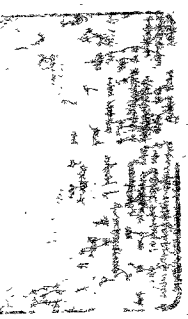
通信路に生ずるバースト誤りとその誤りを訂正する符号に関する研究



1970年1月

藤原値賀人

通信路に生ずるバースト誤りとその誤りを訂正する符号に関する研究

1970年1月

藤原値賀人

内　容　梗　概

本論文は，筆者が大阪大学大学院工学研究科（通信工学専攻）在学中に行なった“通信路に生ずるバースト誤りとその誤りを訂正する符号に関する研究”を6章に分けてまとめたものである．

第1章は緒論であって，バースト誤りおよびバースト誤り訂正符号に関するこれまでの研究のあらましを述べるとともに，本論文の占める位置を明らかにしている．

第2章は発表論文(1)，(2)，(3)を中心にして，任意長の符号内に生じる任意長のバースト誤りの確率の一般式を示したものである．すなわち，バースト誤りを生じる通信路のモデルとして，実際の通信路にかなり近似しうるGilbertのモデルを用いて母関数を導入することにより確率式誘導の手順を見い出し，近似を行なうことなく集中形および分離形のバースト誤りの確率の一般式を導いている．また同時にシミュレーションを行ない両者の一致を確かめ以下の二つの章における解析に利用している．

第3章では発表論文(4)，(5)を中心にして実用的なバースト誤り訂正符号の一構成法を示している．すなわち，最も符号構成に自由度を有するFire符号より構成の自由度はやや劣るが，訂正能力，装置の簡単さおよび生成多項式決定の容易さでまさる符号であり，その能力は，冗長数の1/3までの長さの誤りをすべて訂正でき，これを越えてほぼ冗長数の半分までの長さの誤りのほとんどすべてを訂正できるようなものである．

第4章では発表論文(1)，(3)，(6)，(7)を中心にしてバースト誤り訂正方式の効果について述べている．すなわち，信頼度および伝送能率を現実的な立場で定義し，バースト誤り訂正符号の効果について考察し，符号長および訂正

能力が信頼度と伝送能率に重大な影響を与えることを明らかにし，また最適符号長が顕著に存在することを示している．

第5章では発表論文(8)，(9)，(10)を中心にして，従来の畳み込み符号の有する欠点を改善できる符号化法を示している．すなわち，従来の符号化がシフトレジスタを用いているのに対し，フィードバック・シフトレジスタを用いて符号化を行なうことにより確率的に長い拘束長を確保し，復号側での同期引き込みやオーバーフロー後の処理が簡単となる方法を示し，また符号化回路の最適な結線多項式に関する条件を明らかにし，その条件より最適結線多項式を次数12まで求めている．

第6章は結論であって，本論文で得た諸結果を検討し，今後の方向について述べている．

関連発表論文

(1) 藤原，中西，笠原(正)，手塚，笠原(芳)，石田："バースト誤り訂正符号の最適符号長"，信学会インホメーション理研資（1965－11）．

(2) 藤原，中西，笠原(正)．手塚，笠原(芳)："バースト誤りを生ずる通信路に関する二，三の考察"，信学会インホメーション理研資，IT67－33（1967－09）．

(3) 藤原，中西，笠原(正)，手塚，笠原(芳)："バースト誤りを生ずる通信路とその信頼度の改善に関する考察"，信学誌，51－A，8，p.311（昭43－08）．

(4) 藤原，笠原(正)，手塚，笠原(芳)："バースト誤り訂正符号の一構成法"，信学会インホメーション理研資，IT69－04（1969－04）．

(5) 藤原，笠原(正)，手塚，笠原(芳)：“バースト誤り訂正符号の一構成法”，信学誌

(6) 藤原，中西，笠原(正)，手塚，笠原(芳)：“巡回符号の最適符号長に関する一考察”，信学全大（昭39－11）．

(7) 藤原，中西，笠原(正)，手塚，笠原(芳)：“バースト誤り訂正符号の最適符号長に関する考察”，信学全大（昭40－11）．

(8) 藤原，高橋，笠原(正)，手塚，笠原(芳)：“Convolutional Codeに関する研究(I)符号化”，信学全大（昭43－10）．

(9) 高橋，藤原，手塚，笠原(芳)：“Convolutional符号の構成に関する一考察”，信学会インホメーション理研資，IT68－64（1969－03）．

(10) 藤原，高橋，手塚，笠原(芳)：“フィードバック・シフトレジスタを用いた畳み込み符号の一構成法”，信学誌投稿中．

通信路に生ずるバースト誤りと
その誤りを訂正する符号に関する研究

目　　次

第1章　緒　　論

近年ディジタル・データの通信量の増大にともないさまざまの問題が提起されてきたが，その一つは伝送中に雑音の影響によって引き起されるデータの誤りである．データが文章を表わすようなものであれば，たとえ少々誤りにおかされてもその前後の関係から訂正することが可能な場合もあるが，データが金額を表わすような数字情報であるような場合には誤りの影響は重大なものである．

一方，このような誤りの発生は独立的ではなく，バースト誤りとして集中的に発生するという特徴があることが指摘され，１９６０年にE.N.Gilbertが２状態のマルコフ連鎖を用いた通信路のモデルを提案し[1]，実際の通信路にかなり近似させうることを示した．しかし，このようなすぐれたモデルが提案されたにもかかわらず，バースト誤りを生じる通信路を対象としたシステムの解析に必要な，有限長の符号内に生じる有限長のバースト誤りの確率式は示されず，ただわずかにM.Horsteinによって有限長の符号内に全く誤りが生じない確率式が示された[2]にすぎなかった．

本論文では第２章で母関数を導入することにより確率式誘導の手順を見い出し，近似を行なうことなく集中形および分離形のバースト誤りの確率の一般式を見い出し[3],[4]．また同時にシミュレーションを行ない[5]両者の一致を確かめている．

１９４９年，C.E.Shannonは有名な離散的な通信路に関する定理[6]を与え，これを基礎として符号理論は出発したがその流れには大きく分けて二つのものがあった．その一つは“ブロック符号”と呼ばれ．符号間の拘束に重なりがないものであり，他は“畳み込み符号”と呼ばれ，符号間の拘束が

重なり合った連続的なものである.

ブロック符号については１９５０年にR.W. Hamming が１ビットの誤りを訂正できる符号を示した[7] のを発端としてそれ以後種々の誤り訂正符号が示された．１９５７年にはE.Prange が巡回符号を見い出した[8]が，これが以後の符号理論の発展に大なる寄与をしている．すなわち，その後に発表されたブロック符号の大部分は巡回符号であり，Hamming の符号も巡回符号のあるものと等価であることが示された.

ついで１９５９年にN.M. Abramson[9]およびP.Fire[10] らはバースト誤りを訂正できる符号を発表し，バースト誤り訂正符号の研究が始まった．Abramson 符号は符号長が（$2^{2i}-1$）；（$i \geq 2$）で，３ビットまでのバースト誤りを訂正できる最小冗長符号* であり，Fire 符号は任意の長さのバースト誤りを訂正できるような符号構成ができる符号であるが，冗長が有効に使われていない場合が多い.

その後より能率の良い，バースト誤りを訂正するブロック符号が嵩忠雄[11], C.M. Melas[12], S.H. Reiger[13], J.E. Meggitt[14], B.Elspas およびR.A. Short[15]らによって求められた．また１９６２年には嵩が，符号長５１１で長さ４ビットまでのバースト誤りを訂正できる最小冗長符号を示し，合わせて符号長が１０２２以下でバースト誤り訂正能力が４以上の符号の中で最小冗長符号はこれ以外には存在しないことを示した[16].

これらのブロック符号はある長さまでの誤りをすべて訂正し，かつ能率の良いものであるが符号構成の自由度は少ない．一方Fire 符号は符号構成に自由度を有するが冗長が多過ぎる．そこでこのFire 符号の欠点を除くため

---

* ある符号を構成するのに理論上必要とされる最小数の冗長によって実現される符号をいう.

に生成多項式を変形して冗長数を減少させ，その反面もとのFire符号が訂正できるバースト誤りのすべてを訂正できないが，そのほとんどすべてを訂正でき，実質的な能力には殆んど差のないような符号が１９６５年笠原正雄によって示された.[17] このようにある長さまでの誤りのすべてを訂正しないがほとんどすべてを訂正できるような符号については，下記の条件を満足する場合には実用的な面から見て望ましい符号と考えられる.

(1) 発生確率の大きい短いバースト誤りのすべてを訂正できること.

(2) 最終的に信頼度を高くすることができること（このためには条件(1)が不可欠である）.

(3) 符号化および復号装置が簡単であること.

(4) 冗長が少ないこと.

(5) 符号構成に自由度を有すること.

本論文では第3章でこのような符号，すなわち構成の自由度，冗長の有効な利用，符号生成多項式の決定の容易さおよび装置の簡単さに重点をおいた符号の一構成法[18],[19]を示す．この符号は同じ冗長数のFire符号が訂正できる誤りと同じ長さまでの誤りを完全に訂正できるだけでなく，Fire符号では訂正できない誤りについても，ほぼ冗長数の半分の長さまでの誤りのほとんどすべてを訂正でき，したがって同じ冗長数のFire符号より信頼度を高めることができる．また装置はFire符号より簡単で，冗長も比較的少なく，符号構成の自由度はFire符号にやや劣るがなおもかなりの自由度を有するので前述の条件を満足する実用的な符号の一つと考えられる.

これまでに述べたように多くのバースト誤り訂正符号が発表されてきたが，これらの符号を用いればどの程度信頼度が改善されるかという問題や，符号長が信頼度および伝送能率に与える影響および符号長と訂正能力をどのよう

に選べば目的とする信頼度を確保しつつ最も能率の良い伝送を行ないうるかという問題については殆んど解答が与えられていない．しかしこれはバースト誤り訂正符号を採用する場合に重大な問題となるので本論文では第4章においてこれに対する解答を与えている[4],[5],[20],[21]．その結果バースト誤りを訂正するブロック符号を用いて得られる信頼度は“誤り検出自動再送要求方式（ARQ方式）”の一つである“空RQ方式（Idle-RQ方式）[22],[23],[24]”にまさるが，“位置情報を有する空RQ方式[25]”や“Dual-RQ方式[22],[26]”には劣り，また最適な符号長の存在が顕著であることが明らかになった[4],[5]．

つぎに畳み込み符号は1955年P. Elias[27]によって提案され，引き続きJ.L.Massey[28]，J.P.Robinson[29]およびD.W.Hagelbarger[30]らによって研究されてきた．畳み込み符号は復号をハードウエアで実行することを目的とした冗長度の比較的小さいもの（冗長度≦1/2）と逐次復号法（Sequential Decoding）を適用することを目的とした冗長度の大きなもの（冗長度≧1/2）とに分けられる．

逐次復号法を適用する冗長度の大きな畳み込み符号は従来シフトレジスタを用いて符号化されているが，この方法によれば受信側では符号化装置のシフトレジスタの初期値を正しく知っていないと以後の復号が不可能であり，したがって一度同期くずれが生じたり，復号におけるオーバーフロー[31]が生じると正常状態に復帰し難いという欠点がある．

本論文では第5章でこれらの欠点を改善できるフィードバック・シフトレジスタを用いた符号化法を示し，その条件より最適な結線多項式を次数12まで求めている[32],[33],[34]．

第2章　通信路に生ずるバースト誤りの分布

2．1　序　　言

通信路に発生する誤りは独立的ではなく，バースト誤りとして集中的に発生することはよく知られている．独立な誤りの発生確率は簡単に数式化できるが，バースト誤りの発生確率の数式化は適当なモデルを必要とする．1960年にE.N.Gilbertはこの必要を満たすべく一つのモデルを提案した[1]．このモデルは二つの状態から成るマルコフ連鎖であり，実際の通信路にかなり近似させうることが示された．しかしながらバースト誤りを生じる通信路を対象としたシステムの解析に必要と思われる，任意の有限長の符号内に生じる任意長のバースト誤りの確率の一般式は示されず，わずかにM.Horsteinによって任意の有限長の符号内に全く誤りが生じない確率式が示された[2]にすぎなかった．

本章では母関数を導入することにより確率式誘導の手順を見い出し，近似を行なうことなくバースト誤りの確率の一般式を導いている[3],[4]．また同時にシミュレーションを行ない[5]両者の一致を確かめている．

2．2　通信路のモデル

E.N.Gilbert はバースト誤りを生じる通信路のモデルとして図2．1に示すモデルを提案した[1]．ここでPは状態G（Good State）から状態B（Bad State）への遷移確率を示す．また逆にpは状態Bから状態Gへの遷移確率を示す．なお状態Gでは誤りが発生せず，状態Bでは確率（$1-h$）；（$0 \leq h \leq 1$）で誤ったビットが現われるとする．

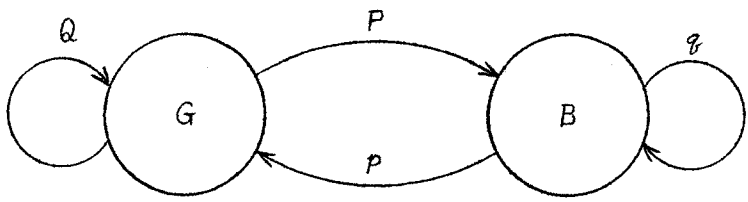


図２．１　通信路のモデル

つぎにこの通信路の平均のビット誤り率を P_b とすると，状態 G の平均長は $1/P$，状態 B の平均長は $1/p$ であり，誤りは状態 G では発生せず，状態 B で確率（１－ h ）で発生するから

$$P_b = \frac{(1-h)\dfrac{1}{p}}{\dfrac{1}{p}+\dfrac{1}{P}} = \frac{(1-h)\,P}{p+P} \tag{2.1}$$

と表わされる．またバースト誤りの平均長 $\overline{B}'$ は

$$\overline{B}' = \frac{(1-h)p}{(1-hq)^2}\left\{h + \frac{1-h}{p^2}\right\} \tag{2.2.a}$$

と表わされる（付録１参照）．ビット誤り率，バースト誤りの平均長および誤りのない部分の平均長を測定すれば h，P，p，Q および q を決定できる．なお，$h=0.5$　で $q \cong 1$ の場合にはつぎのようになる．

$$\overline{B}' \cong \frac{1}{p} - 2 \tag{2.2.b}$$

2．3　有限長の符号内に生じるバースト誤りの確率

ここで用いる記号の中で複雑と思われるものを特に表２．１に示す．

表２．１　複雑と思われる記号とその意味

（B_{-1} および G_{-1} は最初の状態の一つ前の状態がそれぞれ B および G であることを示す．）

記　　号	意　　味
$P(1)$	ある任意の状態が誤っている確率．
$P(0^{i-1}1)$	始めの（$i-1$）ステップは正しく，i ステップ目が誤っている確率．
$P(G^{i-1}B \mid B_{-1})$	始めの（$i-1$）ステップは状態 G であり，i ステップ目が状態 B である確率．
$P(0^{i} \mid B_{-1})$，$P(0^{i} \mid G_{-1})$	始めの i ステップが正しい確率．
$P\{0^{i-1}B(=0) \mid B_{-1}\}$	始めの（$i-1$）ステップは正しく，i ステップ目は状態 B であるが誤っていない確率．
$P(0^{i-1}1 \mid B_{-1})$	始めの（$i-1$）ステップは正しく，i ステップ目が誤っている確率．
$P(r^{i-1}1 \mid B_{-1})$	始めの（$i-1$）ステップはどういう状態でもよく，i ステップ目が誤っている確率．
$P\{G^{i-1}B(=0) \mid G_{-1}\}$	始めの（$i-1$）ステップは状態 G であり，i ステップ目は状態 B であるが正しい確率．
$P(G^{i-1}1 \mid G_{-1})$	始めの（$i-1$）ステップは状態 G で，i ステップ目が誤っている確率．
$P(G^{i} \mid B_{-1})$，$P(G^{i} \mid G_{-1})$	始めの i ステップが状態 G である確率．

2．3．1　誤りのない場合

最初の状態の一つ前の状態がBで，それ以後nステップで始めて再び状態Bに戻る条件付確率をf_nとすると

$$\left.\begin{aligned} f_n &= P(G^{n-1}B \mid B_{-1}) = pQ^{n-2}P \quad ; \quad n \geqq 2 \\ f_1 &= q \end{aligned}\right\} \tag{2.3}$$

と表わせ，またf_nの母関数$F(t)$はつぎのように表わされる．

$$F(t) = \sum_{n=1}^{\infty} f_n t^n = qt + \frac{pPt^2}{1-Qt} \tag{2.4}$$

つぎに，最初の状態の一つ前の状態がBで，それよりnステップ目の状態がBであり，そのn個の状態の中で全体としてm個の状態Bが現われる条件付確率を$f_n^{(m)}$とすると

$$f_n^{(m)}\text{の母関数} = \sum_{n=m}^{\infty} f_n^{(m)} t^n = [F(t)]^m \tag{2.5}$$

と表わされる[1]．また誤りを1，正しいものを0で表わし，長さnの符号内に誤りが発生しない確率を$P_n(0)$とすると

$$\begin{aligned} P_n(0)\text{の母関数} = {} & \frac{P}{p+P}\left[P(0^n \mid B_{-1})\text{の母関数}\right] \\ & + \frac{p}{p+P}\left[P(0^n \mid G_{-1})\text{の母関数}\right] \end{aligned} \tag{2.6}$$

となり，一方

$$\begin{aligned} & P(0^n \mid B_{-1})\text{の母関数} \\ & = \left[P\{0^{n-1}B(=0) \mid B_{-1}\}\text{の母関数}\right]\left[P(G^n \mid B_{-1})\text{の母関数}\right] \end{aligned} \tag{2.7}$$

と表わせる．ここで

$P\{0^{n-1}B(=0)\,|\,B_{-1}\}$ の母関数

$$=1+\sum_{n=1}^{\infty}\sum_{m=1}^{n}h^{m}f_{n}^{(m)}t^{n}=\frac{1}{1-hF(t)} \tag{2.8}$$

$P(G^{n}|B_{-1})$ の母関数

$$=1+\sum_{n=1}^{\infty}pQ^{n-1}t^{n}=\frac{1+(p-Q)t}{1-Qt} \tag{2.9}$$

となるから

$P(0^{n}|B_{-1})$ の母関数

$$=\frac{1}{1-hF(t)}\cdot\frac{1+(p-Q)t}{1-Qt}=\frac{1-Nt}{(1-Jt)(1-Lt)} \tag{2.10}$$

となる．ただし

$$\left.\begin{aligned}J&=\frac{Q+hq+\sqrt{(Q+hq)^{2}-4hN}}{2}\\L&=\frac{Q+hq-\sqrt{(Q+hq)^{2}-4hN}}{2}\\N&=Q-p\end{aligned}\right\} \tag{2.11}$$

つぎに

$P(0^{n}|G_{-1})$ の母関数 $=P(G^{n}|G_{-1})$ の母関数

$+$〔$P\{G^{n-1}B(=0)\,|\,G_{-1}\}$ の母関数〕

〔$P\{0^{n-1}B(=0)\,|\,B_{-1}\}$ の母関数〕

〔$P(G^{n}|B_{-1})$ の母関数〕 (2.12)

と表わせ，またつぎの式が成り立つ．

$P\{G^{n-1}B(=0)\,|G_{-1}\}$ の母関数

$$=h\sum_{n=1}^{\infty}Q^{n-1}Pt^{n}=\frac{hPt}{1-Qt} \tag{2.13}$$

$P(G^{n}\,|G_{-1})$ の母関数

$$=1+\sum_{n=1}^{\infty}Q^{n}t^{n}=\frac{1}{1-Qt} \tag{2.14}$$

式(2．8)，(2．9)，(2．13)および(2．14)を式(2．12)に代入すると

$$P(0^{n}\,|G_{-1})\text{の母関数}=\frac{1}{1-Qt}$$

$$+\frac{hPt}{1-Qt}\cdot\frac{1}{1-hF(t)}\cdot\frac{1+(p-Q)t}{1-Qt}$$

$$=\frac{1-hNt}{(1-Jt)(1-Lt)} \tag{2.15}$$

が得られる．式(2．10)および(2．15)を式(2．6)に代入すると

$$P_{n}(0)\text{の母関数}=\frac{p+P-N(hp+P)t}{(p+P)(1-Jt)(1-Lt)} \tag{2.16}$$

となる．したがって $P_{n}(0)$ は

$$P_{n}(0)=\frac{1}{(p+P)(J-L)}\{(p+P)(J^{n+1}-L^{n+1})$$

$$-N(hp+P)(J^{n}-L^{n})\} \tag{2.17}$$

となる．

2．3．2　単一誤りの場合

長さnの符号内で1ビットのみが誤る確率を$P_n(1)$とすると

$$P_n(1)=\sum_{k=1}^{n} P(0^{k-1}1)\ P(0^{n-k}|B_{-1})$$

と表わせ，したがって

$P_n(1)$の母関数

$$=〔P(0^{n-1}1)の母関数〕〔P(0^{n}|B_{-1})の母関数〕 \quad (2.18)$$

となる．一方

$P(0^{n-1}1)$の母関数

$$=\frac{P}{p+P}〔P(0^{n-1}1|B_{-1})の母関数〕$$

$$+\frac{p}{p+P}〔P(0^{n-1}1|G_{-1})の母関数〕 \quad (2.19)$$

となり，また

$P(0^{n-1}1|B_{-1})$の母関数

$$=\sum_{n=1}^{\infty}\sum_{m=1}^{n} f_n^{(m)}\ h^{m-1}(1-h)\ t^n$$

$$=\frac{(1-h)F(t)}{1-hF(t)}=\frac{(1-h)t(q-Nt)}{(1-Jt)(1-Lt)} \quad (2.20)$$

$P(0^{n-1}1|G_{-1})$の母関数

$$=〔P\{G^{n-1}B(=0)|G_{-1}\}の母関数〕$$

$$〔P(0^{n-1}1|B_{-1})の母関数〕$$

$$+P(G^{n-1}1|G_{-1})\text{の母関数} \tag{2.21}$$

と表わされる．一方，式(2．13)を用いると

$$P(G^{n-1}1|G_{-1})\text{の母関数}$$

$$=\left[P\{G^{n-1}B(=0)|G_{-1}\}\text{の母関数}\right]\frac{1-h}{h} \tag{2.22}$$

が得られる．したがって，式(2．13)，(2．20)および(2．22)を式(2．21)に代入するとつぎの式が得られる．

$$P(0^{n-1}1|G_{-1})\text{の母関数}=\frac{hPt}{1-Qt}\left\{\frac{(1-h)F(t)}{1-hF(t)}+\frac{1-h}{h}\right\}$$

$$=\frac{(1-h)Pt}{(1-Jt)(1-Lt)} \tag{2.23}$$

式(2．20)および(2．23)を式(2．19)に代入すると

$$P(0^{n-1}1)\text{の母関数}=\frac{(1-h)Pt(1-Nt)}{(p+P)(1-Jt)(1-Lt)} \tag{2.24}$$

さらに式(2．10)および(2．24)を式(2．18)に代入すると

$$P_n(1)\text{の母関数}=\frac{P(1-h)\,t\,(1-Nt)^2}{(p+P)(1-Jt)^2(1-Lt)^2}$$

$$=\frac{P(1-h)\,t\,(1-2Nt+N^2t^2)}{(p+P)(J-L)^3}\left\{J^2\frac{2JLt+J-3L}{(1-Jt)^2}-L^2\frac{2LJt+L-3J}{(1-Lt)^2}\right\} \tag{2.25}$$

が得られ，したがって$P_n(1)$はつぎのようになる．

$$P_n(1)=\frac{P(1-h)}{(p+P)(J-L)^3}\left[J^{n-1}(J-N)\{n(J-L)(J-N)-2J(L-N)\}\right.$$

$$-L^{n-1}(L-N)\{n(L-J)(L-N)-2L(J-N)\}\rbrack\ ;\ n \geqq 3 \qquad (2.26.a)$$

$$P_2(1) = \frac{2P(1-h)(hq+p)}{p+P} \qquad (2.26.b)$$

$$P_1(1) = \frac{(1-h)P}{p+P} \qquad (2.26.c)$$

2．3．3　長さ2以上のバースト誤りの場合

本章では，単一バースト誤り訂正巡回符号を対象とし，訂正可能な長さ c のバースト誤りをつぎのように定義する．

〔定義2．1〕長さ n の符号の前後を連結して巡回的に考え，その中で連続して誤りのない最大の部分の長さが（$n-c$）であるとき，残りの長さ c の部分を長さ c のバースト誤りとする．

符号の前後の連結点がバースト誤りの中にある場合を図2．2に示し，これを分離形バースト誤りと呼び，また連結点がバースト誤りの外にある場合を図2．3に示し，これを集中形バースト誤りと呼ぶことにする．なお，図

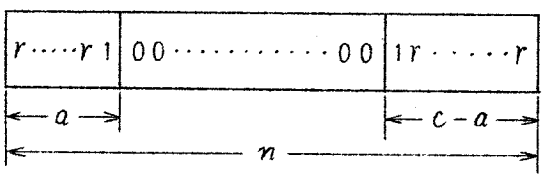


図2．2　長さ n の符号内に発生した長さ c の分離形バースト誤り．

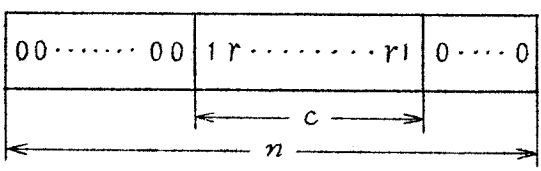


図2．3　長さ n の符号内に発生した長さ c の集中形バースト誤り．

において1は誤りを，0は誤りでないことを，rは誤っていてもいなくてもよいことをそれぞれ示している．

(I) 分離形バースト誤りの場合

分離形バースト誤りの位置は$a=1$から$a=c-1$までの$(c-1)$種類あり，それぞれの確率は明らかに等しい．この確率を$P_{ns}(c)$とすると

$$P_{ns}(c)=(c-1)P(1)P(0^{n-c}1|B_{-1}) \tag{2.27}$$

と表わせる．ここで$P(1)$はビット誤り率P_b，すなわち式(2．1)で表わされる．

式(2．20)より$P(0^{n-c}1|B_{-1})$を求め式(2．27)に代入すると

$$P_{ns}(c)=\frac{(1-h)^2(c-1)P}{(b+P)(J-L)}\{J^{n-c}(qJ-N)-L^{n-c}(qL-N)\} \tag{2.28}$$

となる．つぎに長さnの符号内に長さが2からbまでの分離形バースト誤りが発生する確率を$F_{ns}(b)$とすると，式(2．28)より

$$\begin{aligned}F_{ns}(b)&=\sum_{c=2}^{b}P_{ns}(c)\\&=\frac{(1-h)^2P}{(b+P)(J-L)}\left\{(qJ-N)J^{n-b}\frac{J^b-bJ+b-1}{(1-J)^2}\right.\\&\qquad\left.-(qL-N)L^{n-b}\frac{L^b-bL+b-1}{(1-L)^2}\right\}\end{aligned} \tag{2.29}$$

が得られる．

(II) 集中形バースト誤りの場合

長さnの符号内に長さcの集中形バースト誤りが発生する確率を$P_{nl}(c)$とすると

$$P_{nl}(c)=\sum_{k=0}^{n-c} P(0^{k}1)\,P(r^{c-2}1\,|\,B_{-1})\,P(0^{n-c-k}\,|\,B_{-1})$$

と表わせる．ただし r はさきに述べたように 0 および 1 のいずれでもよいことを示す．したがって

$$P_{nl}(c)\text{の母関数}=\left[P(0^{n-1}1)\text{の母関数}\right]$$

$$\left[P(0^{n}\,|\,B_{-1})\text{の母関数}\right]t^{c-1}P(r^{c-2}1\,|\,B_{-1}) \qquad (2.30)$$

と表わせる．ここで

$$P(r^{n-1}1\,|\,B_{-1})\text{の母関数}=\sum_{n=1}^{\infty}\sum_{m=1}^{n} f_{n}^{(m)}(1-h)\,t^{n}$$

$$=\frac{(1-h)\,t\,(q-Nt)}{(1-t)(1-Nt)}$$

となるからつぎの式が得られる．

$$P(r^{c-2}1\,|\,B_{-1})=\frac{(1-h)(P+pN^{c-1})}{1-N}$$

$$=\frac{(1-h)(P+pN^{c-1})}{p+P} \qquad (2.31)$$

式(2．10)，(2．24)および(2．31)を式(2．30) に代入すると

$$P_{nl}(c)\text{の母関数}=\frac{(1-h)^{2}Pt^{c}\,(1-Nt)^{2}\,(P+pN^{c-1})}{(p+P)^{2}\,(1-Jt)^{2}\,(1-Lt)^{2}}$$

$$=\frac{(1-h)^{2}P(P+pN^{c-1})}{(p+P)^{2}(J-L)^{3}}\,t^{c}\,(1-2Nt+N^{2}t^{2})$$

$$\left\{J^{2}\frac{2JLt+J-3L}{(1-Jt)^{2}}-L^{2}\frac{2LJt+L-3J}{(1-Lt)^{2}}\right\} \qquad (2.32)$$

が得られる．したがって

$$P_{nl}(c)=\frac{(1-h)^2(P+pN^{c-1})P}{(p+P)^2(J-L)^3}\{f_1(J,L)-f_1(L,J)\} \quad (2.33)$$

ただし

$$f_1(x,y)=x^{n-c}\left[x^2\{x(n+1)-y(n+3)\}-2xN\{xn-y(n+2)\}\right.$$

$$\left.+N^2\{x(n-1)-y(n+1)\}-c(x-y)(x-N)^2\right]$$

となる．つぎに長さnの符号内に長さ2からbまでの集中形バースト誤りが発生する確率を$F_{nl}(b)$とすると

$$F_{nl}(b)=\sum_{c=2}^{b}P_{nl}(c)$$

$$=\frac{(1-h)^2P}{(p+P)^2(J-L)^3}\{f_2(J,L)-f_2(L,J)\} \quad (2.34)$$

ただし

$$f_2(x,y)=x^{n-b}\left\langle\left[x^2\{x(n+1)-y(n+3)\}-2xN\{xn-y(n+2)\}\right.\right.$$

$$\left.+N^2\{x(n-1)-y(n+1)\}\right]\left(P\frac{1-x^{b-1}}{1-x}+pN\frac{x^{b-1}-N^{b-1}}{x-N}\right)$$

$$-(x-y)\left[P(x-N)^2\frac{2x^b-x^{b-1}-(b+1)x+b}{(1-x)^2}\right.$$

$$\left.\left.+pN\{2x^b-x^{b-1}N-(b+1)xN^{b-1}+bN^b\}\right]\right\rangle$$

となる．一方，長さnの符号内に，長さbまでの単一バースト誤りが発生する確率$F_n(b)$は

$$\left.\begin{aligned} F_n(0) &= P_n(0) \\ F_n(1) &= P_n(0) + P_n(1) \\ F_n(b) &= P_n(0) + P_n(1) + F_{ns}(b) + F_{nl}(b) \quad ; \ b \geqq 2 \end{aligned}\right\} \tag{2.35}$$

と表わせるから，式(2．17)，(2．26)，(2．29)および(2．34)を式(2．35)に代入すれば分布関数$F_n(b)$が得られる．

上で導いた式はすべて$0 \leqq b$，$c \leqq \left[\frac{n+1}{2}\right]$の範囲で成り立つ．ここで記号〔　〕はガウスの記号である．

2．4　シミュレーション

バースト誤りを生ずる通信路のモデルとして．2．2で示したGilbertのモデルを考えると，状態Gが長さtだけ続く確率$P_G(t)$は

$$P_G(t) = \begin{cases} PQ^{t-1} & ; \ t \geqq 1 \\ 0 & ; \ t \leqq 0 \end{cases} \tag{2.36}$$

となり，また状態Bがtだけ続く確率$P_B(t)$は

$$P_B(t) = \begin{cases} pq^{t-1} & ; \ t \geqq 1 \\ 0 & ; \ t \leqq 0 \end{cases} \tag{2.37}$$

となる．つぎに

$$Q = e^{-\lambda} \tag{2.38}$$

$$q = e^{-\lambda'} \tag{2.39}$$

とおくと，式(2．36)および(2．37)はそれぞれ

$$P_G(t) = (1 - e^{-\lambda}) e^{-\lambda(t-1)} \tag{2.40}$$

$$P_B(t) = (1 - e^{-\lambda'}) e^{-\lambda'(t-1)} \tag{2.41}$$

となる.

つぎに一般に連続な確率密度関数 $f(t)$ に従う乱数を S, (0, 1) の一様乱数を r とすると

$$r = \int_S^\infty f(t)\,dt \tag{2.42}$$

なる関係が成り立つことが知られている. ここで離散的な確率密度関数, 式 (2.40) に従う乱数 S を考えると, この乱数 S は (0, 1) の一様乱数 r の一部 r' と1対1の対応がつけられる. すなわち r' を

$$e^{-\lambda S} < r \leqq e^{-\lambda(S-1)} \tag{2.43}$$

なる範囲の r とすると

$$r' = \sum_{t=S}^{\infty} (1 - e^{-\lambda}) e^{-\lambda(t-1)}$$

$$= e^{-\lambda(S-1)} \tag{2.44}$$

なる対応づけができ, この式を変形すると

$$S = 1 - \frac{log_e r'}{\lambda}$$

が得られる. また式 (2.43) を変形すると

$$S \leqq 1 - \frac{log_e r}{\lambda} < S + 1$$

となり, これより

$$-\frac{log_e r}{\lambda} < S \leqq 1 - \frac{log_e r}{\lambda} \tag{2.45}$$

が得られるから, 幾何分布に従う乱数 S は (0, 1) の一様乱数 r より { 1

$-(\log_e r)/\lambda\}$を求め，その小数点以下を切り捨てればよいことになる．ガウスの記号〔　〕を用いると式(2.45)は

$$S = \left[1 - \frac{\log_e r}{\lambda}\right] \tag{2.46}$$

となり，同様に式(2.41)に従う乱数をS'とすると

$$S' = \left[1 - \frac{\log_e r}{\lambda'}\right] \tag{2.47}$$

となる．なおこの幾何乱数Sと(0, 1)の一様乱数rとの$\lambda = 1$の場合の対応を図2.4に示す．

本論文では(0, 1)の一様乱数として，NEAC-2206のライブラリー・ルーチンの中の乗算型合同式法を用いた．これは$x_{n+1} = k x_n \pmod{M}$で乱数列x_0, x_1, x_2, ……をつくるもので，$k = 23$, $M = 10^8 + 1$で8桁の乱数が得られ，周期は5882352である．

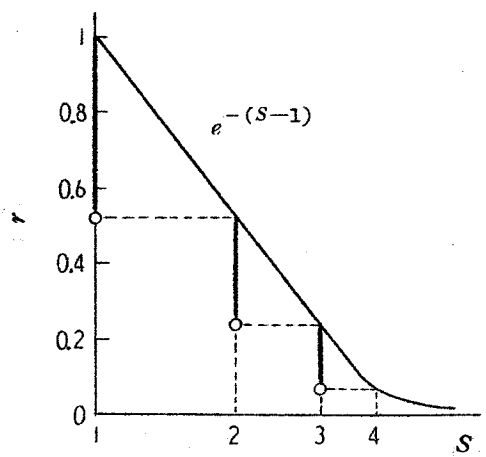


図2.4　一様乱数rと幾何乱数Sとの対応

幾何乱数を発生させる場合，式(2.46)および(2.47)からわかるように，SおよびS'ともに$(-\log_e r)$を共通に用いて発生させられる．したがって$(-\log_e r)$をあらかじめ磁気テープに記録し，この$(-\log_e r)$の値から式(2.46)および(2.47)に従って状態GおよびBの長さを得る．状態Bにおいて

は確率0.5で各ビットは誤っていると考え* ると，バースト誤りの長さは実際には状態Bの長さより短くなる場合がある．ここで状態GおよびBの長さをそれぞれG_L およびB_L で表わし，誤りの生じていない区間の長さをG'_L，バースト誤りの長さをB'_L で表わすことにする．

シミュレーションにおいてG_L およびB_L よりG'_L およびB'_L を求めるにはつぎのようにする．すなわち，B_L の両端の誤りのない部分を求めるために2進乱数の0の連を二つ求め，それぞれの長さをE_{L1} およびE_{L2} とし，$B_L > E_{L1} + E_{L2}$ の場合にはE_{L1} を前のG_L に加えてG'_L とし，またE_{L2} は後のG_L に加える．この模様を図2．5に示す．

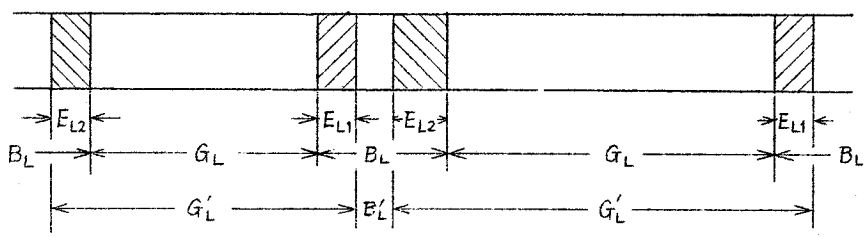


図2．5　$B_L > E_{L1} + E_{L2}$ の場合

また$B_L \leqq E_{L1}$ のときはB_L とその前後のG_L を加えたものを新らしくG_L とし同様の手順を繰り返す．この模様を図2．6に示す．

つぎに$B_L > E_{L1}$ で$B_L \leqq E_{L1} + E_{L2} + 1$の場合は$E_{L1}$ を前のG_L に加えてG'_L とし，B_L の後の（$B_L - E_{L1} - 1$）の部分を後のG_L に加えてG'_L とする．この模様を図2．7に示す．このようにして得られたG'_L およびB'_L を交互に磁気テープに記録する．

＊通常符号は0と1とをほぼ等しい割合で含んでいると考えられるのでバースト誤りにおかされた後は各ビットはほぼ確率0.5で誤っていると考えてよい．

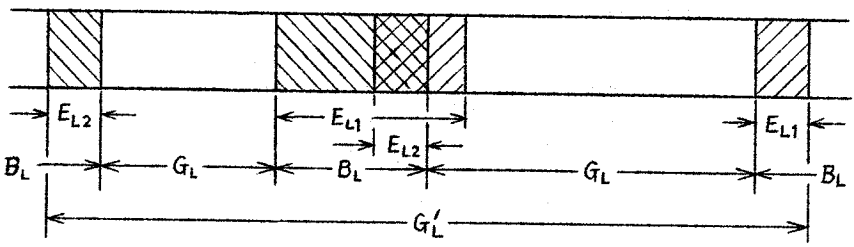


図２．６　$B_L \leqq E_{L1}$ の場合

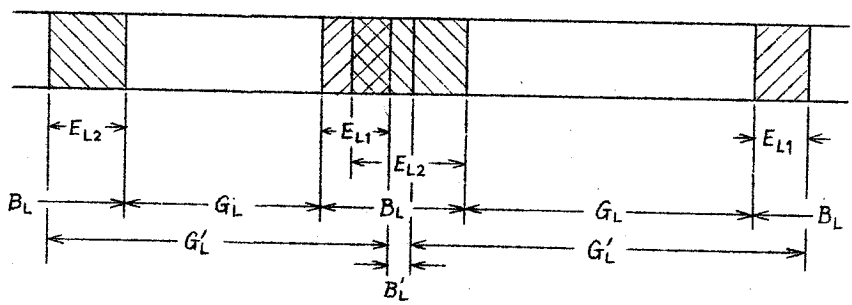
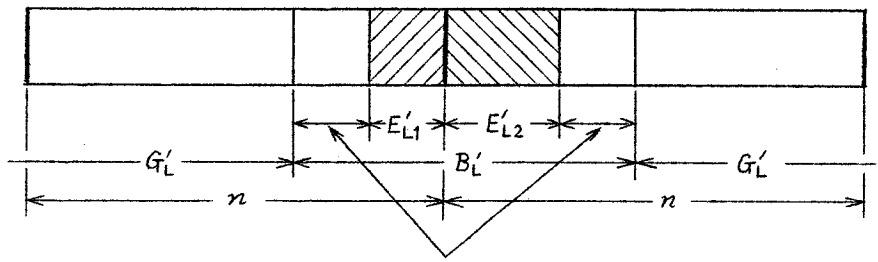


図２．７　$B_L > E_{L1}$ かつ $B_L \leqq E_{L1} + E_{L2} + 1$ の場合

シミュレーションの実行に際しては磁気テープに交互にならべて記録された G'_L および B'_L を読み出し，それを端から符号長 n で区切っていって訂正能力を越えた誤りにおかされた符号語の割合を求めるわけであるが，バースト誤りの途中，すなわち B'_L の中で符号の区切りがついた場合は，B'_L の両端は誤り，すなわち１で，他は０と１とがランダムに現われていると考えられるので，その区切りでは０の連が存在し，実際には誤りの長さが短くなっている可能性がある．したがって，それらの０の連の長さ E_{L1}' および E_{L2}' をあらかじめ他の磁気テープに記録しておき，B'_L で符号の区切りがつく毎にそれを利用することにした．この模様を図２．８に示す．



実際のバースト誤り長

図２．８　バースト誤りの中で符号の区切りがついた場合

２．５　数　値　例

ここでは２．３で導いたバースト誤りの分布関数の計算値とシミュレーションによる値を示す．なおビット誤り率P_b を10^{-2} および10^{-4} とし，状態Bの平均長$\bar{B}$を２０としている*．これらの結果を図２．９および図２．１０に示す．なお符号には０と１とが等しく用いられたと仮定し$h=0.5$ とした．

これらの結果からわかるように，計算値とシミュレーションの結果とがきわめて類似した結果を示し，また分布関数値は符号長の半分程度のバースト誤りのところで飽和に近づいていることが明らかになった．したがって誤り訂正符号には符号長の半分以上の長さの訂正能力をもたせる必要はないと考えられる．

＊　バースト誤りの平均長に換算するとほぼ１８となる．

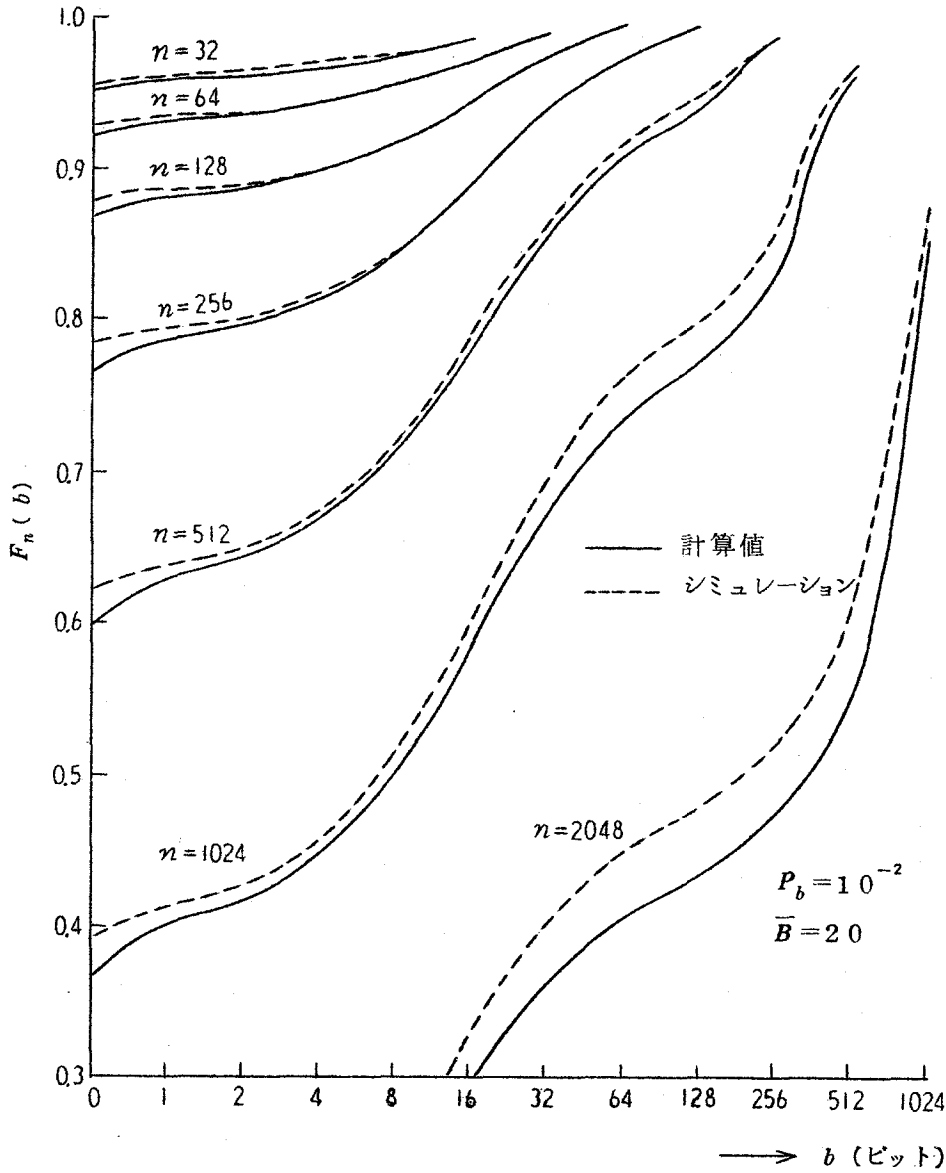


図２．９　単一バースト誤りの分布関数値

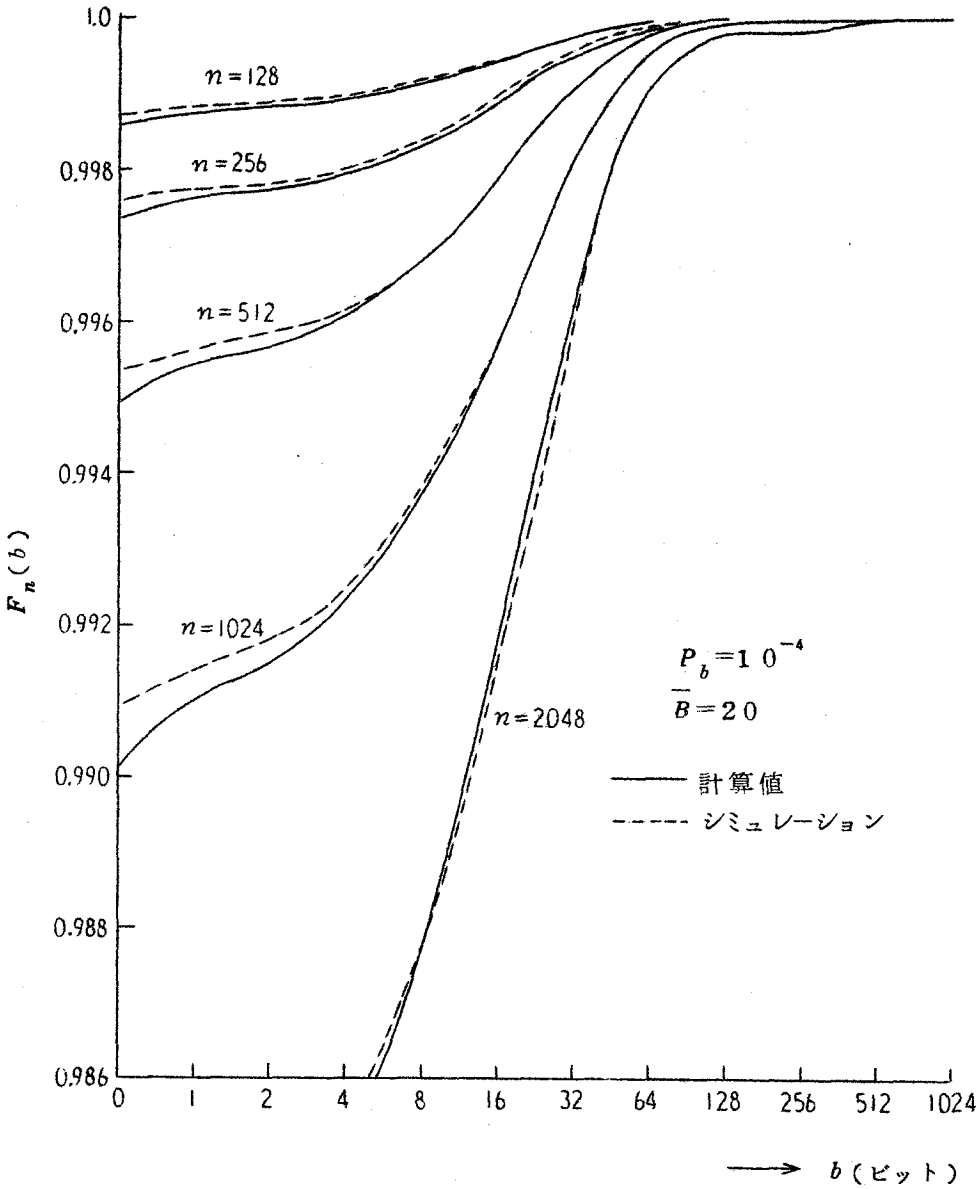


図２・１０　単一バースト誤りの分布関数値

2・6 結　　言

本章ではバースト誤りを生じる通信路のモデルとしてE.N.Gilbertの提案による2状態のマルコフ連鎖を用いたモデル[1]を採用し，任意長の符号内に生じるバースト誤りの確率密度関数および分布関数を導き，また合わせてシミュレーションを行なっている．その結果両者は密接に一致し，両者の妥当性が明らかになった．これらの確率の一般式はバースト誤りを生じる通信路を対象としたシステムの解析に有用であり，本論文では第3章および第4章で利用している．

第3章　バースト誤りを訂正するブロック符号の一構成法

3．1　序　　言

符号長がnビットで，長さbビットまでの単一バースト誤りを訂正できる巡回符号の冗長ビット数をgとすると，gはつぎの条件

$$g \geqq 2b \qquad (3.1)^{(16)}$$

$$2^g \geqq n\,2^{b-1} + 1 \qquad (3.2)^{(9)}$$

を同時に満足しなければならないことが知られている．この二つの条件を同時に満足する最小の冗長数gによって実現される符号を最小冗長符号とよぶが，最小冗長符号は冗長が最も有効に用いられているのですぐれた符号でありその発見が望まれた．１９６０年，N.M.Abramson は訂正能力$b=3$で符号長$n=2^{2i}-1$；（$i \geqq 2$）なる最小冗長符号を見いだし[9]，また１９６２年には高氏が訂正能力$b=4$で符号長$n=511$なる最小冗長符号を見いだし，同時に$b \geqq 4$，$n \leqq 1022$の範囲ではこれ以外には最小冗長符号が存在しないことを示した[16]．したがって最小冗長符号はすぐれた符号であるが，その構成における自由度がきわめて低いことがわかる．

一方，１９５９年Fire によって示された符号[10]は現在知られている符号の中で，最も自由に符号の構成を行なうことが可能（任意の訂正能力をもつ符号を構成できる．ただし，同時に冗長数および符号長に条件を課すことは困難である）で，また符号化および復号装置も簡単である．しかしFire符号は一般には符号長をかなり短縮して用いられることが多く（ある訂正能力を有するFire 符号を構成すると，その自然長が実用的な符号長より長くなることが多い），また長さbビットまでのバースト誤りを訂正するために

は，少なくともつねに（3 b－1）ビット以上の冗長を必要とする[10] ので先の式（3．2）より見て冗長が有効に利用されていないといえる．

また冗長が比較的少なく，かつ自由度の高い符号として，多重バースト誤りも訂正できるReed-Solomon 符号[35] があるが，この符号は装置が複雑で，単一バースト誤りのみを訂正することを目的とする場合は実用性では不利と思われる．

他方，先に述べたFire 符号の冗長が多過ぎるという欠点を除くために，Fire 符号の生成多項式を変形して冗長数を減らし，その反面もとのFire 符号が訂正できるバースト誤りのすべてを訂正できないが，そのほとんどすべてを訂正できるような符号も研究されている.[17] このような符号については，下記の条件を満足する場合には実用的な面から見て望ましい符号と考えられる．

(i) 発生確率の大きい短いバースト誤りをすべて訂正できること．

(ii) 最終的に信頼度を高くすることができること（このためには条件(i)が不可欠である）．

(iii) 符号化および復号装置が簡単であること．

(iv) 冗長が少ないこと．

(v) 符号構成に自由度を有すること．

文献（17）のFire符号を変形した符号は上記の条件をかなり満足し有効な符号といえるが，同じ冗長数のFire 符号が訂正できる長さまでの誤りのすべてを完全には訂正できず，効果的に用いるためには符号長 n および訂正能力 b なるパラメータをそれぞれ $n \geqq 1000$ および $b \geqq 100$ 程度に選ぶ必要があると思われる．

本論文では構成の自由度，冗長の有効な利用，符号生成多項式の決定の容

易さおよび装置の簡単さに重点をおいた符号の一構成法を示す．この符号は同じ冗長数のFire符号が訂正できる誤りと同じ長さまでの誤りを完全に訂正できるだけではなく，Fire符号では訂正できない誤りについても，ほぼ冗長数の半分の長さまでの誤りのほとんどすべてを訂正できる．例えば冗長数52ビットのFire符号で訂正できる誤りの長さは17ビットであるが，本符号では長さ22ビットの誤りまで完全に訂正可能で，長さ23ビットの誤りについては99.8％以上のものを訂正できる．したがって符号のパラメータ n および b が小さい場合でも有効であり，同じ冗長数のFire符号より信頼度を高めることができる．また装置はFire符号より簡単で，冗長も比較的少なく，符号構成の自由度はFire符号よりやや劣るがなおもかなりの自由度を有するので前述の条件を満足する実用的な符号の一つと考えられる．

3．2　符号構成法

符号の生成多項式 $G(X)$ として，ガロア体 $GF(2)$ の上でつぎのものを考える．

$$G(X)=(X^{c}+1)(X^{c'}+1) \tag{3.3}$$

ただし c および c' は素数で，c' は c より大で c に最も近い素数．

この符号の符号化回路としては従来用いられているものと同様のものを用いればよく，それを図3．1に示す．すなわち情報符号に $X^{c+c'}$ を乗じた後 $G(X)$ で割り，その剰余を情報符号の後につけて送り出す．図3．1からわかるようにきわめて簡単な回路となる．

この符号は後に示すように，符号長 n は最大 $n=cc'$ までとることができ，冗長ビット数 g は $g=c+c'$ である．また訂正能力は，〔$(c+c')/3$〕

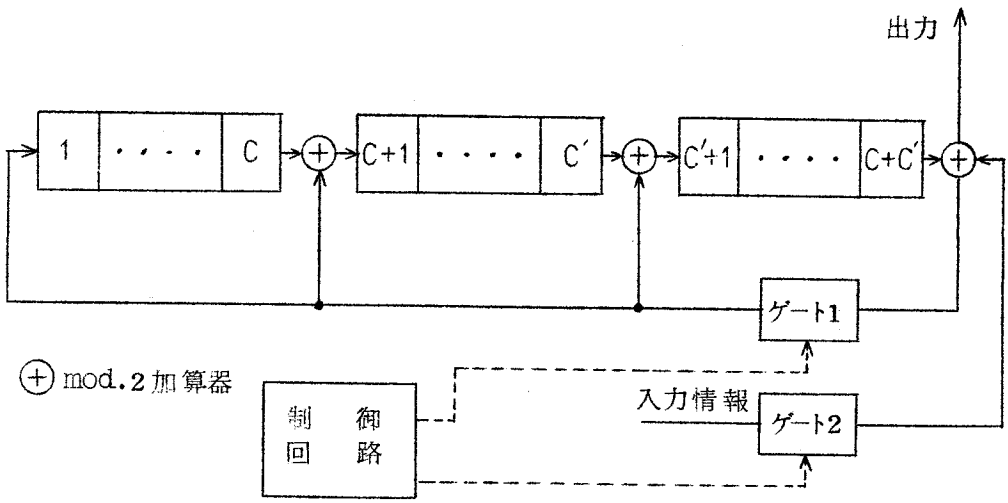


図３．１　符号化回路

（ただし〔　〕はガウス記号）までのバースト誤りをすべて訂正でき，

〔（$c+c'$）／3〕＋1 ≦ b ≦ c　なる長さのバースト誤りのすべてまたはほとんどすべてを訂正できる．

つぎに復号回路を図３．２に示す．復号側では（X^c+1）および（$X^{c'}+1$）なる二つの多項式に相当するフィードバック・シフトレジスタ（以後 $F.S.R.$ と略記する．）をシフトすることにより，誤りのパターンと位置を見い出して訂正する．以後（X^c+1）に対応する $F.S.R.$ を $F.S.R.$ Ⅰ，また（$X^{c'}+1$）に対応する $F.S.R.$ を $F.S.R.$ Ⅱと呼ぶことにする．

３．３　符号長および訂正能力

巡回符号の周期の定義によれば，ある多項式 $f(X)$ に対して $X^e-1 \equiv 0 \pmod{f(X)}$ を満足する最小の e が $f(X)$ の周期である[36]．また $f(X)$ が

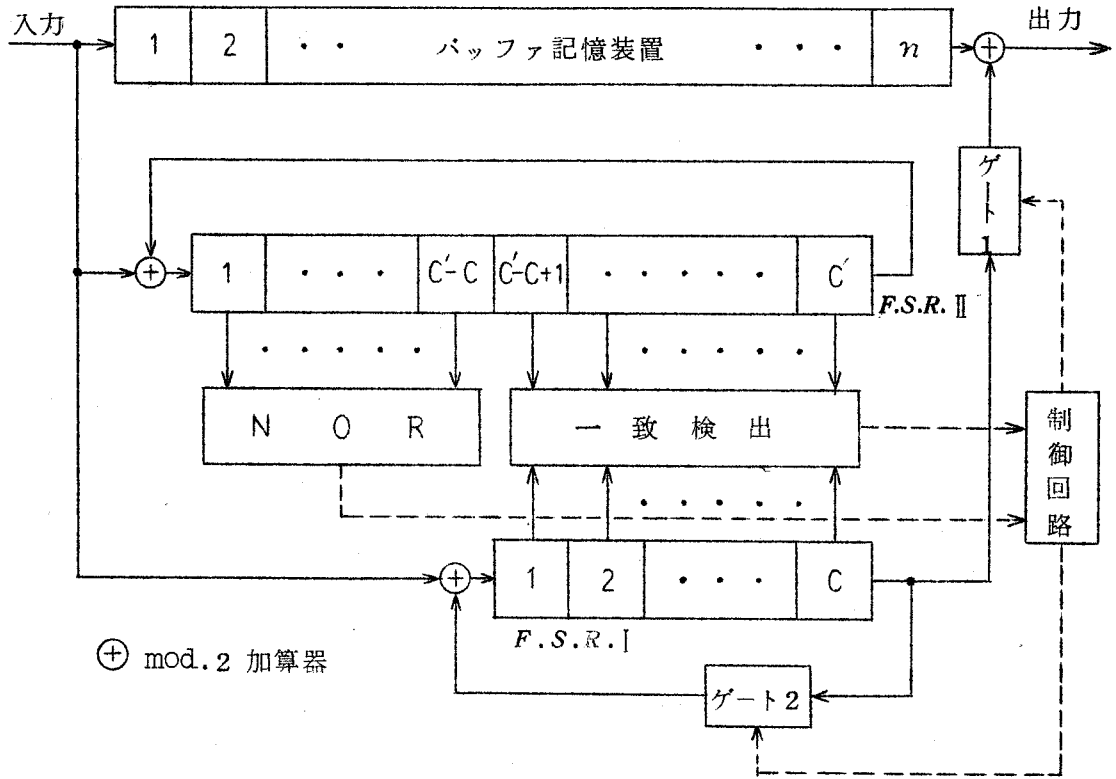

入力
1
2
・・
バッファ記憶装置
・・・
n
出力
ゲート1
1
・・・
C'-C
C'-C+1
・・・・・
C'
F.S.R. Ⅱ
N O R
一致検出
制御回路
1
2
・・・
C
F.S.R. Ⅰ
⊕ mod.2 加算器
ゲート2

図3．2　復　号　回　路

$$f(X)=\left[f_1(X)\right]^{\alpha_1}\cdots\left[f_i(X)\right]^{\alpha_i}\cdots\left[f_v(X)\right]^{\alpha_v}\quad;\ \alpha_i\geqq 1 \tag{3.4}$$

と素因子分解され，$f_i(X)$ の周期を e_i とし，γ_i を

$$2^{\gamma_i-1}<\alpha_i\leqq 2^{\gamma_i} \tag{3.5}$$

を満足する整数とすると，$\left[f_i(X)\right]^{\alpha_i}$ の周期は $2^{\gamma_i}e_i$ となる．また $f(X)$ の周期は $2^{\gamma_i}e_i$ $(1\leqq i\leqq v)$ の最小公倍数

$$e=LCM(2^{\gamma_1}e_1,\ 2^{\gamma_2}e_2,\cdots\cdots,2^{\gamma_v}e_v) \tag{3.6}$$

となる[16],[37]．

つぎに本符号の周期を上の手順により求めるため，$G(X)$ をつぎのように分解する．

$$G(X)=(X+1)^2(X^{c-1}+X^{c-2}+\cdots\cdots+X+1)(X^{c'-1}+X^{c'-2}+\cdots\cdots+X+1) \tag{3.7}$$

式(3.7)において $(X+1)$ は既約多項式であるが他の二つの項は既約多項式とは限らない．しかしこれら二つの多項式の周期は明らかにそれぞれ c および c' なる素数であるので，つぎのように素因子分解される．

$$\left.\begin{aligned}
&X^{c-1}+\cdots\cdots+X+1=g_1(X)\cdots\cdots g_i(X)\cdots\cdots g_t(X)\\
&X^{c'-1}+\cdots\cdots+X+1=h_1(X)\cdots\cdots h_i(X)\cdots\cdots h_u(X)\\
&g_i(X)\neq g_j(X)\quad;\ i\neq j,\ 1\leqq i,\ j\leqq t\\
&h_i(X)\neq h_j(X)\quad;\ i\neq j,\ 1\leqq i,\ j\leqq u
\end{aligned}\right\} \tag{3.8}$$

ここで $(X^{c-1}+\cdots\cdots+X+1)$ および $(X^{c'-1}+\cdots\cdots+X+1)$ の周期がそれぞれ c および c' なる素数であることおよび式(3・6)より，$g_i(X)$；$(i=1,\cdots\cdots,t)$ の周期は c であり，$h_i(X)$；$(i=1,\cdots\cdots,u)$ の周期は c' となる．一方 $(X+1)^2$ の周期は2であるから，結局 $G(X)$ の周期は $LCM(2,c,c')=2cc'$ となる．

しかし，$(X+1)$ を因数にもつような $(c-1)$ 次以下の多項式 $B(X)$ と $G(X)$ との最大公約多項式による $G(X)$ の商 $G'(X)$，すなわち

$$G'(X)=\frac{G(X)}{GCM(G(X),B(X))}=\frac{(X+1)(X^{c-1}+\cdots+X+1)(X^{c'-1}+\cdots+X+1)}{GCM\left(G(X),\dfrac{B(X)}{X+1}\right)} \tag{3.9}$$

の周期は明らかに cc' となる．したがって本符号の符号長は cc' までとしなければ，短いバースト誤りでも，$(X+1)$ を因数にもつようなバースト誤りは訂正不能となる．また $B(X)=X^{c-1}+\cdots+X+1$ とすれば

$$G'(X)=(X+1)^2(X^{c'-1}+\cdots+X+1)$$

となり，この周期は $2c'$ であるからこのパターンの誤りは訂正不能である．したがって本符号は，符号長 n を $n=cc'$ までとれ，$(c-1)$ 次以下で $B(X)=X^{c-1}+\cdots+X+1$ なるパターン以外のバースト誤りを訂正できる可能性があるということになる．また符号長 n の満足すべき条件が $n\leqq cc'<2cc'$ であるので本符号は擬巡回符号である．

つぎに，送信符号に $X^iB(X)$ なるバースト誤りが付加され，それを (X^c+1) および $(X^{c'}+1)$ で割った場合の商をそれぞれ $Q_i(X)$ および $Q_i'(X)$，剰余を $R_i(X)$ および $R_i'(X)$ とすると

$$X^iB(X)=Q_i(X)(X^c+1)+R_i(X)=Q_i'(X)(X^{c'}+1)+R_i'(X) \tag{3.10}$$

が成り立つ．つぎにこの余りをそれぞれの $F.S.R.$ の中で何回巡回シフトすればバースト誤りのパターン $B(X)$ が得られるかを見るために

$$X^{i+u}B(X)=Q(X)(X^{c}+1)+B(X)=Q'(X)(X^{c'}+1)+B(X) \quad (3.11)$$

を満足する最小の u を求める．いま，式（3.11）が成り立つためには式（3.10）より，$i+u=ct=c't'$ を満足する整数 t および t' が存在しなければならない．これを満足する最小の t および t' は，c および c' が素数であり，したがって互に素となるので $t=c'$，$t'=c$ となる．よって

$$\left.\begin{aligned} &X^{cc'}B(X)\equiv B(X)\ ;\ \mathrm{mod.}\,(X^{c}-1),\ \mathrm{mod.}\,(X^{c'}-1)\\ &u=cc'-i \end{aligned}\right\} \quad (3.12)$$

が得られるので，$X^{i}B(X)$ を二つの多項式で割った場合の剰余を（$cc'-i$）回巡回シフトすれば，$F.S.R.$ Ⅰ および $F.S.R.$ Ⅱ の内容は $B(X)$ となって一致し，誤りのパターンと位置を決定できる．本符号は擬巡回符号であるが，このことから $n=cc'$ の場合には，符号の両端にまたがって生じた分離形バースト誤り* も訂正可能である．

しかしながら二つの $F.S.R.$ の内容が，（$cc'-i$）回の巡回シフトの間に $B(X)$ 以外のもので一致するようなことはないという保証はない．仮に実際に生じた誤り $X^{i}B(X)$ を二つの $F.S.R.$ で除算した後さらに s 回巡回シフトして $B'(X)$ なる $B(X)$ とは異なる他の（$c-1$）次以下の多項式となって一致すれば，すなわち

$$\left.\begin{aligned} &X^{S+i}B(X)\equiv X^{cc'}B'(X)\equiv B'(X)\ ;\ \mathrm{mod.}\,(X^{c}-1),\ \mathrm{mod.}\,(X^{c'}-1)\\ &s<cc'-i \end{aligned}\right\} \quad (3.13)$$

---

* 2.3.3 を参照

となるような（$c-1$）次以下の多項式$B'(X)$が存在するとすれば，$X^{i}B(X)$なる誤りを$X^{cc'-s}B'(X)$と見なして“誤った訂正”を行なう場合がある．したがって，このような結果を引き起すパターンの割合が問題となる．

上に述べたことを換言すれば，“ある長さcビット以下のパターンの誤りを二つの$F.S.R.$の低次側につめて挿入し，それをcc'回シフトすると，二つの$F.S.R.$の内容は初めて同時に最初のパターンに戻る．しかしそのcc'回の巡回シフトの間で，両者の内容が最初のパターン以外のパターンとなって一致する場合には，誤った訂正を行なう可能性がある.”ということになる．以下でそのようなパターンの数の上限を決定する．

いま1，すなわち誤っているビットの数がlで，長さがb（$\geqq l$）の誤りのパターンを考え，その誤っているビットの位置を低次より順にi_0，i_1，……，i_{l-1}（$i_0=1$，$i_{l-1}=b$）とする．図3．3に示すようにこれを二つの$F.S.R.$の低次側につめて挿入し，つぎに図3．4に示すように$F.S.R.$Ⅰを（$c-i_j+1$）回，また$F.S.R.$Ⅱを（$c'-i_k+1$）回（$1<i_j$，$i_k<b$）巡回シフトした場合に，両者の内容が一致すると仮定する（ただし，$b\leqq$（（c

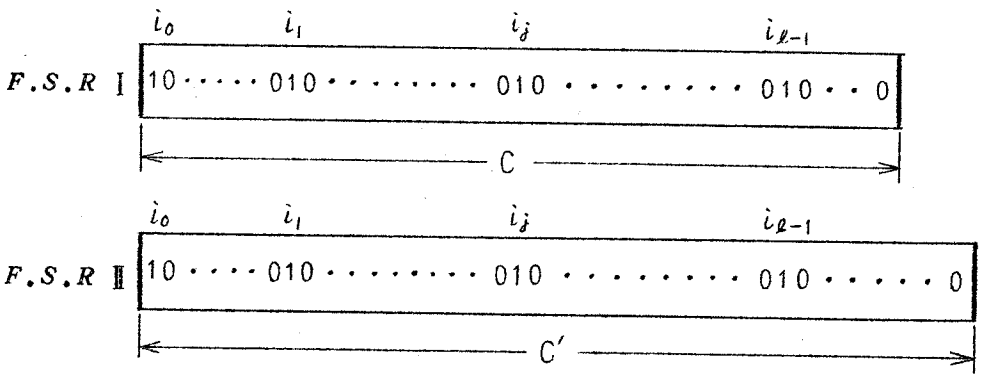


図3．3　巡回シフト前の$F.S.R.$の内容

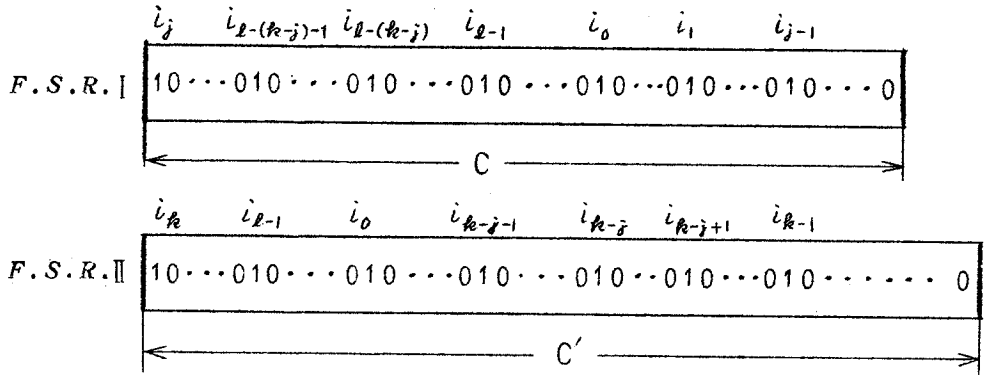


図３．４　巡回シフト後の $F.S.R.$ の内容

$+c')/3$〕の場合には両者の内容が一致することはない（付録２参照）．したがって，このような誤りはさきに述べたように訂正可能である）．

いま $k>j$ と仮定すると，図３．４に示す二つの $F.S.R.$ の内容が一致することから，二つの $F.S.R.$ の中の相隣り合う１の間隔に注目するとつぎの式が成り立つ．

$$i_a - i_{a-1} = i_{a+(k-j)} - i_{a+(k-j)-1} \quad ; 1 \leqq a \leqq l-1 \ 〔 a \not\equiv l-(k-j), \ j \bmod. l 〕 \tag{3.14.a}$$

$$i_{l-(k-j)} - i_{l-(k-j)-1} = i_0 - i_{l-1} + c' \tag{3.14.b}$$

$$i_0 - i_{l-1} + c = i_{k-j} - i_{k-j-1} \tag{3.14.c}$$

$$i_j - i_{j-1} = i_k - i_{k-1} + c - c' \tag{3.14.d}$$

ただし添字は $\bmod. l$ をとる．

式（３．１４）は一つ以上のいくつかの閉じた式の組み合わせに分けられる．

ここで式（3．14．b）および（3．14．c）は明らかに同じ組み合わせの中に入るが，前者の値は $i_0 - i_{l-1} + c' = 1 - b + c'$ であり，後者の値は $i_0 - i_{l-1} + c = 1 - b + c$ となって異なっている．したがってこの組み合わせの中には，途中でその値を変える項，すなわち式（3．14．d）が含まれなければならず，また式（3．14．c）を含む閉じた式の組み合わせの中の左辺第一項の添字は 0，$k-j$，$2(k-j)$，……，$l-(k-j)$ (mod. l) なる数列で示すことができる．したがって式（3．14．d）の左辺第一項の添字 j はこの中に含まれるので

$$j = q(k-j) - pl \tag{3.15}$$

となるような正整数 q および p が存在しなければならない．また同様にして

$$k = r(j-k) - sl \tag{3.16}$$

を満足する正整数 r および s が存在しなければならない．またこれらの閉じた式の組み合わせの中に含まれる式の個数を d とすると，d はさきの数列の項数に等しいので $d'(k-j) = fl$ を満足するような最小の正整数 d' に等しい．したがって

$$d(k-j) = fl = LCM(k-j,\ l)$$

となり，これより

$$d = \frac{LCM(k-j,\ l)}{k-j} = \frac{l}{GCD(k-j,\ l)} \tag{3.17}$$

となる．したがって式（3．14）の中の閉じた式の組み合わせの数を e とすると $e = l/d$ となり，各々 d 個の式を含む．この e 個の組み合わせの中の一つは，長さ $(c+1-b)$ の $(i_0 - i_{l-1} + c)$ および $(i_{a(k-j)} - i_{a(k-j)-1};\ a = 1, 2, \quad , q-1)$* の q 個，長さ $(c'+1-b)$ の $(i_{a\{l-(k-j)\}} -$

---

* ただし添字は mod. ℓ をとる．

$i_{a\{i-(k-j)\}-1}$; $a=1,\ 2,\cdots\cdots,\ r$) の r 個を含む式および式（3．14．d）の合計（$q+r+1$）個の式から成り，各々の閉じた式の組み合わせの中に含まれる式の個数は d であるからつぎの式が成り立つ．

$$q+r+1=d \tag{3.18}$$

一方，残りの（$e-1$）個の組み合わせの中における００……０１の連の長さを m_j（$\geqq 1$; $j=1,\ 2,\cdots\cdots,\ e-1$）とすると，すべての００……０１の連の和に第１ビットの１を加えたものの長さが誤りの長さ b に等しいのでつぎの式が成り立つ．

$$d\sum_{j=1}^{e-1} m_j + r(c'+1-b) + q(c+1-b) + 1 = b \tag{3.19}$$

式（3．18）および（3．19）より

$$b=\sum_{j=1}^{e-1} m_j + c' + 1 - \frac{q(c'-c)+c'}{d} \tag{3.20}$$

が得られる．上式を変形すると

$$b-c'-1+\frac{q(c'-c)+c'}{d}=\sum_{j=1}^{e-1} m_j \tag{3.21}$$

となるが，m_j は００……０１の連の長さであるので $m_j \geqq 1$（$j=1,\ 2,\cdots\cdots,\ e-1$）であるから

$$\sum_{j=1}^{e-1} m_j \geqq e-1$$

でなければならず，したがって

$$b-c'-1+\frac{q(c'-c)+c'}{d} \geqq e-1 \tag{3.22}$$

なる条件が満足されなければならない．ここで

$$x = b - c' - 1 + \frac{q(c'-c)+c'}{d} \tag{3.23}$$

とおくと，x を（$e-1$）個の m_j に少なくとも一つ配分する方法の数は ${}_{x-1}C_{e-2}$ となる[37]．したがってこの場合には，長さ b の訂正不能のパターンの数は ${}_{x-1}C_{e-2}$ となる．

つぎに $j = k$（$\neq 0$）のときは明らかに二つの $F.S.R.$ の内容が一致することはない．また，$j > k$ の場合も $k > j$ の場合と同様にすればよく，結局 $j > k$，$j < k$ にかかわらず

$$\left.\begin{aligned} j &= q(k-j) - p'l \\ k &= r(j-k) - s'l \end{aligned}\right\} \quad ; q,\ r \geqq 1 \tag{3.24}$$

と表わせる．ただし p' および s' は正または負の整数である．

つぎに式（3.20）で得られるバースト誤りの長さ b は整数でなければならないから，$\{q(c'-c)+c'\}$ は d の整数倍にならなければならない．また $\{q(c'-c)+c'\}$ は奇数であるので，d は奇数でなければならない．

つぎに

$$a = GCD(k-j,\ l)$$

とおくと式（3.17）より

$$l = ad \tag{3.25}$$

$$k - j = az \tag{3.26}$$

となるような，d と互に素な整数 z が存在する．また

$$-l + 2 \leqq k - j \leqq l - 2 \tag{3.27}$$

なる不等式が成り立ち，式（3.25），（3.26）および（3.27）より

$$-ad + 2 \leqq az \leqq ad - 2$$

が得られ，これより

$$-d+\frac{2}{a} \leqq z \leqq d-\frac{2}{a} \tag{3.28}$$

が得られる．式（3．28）より

$$-d+2 \leqq z \leqq d-2 \quad ; a=1 \tag{3.29.a}$$

$$-d+1 \leqq z \leqq d-1 \quad ; a \geqq 2 \tag{3.29.b}$$

が得られ，$z=0$，すなわち $k=j$ の場合はさきに述べたように考慮しなくともよく，また d と z が互に素であるので，z は a の値にかかわらず最大（$2d-2$）個の値を取り得る．しかし

$$k-j=m \quad ; \quad 1 \leqq m \leqq l-1$$

とすれば

$$m \equiv m-l \ ; \text{mod. } l$$

$$1-l \leqq m-l \leqq -1$$

となるので，上の（$2d-2$）個の z の中には同じものが半分含まれて重複しているので，結局最大 $(2d-2)/2=d-1$ 個の $(k-j)$ の値が可能である．したがって長さ b のバースト誤りで，誤りの位置が（$i_0, \cdots, i_{l-1}$）なるパターンで代表されるものについては，それ自身を含めて最大（$d-1$）個のパターンの誤りが互に識別不能，したがって訂正不能となる．またこれらの互に識別不能なパターンの長さは式（3．14）より

$$i_j - i_{j-1} = c-b+1$$

であるから b となり，すべて等しい．

以上の制限条件にもとづいて計算した訂正不能のパターンの割合，すなわち上限値の，長さ b のバースト誤りのパターンの総数 2^{b-2} に対する割合を $P_u(b)$ とし，これを図3．5に示す．

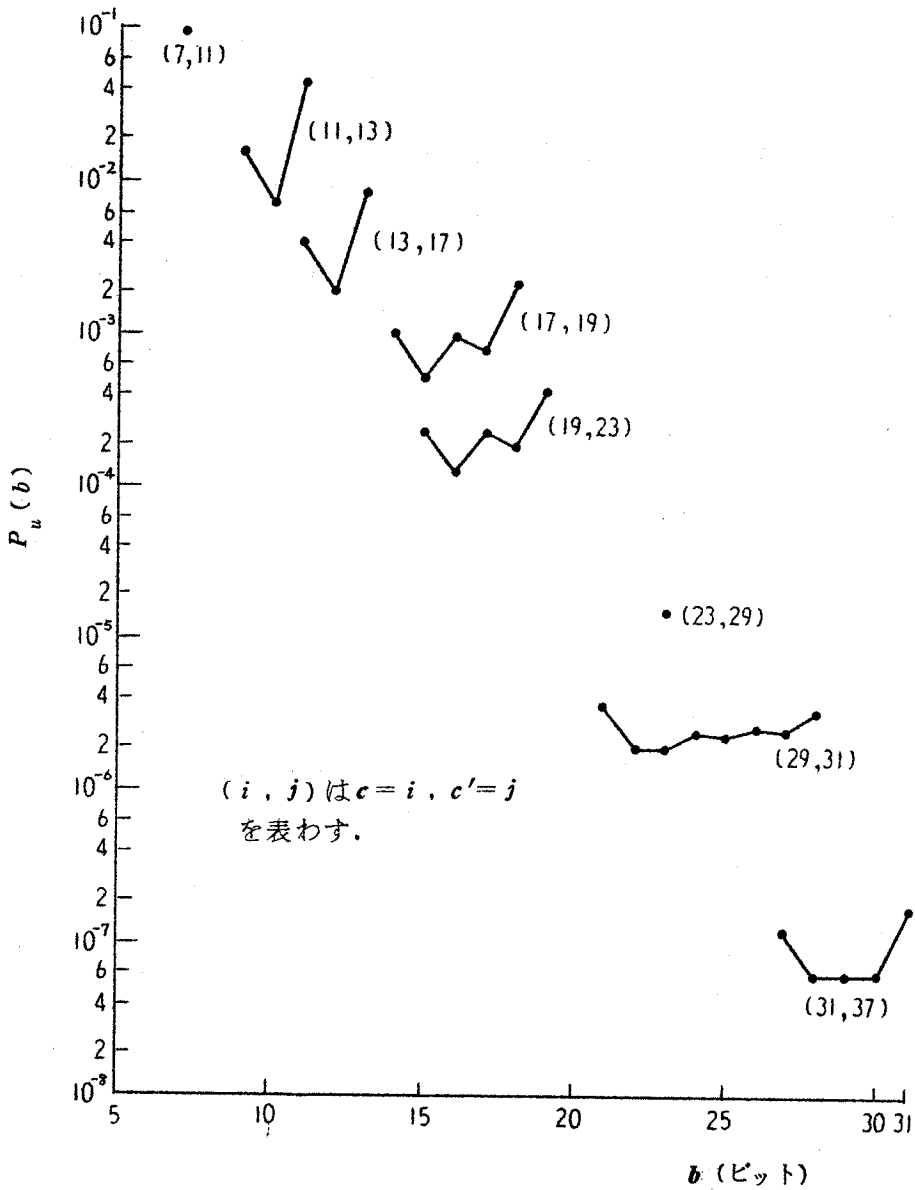


図３．５　誤りの長さと訂正不能割合との関係

図３．５に示すように $c \geqq 23$ 程度に選べば，訂正不能のパターンの割合は問題とならず，長さ c までのバースト誤りの殆んどすべてを訂正できるとしてよい．しかし c が小さい場合には誤った訂正の可能性を無視できないので，図３．２に示す復号回路において，cc' 回のシフトの間に２回以上二つの $F.S.R.$ の内容が一致した場合には訂正を行なわず，検出する機能を制御回路にもたせることが望ましい．

３．４　バースト誤りが生ずる通信路のもとでの訂正可能な符号の割合

バースト誤りを生じる通信路を表わすGilbert のモデル[1] によれば，長さ b の集中型バースト誤り* が長さ n の符号内に生じる確率を $P_{nl}(b)$ とすると，式（２．１７），（２．２６）および（２．３３）に示されるように

$$P_{nl}(0)=\frac{1}{(p+P)(J-L)}\{(p+P)(J^{n+1}-L^{n+1}) - N(hp+P)(J^{n}-L^{n})\} \tag{3.30.a}$$

$$P_{nl}(1)=\frac{P(1-h)}{(p+P)(J-L)^{3}}\left[J^{n-1}(J-N)\{n(J-L)(J-N)-2J(L-N)\} - L^{n-1}(L-N)\{n(L-J)(L-N)-2L(J-N)\}\right] ; n \geqq 3 \tag{3.30.b}$$

$$P_{nl}(b)=\frac{(1-h)^{2}(P+pN^{b-1})P}{(p+P)^{2}(J-L)^{3}}\{f_{1}(J,L)-f_{1}(L,J)\} ; b \geqq 2 \tag{3.30.c}$$

ただし

---

* 通常符号は短縮された擬巡回符号として用いられることが多く，このような符号は分離形バースト誤りを訂正できないので集中形バースト誤りのみを考える．

$$f_1(x,y)=x^{n-b}\left[x^2\{x(n+1)-y(n+3)\}-2xN\{xn-y(n+2)\}\right.$$
$$\left.+N^2\{x(n-1)-y(n+1)\}-b(x-y)(x-N)^2\right] \qquad (3.31)$$

であり，したがって長さ b までの集中型バースト誤りが長さ n の符号内に生じる確率を $F_{nl}(b)$ とすると式（2．34）より

$$F_{nl}(0)=P_{nl}(0) \qquad (3.32.a)$$

$$F_{nl}(1)=P_{nl}(0)+P_{nl}(1) \qquad (3.32.b)$$

$$F_{nl}(b)=P_{nl}(0)+P_{nl}(1)+\frac{(1-h)^2P}{(p+P)^2(J-L)^3}\{f_2(J,L)-f_2(L,J)\}$$
$$;\ b\geqq 2 \qquad (3.32.c)$$

ただし

$$f_2(x,y)=x^{n-b}\left\langle\left[x^2\{x(n+1)-y(n+3)\}-2xN\{xn-y(n+2)\}\right.\right.$$
$$\left.+N^2\{x(n-1)-y(n+1)\}\right]\left(P\frac{1-x^{b-1}}{1-x}+pN\frac{x^{b-1}-N^{b-1}}{x-N}\right)$$
$$-(x-y)\left[P(x-N)^2\frac{2x^b-x^{b-1}-(b+1)x+b}{(1-x)^2}\right.$$
$$\left.\left.+pN\{2x^b-x^{b-1}N-(b+1)xN^{b-1}+bN^b\}\right]\right\rangle \qquad (3.33)$$

が得られる．

本章で示した符号は図3．5からわかるように，$c\geqq 23$ では長さ c ビットまでの誤りはすべて訂正可能としても実質上さしさわりがないので，長さ n の符号が受信側で訂正可能である確率を $P_{cn}(b)$ とすると

$$P_{cn}(b)=F_{nl}\left(\left[\frac{c+c'}{3}\right]\right)+\sum_{i=\left[\frac{c+c'}{3}\right]+1}^{c}P_{nl}(i)\{1-P_u(i)\}\ ;\ c<23 \tag{3.34.a}$$

$$P_{cn}(b)\cong F_{nl}(c)\qquad ;\ c\geqq 23 \tag{3.34.b}$$

と表わされる．ただしこれは$n=cc'$の場合に成り立ち，$n<cc'$の場合は誤った訂正が減少する* ために$P_u(i)$は小さくなるが，ここでは安全側をとり，３．３で得た$P_u(i)$をそのまま用いた．

つぎに，長さbまでのバースト誤りを訂正できる，$(3b-1)$ビットの冗長をもった，長さnビットのFire符号を考え，それを用いた場合に得られる訂正可能な符号の割合を$P_{Fcn}(b)$とすると

$$P_{Fcn}(b)=F_{nl}(b) \tag{3.35}$$

となる．式（３．３４）および（３．３５）より計算した，冗長度g/nと，訂正不能となる符号の割合

$$P_{un}(b)=1-P_{cn}(b)$$

$$P_{Fun}(b)=1-P_{Fcn}(b)$$

との関係を，符号長nをパラメータとして図３．６に示す．

図３．６より，本符号は同じ冗長度のFire符号より訂正不能の割合は小，すなわち訂正可能の割合は大きいことがわかる．なお計算にあたり，ビット誤り率P_bを10^{-4}とし，状態Bの平均長$\bar{B}$を１０** として行なった．

---

* 巡回符号において共通のこの性質を利用して構成された擬巡回符がある．(35)

** バースト誤りの平均長$\bar{B}'$は（２．２．b）より約8となる．

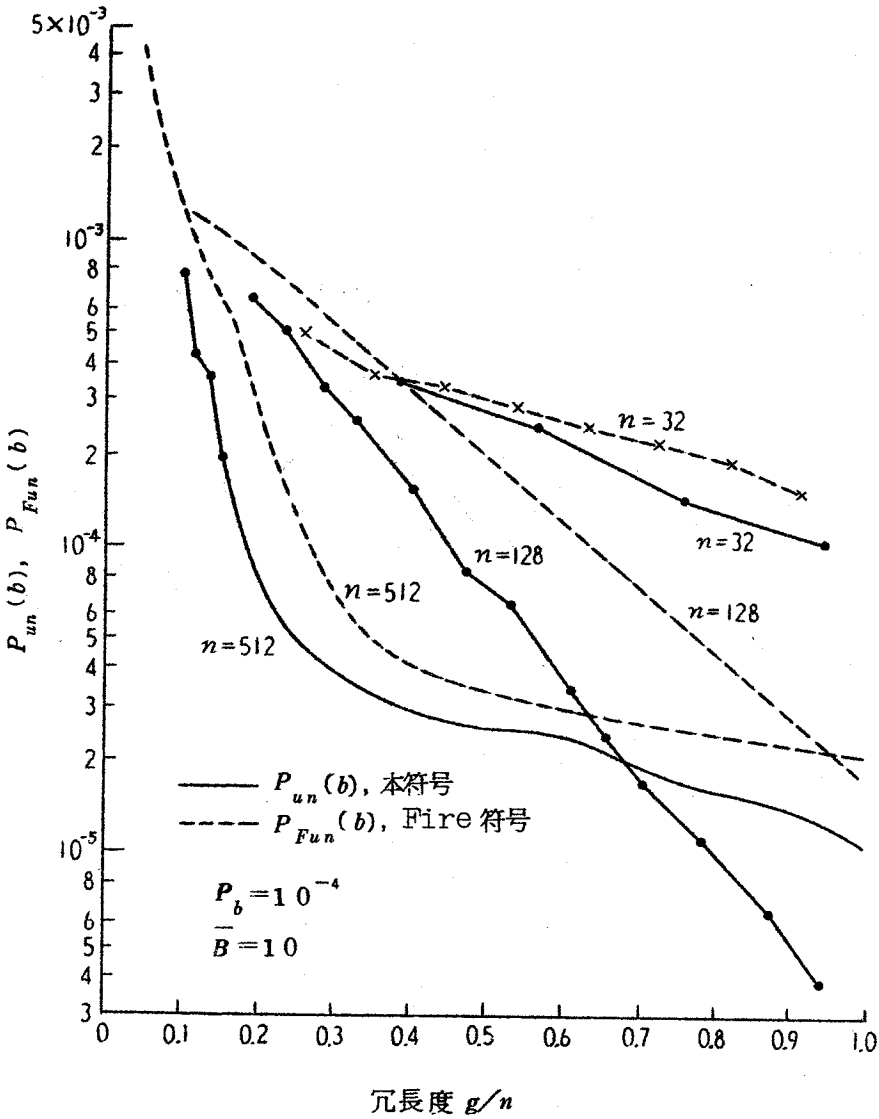


図３．６　冗長度と受信符号が訂正不能となる割合との関係

3．5 結　　言

符号の構成にかなり自由度を有し，かつ装置が非常に簡単な単一バースト誤り訂正符号を示し，その訂正能力について解析した．本符号は訂正能力を大，すなわち冗長を大にすると，ほぼ冗長数の半分の長さまでのバースト誤りをほとんどすべて訂正できる．また同じ冗長数のFire符号に比べ，実際の訂正能力を大きくできる．ただし，符号を構成する場合，特性多項式$G(X)=(X^c+1)(X^{c'}+1)$において，cとc'を素数としなければならないので，符号構成の自由度においてFire符号に劣るが，素数はその大きさが小さくなるにしたがい存在が密となるので実用上問題ないと思われる．

また素数の探索は比較的容易であるので，大きい訂正能力をもつ符号を簡単に構成できる．この特徴は，データ伝送の速度が上昇し，符号長が大となり，したがって訂正能力を大きくすることが要求される傾向にあるので望ましいものである．

第4章　バースト誤りを訂正するブロック符号の最適符号長

4．1　序　　言

第3章で示したバースト誤り訂正符号を含めて多くのバースト誤り訂正符号がAbramson[9]，Fire[10]，嵩[11],[16]，Melas[12]，Meggitt[14] ElspasおよびShort[15]，および笠原[17]らによって示されたが，バースト誤り訂正符号を用いればどれぐらい信頼度を改善できるか，あるいは符号長により伝送能率はどのように変化し，また最適な符号長が存在するかという問題については，情報理論的にも興味があり，しかも重要な意義を有するにもかかわらず殆んど研究されてこなかった．そこで本章では符号として最小冗長符号を仮定し，信頼度および伝送能率を現実的な立場で定義して，その符号を用いることによる信頼度の改善および符号長による伝送能率の著しい変化と最適符号長の存在を示す．

4．2　信頼度および伝送能率

本章では，符号はつぎのように構成されているとする．すなわち，一つの記号を構成する最小構成単位を小ブロック（mビット）とし，一つの符号はこの小ブロックをいくつかまとめて，それに検査ビット（gビット）を付加し，全体として単一バースト誤り訂正符号を構成する．これを大ブロックと呼び，大ブロック長nは小ブロック長mの整数倍になるようgを選ぶものとする．またこの符号は長さbまでの単一バースト誤りを訂正できるが，b以上の長さのバースト誤りにおかされた符号は全く他の符号となる* か，ある

---

* 通常このような全く他の符号に変ってしまうものが訂正能力を越えた誤りにおかされたものの中に占める割合は$1/(n2^{b-1}+1)$である．

いは正しく復号されず，誤りを受ける前とは全く異なった他の符号に復号される* （これを“誤った訂正”と呼ぶ）ような理想的な単一バースト誤り訂正符号とする．するとこれらの n，g および b の間にはつぎの関係が成り立つ(9)．

$$n2^{b-1}+1=2^{g} \tag{4.1}$$

したがって $2^{g} \gg 1$ のときには

$$g \cong b-1+log_2 n \tag{4.2}$$

が成り立つ．

つぎに従来のようにビット誤りでなく，記号を構成する最小構成単位，すなわち小ブロックの誤りに着目して信頼度を定義する．

〔定義４．１〕バースト誤り訂正方式の信頼度を，受信した情報に関する小ブロックの総数に対する，復号後誤っていない情報に関する小ブロックの総数の割合とする．

さきに述べた“誤った訂正”によりさらに付加される誤りのパターンは訂正可能な誤りのパターンの中の一つになり，それはどのパターンについても等しい割合で行なわれると考えられる(38)．この復号側の誤った訂正により，さらに誤りを付加される小ブロック数の期待値 E_e を求める．

〔補題４．１〕大ブロック長 n，小ブロック長 m の符号に長さ x の誤りが付加されたとき，誤りにおかされる小ブロック数の期待値 E_x はつぎのようになる．

＊ この割合は $n2^{b-1}/(n2^{b-1}+1)$ である．

$$E_x = \left\{ \begin{array}{ll} \dfrac{m+x-1}{m} & ; 1 \leqq x \leqq n-m+1 \\ \dfrac{n}{m} & ; n-m+2 \leqq x \leqq n \end{array} \right\} \qquad (4.3)$$

〔証明〕 $x=1$ のときは明らかに $E_1=1$ となり，式（4.3）は満足される．つぎに

$$am+2 \leqq x \leqq (a+1)m+1 \quad ; 0 \leqq a \leqq \frac{n}{m}-2$$

の場合を考えると，長さ x の誤りが付加される場合の数は n であり，その中で（$a+2$）個の小ブロックにまたがって付加されるものは（$x-am-1$）n/m 個，また（$a+1$）個の小ブロックにまたがって付加されるものは $\{n-(x-am-1)n/m\}$ 個ある．したがって E_x は

$$E_x = \frac{1}{n}\left[(a+2)(x-am-1)\frac{n}{m} + (a+1)\left\{n-(x-am-1)\frac{n}{m}\right\}\right]$$

$$= \frac{x+m-1}{m}$$

となる．また $n-m+2 \leqq x \leqq n$ なる x に対しては常に

$$E_x = \frac{n}{m}$$

となる．

（証明終り）

バースト誤りは両端が誤っていて，その間のビットは誤っていても誤っていなくてもよい．したがって，長さ c のバースト誤りのパターンは 2^{c-2} 種類あり，長さ b までのバースト誤りのパターンは 2^{b-1} 種類ある．したがって式（4．3）よりつぎの式が得られる．

$$E_e = \frac{1}{2^{b-1}} \left\{ \frac{m}{m} + \frac{m+1}{m} + \frac{2(m+2)}{m} + \cdots + \frac{2^{b-2}(m+b-1)}{m} \right\}$$

$$= \frac{1}{m\,2^{b-1}} \{ (m+b-2)\,2^{b-1} + 1 \} \qquad (4.4)$$

ここでT，N_b およびM_b をつぎのように定義すると，信頼度Rは式（4・5）のようになる．

T：受信した大ブロックの総数．

N_b：伝送中に誤りが生じなかったか，あるいは訂正可能な誤りが生じた大ブロックの総数．

M_b：伝送中に訂正能力を越えた誤りが生じた大ブロックの中で，誤りにおかされていない小ブロックの総数．

$$R = \frac{N_b \frac{n-g}{n}}{T \frac{n-g}{n}} + \frac{M_b \frac{n-g}{n}}{T \frac{n}{m} \cdot \frac{n-g}{n}} \cdot \frac{1}{n\,2^{b-1}+1}$$

$$+ \frac{n\,2^{b-1}}{n\,2^{b-1}+1} \cdot \frac{1}{T \frac{n}{m} \cdot \frac{n-g}{n}} \left\{ M_b \frac{n-g}{n} - (T - N_b) \left(\frac{m+b-2}{m} + \frac{1}{m\,2^{b-1}} \right) \frac{M_b \frac{n-g}{n}}{(T-N_b)\frac{n}{m}} \right\} \qquad (4.5)$$

式（4．5）の右辺第1項は受信した情報に関する小ブロックの総数に対する，復号後誤りをもたない大ブロックの中の情報に関する小ブロックの総数の割合を示す．第2項は，訂正能力を越えた誤りにおかされて他の符号語となったために，そのまま復号されてしまうものの中の情報に関する正しい小ブロックの総数の割合を示す．第3項は，訂正能力を越えた誤りにおかされた大ブロックの中で，復号側で誤った訂正を受けた後になお正しい情報に関する小ブロックの総数の割合を示す．式（4．5）を簡単にするとつぎの式が得られる．

$$R=\frac{N_b}{T}+\frac{M_b}{T}\cdot\frac{m}{n}\cdot\frac{n-m-b+2}{n+2^{1-b}} \tag{4.6.a}$$

なお $b=0$，すなわち検査ビットを付加しない場合は

$$R=\frac{N_0}{T}+\frac{M_0}{T}\cdot\frac{m}{n} \tag{4.6.b}$$

となる．また N_b/T は訂正可能な長さ b までのバースト誤りが生じたか，または誤りが生じなかった大ブロックの割合であるから第2章で示した長さ b までのバースト誤りが生じる分布関数 $F_n(b)$ に等しいので

$$\frac{N_b}{T}=F_n(b) \tag{4.7}$$

であり，また $mM_b/(nT)$ はつぎのような近似式で表わせる（付録3参照）．

$$\frac{M_b}{T}\cdot\frac{m}{n}\cong\frac{M_0}{T}\cdot\frac{m}{n}\cdot\frac{1-F_n(b)}{1-F_n(0)}\cdot\frac{n-b-1}{n-1} \tag{4.8}$$

一方

$$\frac{M_0}{T}\cdot\frac{m}{n}=F_m(0)-F_n(0) \tag{4.9}$$

と表わせるから式（4．6）はつぎのように変形される．

$$R = F_n(b) + \{F_m(0) - F_n(0)\} \frac{1-F_n(b)}{1-F_n(0)} \cdot \frac{n-b-1}{n-1} \cdot \frac{n-m-b+2}{n+2^{1-b}} \quad ; \ b \geqq 1$$

$$R = F_m(0) \quad ; \ b = 0 \qquad (4.10)$$

つぎに符号の復号側における能率を考え，伝送能率をつぎのように定義する．

〔定義4．2〕符号の伝送能率を，受信した小ブロックの総数に対する，復号後誤っていない情報に関する小ブロックの総数の割合とする．

伝送能率をEで表わすとつぎの関係が成り立つ．

$$E = \frac{n-g}{n} R \qquad (4.11)$$

4．3　計算結果

符号の訂正能力bと誤字率（$1-R$）との関係を，大ブロック長nをパラメータとして図4．1に示す．また誤字率を10^{-5}とした場合の伝送能率Eと大ブロック長nとの関係を図4．2に示す．またARQ方式との比較のため，位置情報を有する空RQ方式[25]とDual-RQ方式[22],[26]の結果も示した．なお，空RQ方式[22],[23],[24]は10^{-5}の誤字率をうるのが困難であるので示していない．

位置情報を有する空RQ方式とDual-RQ方式は容易に高い信頼度が得られ，また図4．2からわかるように，それらの伝送能率は単一バースト誤り訂正方式の伝送能率より大である．したがって，単一バースト誤り訂正方式は空RQ方式よりすぐれているが，位置情報を有する空RQ方式やDual-RQ

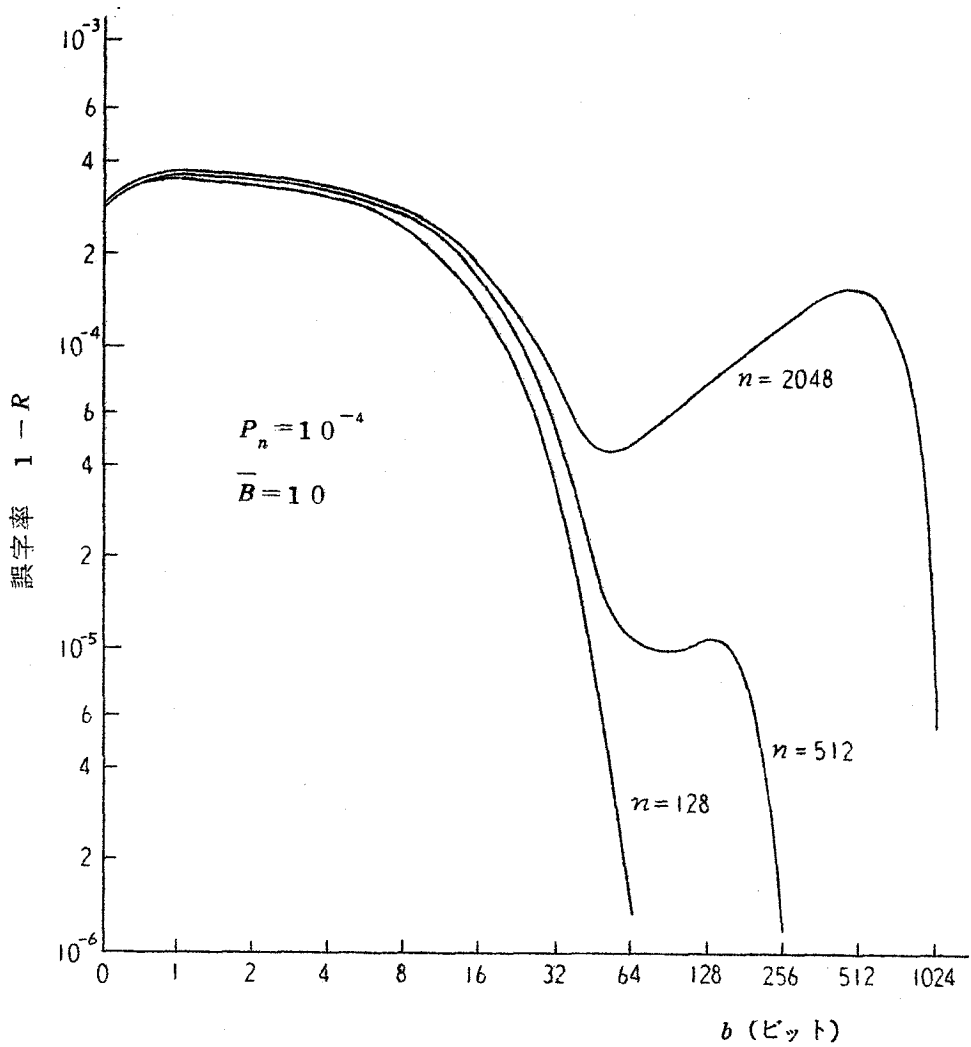


図４．１　訂正能力と誤字率との関係

方式より劣っていることがわかる．

また図４．１からわかるように，数ビット程度の長さの単一バースト誤りを訂正できるような符号は，検査ビットを全然付加しない場合よりも信頼度は悪化する．これは数ビット程度までの長さの誤りが生ずる割合はそれ以上

の長さの誤りが生ずる割合よりも小さく，訂正される小ブロックよりも誤った訂正を受ける小ブロックの方が多いからである．したがって，能力の低い単一バースト誤り訂正符号を用いることは不利となる．また大ブロック長が大きい場合には，訂正能力を増加しても誤字率が逆に増加するところがあるが，この理由はつぎのように考えられる．すなわち，大ブロック長が増大するにつれて多重バースト誤り（主に二重バースト誤り）におかされる確率は増加する．二重バースト誤りは単一バースト誤りに比べて長大となるから少

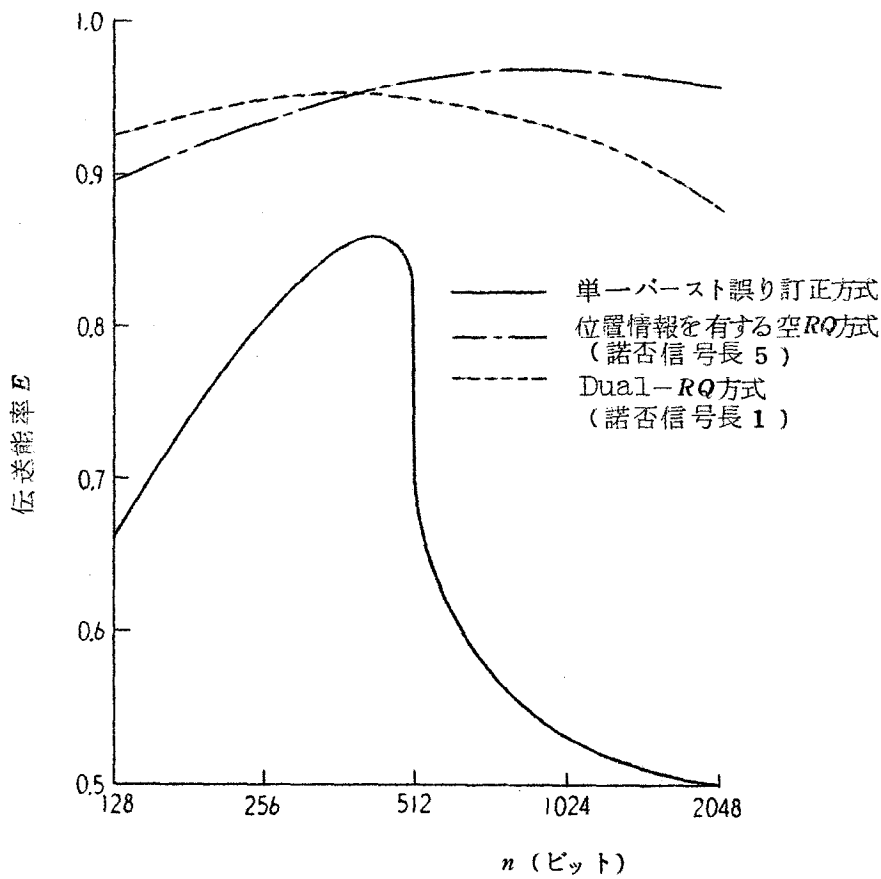


図４．２　符号長と伝送能率との関係

々訂正能力を増加しても訂正できるものは余り増加せず，逆に誤った訂正による正しい小ブロックの減少の効果が大きくなり，全体として信頼度が減少することが想像できる．しかし，二重バースト誤りで，その長さが大ブロック長の半分以上になるものは少ないと考えられるので，大ブロック長の半分程度の訂正能力を付加すればほとんど訂正できることになり，再び信頼度が向上すると考えられる．また誤字率が増加し始める点は，さきに述べたバースト誤りの分布関数値の飽和点に等しいことがわかる．したがって，飽和点以上の訂正能力を付加することは非能率的であるといえる．そこで単一バースト誤り訂正符号を用いる場合，その訂正能力を十分慎重に選ばなければならないことが明らかになった．

また図4.2からわかるように，単一バースト誤り訂正符号はARQ 方式に比べて，大ブロック長により伝送能率は著しく変化し，最適符号長は$n_{opt}=450$程度であり，その最適点の存在は顕著である．したがって，符号長選択が重要な問題になるといえる．

4．4 結　　言

第2章で導いたバースト誤りの確率の一般式を用いて単一バースト誤り訂正方式の解析に用いた．その結果，単一バースト誤り訂正方式は信頼度の点で“空RQ 方式[22],[23],[24]” よりすぐれているが，“位置情報を有する空RQ 方式[25]”や Dual-RQ 方式[22],[26]” には信頼度および伝送能率の点で劣ることが明らかになった．したがってフィードバック通信路が適用できる伝搬時間の短い短距離通信にはARQ 方式が適し，長距離通信や実時間処理が要求される場合には誤り訂正方式が適しているといえる．

また最も能率の良い伝送を行なえるところの最適符号長はARQ 方式以上

にその存在が顕著であり，符号長選択が重要な問題となるばかりでなく，信頼度の面から考えると，訂正能力の決定には十分慎重にならなければならないことが明らかになった．また数ビット程度の長さのバースト誤りを訂正できる符号はかえって信頼度を低下させ，非実用的であることが明らかになった．

第5章　フィードバック・シフトレジスタを用いた畳み込み符号の一構成法

5・1　序　　言

畳み込み符号は1955年Elias[27]によって提案され，それ以後Hagelbarger[30]，Wozencraft およびReiffen[39]，Massey[28]，Peterson[35]らによって発展された．

畳み込み符号はハードウェアで復号することを目的とした比較的冗長度の低いもの（冗長度≦1/2）と，逐次復号法[31]を適用することを目的とした冗長度の高い（冗長度≧1/2），惑星間を航行する衛星からの通信のようなS/Nの悪い通信を目的としたものとに大別される．

本章で提案する符号は後者に属するものであり，この後者に属するものについては，送信側は衛星の積載重量等の制限を受けるので，符号化装置はできるだけ簡単であることが望まれる．しかし受信側は地球上にあるため，極端な実時間処理を望む場合以外は，復号側は多少複雑で復号遅延があっても信頼度を高めることが可能であれば望ましいものと思われる．

しかし従来の“シフトレジスタを用いた符号化法”によれば，信頼度は符号の拘束長に関係するので，信頼度を良くしようとすればシフトレジスタの段数が増加し，それにともなって受信側での同期引き込みやオーバフロー後の処理が複雑となってくる．

本章では従来と異なり，符号化にフィードバック・シフトレジスタ（以後F.S.R.と略記する）を用いて確率的に長い拘束長を確保し，受信側の同期引き込みやオーバーフロー後の処理が簡単となる方法を提案し，また符号化回路の結線多項式の最適性に関する条件を示し，その条件より，最適結線多

項式を次数１２まで求めている．

５．２　符号構成法

ここでは５．２．１で，従来のシフトレジスタによる符号化法について述べつぎに５．２．２でその符号化法にともなう欠点を改善できるフィードバック・シフトレジスタを用いた符号化法について述べる．

５．２．１　シフトレジスタを用いた符号化法

従来から知られている，シフトレジスタを用いた畳み込み符号の符号化回路は図５．１に示すようなものであるが，この符号化法によれば情報ビットがシフトレジスタに１ビット入るとそれに対応して g（$\geqq 2$）ビットの送信符号を生じる．そのとき，入力情報が１か０かにより完全に反転した送信符号が得られるように，シフトレジスタの第１段目は各出力のmod．２ 加算器に接続されている．この方法においては図５．１から明らかなように，各送信符号は k ビットの情報の一次組み合わせによって与えられ，入力情報系列の長さ

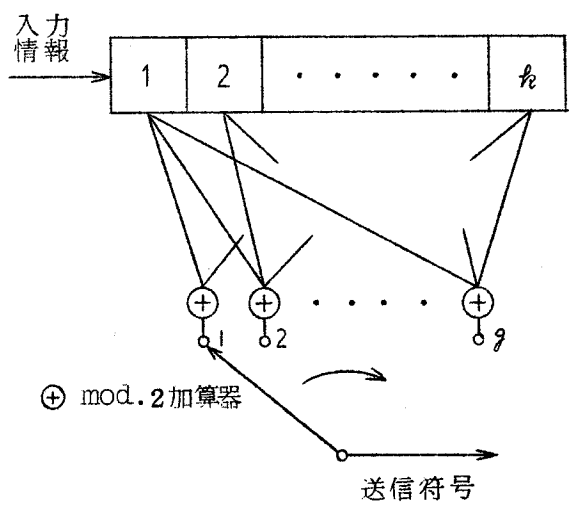


図５．１　シフトレジスタを用いた畳み込み符号の符号化回路

をLとすると，送信符号の長さMはつぎの式で与えられる．

$$M = (L + k)\ g$$

ここで$L \gg k$の場合には，能率Eは$E = L/M \cong 1/g$と近似される．

また送信側の拘束長* は（$k+1$）番目の情報がシフトレジスタに挿入されると，最初の情報ビットは押し出されて消去されることから，明らかにkブロック（kgビット）となり** 一次組み合わせが適当に選ばれた場合には，受信側の拘束長も同じ値となる．しかし，それ以外の場合には送信側での拘束長より短くなる．

つぎに$k=5$で$g=3$の場合の符号化回路の一例を図５．２に示し，シフトレジスタの初期状態を〔００００〕とした場合にその符号化回路により得られる入力情報と送信符号との関係を樹枝状表示で図５．３に示す．

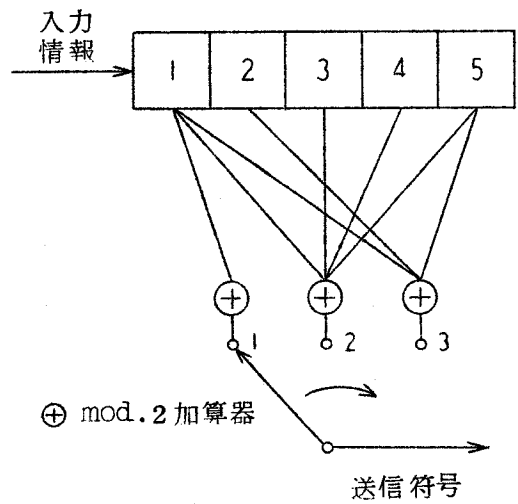


図５．２　シフトレジスタを用いた符号化回路の一例．
$k=5$，　$g=3$

図５．３に示すように入力情報が０か１かにより，それぞれ上または下の枝に進み，そのとき枝に記されている全く反転した形の３ビットの符号が送信符号になる．

---

* 送信側ではkブロックの拘束があるように見えるのにかかわらず，受信側で見ると符号化器の結線により，それより短い拘束しか得られない場合がある[40] ので，このように拘束長を送信側と受信側とに区別する．

** 入力情報１ビットがシフトレジスタに挿入されたとき送信されるgビットを１ブロックと呼ぶ．

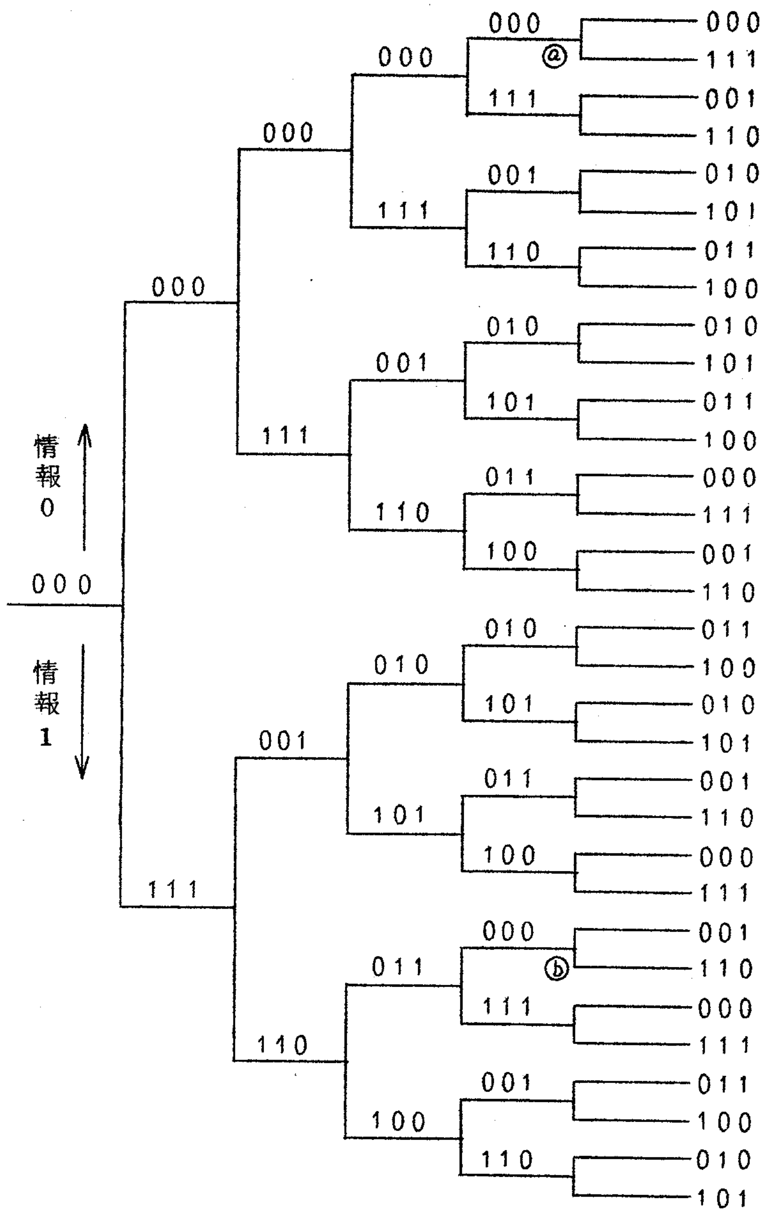


図5．3　入力情報と送信符号の樹枝状表示.

図５．３の枝ⓐおよびⓑに示すように，ある時点での送信符号が同じであってもそれ以後現われる出力系列が等しくならない場合がある．このようなことは通常 $k > g$ の場合に生じる．したがって $k > g$ の場合には受信側ではシフトレジスタの内容，すなわち過去の k ビットの情報を正しく把握していないと以後の復号が不可能になるという欠点がある．結局，ある時点での出力系列よりつぎの時点の出力系列を予想することが困難となる．また k が大きくなるにつれてこの困難さは増大する．

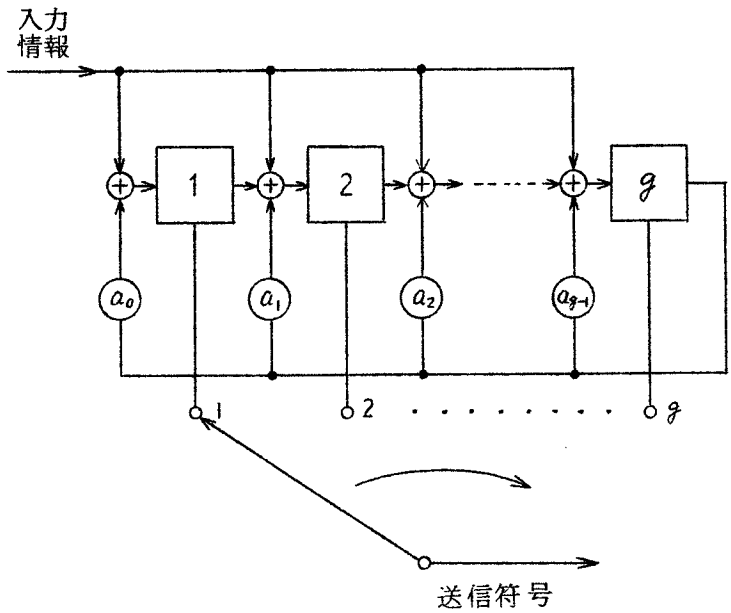
したがって，大きな誤りにおかされた場合はその部分の復号が不可能となることにより，以後の復号が困難となったり，出力系列を把握する時点を一度誤るともとの状態に戻ることが著しく困難となるような不利な点がある．これらの欠点を克服するためには $k = g$ とすればよいが，逐次復号法による訂正能力を増大するためには拘束長 k を大きくすることが必要となる[31]ので $k > g$ とすることが必要になってくる．

これらの欠点を改善できるのがつぎに述べるフィードバック・シフトレジスタを用いた符号化法である．

５．２．２　フィードバック・シフトレジスタを用いた符号化法

５．２．１で述べたように，シフトレジスタを用いた符号化法では $k = g$ とすれば，同期引き込みの困難さや大きな誤りにおかされた後の復号の困難さは改善されるが，訂正能力は拘束長に関連するので，訂正能力に関しては不利になる．

ここではこれらの欠点を除くために図５．４に示すような $k = g$，すなわち g 段のフィードバック・シフトレジスタを用いることにより，確率的に g より長い拘束長が得られる方法[32],[33],[34]を示す．これはフィードバック多項式 $G(X)$ を



$a_i = 0 \text{ or } 1$; $0 \leqq i \leqq g-1$

⊕ mod. 2 加算器

図５．４　フィードバック・シフトレジスタを用いた畳み込み符号の符号化回路.

$$G(X) = X^g + a_{g-1}X^{g-1} + \cdots\cdots + a_1X + a_0 \qquad (5.1)$$

とし，また入力結線多項式$P(X)$を

$$P(X) = X^{g-1} + X^{g-2} + \cdots\cdots + X + 1 \qquad (5.2)$$

としたものである．ここで入力情報がレジスタのすべての段に加えられているのは，入力情報が0か1かにより全く反転した，すなわち距離が最大* の出力を得るためである.

---

* このとき訂正能力が最大となる.

この回路において，$F.S.R.$ の初期値を〔0〕* にしておき，入力情報 I を順次レジスタに挿入していくと，送信符号 t は，レジスタの内容 s と入力情報 I との法2（mod.2）の加算によって得られ，情報が1ビット挿入される毎に g ビットの出力系列を発生する．このようにして符号化を行なうと，5．4で述べるように拘束長は同じ段数のシフトレジスタを用いた従来の方法より確率的に延長され，これを利用してより高い信頼度で復号することが可能となる．

つぎに原始多項式

$$G(X) = X^3 + X + 1 \qquad (5.3)$$

をフィードバック多項式とする符号化回路を図5．5に示し，これを初期状態〔0〕から動作させた場合に情報系列 I に対応する出力系列 t の樹枝状表示を図5．6に示す．

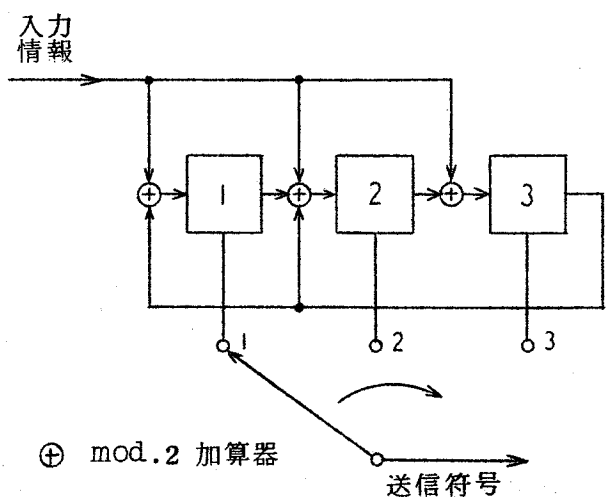


図5．5　$G(X) = X^3+X+1$ による符号化回路

＊　〔0，0，・・・，0〕なる1行 g 列の行列を示す．以後〔1〕の場合も同様とする．

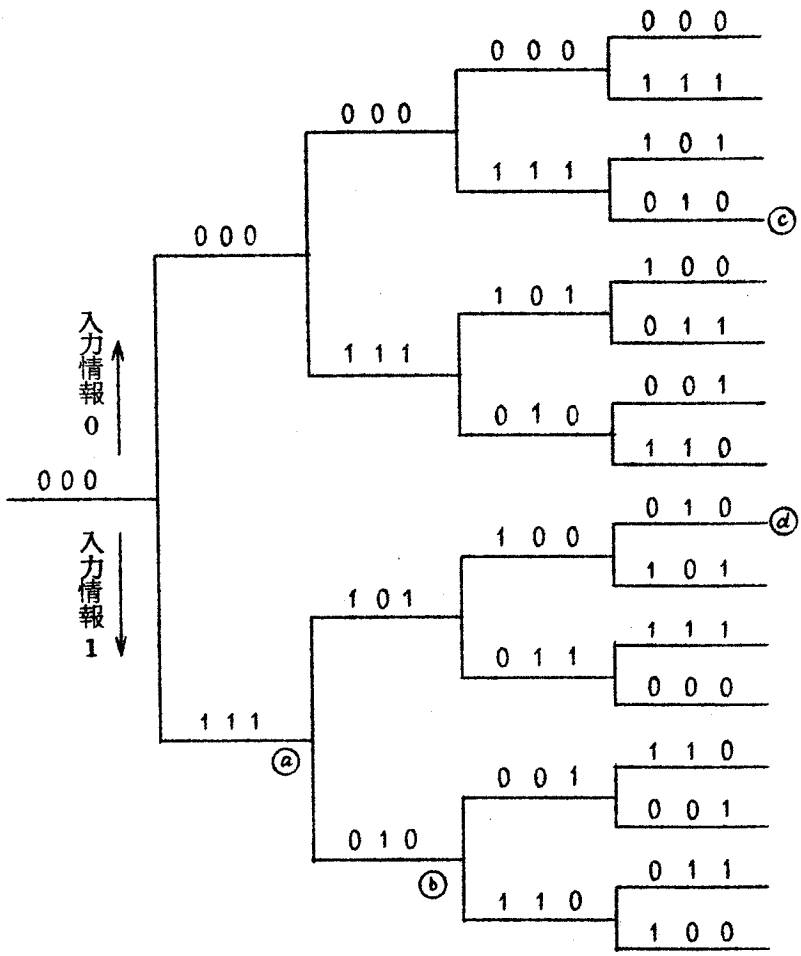


図５．６　$G(X)=X^3+X+1$の場合の入力情報と送信符号の樹枝状表示

この樹枝状表示において，g回の遷移に対する枝の集合をS（g^2ビット）とし，さらにS内で初期情報が０に対応する上半分をS_0，初期情報が１に対応する下半分をS_1で表わす．いま情報系列Iを

$$I=(1,\ 0,\ 1,\ 1,\ 0,\ \cdots\cdots)$$

とすると，これに対応する出力系列（送信符号）t は

$$t = (111,\ 101,\ 011,\ 000,\ 000,\ \cdots\cdots)$$

となり，通信路で雑音

$$N = (001,\ 110,\ 000,\ 001,\ 000,\ \cdots\cdots)$$

が加えられたときには受信符号 r は

$$r = (110,\ 011,\ 011,\ 001,\ 000,\ \cdots\cdots)$$

となる．受信側においては受信符号 r より t を，すなわち情報 I を推定していくのであるが，いま復号に逐次復号法を用いた場合を考えると，最初図５．６のⓐには容易に到達する．しかしつぎの３ビットに誤りが多いためⓑの枝に進む．つぎに枝ⓑからさらに深く進んでいくと，受信系列 r との差がほぼ単調に増加して蓄積されるので誤った経路を仮定していることが判明し，結局正しい経路を大きな確率で見い出すことができる．しかしながら同じ段数のフィードバック・シフトレジスタを用いても，そのフィードバックの結線の方法により，能力や復号時間が異なるので，つぎの５．３で最適な結線方法について述べる．

５．３　フィードバック多項式の決定

５．３．１　拘束長最大の多項式の決定

符号化に *F.S.R.* を用いた畳み込み符号においては，符号化側ではフィードバックの存在のために拘束長は無限大のように見えるが，復号側（受信側）ではそうではない．すなわち，異なった情報系列でも図５．６のⓒとⓓのように等しい出力が得られるところがあり，それ以後の出力系列は両者とも全く等しい．したがって実際にはⓒの点に到達するような系列が送信されても通信路で生じた誤りのために，ⓓに到達する系列に最も近いものとなった場

合には，それまでの g 段の復号は誤ったものとなる．このような場合が最悪の場合であるので復号側の拘束長をつぎのように定義する．

〔定義５．１〕符号の樹枝状表示において，任意の経路をとり，その経路とは出発点では逆方向に進みあとはランダムに m 回遷移する経路を考え，これら二つの経路に同じ状態が生じるまでの m の期待値を拘束長とする．

F.S.R. を用いた方式においては，復号側での拘束長は確率的に延長されるが，誤り訂正能力の下限は絶対的な拘束長の最小値，すなわち，任意の点より最初は反対方向に出発し，m 回の遷移の後で再び一致するような二つの系列（これを m 段の再一致系列と呼ぶことにする．例えば図５．６における系列◎と◎は４段の再一致系列である）の中で最小の m の値* で制限される．また拘束長とともにこれらの再一致系列間の距離が符号の能力を決定する．すなわち再一致系列間のハミング距離 d と訂正可能なビット数 e との間には

$$d \geqq 2e + 1 \qquad (5.4)$$

なる関係式が成り立つことから，その二つの系列間の距離 d が小さいと訂正能力が低下する．一方，S_0 に属する系列が送られた場合で，雑音によって S_1 の系列に近づくと，復号過程において一旦 S_1 の方へ入り込み易く，もとに戻るまでに時間を要して不利となるので，S_1 に属する系列の最小重みについても考慮する必要があるが，このことについては５．３．３で取り扱う．

以上述べたようにフィードバック多項式の決定にあたっては最小段の再一致系列の段数ができるだけ大きく，また S_1 に属する系列の最小重みができるだけ大きなものが望ましいことになる．

つぎに図５．５に示す符号化回路を考えると，これは入力情報に

---

* 図５．６よりわかるように g 段の遷移後の可能な状態は 2^g 個あるので m の最小値は $g+1$ を越えることができない．

$$P(X) = \sum_{i=0}^{g-1} X^i$$

を乗じて

$$G(X) = X^g + a_{g-1} X^{g-1} + \cdots + a_1 X + a_0$$

で割る乗除算回路である．また出力系列は各情報ビットが挿入されたときの剰余である．したがってある時点までの入力情報の多項式表示を $I(X)$，その時点での出力の多項式表示を $R(X)$ とするとつぎの式が成り立つ．

$$I(X)\,P(X) = Q(X)\,G(X) + R(X)$$

つぎにさきに述べたように絶対的な拘束長の最小値が誤り訂正能力に関連しているので拘束長に関する定理を示す．

〔定理５．１〕 g 段の $F.S.R.$ を用いて符号化を行ない，拘束長の下限として g を得るための必要十分条件は入力結線多項式 $P(X)$ とフィードバック多項式 $G(X)$ とが互に素であることである．

〔証明〕 いま $P(X)$ と $G(X)$ とが互に素でないとするとつぎの式が成り立つような多項式 $M(X)$ が存在する．

$$\left.\begin{aligned} P(X) &= M(X)\,P'(X) \\ G(X) &= M(X)\,G'(X) \end{aligned}\right\} \qquad (5.5)$$

また $I_1(X)$ および $I_2(X)$ を互に異なる（$g-1$）次以下のある多項式とすると

$$I_1(X)\,P(X) = Q_1(X)\,G(X) + R_1(X) \qquad (5.6)$$

$$I_2(X)\,P(X) = Q_2(X)\,G(X) + R_2(X) \qquad (5.7)$$

となり，式（５．５）を式（５．６）および（５．７）に代入すると

$$I_1(X)\,M(X)\,P'(X) = Q_1(X)\,M(X)\,G'(X) + R_1(X) \qquad (5.8)$$

$$I_2(X)\,M(X)\,P'(X) = Q_2(X)\,M(X)\,G'(X) + R_2(X) \qquad (5.9)$$

となる．ここで$G'(X)$，$I_1(X)$，および$I_2(X)$は（$g-1$）次以下の多項式であり，$I_1(X)$と$I_2(X)$とは互に異なるとしたので，つぎの式を満足するような$I_1(X)$および$I_2(X)$が必らず存在する．

$$G'(X) = I_1(X) + I_2(X) \qquad (5.10)$$

式（5．10）を式（5．8）に代入すると

$$\{I_2(X) + G'(X)\}\,M(X)\,P'(X) = Q_1(X)\,M(X)\,G'(X) + R_1(X)$$

となり，これを変形すると

$$I_2(X)\,M(X)\,P'(X) = \{Q_1(X) + P'(X)\}\,M(X)\,G'(X) + R_1(X) \qquad (5.11)$$

となる．式（5．9）および（5．11）より

$$R_1(X) = R_2(X)$$

となる．よって$P(X)$と$G(X)$とは互に素であることが必要である．

つぎに$I_1(X) \neq I_2(X)$で$I_1(X) \neq 0$，$I_2(X) \neq 0$なる任意の（$g-1$）次以下の多項式$I_1(X)$および$I_2(X)$を選び，また$P(X)$と$G(X)$とが互に素であると仮定する．いま$R_1(X) = R_2(X)$とすると式（5．6）および（5．7）を加えると

$$\{I_1(X) + I_2(X)\}\,P(X) = \{Q_1(X) + Q_2(X)\}\,G(X) \qquad (5.12)$$

が得られ

$$I_1(X) + I_2(X) = I_3(X)$$

$$Q_1(X) + Q_2(X) = Q_3(X)$$

とすると式（5．12）は

$$I_3(X)\,P(X) = Q_3(X)\,G(X) \qquad (5.13)$$

となる．ここで$P(X)$と$G(X)$は互に素であるので式（5．13）は$P(X)G(X)$

を因数としてもたなければならない．したがって

$$I_3(X)\ P(X) = Q_3(X)\ G(X) = N(X)\ P(X)\ G(X) \qquad (5.14)$$

を満足する多項式$N(X)$が存在しなければならない．しかし$I_3(X)$の次数は（$g-1$）次以下であるので$I_3(X)\ P(X)$の次数は（$2g-2$）次以下となる．一方$N(X)\ P(X)\ G(X)$は0かまたはその次数が（$2g-1$）次以上であるので式（5．14）を満足するような$N(X)$は$N(X)=0$のみである．$N(X)=0$とすると$I_3(X)=0$　となり，したがって$I_1(X)=I_2(X)$　となるが，これは始めの仮定に反する．よって$P(X)$と$G(X)$とが互に素であれば十分である．　〔証明終り〕

定理５．１からわかるように，拘束長の下限としてgを得るためには$G(X)$を既約多項式とすれば十分であるということがわかる．

５．３．２　再一致系列間の距離

g段の$F.S.R.$を用いて符号化装置を構成する場合，最低g段の拘束長を得るための必要十分条件は“多項式$G(X)$と$P(X)$とを互に素になるように選ぶこと”であるということはさきの定理５．１で述べたが，このような条件を満足する多項式は各次数において多数存在する．そこで上の条件を満足する多項式の中で，ある状態から分岐し，再び一致するような最短の二つの系列の対，すなわち最小段の再一致系列間の距離が問題となる．

いま，二つの最小段の再一致系列間の距離をdで表わし，最悪の場合でも誤り訂正が可能なビット数をeとするとdとeの間には式（５．４）の関係が成り立つ．

そこである一つの系列に相当する符号を送信する場合，この系列に対応する最小段の再一致系列にはできるだけ落ち込まないように符号を構成する必要がある．このためには最小段の再一致系列間の距離dに関してつぎの定理

が成り立つ．

〔定理５．２〕最低 g 段（g^2ビット）までの拘束が保証されるような多項式の最小段（$g+1$ 段）の再一致系列を与える入力

$$I_1(X) = b_g X^g + b_{g-1} X^{g-1} + \cdots + b_1 X + b_0$$

と

$$I_2(X) = c_g X^g + c_{g-1} X^{g-1} + \cdots + c_1 X + c_0$$

との間にはつぎの関係が成り立つ．

$$c_i = b_i + a_i \quad ; \ 0 \leqq i \leqq g-1$$

$$c_i = \overline{b}_i \quad ; \quad i = g$$

ただし a_i は

$$G(X) = X^g + a_{g-1} X^{g-1} + \cdots + a_1 X + a_0$$

なるフィードバック多項式の次数 i の係数である．

また（$g+1$）段の再一致系列間の距離は，最初が１であるような（$g+1$）ビットのある情報が加えられたときの送信符号が，すべて０のパターンになるような情報系列のはじめの g ビットまで加えられたときに得られる送信符号の重みの総和に等しくそのような入力情報系列を多項式表示すると $G(X)$ と等しくなる（図５．５に示す符号化回路では，フィードバック多項式 $G(X)$ が

$$G(X) = X^3 + X + 1$$

であることから，情報系列（1，0，1，1）が加えられたときの送信符号の重み7が（$g+1$）段の再一致系列間の距離となることが図5．6よりわかる）．

〔証明〕任意の二つの（$g+1$）段の再一致系列を生じる入力情報をそれぞれ$I_1(X)$および$I_2(X)$（$I_1(X) \neq I_2(X)$で，ともにg次以下）とすると，（$g+1$）段の再一致系列となることから

$$I_1(X)\ (X^{g-1}+X^{g-2}+\cdots+X+1)$$

$$\equiv I_2(X)\ (X^{g-1}+X^{g-2}+\cdots+X+1)\ ;\mathrm{mod}.G(X) \quad (5.15)$$

となる．式（5．15）より

$$\{I_1(X)+I_2(X)\}\ (X^{g-1}+X^{g-2}+\cdots+X+1) \equiv 0 \quad ;\mathrm{mod}.G(X)$$

が得られ，$P(X)=X^{g-1}+X^{g-2}+\cdots+X+1$と$G(X)$とは互に素であることから

$$I_1(X)+I_2(X)=N(X)\,G(X)\equiv 0 \qquad ;\mathrm{mod}.G(X) \qquad (5.16)$$

となる．これを満足するためには，$I_1(X)$および$I_2(X)$がともにg次以下であり，かつ$I_1(X) \neq I_2(X)$であるので

$$\left.\begin{array}{l} I_1(X)+I_2(X)=G(X) \\ (N(X)=1) \end{array}\right\} \qquad (5.17)$$

でなければならない．そこで$I_1(X)$および$I_2(X)$をそれぞれ

$$I_1(X)=b_gX^g+b_{g-1}X^{g-1}+\cdots+b_1X+b_0 \qquad (5.18)$$

$$I_2(X) = c_g X^g + c_{g-1} X^{g-1} + \cdots + c_1 + c_0 \qquad (5.19)$$

とし，またフィードバック多項式$G(X)$を

$$G(X) = X^g + a_{g-1} X^{g-1} + \cdots + a_1 X + a_0 \qquad (5.20)$$

と表わすと，式（5．17），（5．18），（5．19）および（5．20）より

$$(b_g X^g + b_{g-1} X^{g-1} + \cdots + b_1 X + b_0) + (c_g X^g + c_{g-1} X^{g-1} + \cdots + c_1 X + c_0)$$
$$+ (X^g + a_{g-1} X^{g-1} + \cdots + a_1 X + a_0) = 0$$

となる．上式を変形すると

$$(b_g + c_g + 1) X^g + (b_{g-1} + c_{g-1} + a_{g-1}) X^{g-1} + \cdots + (b_1 + c_1 + a_1) X$$
$$+ (b_0 + c_0 + a_0) = 0 \qquad (5.21)$$

となり，式（5．21）が常に成り立つことにより

$$\left.\begin{aligned} b_i + c_i + a_i &= 0 \qquad ; 0 \leqq i \leqq g-1 \\ b_i + c_i + 1 &= 0 \qquad ; i = g \end{aligned}\right\} \qquad (5.22)$$

となり，フィードバック多項式の係数が1である次数に相当する次数では異なり，他は一致するような二つの（$g+1$）ビットの入力に対応する最終出力は一致する．また式（5．6）および（5．7）より

$$I_1(X)(X^{g-1} + X^{g-2} + \cdots + X + 1) = Q_1(X) G(X) + R_1(X)$$

$$I_2(X)(X^{g-1} + X^{g-2} + \cdots + X + 1) = Q_2(X) G(X) + R_2(X)$$

と表わせ，両式の両辺を加えると

$$\{ I_1(X) + I_2(X) \}(X^{g-1}+X^{g-2}+ \cdots +X+1) = \{ Q_1(X) + Q_2(X) \} G(X)$$

$$+ R_1(X) + R_2(X) \qquad (5.23)$$

が得られるから，二つの入力 $I_1(X)$ および $I_2(X)$ が加えられた場合の出力間の距離は $\{ I_1(X) + I_2(X) = G(X) \}$ なる入力と，すべてが0の入力が加えられた場合の出力〔0〕との距離，すなわち $G(X)$ なる入力が加えられた場合の出力の重みに等しい．　〔証明終り〕

上の定理より，（$g+1$）回の遷移で〔0〕に到達するような経路の重みの総和で，すべての（$g+1$）段の再一致系列間の距離が代表される．

〔補題5．1〕多項式

$$P(X) = X^{g-1}+X^{g-2}+ \cdots +X+1$$

と

$$G(X) = X^g + a_{g-1}X^{g-1} + \cdots + a_1X + a_0$$

とが互に素であると仮定すると，$G(X)$ と最大次数項は一致するが，他の項はすべて補の関係にある多項式（以後同値多項式と呼ぶ）

$$G'(X) = X^g + \bar{a}_{g-1}X^{g-1} + \cdots + \bar{a}_1X + \bar{a}_0 \qquad (5.24)$$

と $P(X)$ も互に素となる．

〔証明〕多項式 $G'(X)$ は式（5．24）を変形することにより

$$G'(X) = X^g + \bar{a}_{g-1}X^{g-1} + \cdots + \bar{a}_1X + \bar{a}_0$$

$$= X^g + (1+a_{g-1})X^{g-1} + \cdots + (1+a_1)X + (1+a_0)$$

$$= X^{g-1} + X^{g-2} + \cdots + X + 1 + G(X)$$

$$= P(X) + G(X) \qquad (5.25)$$

と表わされ，$G(X)$ と $P(X)$ は互に素であるから，$G'(X)$ と $P(X)$ も互に素となる．　〔証明終り〕

〔定理５．３〕フィードバック多項式 $G(X)$ および $G'(X)$ を有する二つの異なった符号化回路において，状態〔０〕から出発し，（$g+1$）ビットの入力系列により再び状態〔０〕へ到達するまでの出力系列は一致する．したがって（$g+1$）段の再一致系列間の距離も $G(X)$ と $G'(X)$ とでは等しくなる．

〔証明〕二つの多項式 $G(X)$ および $G'(X)$ をもった符号化回路において，状態〔０〕から出発して（$g+1$）ブロック目で再び〔０〕へ到達するような入力系列をそれぞれ g 次の多項式 $I(X)$ および $I'(X)$ とすると

$$\left.\begin{aligned} I(X)\ P(X) &= Q(X)\ G(X) \\ I'(X)\ P(X) &= Q'(X)\ G'(X) \end{aligned}\right\} \qquad (5.26)$$

と表わせる．$P(X)$ と，$G(X)$ および $G'(X)$ は互に素であるので，式（５．２６）を満足する $Q(X)$，$Q'(X)$，$I(X)$ および $I'(X)$ は

$$\left.\begin{aligned} Q(X) = Q'(X) &= P(X) = X^{g-1} + X^{g-2} + \cdots + X + 1 \\ I(X) &= G(X) = X^g + a_{g-1}X^{g-1} + \cdots + a_1 X + a_0 \\ I'(X) &= G'(X) = X^g + \bar{a}_{g-1}X^{g-1} + \cdots + \bar{a}_1 X + \bar{a}_0 \end{aligned}\right\} \qquad (5.27)$$

となる．よって $I(X)$ および $I'(X)$ の上位の（$k+1$）ビット，すなわち

$$I_k(X) = X^k + a_{g-1}X^{k-1} + \cdots + a_{g-k+1}X + a_{g-k}$$

$$I_k'(X) = X^k + \bar{a}_{g-1}X^{k-1} + \cdots + \bar{a}_{g-k+1}X + \bar{a}_{g-k}$$

が加えられた場合の商 $Q_k(X)$ および $Q_k'(X)$ は

$$Q_k(X) = Q_k'(X) = X^{k-1} + X^{k-2} + \cdots + X + 1$$

となり，そのときの出力，すなわち剰余をそれぞれ $R_k(X)$ および $R_k'(X)$ とするとつぎの式が成り立つ．

$$(X^k + a_{g-1}X^{k-1} + \cdots + a_{g-k+1}X + a_{g-k})P(X) = (X^{k-1} + X^{k-2} + \cdots + X + 1)G(X) + R_k(X) \qquad (5.28)$$

$$(X^k + \bar{a}_{g-1}X^{k-1} + \cdots + \bar{a}_{g-k+1}X + \bar{a}_{g-k})P(X) = (X^{k-1} + X^{k-2} + \cdots + X + 1)G'(X) + R_k'(X) \qquad (5.29)$$

両式の両辺を加えると式（5．25）より

$$(X^{k-1} + X^{k-2} + \cdots + X + 1)P(X) = (X^{k-1} + X^{k-2} + \cdots + X + 1)P(X) + R_k(X) + R_k'(X) \qquad (5.30)$$

となり，これより $R_k(X) + R_k'(X) = 0$ すなわち $R_k(X) = R_k'(X)$ が得られる．したがって $G(X)$ と $G'(X)$ とをそれぞれの符号化回路のフィードバック多項式とすると，状態〔0〕から〔0〕への遷移における再一致系列の内容はすべて一致する．これより，再一致系列間の距離も等しくなる．

〔証明終り〕

5．3．3　符号の最小重み

5．3．1および5．3．2で述べたフィードバック多項式の決定条件は，符号の誤り訂正能力の増大をねらいとするものであった．これに対しここでは，畳み込み符号における大きな問題の一つである，復号に要する時間の短縮，すなわち，誤りに対して強く，たとえ誤りが生じたとして迅速にそれを検出できるように符号を構成することを目的としている．

本符号化法の場合，受信側において受信符号より送信符号，すなわち送信情報を推定する際，送信符号が有する拘束により，情報1ビットの決定は受信符号g^2ビットを見て行なう．これを樹枝状表示で見ると，ある時間においてはS全体より1ビットの情報を復号していくことになる．このことからSの上半分S_0と下半分S_1との間の最小距離が問題となる．いま，S_0とS_1に属する任意の枝をx_0およびx_1とすると，x_0とx_1との間のハミング距離dはつぎの式で与えられる．

$$d(x_0, x_1) = w(x)$$

ただし　$x = x_0 + x_1$　でwは重みを示す関数である．

またSの性質より明らかなようにxなる枝はS_1に属する．したがって，S_0とS_1における枝の間の距離は，S_1に属するある一つの枝の重みによって代表される．結局，通信路において送信符号に付加された誤りをできるだけ多く，かつ迅速に検出するためにはS_0とS_1との最小距離，すなわちS_1に属する枝の最小重みをできるだけ大きくとることが望ましい．

5．3．4　最適なフィードバック多項式

いままでに述べたすべての条件，すなわち

(1)　最小段の再一致系列の段数が，フィードバック多項式の次数をgとすると$(g+1)$になること．

(2) （$g+1$）段の再一致系列間の距離が最大であること．

(3) S_1に属する枝の重みの最小値ができるだけ大きいこと．

なる三つの要素を考慮して，畳み込み符号の符号化回路に用いる最適なフィードバック多項式を計算機により探索したものを表５．１に示す．

表５．１　最適なフィードバック多項式

次数g	フィードバック多項式$G(X)$	$(g+1)$段の再一致系列間の距離	S_1の最小重み
3	X^3+X^2	7	5
4	X^4+X^3+X	12	8
5	$X^5+X^4+X^2$	19	11
6	$X^6+X^5+X^4+X^2+X$	27	13
7	$X^7+X^6+X^4+X^3+X^2$	37	22
8	$X^8+X^7+X^5+X^3+X^2$	48	26
9	$X^9+X^8+X^7+X^5+X^4+X^3+X$	61	32
10	$X^{10}+X^9+X^7+X^6+X^5+X^3+X^2$	75	38
11	$X^{11}+X^{10}+X^7+X^6+X^5+X^4+X^3+X^2+X$	94	45
12	$X^{12}+X^{11}+X^9+X^7+X^6+X^4+X^2$	108	47

ただし表５．１に示した多項式は定数項をもたないものであり，これらの同値多項式（５．３．2参照）も全く同一の能力を有する．このように定数項を有しないフィードバック多項式を用いると，情報そのものを送信符号の一部として送り出すことが可能である．このことは復号において利点があると考えられるのでこれをもって代表させた．

表５．１に示した多項式を用いた場合の符号の訂正能力は，（$g+1$）段

の再一致系列に落ち込んだ最悪の場合でも，再一致系列間の距離をdとすると$\left[\frac{d-1}{2}\right]^{*}$までの誤りは訂正可能である．また大きな誤りのためにある部分が復号不能となった場合も，それ以後の情報は正しく復号される．これは従来の方式に比較して大きな利点である．

5．4　拘束長の期待値

すでに述べたように，符号化回路のフィードバック多項式として5．3．4で示した最適な多項式を用いても，g次の多項式の場合は拘束長の下限はgブロックとなる．これは樹枝状表示において，任意の点から出発して（$g+1$）回の遷移に対応する枝が誤りのため再一致系列をたどった場合である．しかしながら，誤ってこの系列に落ち込む確率は小さく，確率的に見ると拘束長は定義5．1で述べたようにかなり延長される．ここではその拘束長の期待値を求める．

いま，最適なg次のフィードバック多項式で符号化する場合を考える．ここで〔0，0，・・・〕なる入力系列を加えたときに得られる出力系列を送信符号とすると，この枝の再一致系列はさきに述べたようにg回の遷移までは発生しない．そして（$g+1$）回の遷移以後に新らしく発生する再一致系列の数を$f(m)$で表わす．ここでmはその再一致系列が生じる遷移回数を示す．いまm段目でのS_iにおける〔0〕の数は$2^{m-(g+1)}$であるからつぎの式が成り立つ．

$$f(m)=2^{m-(g+1)}-\{f(m-1)+f(m-2)+\cdots f(m-g)\}$$

$$-\{2f(m-g-1)+2^{2}f(m-g-2)+\cdots+2^{m-2g-1}f(g+1)\} \tag{5.31}$$

＊　〔　〕はガウス記号．

式（5．31）より

$$f(m-1)=2^{m-(g+2)}-\{f(m-2)+f(m-3)+\cdots+f(m-g-1)\}$$

$$-\{2f(m-g-2)+2^2f(m-g-2)+\cdots+2^{m-2g-2}f(g+1)\} \qquad (5.32)$$

が得られる．したがって式（5．31）および（5．32）より

$$f(m)-2f(m-1)=-f(m-1)+f(m-2)+f(m-3)+\cdots$$

$$+f(m-g)$$

が得られ，これより

$$f(m)=\sum_{i=m-g}^{m-1}f(i) \qquad (5.33)$$

ただし初期条件は

$f(1)=f(2)=\cdots=f(g)=0$

$f(g+1)=1$

となる．また $g=2$ のときは上式を解くと

$$\left.\begin{aligned} f(m)&=\frac{\left(\frac{1+\sqrt{5}}{2}\right)^{m-2}-\left(\frac{1-\sqrt{5}}{2}\right)^{m-2}}{\sqrt{5}} \quad ; m\geqq 2 \\ f(1)&=0 \end{aligned}\right\} \qquad (5.34)$$

が得られる．$g\geqq 3$ のときは近似式

$$\left.f(m)\cong\frac{1-t_1}{(g+1-2gt_1)\,t_1^{m-(g+1)}} \quad ; m\geqq g+2\right\} \qquad (3.35)$$

$$f(g+1)=1$$
$$f(1)=f(2)=\cdots=f(g)=0$$

が成り立つ(41).

ここでS_1においてm段の再一致系列が生じる確率を$P(m)$とすると

$$P(m)=\frac{f(m)}{2^{m-1}} \tag{5.36}$$

となる．したがって拘束長の期待値E_{cL}は

$$E_{cL}=\sum_{m=g+1}^{\infty} mP(m)\begin{cases}=7 & ;\ g=2\\ \cong\dfrac{g+1}{2g}+\dfrac{1-t_1}{(g+1-2gt_1)2^g}\cdot\dfrac{4t_1-1}{(2t_1-1)^2} & ;\ g\geqq 3\end{cases} \tag{5.37}$$

となる．

式（5．37）の計算結果を表5．2に示す．表5．2に示すように拘束長の期待値は拘束長の下限gよりかなり大きいことがわかる．

表5．2　拘束長の期待値

次数 g	拘束長の期待値 E_{cL}
2	7
3	12
4	27
5	58
6	121
7	248
8	503

5．5　結　　言

従来の畳み込み符号の符号化回路よりも段数の少ないシフトレジスタに適当なフィードバックを設けることにより，確率的に長い拘束長を得，かつ従来の方法の最大の欠点の一つであった同期復帰の困難さおよび大きな誤りにおかされた後の正常状態への復帰の困

難さを改善できる方法を提案した.

またフィードバック多項式と送信符号のパターンとの関係を明らかにし,最適なフィードバック多項式を示した.

訂正能力の点だけについて考えると,多段のフィードバック・シフトレジスタの一部を送信する[32]ことが拘束長を増大できるので望ましいが,復号の手順が従来の方法と同様となり非常に複雑になるので取り扱わなかった.しかしこの方法によれば,従来の方法よりさらに信頼度の向上を期待できる.

また逐次復号法の適用において,本符号は復号過程における時間の短縮,あるいは情報の予測可能など有利な面があり,その他送信符号中に情報をそのままの形で残せるという利点もある.

第6章　結　　論

本論文では第2章で任意長の符号内に生じる任意長の単一バースト誤りの確率の一般式を示した．すなわち，母関数を用いることにより一般式誘導の手順を求め，近似を行なうことなく導いた．なお通信路のモデルとして近似度の高いGilbert のモデルを用いた．また同時にシミュレーションを行ないその妥当性を確かめた．この確率式はバースト誤りを対象としたシステムの解析に有用と思われる．

本章では単一バースト誤りの確率のみを示したが，今後多重バースト誤り訂正符号の復号の問題点が解決されると実用化の可能性が強くなると思われるので，多重バースト誤りの確率式が将来必要になると思われる．

また現在までにバースト誤りを訂正できる符号は多数見い出されているが，能率の良い符号は構成の自由度が小さく，また構成に自由度を有するFire符号は能率が悪いという欠点があった．そこで第3章で，構成の自由度はFire符号に比べてやや劣るが，訂正能力，装置の簡単さおよび生成多項式の決定の容易さでまさり，大きな訂正能力をもった符号を容易に構成できる方法を示した．

一方，このようなバースト誤り訂正符号を用いた場合の効果については殆んど研究されていなかった．そこで第4章で，信頼度および伝送能率を現実的な立場で定義し，バースト誤り訂正方式の効果について考察し，同時に最適符号長が顕著に存在することを示した．また*ARQ* 方式と比較し，信頼度および伝送能率の点では*ARQ* 方式の方にすぐれているものが多く，したがって*ARQ* 方式はフィードバック通信路を利用できる短距離通信に適し，誤り訂正方式は実時間処理が要求される場合や長距離通信に適していることを

示した．

第5章では従来のシフトレジスタを用いて構成された畳み込み符号の有する，同期引き込みの困難さおよび大きな誤りにおかされた後の復号の困難さという欠点を改善できるフィードバック・シフトレジスタを用いた符号化法を示した．

この方法によれば，従来の同じ段数のシフトレジスタを用いた方法に比べて確率的に拘束長を増大でき，結局誤り訂正能力を増大することができる．

また畳み込み符号については，ハードウエアとソフトウエアを巧みに結合することにより，逐次復号法におけるオーバーフローの問題を解決できるものが今後望まれるであろう．

謝　　辞

本研究の全過程を通じ直接ご指導を賜った笠原芳郎教授に心よりお礼申し上げる．

大学院修士および博士課程においてご指導，ご教示賜った通信工学教室の熊谷三郎名誉教授，青柳健次教授，板倉清保教授，滑川敏彦教授，電子工学教室の尾崎弘教授，基礎工学部の嵩忠雄教授，牧本利夫教授，産業科学研究所の加藤金正教授ならびに松尾幸人教授に対し厚くお礼申し上げる．

また終始懇切にご指導，ご助言下さった手塚慶一助教授に深謝する．

筆者の属する笠原研究室の笠原正雄助手には特に熱心なご討論，ご教示をいただいた．また凌舜堂助手，真田英彦助手には適切なご助言をいただいた．筆者と同じく符号理論およびデータ伝送を研究されている中西暉助手，大学院学生の浅部勉氏，山崎文昭氏には熱心なご討論をいただいた．また笠原研究室の大学院学生諸氏，および本学卒業生の宮崎順介氏，石田真也氏，高橋修氏，花房慎吾氏には研究途上ご協力いただいた．また京都大学の長谷川利治助教授，大阪大学基礎工学部の豊田順一助教授，北橋忠宏助手には有益なご助言をいただいた．さらに近畿大学の梶谷浩二講師，大阪府立大学の田中初一助手，大阪科学技術センターの中島節夫氏には特にお世話になった．ここに記して以上の方々に深く感謝の意を表する．

文　　献

(1) E.N.Gilbert: "Capacity of a burst-noise channel", Bell Syst. Tech.J., 39, p. 1253 (Sept. 1960).

(2) M.Horstein: "Efficient communication through burst-error channels by means of error detection", IEEE Trans., COM-14, p.117 (April 1966).

(3) 藤原，中西，笠原(正)，手塚，笠原(芳)："バースト誤りを生ずる通信路に関する二，三の考察"，信学会インホメーション理研資，IT67-33 (1967-09).

(4) 藤原，中西，笠原(正)，手塚，笠原(芳)："バースト誤りを生ずる通信路とその信頼度の改善に関する考察"，信学誌，51-A，8，p.311 (昭43-08).

(5) 藤原，中西，笠原(正)，手塚，笠原(芳)，石田："バースト誤り訂正符号の最適符号長"，信学会インホメーション理研資 (1965-11).

(6) C.E.Shannon and W.Weaver: "The mathematical theory of communication", University of Illinois Press, Urbana (1949).

(7) R.W.Hamming: "Error detecting and error correcting codes", Bell Syst.Tech.J., 29, p.147 (1950).

(8) E.Prange: "Cyclic error-correcting codes in two symbols", AFCRC-TN-57-103, Air Force Cambridge Research Center, Cambridge, Mass. (Sept. 1957).

(9) N.M.Abramson: "Error correcting codes from linear

sequential circuits", the fourth London symposium of information theory, p.26 (August 1960).

(10) P.Fire:"A class of multiple-error-correcting binary codes for non-independent errors", Sylvania Electric Products Inc., Mt. View, Calif.Rept., RSL-E-2 (March 1959).

(11) 嵩:"独立でない誤りを訂正するある組織符号系について", 情報処理, 1, p.132 (1960).

(12) C.M.Melas:"A new group of codes for correction of dependent errors in data transmission", IBM J. Res. Dev., 4, p.58 (1960).

(13) S.H.Reiger:"Codes for the correction of clustered errors", IRE Trans., IT-6, p.16 (1960).

(14) J.E.Meggitt:"Error correcting codes for correcting burst of errors", IBM J. Res. Dev., 4, p.329 (1960).

(15) B.Elspas and R.A.Short:"A note on optimum burst-error correcting codes", IRE Trans., IT-8, p.39 (1962).

(16) 嵩:"密集した誤りを訂正する巡回的組織符号", 信学誌, 45, 1, p.9 (昭37-01).

(17) 笠原(正), 笠原(芳):"単一および二重のバースト誤り訂正符号の一構成法", インホメーション理研資 (1964-12).

(18) 藤原, 笠原(正), 手塚, 笠原(芳):"バースト誤り訂正符号の一構成法", 信学会インホメーション理研資, IT69-04 (1969-04).

(19) 藤原，笠原(正)，手塚，笠原(芳)：“バースト誤り訂正符号の一構成法”，信学誌投稿中.

(20) 藤原，中西，笠原(正)，手塚，笠原(芳)：“巡回符号の最適符号長に関する一考察”，信学全大（昭39－11）.

(21) 藤原，中西，笠原(正)，手塚，笠原(芳)：“バースト誤り訂正符号の最適符号長に関する考察”，信学全大（昭40－11）.

(22) R.J.Benice and A.H.Frey,Jr.：“An analysis of retransmission systems”, IEEE Trans., COM－12, p.135 (Dec. 1964).

(23) 中西，笠原(正)，手塚，笠原(芳)，藤原，富田：“誤り検出自動再送要求方式の解析”，信学会通信方式研資（1965－05）.

(24) 中西，藤原，笠原(正)，手塚，笠原(芳)：“誤り検出自動再送要求方式の解析”，信学誌，50，6，p.1013（昭42－06）.

(25) 中西，木谷，笠原(正)，手塚，笠原(芳)，藤原：“誤り訂正機能および位置情報を有するARQ 方式の解析”，信学会通信方式研資（1967－01）.

(26) 中西，木谷，藤原，笠原(正)，手塚，笠原(芳)：“誤り検出自動再送要求方式（Dual－RQ方式）の解析”，信学会通信方式研資，CS67－20（昭42－09）.

(27) P.Elias：“Coding for noisy channels”, IRE Convention Record, pt. 4, p.37 (1955)

(28) J.L.Massey：“Threshold decoding”, MIT and Wiley (1963).

(29) J.P.Robinson：“An upper bound on the minimum dist-

ance of a convolutional code", IEEE Trans., IT-11 p.567 (Oct. 1965).

(30) D.W.Hagelbarger : " Recurrent codes : easily mechanized burst correcting, binary codes", Bell Syst. Tech.J., 38, p.969 (July 1959).

(31) J.M.Wozencraft and J.M.Jacobs : " Principle of communication engineering", Wiley (1965).

(32) 藤原, 高橋, 笠原(正), 手塚, 笠原(芳) : " Convolutional Code に関する研究(I)符号化", 信学全大 (昭43-10).

(33) 高橋, 藤原, 手塚, 笠原(芳) : " Convolutional 符号の構成に関する一考察", 信学会インホメーション理研資, IT68-64 (1969-03).

(34) 藤原, 高橋, 手塚, 笠原(芳) : " フィードバックシフトレジスタを用いた畳み込み符号の一構成法", 信学誌投稿中.

(35) W.W.Peterson : " Error correcting codes", MIT and Wiley (1961).

(36) B.Elspas : " The theory of autonomous linear sequential networks", IRE Trans., CT-6, p.45 (March 1957).

(37) W.Feller : " An introduction to probability theory and its application", John Wiley and Sons (1959).

(38) 笠原(正), 笠原(芳) : " バースト誤りを訂正する巡回符号に関する考察", 信学誌, 47, 4, p.182 (昭39-04).

(39) J.M.Wozencraft and B.Reiffen : " Sequential decoding", MIT and Wiley (1961).

(40) J.J.Bussgang: "Some properties of binary convolutional code generators", IEEE Trans., IT-11, p. 90 (Jan. 1965).

(41) W.H.Kautz: "Fibonacci codes for synchronization control", IEEE Trans., IT-11, p.284 (April 1965).

付　　録

1．一つの状態Bの中で長さkのバースト誤りが生じる確率を$P_B(k)$とすると

$$P_B(1)=\sum_{i=1}^{\infty} i\,(1-h)\,h^{i-1}q^{i-1}p=\frac{(1-h)p}{(1-hq)^2} \tag{A1.1}$$

$$P_B(k)=\sum_{i=1}^{\infty} i\,(1-h)^2 h^{i-1}q^{k-2+i}p=\frac{(1-h)^2pq^{k-1}}{(1-hq)^2};\ k\geqq 2 \tag{A1.2}$$

と表わせる．したがって

$$\bar{B}'=\sum_{k=1}^{\infty} kP_B(k)=\frac{(1-h)p}{(1-hq)^2}\left(h+\frac{1-h}{p^2}\right) \tag{A1.3}$$

となり，式（2．2．a）が得られる．

2．図3．3に示す二つの$F.S.R.$を巡回シフトして図3．4のようにすると，$F.S.R.$ Ⅰの最後尾の長さ（$c-b+1$）の00・・・01の連および$F.S.R.$ Ⅱの中の最後尾の長さ（$c'-b+1$）の00・・・01の連が二つの$F.S.R.$の中間部に入ることになる．そのような状態で二つの$F.S.R.$の内容が一致するためには，バースト誤りの中に長さ（$c-b+1$）および（$c'-b+1$）なる00・・・01の連が同時に少なくとも一つ存在しなければならない．したがって長さbのバースト誤りが訂正不能となるためには

$$\begin{aligned} b &\geqq c-b+1+c'-b+1+1 \\ &= c+c'+2-2b \end{aligned} \tag{A2.1}$$

なる条件を満足することが必要である．これを解くとbは整数であるから

$$b \geqq \left[\frac{c+c'}{3}\right]^{*}+1 \qquad \text{(A2.2)}$$

の場合にのみ訂正不能の誤りが生じる可能性がある．

3．長さiの単一バースト誤りにおかされた大ブロックの中で，誤りにおかされていない小ブロック数をM_i'とすると

$$M_b=\sum_{i=b+1}^{n} M_i' \qquad \text{(A3.1)}$$

と表わせる．また

$$P_n(i)=F_n(i)-F_n(i-1) \qquad \text{(A3.2)}$$

とするとM_i'とM_{i+1}'との間には明らかにつぎの関係が成り立つ．

$$M_{i+1}' \cong M_i' \frac{P_n(i+1)}{P_n(i)} \cdot \frac{n-(i+1)}{n-i} \qquad \text{(A3.3)}$$

したがって，式(A3．1)はつぎのように変形できる．

$$M_b \cong \sum_{i=b}^{n-1} M_i' \frac{P_n(i+1)}{P_n(i)} \cdot \frac{n-(i+1)}{n-i} \qquad \text{(A3.4)}$$

$b \ll n$とし，bの近辺にiをとると

$$\frac{n-(i+1)}{n-i} \cong \frac{n-(b+1)}{n-b} \cdot \frac{P_n(i+1)}{P_n(i)}$$

$$\cong \frac{P_n(b+1)}{P_n(b)}$$

＊ 〔 〕はガウスの記号である．

となる．$j \gg b$ なる j に対して $P_n(j) \ll P_n(b)$ であり，一般に

$$\frac{a}{b} = \frac{c}{d}$$

なら

$$\frac{a}{b} = \frac{a+c}{b+d}$$

となるから

$$\frac{P_n(i+1)}{P_n(i)} \cong \frac{P_n(b+1)}{P_n(b)}$$

$$\cong \frac{P_n(b+1)+P_n(b+2)+\cdots+P_n(n)}{P_n(b)+P_n(b+1)+\cdots+P_n(n)}$$

$$= \frac{1-F_n(b)}{1-F_n(b-1)} \tag{A3.5}$$

となる．またこのような値の j に対しては $M_j' \ll M_b'$ となり，式（A3．4）においてこのようなものを含む項は M_b の値に殆んど寄与しない．したがって

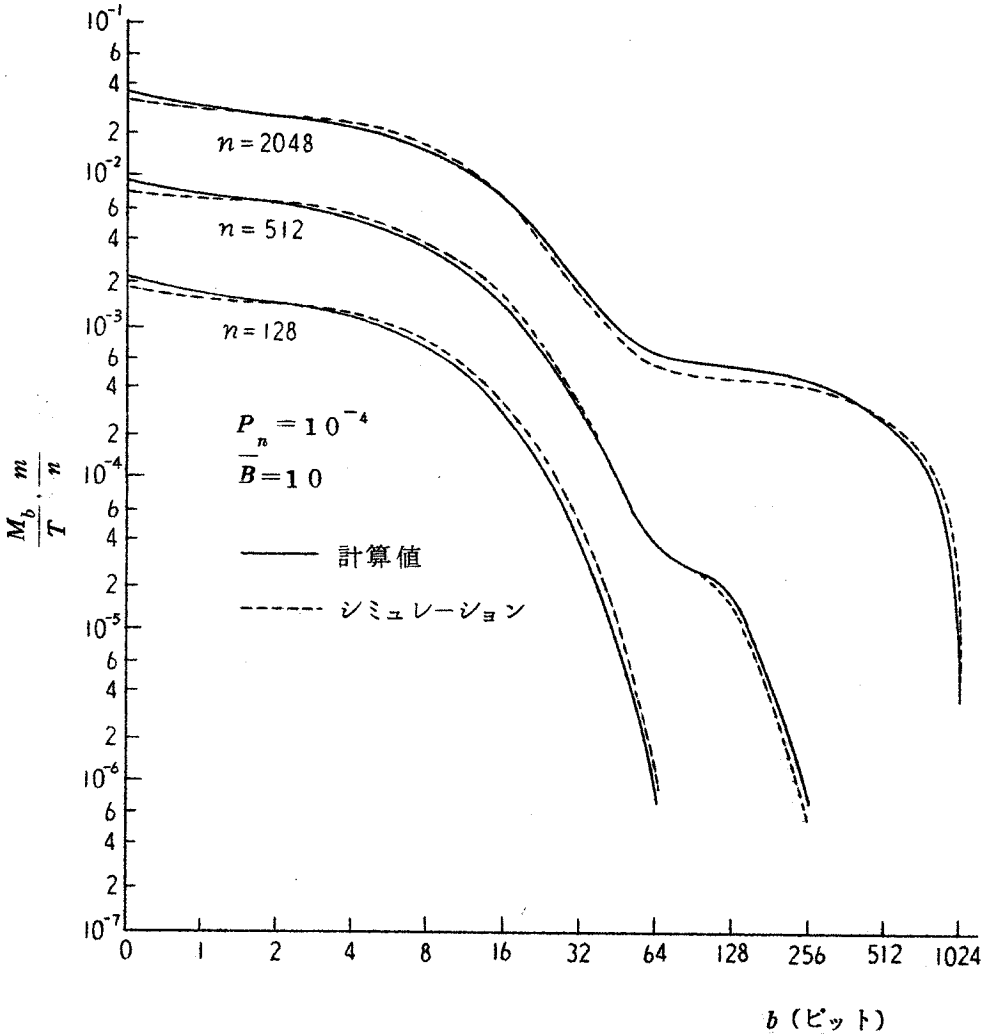
$$M_b \cong \frac{1-F_n(b)}{1-F_n(b-1)} \cdot \frac{n-(b-1)}{n-b} \sum_{i=b}^{n} M_i'$$

$$= M_{b-1} \frac{1-F_n(b)}{1-F_n(b-1)} \cdot \frac{n-b-1}{n-b} \tag{A3.6}$$

が得られ，この漸化式を解くと

$$M_b \cong M_0 \frac{1-F_n(b)}{1-F_n(0)} \cdot \frac{n-b-1}{n-1} \tag{A3.7}$$

が得られ，式（４．８）が求められる．なお，式（４．８）により求めた $mM_b/(nT)$ と，シミュレーションにより求めた $mM_b/(nT)$ とを図Ａ３．１に示す．



図Ａ３．１　式（４．８）による $mM_b/(nT)$ とシミュレーションによる $mM_b/(nT)$ ．