，ギルバート‐バルシャモフ限界を満たす符号が存在することが示されている[14]．

最後に，連接符号の一般化について述べる．すなわち，長さ $K\sum_{j=1}^{J} k_j$ の q 元情報シンボルが与えられたとき，まず，この情報シンボルを，k_j 個の連続する長さ K の系列に分割する．分割した系列を GF(q^K) 上の元とみなし，長さ k_j の q^K 元情報シンボルを，q^K 元 $(n, k_j, d_{\min j})$ 線形符号 $C_{\mathrm{Outer}\,j}$，$j = 1, 2, \ldots, J$，の符号語として，順次符号化する．そして，得られた J 個の符号語を並べ，$JK \times n$ の 2 次元配列をつくり，外部符号化を終了する．次に，GF(q^K) 上の J 個の元を，長さ JK の GF(q) 上の元とみなし，n 個の長さ JK の q 元情報シンボルを，q 元 $(N, JK, D_{\min})$ 符号 C_{Inner} の符号語として内部符号化する．ここで，内部符号 C_{Inner} は，$(N, (J-j+1)K, D_{\min j})$ 符号 $C_{\mathrm{Inner}\,j}$ を部分符号としてもつ，非組織符号である．この結果得られた，長さ nN の q 元系列の集合を，q 元 $(\mathcal{N}, \mathcal{K}, \mathcal{D}_{\min})$ 一般化連接符号 C という[15, 16, 17]．一般化連接符号 C の符号パラメータは，$\mathcal{N} = nN$，$\mathcal{K} = K\sum_{j=1}^{J} k_j$，$\mathcal{D}_{\min} \geq \min_{1\leq j\leq J}[d_{\min j} D_{\min j}]$，である．

式 (4･7) と同一条件で，2 元一般化連接符号 C を構成すれば，符号 C の漸近的距離比は，

$$\delta(\mathcal{R}) \geq \max_{0\leq R\leq 1}\left[\frac{R-\mathcal{R}}{\displaystyle\int_0^{\mathcal{R}} \frac{dx}{H^{-1}(1-x)}}\right] \tag{4･9}$$

で与えられる．式 (4･9) は，2 元一般化連接符号の存在を保証する限界である．

一般化連接符号は，連接符号と同様，レディ‐ロビンソン復号法により，$t = \lfloor \frac{\mathcal{D}_{\min}-1}{2} \rfloor$ 個以下のすべての誤りを訂正することが可能である．

■参考文献

1) 今井秀樹，“符号理論,” 電子情報通信学会, 1990.
2) 平澤茂一，西島利尚，“符号理論入門,” 培風館，1999.
3) S.M. Reddy and J.P. Robinson, “Random error and burst correction by iterated codes,” IEEE Trans. Inform. Theory, vol.IT-18, pp.182-185, 1972.
4) G.D. Forney Jr., “Concatenated Codes,” Cambridge, Ma:MIT Press, 1966.
5) R.E. Blahut, “Algebraic Codes for Data Transmission,” Cambridge, University Press, 2003.
6) P. Elias, “Error-free coding,” IRE Trans. Inform. Theory, vol.PGIT-4, pp.29-37, 1954.
7) S. Hirasawa, M. Kasahara, Y. Sugiyama, and T. Namekawa, “Modified product codes,” IEEE Trans. Inform. Theory, vol.IT-30, pp.299-306, 1984.
8) V.V. Zyablov, “On estimation of complexity of construction of binary linear concatenated codes, Probl. Peredach. Inform., vol.7, pp.5-13, 1972.
9) J. Justesen, “A class of constructive asymptotically good algebraic codes, IEEE Trans. Inform. Theory, vol.IT-18, pp.652-656, 1972.
10) 杉山康夫，笠原正雄，平澤茂一，滑川敏彦，“二次の Concatenation を応用した漸近的に能率の良い代数的符号,” 電子情報通信学会論文誌 (A), vol.57-A, no.2, pp.121-127, 1974.
11) E.J. Weldon,Jr., “Some results on the problem of constructing asymptotically good error-correcting codes,” IEEE Trans. Inform. Theory, vol.IT-21, pp.412-417, 1975.
12) Y. Sugiyama, M. Kasahara, S. Hirasawa, and T. Namekawa, “A modification of the constructive asymptotically good codes of Justesen for low rates,” Inform. Contr., vol.25, pp.341-350, Aug. 1974.
13) Y. Sugiyama, M. Kasahara, S. Hirasawa, and T. Namekawa, “A new class of asymptotically good codes beyond the Zyablov bound,” IEEE Trans. Inform. Theory, vol.IT-24, pp.198-204, 1978.
14) C. Thommesen, “The existence of binary linear concatenated codes with Reed-Solomon outer codes which asymptotically meet the Gilbert-Varshamov bound,” IEEE Trans. Inform. Theory, vol.IT-29, pp.850-853, 1983.
15) S. Hirasawa, M. Kasahara, Y. Sugiyama, and T. Namekawa, “Certain generalizations of concatnated - Exponential error bounds and decoding complexity, IEEE Trans. Inform. Theory, vol.IT-26, pp.527-534, 1980.
16) S. Hirasawa, M. Kasahara, Y. Sugiyama, and T. Namekawa, “An improvement of error exponents at low rates for the generalized version of concatenated codes,” IEEE Trans. Inform. Theory, vol.IT-27, pp.350-352, 1981.
17) E.L. Blokh and V.V. Zyablov, “Existence of linear concatenated codes with optimal correcting properties,” Probl. Peredach. Inform., vol.9, pp.3-10, 1973.