The University of Osaka
Institutional Knowledge Archive

Title	縦接符号化法を用いた誤り制御通信方式およびその性能評価に関する研究
Author(s)	高田, 豊雄
Citation	大阪大学, 1989, 博士論文
Version Type	VoR
URL	https://hdl.handle.net/11094/1627
rights	
Note	

The University of Osaka Institutional Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/

The University of Osaka

縦接符号化法を用いた
誤り制御通信方式および
その性能評価に関する研究

１９８９年１月

高田　豊雄

縦接符号化法を用いた
誤り制御通信方式および
その性能評価に関する研究

1989年1月

高田　豊雄

内容梗概

本論文は，筆者が大阪大学大学院基礎工学研究科（物理系情報工学分野専攻）に在学中，嵩研究室において行なった符号理論とその応用に関する研究のうち，縦接符号化法の誤って復号される確率や，復号失敗確率，及び，縦接符号による誤り訂正と検査記号の再送を組み合わせた誤り制御通信方式の性能評価に関する研究をまとめたものである．

第１章では，まず，内部符号に２元線形符号を用いた縦接符号化法について述べる．次に，その符号化法で構成された符号を，２元対称通信路で用いた場合の，誤って復号される確率の，かなりよい上界と，正しく復号される確率の正確な値を効率よく計算する方法について述べる．また，いくつかの具体例について，実際に誤って復号される確率の上界の値と正しく復号される確率の正確な値を計算し，それらの例が衛星通信に適していることを示した．

第２章では，内部符号にブロック変調符号を用いた縦接符号化法について述べる．この章では，まず縦接符号の内部符号に適したM値位相変調用ブロック変調符号の構成法について述べる．次に，縦接符号の構成法と，それを加法的白色ガウス雑音をもつ通信路で用いた場合の誤って復号される確率や復号に失敗する確率の評価法について述べる．更に，いくつかの具体例を提案し，それらの確率の値を計算した．それらの例が高い伝送効率と高信頼度を要求される衛星通信に適していることを示した．

第３章では，第１，２章で述べた縦接符号による誤り訂正と，検査記号の再送を組み合わせた誤り制御通信方式の１方式について考察する．この章では，まず，ここで取り上げる通信方式の誤り訂正

方式と再送方式について述べる．次に，第１章の誤り確率の解析方法を利用して，ここで取り上げた通信方式の誤り特性と伝送効率特性の解析方法を示す．更に，第１，２章の具体例で用いた内部符号と同じ符号を内部符号に用いたいくつかの具体例を提案し，それらが比較的雑音の多い通信路（例えば，１信号点当りの信号対雑音比が7.8dBの加法的白色ガウス雑音をもつ通信路）においても高信頼性と高伝送効率を満足し，雑音状態が変動しやすい通信路における衛星通信に適していることを示した．

縦接符号化法を用いた
誤り制御通信方式および
その性能評価に関する研究

目　次

緒論 …… 5

関連発表論文 …… 9

第１章　ある縦接符号化法の誤って復号される確率の上界と
正しく復号される確率の計算法

第１節　序言 …… 11

第２節　内部符号に基づく復号の解析 …… 18

第３節　誤って復号される確率の上界の値と
正しく復号される確率の値の計算法 …… 25

第４節　縦接符号化方式の例 …… 28

第５節　結言 …… 43

第２章　変調符号を内部符号に用いた縦接符号化方式

第１節　序言 …… 44

第２節　Ｍ値位相変調用ブロック変調符号 …… 46

第３節　変調符号を内部符号に用いた
縦接符号化方式の符号化法と復号法 …… 60

第４節　誤り特性の解析 …… 62

第５節　変調符号を内部符号に用いた
縦接符号化方式の具体例 …… 67

第６節　結言 …… 92

第３章　縦接符号化法を誤り訂正に用いたある誤り制御通信方式

第１節　序言 …… 93

第２節　誤り訂正方式 …… 95

第３節　再送方式 …… 99

第４節　性能解析 …… 103

第５節　いくつかの具体例の特性解析 …… 110

第６節　結言 …… 121

結論 …… 122

謝辞 …… 124

文献 …… 125

付録 …… 128

緒　論

本論文では，縦接符号化法による符号の構成法と，その符号を2元対称通信路（内部符号に2元線形符号を用いた場合）や加法的白色ガウス雑音をもつ通信路（内部符号にブロック変調符号を用いた場合）で用いたときの，誤って復号される確率や正しく復号される確率の計算法，及び，縦接符号による誤り訂正と検査シンボルの再送を組み合わせた誤り制御通信方式と，その誤り特性や，伝送効率（スループット）特性の解析法について述べている．

2種類の符号を用いて2段階の符号化を行ない新しい符号を構成する方法については，いろいろな方法があり，これまで多くの研究がなされてきた．それらの符号化法は，長い符号長を有する符号を比較的短い符号を組み合わせて構成することにより，復号を相対的に単純なステップの系列に分解できることから，同程度の符号長，同程度の誤り訂正能力を持つ単一の符号と比較して復号を容易に行なうことができるという実用上重要な特徴がある．

縦接符号化法は，それらの符号化法のうちの1つであり，衛星通信やスペースクラフト（惑星，及び深宇宙探査船）の通信等において，高信頼性と高伝送効率が要求される局面の誤り制御方式に，しばしば用いられている．特に，縦接符号を2元対称通信路や加法的白色ガウス雑音をもつ通信路で用いた場合の誤って復号される確率や正しく復号される確率を求めることは，実用上非常に重要である．

本論文で取り上げる縦接符号化法は，内部符号，外部符号共にブロック符号を用い，外部符号は一般の線形符号（非2元線形符号，例えば有限体GF(2^{ℓ})上の線形符号を含む）とし，誤り訂正と検出の両方を行ない，インターリービングが施されるものとする．

第１章では，内部符号に２元線形符号を用いた縦接符号化法を２元対称通信路で用いた場合の誤って復号される確率や正しく復号される確率を求める問題を関連発表論文の(1)～(3)を中心にまとめられている．もちろん，内部符号と外部符号を合わせた縦接符号を１つの線形符号とみなして，その符号，または，その双対符号の重み分布を求めることにより，それらの確率の値を求めることは，原理的には可能である．しかし，実用的なパラメータをもつ縦接符号では，一般に，情報点数，検査点数が大きいので，その方法を用いることは計算時間がかかりすぎるため困難である．また，縦接符号化法の部分クラスである，

１．外部符号はインターリービングを施さない，

２．外部符号による復号では誤り検出のみを行ない，誤り訂正を行なわない，

ような符号化方式については，２元対称通信路における正しく復号される確率と誤り見逃し確率の正確な値を実用的なパラメータをもつ符号に対して過大でない時間で計算する方法が知られている．しかし，本論文では，１や２の制限がない場合を考えているため，その方法の拡張により，それらの確率の値を計算することは困難である．

そのため，ここでは，ここで取り上げる縦接符号化方式を２元対称通信路で用いたときの，誤って復号される確率の，かなりよい上界と，正しく復号される確率の正確な値を計算する方法を新たに示した．その方法では，内部符号による復号によって生じる誤りパターンに関する，いくつかの確率が必要となる．ここでは，まずそれらの確率の定義と導出法を示し，次に，縦接符号全体の誤って復号される確率の上界と，正しく復号される確率の計算法を示す．そし

て，この符号化方式のいくつかの具体例について，それらの確率の値を計算した．その結果，それらの例の誤って復号される確率の値は，通信路が雑音の多い場合でも（例えばビット誤り率が10^{-3}から，1/2の間の値であっても），十分低い値（例えば，10^{-8}以下）であることがわかった．それらの具体例は衛星通信やスペースクラフトの通信のダウンリンク（衛星等から地上へ向けた通信）の誤り制御に適している．

近年，宇宙通信における狭帯域化に対する要求が強くなりつつある．そのため，帯域幅を広げることなく符号化利得を稼ぐための手法として，変調符号が盛んに研究されている．しかし，変調符号の符号化利得を大きくすると，復号器の複雑度と復号時間が共に指数的に増加することから，あまり複雑な変調符号を用いることは困難であり，変調符号単独で用いると，その使用場面によっては信頼性や伝送効率に対する要求が，完全に満足されない場合がある．そこで，内部符号に比較的符号長も短く，復号も容易な変調符号を用いて，外部符号に従来の線形ブロック符号を用いた縦接符号化法を用いることにより，外部符号の使用に伴うわずかな帯域拡大の犠牲の下で，大きな符号化利得を得ることを考える．

第２章では，内部符号にブロック変調符号を用いた縦接符号化法について，関連発表論文(4)～(8)を中心に述べる．この章では，まず縦接符号の内部符号に適したM値位相変調用ブロック変調符号の構成法について述べる．次に，縦接符号の構成法と，それを加法的白色ガウス雑音をもつ通信路で用いた場合の誤って復号される確率や復号に失敗する確率の評価法について述べる．それらの評価法は基本的には第１章で述べた手法を用いる．但し，内部符号による復号によって生じる誤りパターンに関する，いくつかの確率について

は，シミュレーションによる評価と，上界式に基づく評価を用い，縦接符号全体の誤って復号される確率や復号に失敗する確率の計算式の導出は，第1章の方法を用いる．更に，いくつかの具体例を提案し，それらの確率の値を計算した．それらの例が高伝送効率と高信頼度を要求される衛星通信に適していることを示した．

第3章では，縦接符号化法を用いた誤り制御通信方式の1方式とその性能評価法について，関連発表論文(9)～(11)を中心にまとめられている．ここで取り上げる通信方式は縦接符号による誤り訂正と，最初に送信したデータが復号に失敗したときに，より強力な誤り訂正を行なうための検査記号の再送とを組み合わせたものである．この章で取り上げる縦接符号化法の内部符号には，第1章で用いた2元線形ブロック符号と第2章で用いたブロック変調符号の両方を考える．この章では，まず，ここで取り上げる通信方式の誤り訂正方式と再送方式について述べる．次に，第1章で述べた縦接符号化方式の誤って復号される確率の上界と，正しく復号される確率の計算法を利用して，ここで取り上げた通信方式を加法的白色ガウス雑音をもつ通信路で用いたときの誤り特性と伝送効率特性の解析方法を示す．更に，第1，2章の具体例で用いた内部符号と同じ符号を内部符号に用いたいくつかの具体例を提案し，それらが比較的雑音の多い通信路（例えば，1信号点当りの信号対雑音比が7.2dBの加法的白色ガウス雑音をもつ通信路）においても高信頼性（例えば，誤って復号される確率は10^{-8}以下）と高い伝送効率（例えば，誤り訂正に用いる縦接符号のレートの1/2以上）を満足し，雑音状態が変動しやすい通信路における衛星通信に適していることを示した．

関連発表論文

(1) T. Kasami, T. Fujiwara, T. Takata and S. Lin: "A Cascaded Coding Scheme for Error Control and its Performance Analysis", IEEE Transactions on Information Theory, Vol. IT-34, No. 3, pp. 448-462 (May 1988).

(2) 高田，藤原，嵩，Lin: "ある縦接符号化法の誤って復号される確率の上界と正しく復号される確率の計算法"，電子情報通信学会誌（A）（掲載予定）.

(3) S. Lin, T. Kasami, T. Takata and T. Fujiwara: "An Interleaved Error Control Coding Scheme for Satellite and Space Communications", Conference Record of IEEE/IEICE Global Telecommunications Conference 1987, Vol.1, pp.292-296 (November 1987).

(4) T. Kasami, T. Takata, T. Fujiwara, S. Lin and D. J. Costello, Jr.: "Cascaded Coding for Error Control", Proceedings of 1988 Beijing International Workshop on Information Theory, pp. E-1.1 - E-1.4 (July 1988).

(5) T. Kasami, T. Takata, T. Fujiwara and S. Lin: "A Concatenated Coded Modulation Scheme for Error Control", Proceedings of IEEE Global Telecommunications Conference (November 1988).

(6) T. Kasami, T. Takata, T. Fujiwara and S. Lin: "A Concatenated Coded Modulation Scheme for Error Control", IEEE Transactions on Communications（投稿中）.

(7) S. Ujita, T. Takata, T. Fujiwara, T. Kasami and S. Lin: "Structural Properties of 2^{ℓ}-ary PSK Modulation Block Codes and their Performance Analysis", 第11回情報理論とその応用シンポジウム予稿集, pp. 807-812 (1988年12月).

(8) T. Kasami, T. Takata, T. Fujiwara and S. Lin: "On Construction of Bandwidth Efficient Block Codes", IEEE Transactions on Information Theory (投稿中).

(9) T. Takata, T. Fujiwara, T. Kasami and S. Lin: "A Cascaded Error Control System with Parity Retransmissions", 第10回情報理論とその応用シンポジウム予稿集, pp. 387-392 (1987年11月).

(10) T. Takata, T. Fujiwara, T. Kasami and S. Lin: "Performance Analysis of a Coding Scheme with Multiple-Stage Forward Error Corrections", 第11回情報理論とその応用シンポジウム予稿集, pp. 813-818 (1988年12月).

(11) T. Takata, T. Fujiwara, T. Kasami and S. Lin: "An Error Control System with Multiple-Stage Forward Error Corrections", IEEE Transactions on Communications (投稿中).

第１章　ある縦接符号化法の誤って復号される確率の上界と正しく復号される確率の計算法

１．序言

２つの符号を組み合わせて符号化を行なう方法は，これまで多くの研究がなされている[1-5]．この章で扱う縦接符号化法は内部符号，外部符号と呼ばれる２つの線形ブロック符号を用いる．内部符号C_1は最小距離d_1の２元(n_1, k_1)符号である．内部符号はt_1個以下の誤り訂正とλ_1（但し，$\lambda_1 \geqq t_1$，$t_1+\lambda_1+1 \leqq d_1$）個以下の誤り検出を行うことができるものとする．外部符号C_2は有限体$GF(2^\ell)$上の最小距離d_2の(n_2, k_2)符号である．本論文では，$GF(2^\ell)$の適当な基底を用いて，その体の各元を長さℓのビット列で表すものとし，対応するビット列を以下，シンボルと呼ぶ．従って，外部符号は，２元$(n_2\ell, k_2\ell)$符号とみなすこともできる．この符号化法では，k_1，ℓの間にm_1を正整数として次の条件が成立するものとする．

$$k_1 = m_1\ell \tag{1}$$

符号化は図１に示す様に２段階で行う．

(1)　第１段階では$k_2 \times k_1 (=k_2 m_1 \ell)$ビットの通報を図２に示す様に縦$k_2$，横$m_1\ell$の格子状に配置する．$k_2$個の各行それぞれを$m_1$個の長さ$\ell$のビット列に分割する．各$\ell$ビットを$GF(2^\ell)$の元（シンボル）とみなし，縦方向$k_2$個のシンボル列（以下，セクションと呼ぶ）それぞれを外部符号C_2で符号化する．

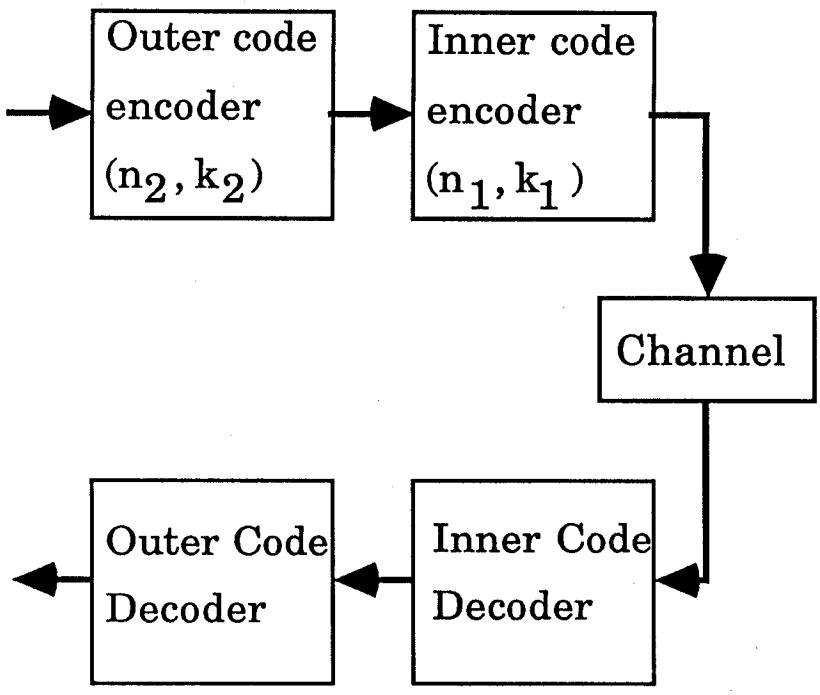
Outer code
encoder
(n_2, k_2)
Inner code
encoder
(n_1, k_1)
Channel
Inner Code
Decoder
Outer Code
Decoder

図1　縦接符号化方式

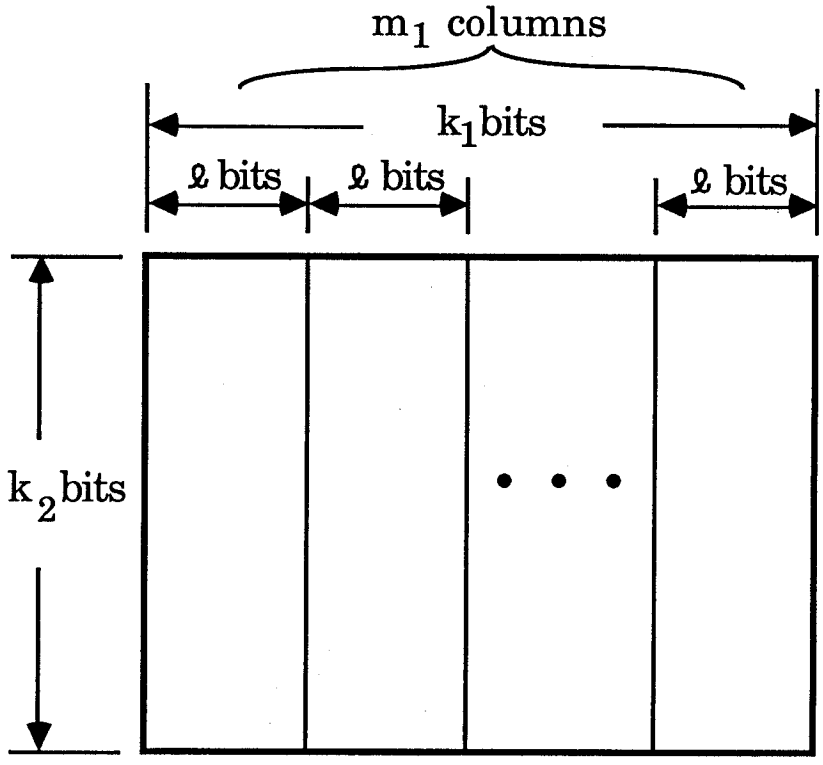

図2 通報の配置方法

(2) 第2段階では第1段階で得られたn_2個の長さ$m_1\ell$の各行ベクトルを（それぞれの行をセグメントと呼び，セグメント中のm_1個のシンボルを左から順に1番目，2番目，…，m_1番目のシンボルという）内部符号C_1で符号化する．内部符号の符号語に対応する長さn_1の行ベクトルをフレームと呼ぶ．得られたn_2個のフレームを順に送信する．このn_2個のフレームの系列をブロック（図3参照）と呼ぶ．

次に復号方法について述べる．このように2つの符号を組み合わせて用いる方式の復号方法としては，いろいろな方法が検討されているが[1,4]，本論文では次の様な2段階の復号方法を考える．

(1) 第1段階では，まず受信された各フレームについて内部符号に基づいてシンドロームを計算し，次のいずれかを行なう．

(1.1) シンドロームがt_1個以下の誤りパターンeに対応するものならば，受信されたフレームにその誤りパターンeを加えることにより誤りを訂正し，その情報ビットの部分（以下，復号後のセグメントと呼ぶ）を，外部符号の復号バッファに送る．この場合，正しく訂正したか否かにかかわらず，そのフレームは復号に成功したという．復号に成功したフレームのセグメントをマークのないセグメントと呼ぶ．

(1.2) シンドロームが，t_1個を越える誤りパターンに対応する場合，そのフレームは復号に失敗したといい，次のいずれかを行う．

(a) 消去操作：そのセグメントを消去する．

(b) マーク付け操作：全く訂正を行わずに，フレームの情報ビット部分だけを，そのまま外部符号の復号バッファに送る．そのセグメントをマーク付きセグメントと呼ぶ．

いずれの場合も，そのセグメントでt_1個を越える誤りが発生したことを外部符号の復号器に伝達する．

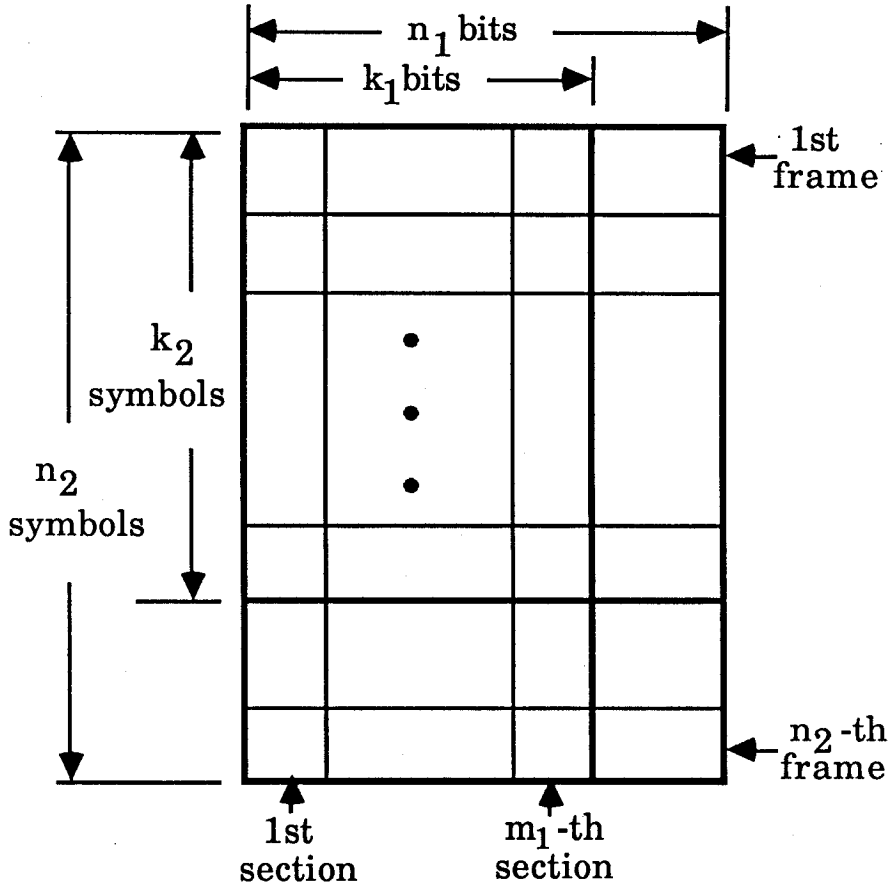
n1 bits
k1 bits
1st
frame
k2
symbols
n2
symbols
n2 -th
frame
1st
section
m1 -th
section

図3　ブロックの形式

(2) 第2段階では外部符号に基づき，シンボル誤りとシンボル消去の訂正を行う．予め，d_2-1以下の非負整数T_{es}と，各$0 \leqq i \leqq T_{es}$に対して，$(d_2-1-i)/2$以下の非負整数$T_{e\ell}(i)$，$t_2(i)$が定められているとする．

(2.1) 消去されたセグメントの個数iが，T_{es}を越えるか，マーク付きセグメントの個数hが$T_{e\ell}(i)$を越えるときには，そのブロック全体を消去する．

(2.2) (2.1)以外のとき，ブロックの各セクション毎に外部符号に基づいて計算したシンドロームが，i個のシンボル消去と$t_2(i)$個以下のシンボル誤りに対応するならば，それらの訂正を行う．そうでなければ，ブロック全体を消去する．

すべてのセクションが正しく復号されたとき，そのブロックは正しく復号されたという．逆に，セクションが1つでも誤って復号されたとき（または，復号に失敗したとき），ブロックは誤って復号された（または，復号に失敗した）という．

以下，この章では，通信路として2元対称通信路を考える．

この章では，以上述べたような縦接符号化法の，正しく復号される確率P_cの値と誤って復号される確率P_{er}の値の計算法を考える．もちろん，内部符号と外部符号を合わせた縦接符号を1つの線形符号とみなして，その符号，または，その双対符号の重み分布を求めることにより，それらの確率の値を求めることは，原理的には可能である．しかし，実用的なパラメータをもつ縦接符号では，一般に，情報点数，検査点数が大きく，その方法を用いることは計算時間がかかりすぎるため困難である．また，文献(5)では，縦接符号化法の部分クラスである，

1．外部符号はインターリービングを施さない，

2．外部符号による復号のでは誤り検出のみを行ない，誤り訂正を行なわない，

ような符号化方式については，2元対称通信路における正しく復号される確率と誤り見逃し確率の正確な値を実用的なパラメータをもつ符号に対して過大でない時間で計算する方法が示されている．しかし，本論文では，1や2の制限がない場合を考えているため，文献(5)の方法の拡張により，それらの確率の値を計算することは容易ではない．

ここでは，縦接符号化法の，正しく復号される確率P_cの正確な値と誤って復号される確率P_{er}の値の上界の値の計算法を新たに導出する．それらの計算法では，セグメントの特定のシンボル位置の誤りパターンに着目したいくつかの確率が必要となる．第2節で，それらの確率の計算法を示す．第3節で P_cの値とP_{er}の上界の値の計算法を示す．第4節で，内部符号に様々なレートの符号（最も高いもので0.873，最も低いもので0.188）を用いた縦接符号の具体例に対する正しく復号される確率P_cの値と誤って復号される確率P_{er}の上界の値の計算結果を示す．それらの符号例は衛星通信（内部符号に高レートの符号を用いた場合），及び，スペースクラフト（惑星及び深宇宙探査船）の通信（内部符号に低レートの符号を用いた場合）の誤り制御への応用が考えられる．さらに，内部符号に基づく復号段階でシンドロームがt_1個を越える誤りに対応する場合の操作として，消去操作のみを行ったときとマーク付け操作のみを行ったときの，それらの確率の値の比較について考察する．

2．内部符号に基づく復号の解析

この節では第1節で述べた符号化方式をビット誤り率εの2元対称通信路で用いたときの内部符号に基づく復号について解析を行う．$P_c^{(1)}$，$P_{ic}^{(1)}$をそれぞれ受信フレームが正しく復号される確率，誤って復号される確率とする．$P_c^{(1)}$は次の式で与えられる．

$$P_c^{(1)} = \sum_{i=0}^{t_1} \binom{n_1}{i} \varepsilon^i (1-\varepsilon)^{n_1-i} \tag{2}$$

また，$P_c^{(1)}$，$P_{ic}^{(1)}$について次の式が成立する[6]．

$$P_c^{(1)} + P_{ic}^{(1)}$$

$$= \sum_{i=0}^{n_1} A_i^{(1)} \sum_{j=0}^{n_1} \sum_{s=0}^{t_1} W_{j,s}^{(i)}(n_1) \varepsilon^j (1-\varepsilon)^{n_1-j} \tag{3}$$

$$= 2^{-r_1} \sum_{i=0}^{n_1} B_i^{(1)} (1-2\varepsilon)^i P_{t_1}(i-1, n_1-1) \tag{4}$$

但し，$A_i^{(1)}$，及び，$B_i^{(1)}$はそれぞれ2元重みiのC_1，及び，その双対符号の符号語の個数であり，$W_{j,s}^{(i)}(n)$は長さnの重みiの1つの2元ベクトルに対して，そのベクトルからの距離がsで，重みがjのベクトルの個数である．また，$P_s(\cdot,\cdot)$はKrawtchoukの多項式である[7]．

$P_{es}^{(1)}$および$P_{e\ell}^{(1)}$をそれぞれ受信セグメントが消去される確率，セグメントにマークが付けられる確率とすれば次の式が成立する．

$$P_{es}^{(1)} + P_{e\ell}^{(1)} + P_c^{(1)} + P_{ic}^{(1)} = 1 \tag{5}$$

式(3)または(4)と(5)を用いれば，$P_{es}^{(1)}$または$P_{e\ell}^{(1)}$のどちらか一方の値がわかれば，他方の値を求めることができる．いま内部符号に基づく復号段階でt_1個以上の誤りが検出されたらそのセグメントを必ず消去すると仮定すれば$P_{e\ell}^{(1)}=0$であり，そのセグメントに必ずマーク付け操作を行うと仮定すれば$P_{es}^{(1)}=0$であるから，それらの場合には，$P_{es}^{(1)}$，$P_{e\ell}^{(1)}$の値を求めることができる．

次に，特定のシンボル位置に与えられた誤りパターンが起こる確率の計算法について述べる．αを$GF(2^{\ell})$の元とする．$p_{e\ell}(u,\alpha)$（または$p_e(u,\alpha)$）をそれぞれ，あるセグメントがマーク付きセグメントとなり　（または，復号に成功し）かつ，そのセグメントのu番目のシンボル位置の誤りシンボルがαとなる確率とする．

$p_{e\ell}(u,\alpha)$について次の等式が成立する（証明は付録Aに示す）．

$$
\begin{aligned}
& p_{e\ell}(u,\alpha) \\
&= \varepsilon^{|\alpha|}(1-\varepsilon)^{\ell-|\alpha|} \\
&\quad - \sum_{i=0}^{n_1-\ell} \sum_{\substack{\beta\in GF(2^{\ell}) \\ |\alpha-\beta|\le t_1}} A_i^{(1)}(u,\beta) \sum_{j=0}^{n_1-\ell} \sum_{s=0}^{t_1-|\alpha-\beta|} \\
&\quad W_{j,s}^{(i)}(n_1-\ell)\ \varepsilon^{j+|\alpha|}(1-\varepsilon)^{n_1-j-|\alpha|} \qquad (6) \\
&= \varepsilon^{|\alpha|}(1-\varepsilon)^{\ell-|\alpha|}\ \{ \\
&\quad 1 - 2^{-r_1} \sum_{h=0}^{n_1-\ell} \sum_{\gamma\in GF(2^{\ell})} B_h^{(1)}(u,\gamma)\ (1-2\varepsilon)^h
\end{aligned}
$$

$$\sum_{\substack{\beta \in GF(2^{\ell}) \\ |\alpha-\beta| \leq t_1}} \sum_{s=0}^{t_1-|\alpha-\beta|} P_s(h, n_1-\ell)$$

$$(-1)^{(|\beta|+|\gamma|-|\beta+\gamma|)/2} \} \qquad (7)$$

但し，$A_i^{(1)}(u, \beta)$，及び$B_i^{(1)}(u, \beta)$は，それぞれC_1及びC_1の双対符号の符号語のうちでu番目のシンボル位置のシンボルがβであり，かつ，2元重みが$i+|\beta|$（但し，$|\beta|$はβに対応するビット列の重みを表す）であるような符号語の個数である．また，r_1はC_1の検査ビット数である．

確率$p_e(u, \alpha)$について次の式が成立する（証明は付録Bに示す）．

$$p_e(u, \alpha)$$

$$= \sum_{i=0}^{n_1-\ell} A_i^{(1)}(u, \alpha) \sum_{j=0}^{n_1-\ell} \sum_{j'=0}^{\ell} \sum_{s=0}^{t_1} \sum_{s'=0}^{t_1-s}$$

$$W_{j,s}^{(i)}(n_1-\ell)\ W_{j',s'}^{(|\alpha|)}(\ell)\ \varepsilon^{j+j'}\ (1-\varepsilon)^{n_1-j-j'} \qquad (8)$$

$$= 2^{-r_1}\ (1-\varepsilon)^{\ell} \sum_{h=0}^{n_1-\ell} (1-2\varepsilon)^h \sum_{s=0}^{t_1} \sum_{f=0}^{s}$$

$$P_{s-f}(h, n_1-\ell) \sum_{j=0}^{\ell} W_{j,f}^{(|\alpha|)}(\ell)\ (\varepsilon/(1-\varepsilon))^j$$

$$\sum_{\beta \in GF(2^{\ell})} B_h^{(1)}(u, \beta)\ (-1)^{(|\alpha|+|\beta|-|\alpha+\beta|)/2} \qquad (9)$$

$\bar{P}_e(u)$および$\bar{P}_{e\ell}(u)$をそれぞれマークのないセグメントのu番目のシンボルが誤りである確率とマーク付きセグメントのu番目のシンボルが誤りである確率とすれば次の式が成立する．

$$\bar{P}_e(u) = \sum_{\alpha \in GF(2^{\ell})-\{0\}} p_e(u, \alpha) \tag{10}$$

$$\bar{P}_{e\ell}(u) = \sum_{\alpha \in GF(2^{\ell})-\{0\}} p_{e\ell}(u, \alpha) \tag{11}$$

次にブロック全体の正しく復号される確率を計算するために必要な，セグメントの与えられた位置（複数でもよい）に誤りが起こる確率の計算法について述べる．$(a_1, a_2, \cdots, a_{m_1})$ を長さ m_1 の２元ベクトルとする．確率 $P^{(1)}_{e\ell, a_1, a_2, \cdots, a_{m_1}}$（または，$P^{(1)}_{e, a_1, a_2, \cdots, a_{m_1}}$）をある受信フレームに対してマーク付け操作が行なわれ（または復号に成功し），かつ，復号後のセグメントにおいて，$a_u=0$ をみたす u については u 番目のシンボルに誤りがなく，$a_u=1$ をみたす u については u 番目のシンボルに誤りがある確率とする．

$P^{(1)}_{e\ell, a_1, a_2, \cdots, a_{m_1}}$ は次の式で与えられる（証明は付録Ｃに示す）．

$$P^{(1)}_{e\ell, a_1, a_2, \cdots, a_{m_1}}$$

$$= (1-\varepsilon)^{k_1 \ell |H|} [1-(1-\varepsilon)^{\ell}]^{|H|}$$

$$- \sum_{i_1=0}^{\ell} \cdots \sum_{i_{m_1}=0}^{\ell} \sum_{i_{m_1+1}=0}^{r_1} A^{(1)}_{i_1, i_2, \cdots, i_{m_1+1}}$$

$$\sum_{J(H)} \sum_{S(t_1)} \left[\prod_{h=1}^{m_1} W^{(i_h)}_{j_h, s_h}(\ell) \, \varepsilon^{j_h} (1-\varepsilon)^{\ell - j_h} \right]$$

$$W^{(i_{m_1+1})}_{j_{m_1+1}, s_{m_1+1}}(r_1) \, \varepsilon^{j_{m_1+1}} (1-\varepsilon)^{r_1 - j_{m_1+1}} \Big] \tag{12}$$

$$= (1-\varepsilon)^{k_1 \ell |H|} \{ [1-(1-\varepsilon)^{\ell}]^{|H|}$$

$$- \quad 2^{-r_1} \sum_{i_1=0}^{\ell} \cdots \sum_{i_{m_1}=0}^{\ell} \sum_{i_{m_1+1}=0}^{r_1} B^{(1)}_{i_1, i_2, \cdots, i_{m_1+1}} (1-2\varepsilon)^{i_{m_1+1}}$$

$$P_{t_1}\left(\sum_{h=0}^{m_1+1} i_h - 1, n_1 - 1\right) \prod_{h \in H} \{(1-2\varepsilon)^{i_h} - (1-\varepsilon)^{\ell}\} \qquad (13)$$

但し，整数の組 $(i_1, \cdots, i_{m_1+1})$，但し，$0 \leqq i_j \leqq \ell$ $(1 \leqq j \leqq m_1)$，かつ，$0 \leqq i_{m_1+1} \leqq r_1$について，$A^{(1)}_{i_1, i_2, \cdots, i_{m_1+1}}$，及び，$B^{(1)}_{i_1, i_2, \cdots, i_{m_1+1}}$は，それぞれ$C_1$，及び，その双対符号の符号語のうち，j番目$(1 \leqq j \leqq m_1)$のシンボル位置の2元重みが$i_j$であり，かつ，$1, 2, \cdots, m_1$番目のシンボル位置以外の部分の重みが$i_{m_1+1}$であるような符号語の個数である．また，$H = \{i \mid a_i = 1 (1 \leqq i \leqq m_1)\}$，$\bar{H} = \{1, 2, \cdots, m_1\} - H$，$|H|$はHの要素の個数を表すものとし，$J(H)$，$S(t_1)$は次の式で定義される集合とする．

$$J(H) \triangleq \{(j_1, j_2, \cdots, j_{m_1+1}) \mid 0 \leqq j_{m_1+1} \leqq r_1 \text{かつ，各} 1 \leqq h \leqq m_1 \text{について} h \notin H \text{のとき} j_h = 0,\ h \in H \text{のとき} 0 \leqq j_h \leqq \ell\} \qquad (14)$$

$$S(t_1) \triangleq \{(s_1, s_2, \cdots, s_{m_1+1}) \mid \text{各} 1 \leqq h \leqq m_1 \text{について} 0 \leqq s_h \leqq \ell,\ 0 \leqq s_{m_1+1} \leqq r_1, \text{かつ} \sum_{h=1}^{m_1} s_h \leqq t_1\} \qquad (15)$$

与えられた$(a_1, a_2, \cdots, a_{m_1})$と$\varepsilon$に対する，確率$P^{(1)}_{e, a_1, a_2, \cdots, a_{m_1}}$は次の式で表される．

$$P^{(1)}_{e, a_1, a_2, \cdots, a_{m_1}} = \sum_{s=0}^{|W|} (-1)^{|W|-s} \sum_{\substack{\bar{H} \subseteq W \\ |\bar{H}| = s}} P_e(H) \qquad (16)$$

但し，$P^{(1)}_e(H)$は$h \in H$ならば復号後のh番目のシンボルに誤りが

ない（$h \notin H$ならば誤りがあってもなくてもよい）確率であり，次の式で表される（証明は付録Dに示す）．

$$
\begin{aligned}
& P_e^{(1)}(H) \\
&= \sum_{(i_1,\cdots,i_{m_1+1}) \in I(H)} A^{(1)}_{i_1,i_2,\cdots,i_{m_1+1}} \sum_{j_1=0}^{\ell} \cdots \sum_{j_{m_1}=0}^{\ell} \\
&\quad \sum_{j_{m_1+1}=0}^{r_1} \sum_{(s_1,s_2,\cdots,s_{m_1+1}) \in S(t_1)} \left[\prod_{h=1}^{m_1} W^{(i_h)}_{j_h,s_h}(\ell) \right] \\
&\quad W^{(i_{m_1+1})}_{j_{m_1+1},s_{m_1+1}}(r_1)(1-\varepsilon)^{n_1} \left[\prod_{h=1}^{m_1} (\varepsilon/(1-\varepsilon))^{j_h} \right] \qquad (17) \\
&= 2^{-r_1} \sum_{i_1=0}^{\ell} \cdots \sum_{i_{m_1}=0}^{\ell} \sum_{i_{m_1+1}=0}^{r_1} B^{(1)}_{i_1,i_2,\cdots,i_{m_1+1}} \\
&\quad \left[\prod_{h \in \bar{H}} (1-2\varepsilon)^{i_h} \right] (1-\varepsilon)^{\ell |H|} \sum_{s=0}^{t_1} (\varepsilon/(1-\varepsilon))^{n_1-\ell|H|} \\
&\quad \sum_{j=0}^{s} \binom{\ell |H|}{j} P_{s-j}\left(\sum_{h \in \bar{H}} i_h, n_1 - \ell |H| \right) \qquad (18)
\end{aligned}
$$

但し，$I(H)$は，次の式で定義されるm_1+1字組の集合である．

$$
\begin{aligned}
I(H) \triangleq \{ & (i_1,\cdots,i_{m_1+1}) \mid 0 \leqq i_{m_1+1} \leqq r_1 \text{かつ，各} 1 \leqq h \leqq m_1 \\
& \text{について} h \in H \text{のとき} i_h = 0,\ h \notin H \text{のとき} 0 \leqq i_h \leqq \ell \}
\end{aligned}
\qquad (19)
$$

これまで述べてきた内部符号に関する確率の計算法を用いれば，それらの確率はC_1，または，その双対符号の符号語をすべて生成することにより時間計算量$O(2^{\min\{k_1,r_1\}})$で計算できる．例えば，第4節で述べる符号の具体例で用いられている内部符号では，

$\min\{k_1, r_1\}$の値は高々24であるから，内部符号，または，その双対符号の符号語をすべて発生させることにより，これらの式の値を計算することができる．

3．誤って復号される確率の上界の値と正しく復号される確率の値の計算法

この節では，第2節で述べた内部符号の誤り確率を用いて，ブロック全体が誤って復号される確率P_{er}の上界と正しく復号される確率P_cを計算する方法について述べる．まず，P_{er}の上界の計算法について述べる．

以下，iを消去されたセグメントの個数とするとき，$T_{e\ell}(i)$，$t_2(i)$を，それぞれ$T_{e\ell}$，t_2と略記する．

$P_{er}(u)$をu番目のセクションが誤って復号される確率とすると，次式が成立する（証明を付録Eに示す）．

$$
\begin{aligned}
P_{er}(u) \leqq & \sum_{i=0}^{T_{es}} \binom{n_2}{i} \sum_{w=d_2-i}^{n_2-i} \binom{n_2-i}{w} \\
& \sum_{h=0}^{\min\{t_2,\, n_2-i-w\}} \binom{n_2-i-w}{h} \sum_{j=w+h-t_2}^{w} \binom{w}{j} \\
& \sum_{z_2=0}^{\min\{T_{e\ell},\, n_2-i-w-h\}} \binom{n_2-i-w-h}{z_2} \sum_{h_2=0}^{\min\{T_{e\ell}-z_2,\, h\}} \binom{h}{h_2} \\
& \sum_{s_2=0}^{\min\{T_{e\ell}-z_2-h_2,\, w-j\}} \binom{w-j}{s_2} \sum_{j_2=0}^{\min\{T_{e\ell}-z_2-h_2-s_2,\, j\}} \binom{j}{j_2} \\
& [\bar{p}_e(u)]^{j-j_2-b+h-h_2} \, [\bar{p}_{e\ell}(u)]^{j_2-d_2+i+w-j+b} \\
& [P_{es}^{(1)}]^{i} \, [P_e(u,0)]^{n_2-i-w-h-z_2} \, [P_{e\ell}(u,0)]^{z_2} \\
& (1-P_{es}^{(1)}-P_{e\ell}^{(1)})^{w-j-f_2} \, [P_{e\ell}^{(1)}]^{f_2}
\end{aligned}
$$

$$\sum_{q=0}^{2^{\ell}-2}[p_e(u,\gamma^q)]^b \sum_{q=0}^{2^{\ell}-2}[p_{e\ell}(u,\gamma^q)]^{j+d_2-i-w-b} \quad (20)$$

$P_{er}(u)$に関する上の上界式は，内部符号の復号段階でｉ個（但し，$0 \leqq i \leqq T_{es}$）のシンボル消去と，d_2-i-t_2個以上のシンボル誤りが起こったときには，そのセクションの復号を必ず誤ると仮定することにより得られる上界式（例えば，文献(8)の式(47)，及び，文献(9)の第５章）より，かなりよい上界式となっている．例えば，第４節で述べる符号例では，ビット誤り率10^{-2}のところで，１０進で２桁から４桁改善される．

(20)式の右辺を$\bar{P}_{er}(u)$で表すとP_{er}について次の上界式が得られる．

$$P_{er} \leqq \sum_{u=1}^{m_1} \bar{P}_{er}(u) \quad (21)$$

次に，ブロック全体が正しく復号される確率P_cは次の式で与えらえる．

$$P_c = \sum_{i=0}^{T_{es}} \binom{n_2}{i} [P_{es}^{(1)}]^i \sum_{j_1=0}^{t_2} \sum_{j_2=0}^{t_2} \cdots \sum_{j_{m_1}=0}^{t_2}$$

$$\sum_{h=0}^{T_{e\ell}} P_{e,j_1,j_2,\cdots,j_{m_1}}(n_2-i,h) \quad (22)$$

但し，各u，$1 \leqq u \leqq m_1$について$0 \leqq j_u \leqq n_2-i$を満たすj_uと，$0 \leqq h \leqq n_2-i$を満たす整数ｈについて，確率$P_{e,j_1,j_2,\cdots,j_{m_1}}(n_2-i,h)$は次の式で定義される．

$$\binom{n_2-i}{h}[\sum_{(a_1,a_2,\cdots,a_{m_1})\in\{0,1\}^{m_1}} P_{e,a_1,a_2,\cdots,a_{m_1}}^{(1)}$$

$$X_1^{a_1} X_2^{a_2} \cdots X_{m_1}^{a_{m_1}}]^{n_2-i-h}$$

$$[\sum_{(a_1, a_2, \cdots, a_{m_1}) \in \{0,1\}^{m_1}} P_{e\ell, a_1, a_2, \cdots, a_{m_1}}^{(1)}$$

$$X_1^{a_1} X_2^{a_2} \cdots X_{m_1}^{a_{m_1}}]^{h}$$

$$= \sum_{j_1=0}^{n_2-i} \sum_{j_2=0}^{n_2-i} \cdots \sum_{j_{m_1}=0}^{n_2-i} P_{e, j_1, j_2, \cdots, j_{m_1}}(n_2-i, h)$$

$$X_1^{j_1} X_2^{j_2} \cdots X_{m_1}^{j_{m_1}} \tag{23}$$

上式はm_1, t_2が小さいとき（例えば，筆者が使用した大阪大学大型計算機センターのACOS-1000では，$m_1=3$のとき$t_2 \leqq 15$, $m_1=4$のとき$t_2 \leqq 6$, $m_1=5$のとき$t_2 \leqq 4$)には実用的な計算時間で計算可能である．

4．縦接符号化方式の例

いくつかの具体例について，前節までに述べた方法に基づき，P_{er}の上界及び，P_cの計算を行った．それらの例では，外部符号に$GF(2^{\ell})$の上のリードソロモン符号（以下，RS符号と呼ぶ）を用い，内部符号には表1に示す14種類の符号を用いた．

［例1］例1では，外部符号として$GF(2^8)$の上の符号長$n_2=255$のRS符号を用いた．外部符号の最小距離と内部符号は表2に示す3つの組合せのものを用いた．また，内部符号に基づく復号のときにt_1個を越える誤りを検出したときの処理として，消去操作だけを行う場合（以下ではE-復号法と呼ぶ）とマーク付け操作だけを行う場合（以下ではM-復号法と呼ぶ）の2つを考えた．尚，表1に示した復号パラメータについては，$\bar{P}_{er}$がビット誤り率の全範囲で10^{-10}を越えず，かつ，ビット誤り率$\varepsilon=0.005$におけるP_cの値が最も大きくなるように，T_{es}とt_2(E-復号法の場合）または，$T_{e\ell}$とt_2（M-復号法の場合)を選んだ．

内部符号に表1の$C_1(7)$，$C_1(6)$，$C_1(3)$を用いたときの$\bar{P}_{er}$，$1-P_c$（ブロックが消去される確率と誤って復号される確率の和）をそれぞれ，図4，5，6，7，8，9に示す．

次に，E-復号法とM-復号法を比較する．一般に，ビット誤り率が比較的高いときには1つのセグメント中の誤りシンボルが多くなるのでセグメントを消去して外部符号の復号時に消失シンボルとして訂正を行った方がブロックが消去される確率が低くなるのでE-復号法の方が有利である．また，ビット誤り率が比較的低いときには内部符号に基づく復号時にt_1個を越える誤りを検出しても，セグメン

表1　具体例で用いる内部符号

内部符号		(n_1,k_1)	レート	ℓ	m_1	d_1	t_1	生成多項式
$C_1(1)$	shortened Hamming code	(55,48)	0.873	8	6	4	1	$(1+X)\phi_1(X)$
$C_1(2)$	shortened Hamming code	(56,48)	0.857	8	6	4	1	$(1+X)(1+X+X^7)$
$C_1(3)$	shortened Hamming code	(30,24)	0.800	8	3	4	1	$(1+X)(1+X^2+X^5)$
$C_1(4)$	shortened BCH code	(61,48)	0.787	8	6	6	2	$(1+X)\phi_1(X)\phi_3(X)$
$C_1(5)$	shortened BCH code	(53,40)	0.755	8	5	6	2	$(1+X)\phi_1(X)\phi_3(X)$
$C_1(6)$	shortened BCH code	(45,32)	0.711	8	4	6	2	$(1+X)\phi_1(X)\phi_3(X)$
$C_1(7)$	shortend BCH code	(59,40)	0.678	8	5	8	3	$(1+X)\phi_1(X)\phi_3(X)$ $\phi_5(X)$
$C_1(8)$	Goppa code	(64,40)	0.625	8	5	9	4	
$C_1(9)$	extended BCH code	(32,16)	0.500	8	2	8	3	
$C_1(10)$	extended Golay code	(24,12)	0.500	6	2	8	3	
$C_1(11)$	biorthogonal code	(8,4)	0.500	4	1	4	1	
$C_1(12)$	shortened Type 0 DTI code	(51,24)	0.471	8	3	10	4	$(1+X)\phi_1(X)\phi_3(X)$ $\phi_5(X)\phi_7(X)\phi_{21}(X)$
$C_1(13)$	biorthogonal code	(16,5)	0.313	5	1	8	3	
$C_1(14)$	biorthogonal code	(32,6)	0.188	6	1	16	7	

(*) αを$1+X+X^6$の根とするとき，$\phi_i(X)$は，α^iの最小多項式を表す．

表2.　計算例1で用いた内部符号と外部符号のパラメータ

内部符号	d_2	レート	復号法(*)	T_{es}	$T_{e\ell}$	t_2
$C_1(7)$	7	0.593	E	2	–	0
			M	–	1	1
$C_1(6)$	11	0.622	E	6	–	0
			M	–	4	2
$C_1(3)$	33	0.700	E	18	–	3
			M	–	15	10

(*) 記号E,Mは,それぞれE-復号法,M-復号法を表す.

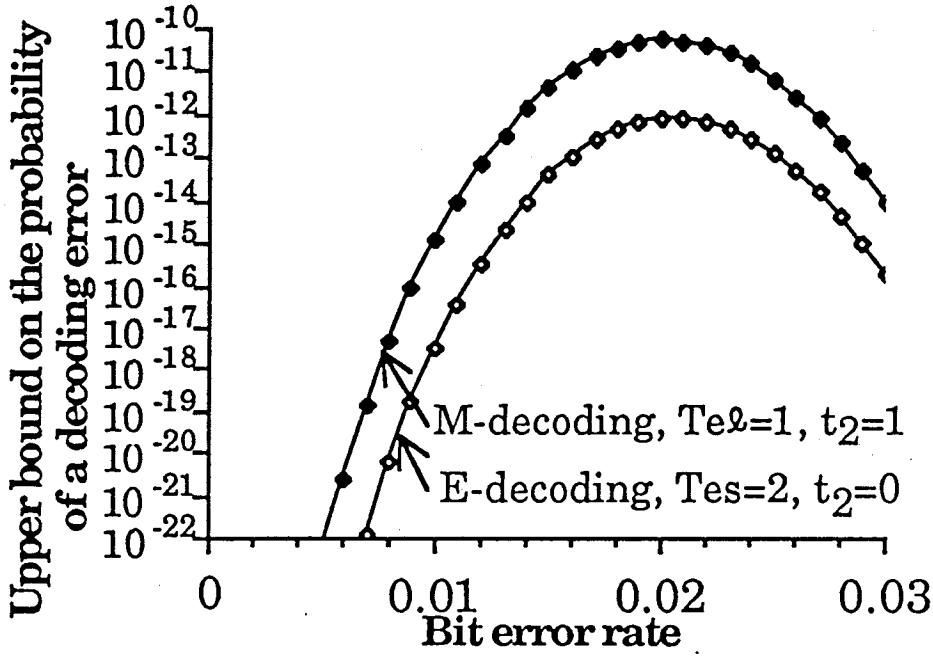

図4 誤って復号する確率の上界
（$C_1(7)$と(255,249)RS符号）

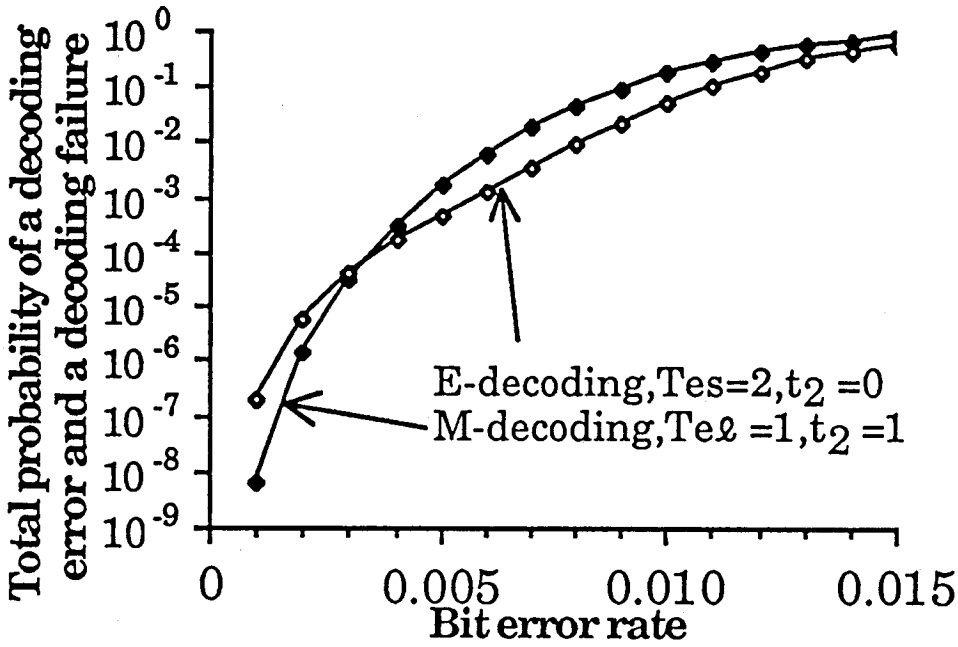

図5 ブロックが消去される確率と誤って復号する確率の和
（$C_1(7)$と(255,249)RS符号）

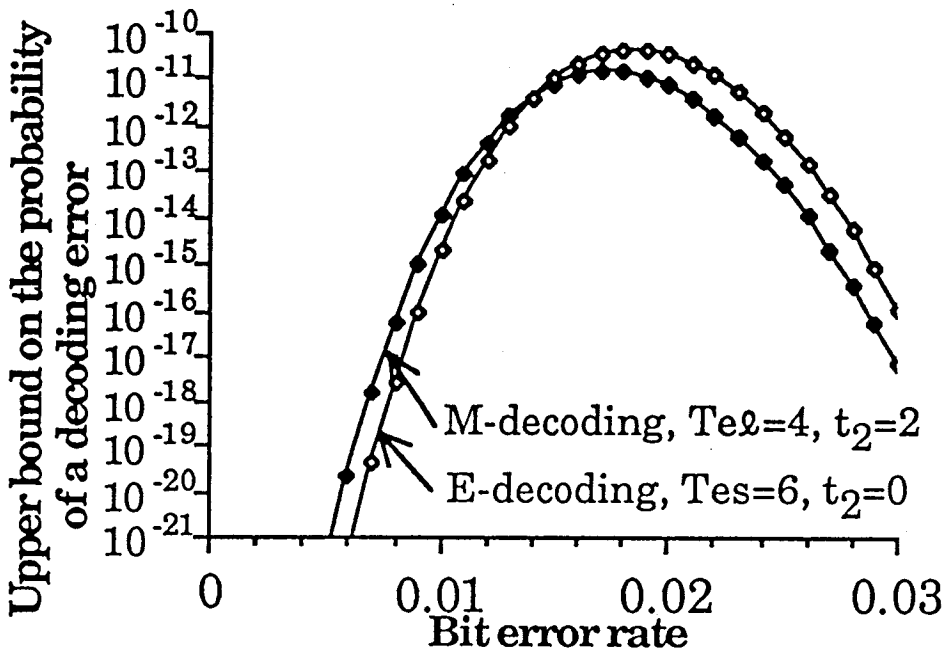

図6 誤って復号する確率の上界
（$C_1(6)$と(255,245)RS符号）

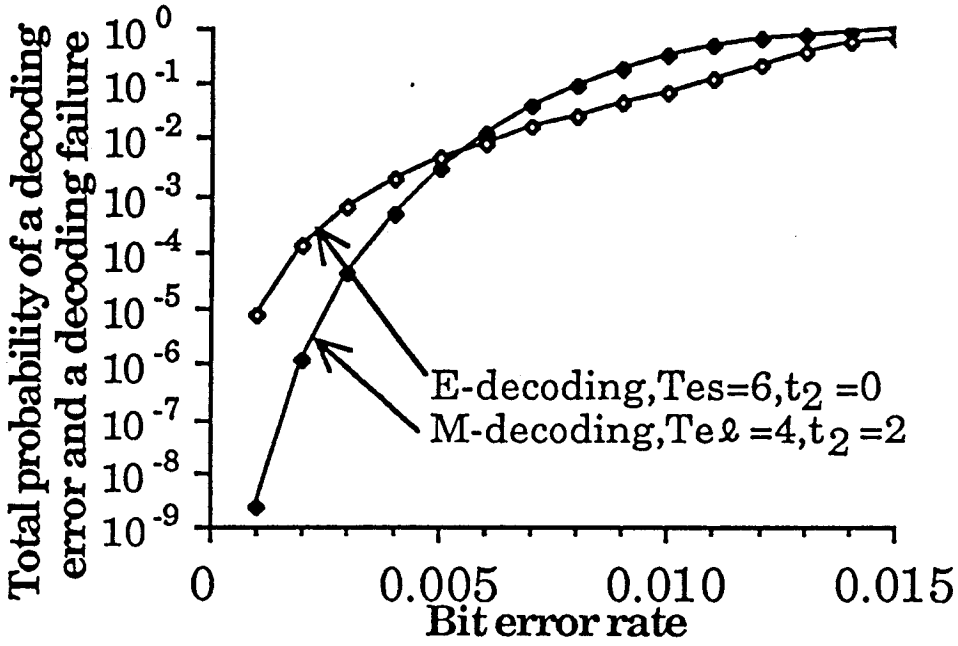

図7 ブロックが消去される確率と誤って復号する確率の和
（$C_1(6)$と(255,245)RS符号）

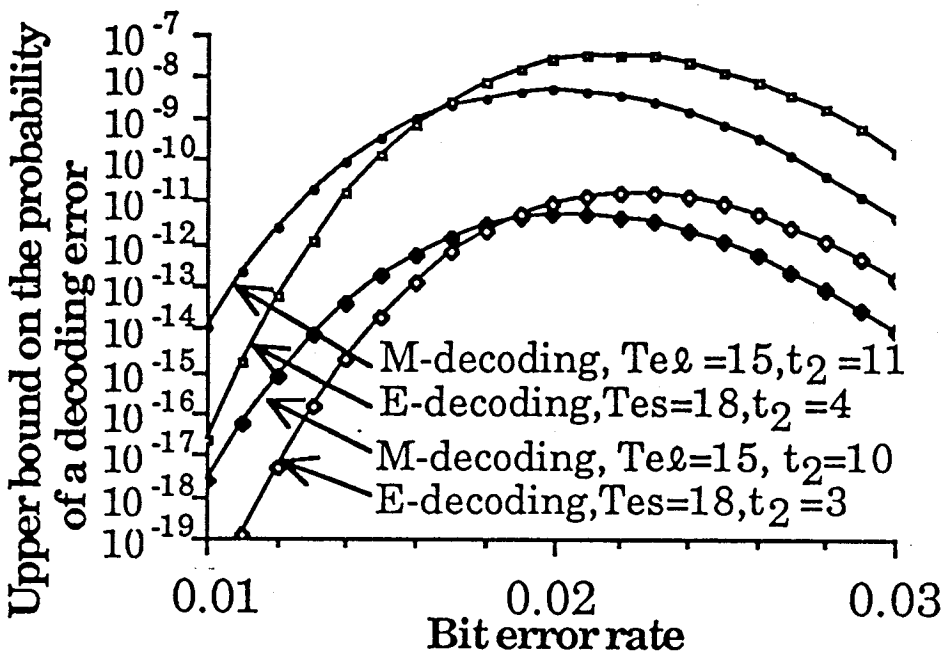

図8 誤って復号する確率の上界
（C_1(3)と(255,223)RS符号）

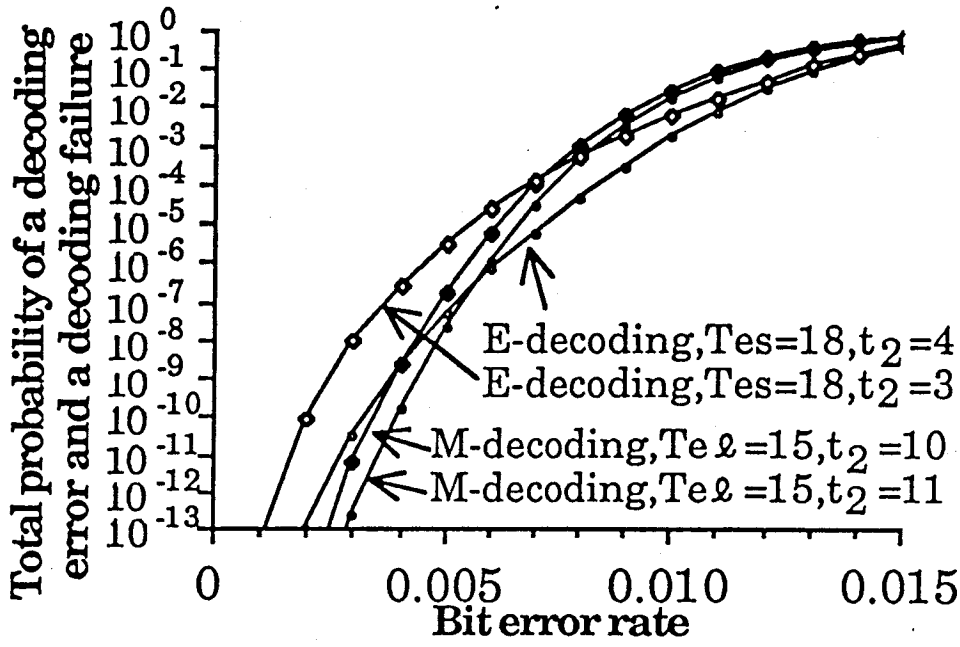

図9 ブロックが消去される確率と誤って復号する確率の和
（$C_1(3)$と(255,223)RS符号）

ト中には誤りのないシンボルを含むことが多いので，セグメントをそのままにして，外部符号の復号時に訂正を行った方がブロックが消去される確率が低くなるのでM-復号法の方が有利である．実際，表２の内部符号と外部符号の組合せにおいて，それぞれ，ビット誤り率0.003，0.005，0.007以下のとき，E-復号法よりM-復号法を用いた例の方がブロックが消去される確率と誤って復号される確率の和が低い値となった．

また，図8，9では内部符号，外部符号として表２の３番目の符号と同じものを用いて，(1)復号パラメータがT_{es}=18，t_2=4であるE-復号法と，(2)$T_{e\ell}$=15，t_2=11であるM-復号法に対する$\bar{P}_{er}$と$1-P_c$の値を示す．

一般に，内部符号と外部符号が同じならば，T_{es}，$T_{e\ell}$，t_2を増やすとブロックが復号に失敗する確率は減少するが，誤って復号される確率は増加する．図9に示した例では，ビット誤り率0.005における$1-P_c$の値は，それぞれ，3.22×10^{-6}(T_{es}=18，t_2=3，E-復号法)，5.30×10^{-8}(T_{es}=18，t_2=4，E-復号法)，1.82×10^{-7}($T_{e\ell}$=15，t_2=10，M-復号法)，2.17×10^{-8}($T_{e\ell}$=15，t_2=11，M-復号法)となる．また，ビット誤り率0.01における$\bar{P}_{er}$の値は，それぞれ，1.17×10^{-21}(T_{es}= 18，t_2=3，E-復号法)，2.07×10^{-17}(T_{es}=18，t_2=4，E-復号法)，2.24×10^{-18}($T_{e\ell}$=15，t_2=10，M-復号法)，1.07×10^{-14}($T_{e\ell}$=15，t_2=11，M-復号法)となる．

［例２］例２では，外部符号としてGF(2^8)の上の符号長n_2=255，k_2=223のＮＡＳＡ標準RS符号を用いた．内部符号は表３，４に示すものを用いた．表３では，内部符号を用いない場合の例を併せて示す．内部符号に基づく復号のときにt_1個を越える誤りを検出したときの

表３　いくつかの縦接符号の具体例における，ブロックが
復号に失敗する確率と誤って復号される確率の和と
誤って復号される確率の上界の値

Rate	n_2	k_2	d_2	m_1	T_{es}	t_2	Inner code		Bit-error rate				
									$\varepsilon=0.2\times10^{-2}$	$\varepsilon=0.5\times10^{-2}$	$\varepsilon=1\times10^{-2}$	$\varepsilon=2\times10^{-2}$	$\varepsilon=3\times10^{-2}$
0.875	255	223	33	1	0	7	No inner code	$P_{es}+P_{er}$	5.29×10^{-2}	7.88×10^{-1}	1.00×10^{0}	1.00×10^{0}	------
								$\bar{P}_{er}$	1.81×10^{-23}	1.45×10^{-15}	9.93×10^{-12}	5.83×10^{-11}	------
0.764	255	223	33	6	20	2	$C_1(1)$	$P_{es}+P_{er}$	6.13×10^{-6}	1.11×10^{-2}	8.83×10^{-1}	1.00×10^{0}	1.00×10^{0}
								$\bar{P}_{er}$	4.83×10^{-49}	2.01×10^{-24}	1.06×10^{-12}	1.49×10^{-16}	1.02×10^{-29}
0.750	255	223	33	6	22	2	$C_1(2)$	$P_{es}+P_{er}$	8.53×10^{-7}	1.74×10^{-3}	7.98×10^{-1}	1.00×10^{0}	------
								$\bar{P}_{er}$	4.04×10^{-46}	2.97×10^{-22}	2.04×10^{-11}	4.22×10^{-18}	------
0.700	255	223	33	3	20	2	$C_1(3)$	$P_{es}+P_{er}$	5.35×10^{-8}	1.50×10^{-4}	3.38×10^{-2}	9.80×10^{-1}	1.00×10^{0}
								$\bar{P}_{er}$	1.15×10^{-66}	1.70×10^{-39}	7.74×10^{-22}	1.06×10^{-11}	2.41×10^{-13}
0.688	255	223	33	6	21	2	$C_1(4)$	$P_{es}+P_{er}$	7.10×10^{-11}	2.52×10^{-6}	3.69×10^{-3}	9.65×10^{-1}	1.00×10^{0}
								$\bar{P}_{er}$	3.00×10^{-90}	1.19×10^{-51}	6.15×10^{-26}	1.99×10^{-11}	1.20×10^{-16}
0.660	255	223	33	5	22	2	$C_1(5)$	$P_{es}+P_{er}$	5.65×10^{-12}	2.17×10^{-7}	3.95×10^{-4}	4.95×10^{-1}	1.00×10^{0}
								$\bar{P}_{er}$	9.74×10^{-95}	4.18×10^{-56}	1.72×10^{-29}	1.03×10^{-11}	1.59×10^{-12}

表４　いくつかの縦接符号の具体例における，ブロックが
復号に失敗する確率と誤って復号される確率の和と
誤って復号される確率の上界の値

Rate	n_2	k_2	d_2	m_1	T_{es}	t_2	Inner code		Bit-error rate				
									$\varepsilon=1\times10^{-2}$	$\varepsilon=2\times10^{-2}$	$\varepsilon=3\times10^{-2}$	$\varepsilon=4\times10^{-2}$	$\varepsilon=5\times10^{-2}$
0.593	255	223	33	5	21	3	$C_1(7)$	$P_{es}+P_{er}$	5.69×10^{-10}	7.26×10^{-5}	7.55×10^{-1}	1.00×10^{0}	------
								$\bar{P}_{er}$	6.24×10^{-51}	6.38×10^{-21}	1.85×10^{-11}	1.36×10^{-13}	------
0.547	255	223	33	5	23	2	$C_1(8)$	$P_{es}+P_{er}$	8.38×10^{-9}	6.17×10^{-5}	5.57×10^{-3}	8.21×10^{-1}	1.00×10^{0}
								$\bar{P}_{er}$	8.06×10^{-74}	1.47×10^{-34}	4.28×10^{-17}	2.15×10^{-11}	1.80×10^{-14}
0.437	255	223	33	3	24	2	$C_1(9)$	$P_{es}+P_{er}$	5.04×10^{-11}	7.36×10^{-7}	1.38×10^{-4}	3.97×10^{-3}	9.93×10^{-2}
								$\bar{P}_{er}$	3.44×10^{-83}	2.61×10^{-47}	1.51×10^{-28}	1.22×10^{-17}	8.21×10^{-12}
0.412	255	223	33	3	25	2	$C_1(12)$	$P_{es}+P_{er}$	6.40×10^{-15}	4.45×10^{-10}	1.75×10^{-7}	1.03×10^{-3}	6.89×10^{-1}
								$\bar{P}_{er}$	2.10×10^{-93}	1.45×10^{-50}	6.19×10^{-29}	1.59×10^{-17}	3.02×10^{-13}

処理としては，E-復号法を考えた．表３，４に，$\bar{P}_{er}$，$1-P_c$の計算結果を示す．表３，４に示した復号パラメータについては，$\bar{P}_{er}$がビット誤り率の全範囲で10^{-10}を越えず，かつ，ビット誤り率$\varepsilon=0.005$（表３），0.03（表４）におけるP_cの値が最も大きくなるように，T_{es}とt_2を選んだ．

［例３］例３では，内部符号として表５に示すレートの低い符号を用いた例を考える．外部符号は，すべて，$GF(2^{\ell})$上のRS符号である．また，内部符号に基づく復号のときにt_1個を越える誤りを検出したときの処理として，E-復号法を考えた．表５に，$\bar{P}_{er}$，$1-P_c$の計算結果を示す．尚，表５に示した復号パラメータについては，$\bar{P}_{er}$がビット誤り率の全範囲で10^{-10}を越えず，かつ，ビット誤り率$\varepsilon=0.1$におけるP_cの値が最も大きくなるように，T_{es}とt_2を選んだ．これらの例ではビット誤り率がかなり高い（例えば$\varepsilon=0.05$）通信路においても通信可能である．

次に，計算の精度について述べる．筆者は，上述の計算機を用いてこれらの例に対する計算を行った．第２節の内部符号の復号に関する確率の式には正数項と負数項が存在するので，それらの項の値や計算方法によってはいわゆる桁落ちにより有効桁数が十分でない場合が起こり得る．そのため，それらの式の計算においては，正数項だけの和と負数項だけの和をそれぞれ計算し，最後に，その差をとる方法を用いた．以下では，この方法で計算した場合の有効桁数を求める．いま，正数項，負数項の和をそれぞれs_p，s_mとし，その加算回数をそれぞれa_p，a_mとすると，計算結果$s=s_p-s_m$の有効桁数z（10進）は次の式で表される．

表５　内部符号に低レート符号を用いたいくつかの縦接符号の具体例における
ブロックが復号に失敗する確率と誤って復号される確率の和と
誤って復号される確率の上界の値

Rate	n_2	k_2	d_2	m_1	T_{es}	t_2	Inner code		Bit-error rate				
									$\varepsilon=0.2\times10^{-1}$	$\varepsilon=0.5\times10^{-1}$	$\varepsilon=1\times10^{-1}$	$\varepsilon=2\times10^{-1}$	$\varepsilon=3\times10^{-1}$
0.333	63	42	22	2	10	2	$C_1(10)$	$P_{es}+P_{er}$	3.22×10^{-8}	4.49×10^{-3}	8.74×10^{-1}	1.00×10^{0}	1.00×10^{0}
								$\bar{P}_{er}$	1.25×10^{-58}	2.41×10^{-28}	3.64×10^{-13}	4.39×10^{-14}	4.61×10^{-16}
0.200	15	6	10	1	2	0	$C_1(11)$	$P_{es}+P_{er}$	6.50×10^{-3}	1.17×10^{-1}	6.63×10^{-1}	9.99×10^{-1}	1.00×10^{0}
								$\bar{P}_{er}$	9.08×10^{-35}	2.16×10^{-24}	2.14×10^{-17}	3.07×10^{-12}	7.31×10^{-11}
0.151	31	15	17	1	7	2	$C_1(13)$	$P_{es}+P_{er}$	3.72×10^{-13}	1.34×10^{-7}	1.30×10^{-3}	9.28×10^{-1}	1.00×10^{0}
								$\bar{P}_{er}$	5.56×10^{-65}	4.88×10^{-40}	1.80×10^{-23}	7.00×10^{-13}	6.68×10^{-13}
0.092	63	31	33	1	25	2	$C_1(14)$	$P_{es}+P_{er}$	5.00×10^{-25}	3.76×10^{-15}	1.87×10^{-8}	3.67×10^{-2}	1.00×10^{0}
								$\bar{P}_{er}$	******	1.15×10^{-117}	2.31×10^{-56}	8.07×10^{-15}	6.99×10^{-17}

(*) 表中の記号“********”は，その欄の値が10^{-130}以下であることを表す．

$$z = \lfloor q - \log_{10} \{ (\max\{s_p, s_m\}/s) + \max\{a_p, a_m\} \} \rfloor \qquad (24)$$

但し，qは使用する計算機の実数の10進有効桁数であり，上述の計算機の4倍精度浮動小数点実数のそれは34桁である．また，上述の計算では，いずれも$a_p \leqq 10^{12}$，$a_m \leqq 10^{12}$，$\max\{s_p, s_m\}/s \leqq 10^9$であることから，それらの有効桁数は少なくとも10進11桁あることがわかる．

5．結言

この章では，外部符号，内部符号ともに線形ブロック符号を用いた縦接符号化方式を2元対称通信路で用いたときの，正しく復号される確率の値と誤って復号される確率の上界の値を計算する方法を示した．

いくつかの具体例について，それらの計算を行った．その結果，それらの例は，ビット誤り率が10^{-3}から10^{-2}という比較的高いところでも非常に高い信頼性をもつことがわかった．それらの例は衛星通信（内部符号にレートの高い符号を用いたとき）やスペースクラフトの通信（内部符号にレートの低い符号を用いたとき）のダウンリンクの誤り制御への応用が考えられる．また，内部符号で復号に失敗したときの操作として，(1)内部符号の受信語を消去する，(2)内部符号の情報ビットの部分を外部符号の復号バッファに送る，の2通りの方法を考え，その比較を行った．

第２章　変調符号を内部符号に用いた縦接符号化方式

１．序言

最近，帯域幅に制限のある通信路に適した変調符号の研究が精力的に行われている[10-19]．この新しい符号化法は符号化しない時の変調信号点集合を拡大することにより得られた信号点集合を考えて，その上で符号化を行うものである．適切に設計された変調符号は符号化せずに変調のみを行う場合と比較して，帯域幅を拡大することなく（または，わずかな帯域幅拡大で），大きな符号化利得を得ることができる．３から５ｄＢの符号化利得を得るために必要な復号の複雑度は合理的である．しかし，変調符号（ブロック，または；トレリス変調符号）単独で５ｄＢを越える符号化利得を得るために必要な復号の複雑度は急激に増加し，復号器は，たいへん高価で，かつ，低速なものとなる．そのため，復号の複雑度をさほど上げることなく大きな符号化利得を得る方法として，変調符号を内部符号に用いた縦接符号化方式が考えられる．この方式では，内部符号と外部符号を適切に選択することにより，大きな符号化利得や高い信頼度が得ることができ，かつ，実用的な複雑度の復号器が実現可能である．

この章では，内部符号にＭ値位相変調（Phase Shift Keying：以下，ＰＳＫと略する）用ブロック変調符号を用いた縦接符号化法を考える．しかし，第１章と異なり，内部符号の実効レートが高いため，縦接符号全体でみた帯域幅の拡大は少なくなっている．例えば，内部符号の実効レートが１でれば，その縦接符号の帯域幅の拡大は

外部符号の冗長度によるもののみとなる．一般に，縦接符号の外部符号には，最大距離分離符号（例えば，リードソロモン符号）が用いられるので，必要とされる帯域幅の拡大は少ない．もちろん，内部符号の実効レートが1より大きいときには，帯域幅の拡大が必要なくなることもある[14,15]．

以下，この章では，まず，第2節で縦接符号化法に適したM値PSKブロック変調符号の構成法について述べ，いくつかの符号長が短く，最小ユークリッド距離の長いM値PSK変調符号の例を示す．それらの符号は，単純なトレリスダイアグラムをもち，軟判定ヴィタビ復号[20]（最尤復号法の一種）が可能である．更に，それらの符号のいくつかは，45度の位相回転について閉じている．第3節では，縦接符号化法の符号化法と復号法について述べる．ここでの縦接符号化法も第1章と同様，外部符号はバースト誤り訂正能力向上のため，インターリービングが施される．第4節では，ここで述べる縦接符号化法を加法的白色ガウス雑音をもつ通信路で用いたときの誤り特性の解析を行う．第5節では，8値PSKブロック変調符号と有限体GF(2^8)上のNASA標準(255,223)リードソロモン符号を組み合わせた，いくつかの具体例について述べる．

2．M値位相変調用ブロック変調符号

この節では，縦接符号化法の内部符号に適したM値（但し，$M=2^q$とする）PSK変調用ブロック変調符号の構成法について述べる．この方法を用いることにより，短い符号長と，単純なトレリスダイアグラムをもち，軟判定ヴィタビ復号アルゴリズムで復号可能な符号を構成することが可能である．

2．1　符号の構成法

$A=\{0,\ 1,\ \cdots,\ 2^q-1\}$を$2^q$を法とする加法を演算とする整数群とする．Aに属する各元は，2^q値PSK変調の各信号点を表すものとする．s，s'をAの元とするとき，sとs'間の距離d(s,s')を次の式で定義する．

$$d(s,s') = 4\sin^2(2^{-q}\pi(s-s')) \tag{25}$$

明らかに，$d(s,s')=d(s-s',0)$が成立する．このd(s,s')は，2^q値PSK変調信号点s，s'間の2乗ユークリッド距離となっている．各$1\leqq i\leqq q$について，$B_i=\{0,2^{i-1}\}$とする．従って，整数群Aは$A=\{b_1+b_2+\cdots+b_q \mid 各1\leqq i\leqq q について b_i\in B_i\}$と表すことができる．各$1\leqq i\leqq q$について$d_i$を集合$B_i+B_{i+1}+\cdots+B_q$の任意の異なる2つの要素間の最小距離とする．式(25)から次式が成立する．

$$d_i = 4\sin^2(2^{i-1-q}\pi) \tag{26}$$

$d(\cdot,\cdot)$を距離の規準として用いると，符号設計が困難な場合があるため，ここでは，文献(10,11,13)等に従い，以下に示す距離の規準$\underline{d}(\cdot,\cdot)$を考える．$s=b_1+b_2+\cdots+b_q$，$s'=b_1'+b_2'+\cdots+b_q'$をAの元とするとき，$\underline{d}(s,s')$を次式で定義する．

(1)　$s=s'$のとき，　$\underline{d}(s,s') \triangleq 0$　　(27)

(2)　それ以外のとき，$\underline{d}(s,s') \triangleq d_h$　　(28)

但し，hは，$b_h \neq b_h'$となる最初の添字である．

$\underline{d}(\cdot,\cdot)$の定義より，Aの元s，s'について，次式が成立する．

$$d(s,s') \geqq \underline{d}(s,s') \qquad (29)$$

A^nをAの上のn字組の集合とする．s，s'をAの要素とするとき，$g(s,s')$を$A\times A$から実数への写像とする（例えば，$d(\cdot,\cdot)$や$\underline{d}(\cdot,\cdot)$は，この条件を満たす写像である）．そのとき，Aの上の2つのn字組$\bar{s}=(s_1,s_2,\cdots,s_n)$，$\bar{s}'=(s_1',s_2',\cdots,s_n')$から実数への写像$g^{(n)}(\bar{s},\bar{s}')$を次式で定義する．

$$g^{(n)}(\bar{s},\bar{s}') = \sum_{j=1}^{n} g(s_j,s_j') \qquad (30)$$

このとき，$d^{(n)}(\bar{s},\bar{s}')$は，Aの上のn字組$\bar{s}$，$\bar{s}'$の間の2乗ユークリッド距離である．

hをq以下の正整数とするとき，j_1，j_2，…，j_{h+1}を次式の条件を満たすh+1個の整数とする．

$$1 = j_1 < j_2 < \cdots < j_h < j_{h+1} = q+1 \tag{31}$$

各$1 \leqq i \leqq h$について，$\bar{B}_i$をB_{j_i}，B_{j_i+1}，…，$B_{j_{i+1}-1}$の直和とする．つまり，$\bar{B}_i$は，次式で定義される．

$$\bar{B}_i \triangleq \{b_{j_i}+b_{j_i+1}+ \cdots +b_{j_{i+1}-1} \mid \text{各} j_i \leqq k < j_{i+1} \text{について} b_k \in B_k \} \tag{32}$$

このとき，$A = \bar{B}_1+\bar{B}_2+ \cdots +\bar{B}_h$である．

各$1 \leqq i \leqq h$について，C_iを$\bar{B}_i$の上の符号長n，最小ハミング距離δ_iのブロック符号とする．C_1，C_2，…，C_hから，A上のブロック符号Cを次式で表される符号とする．

$$C = \{\bar{v}_1+\bar{v}_2+ \cdots +\bar{v}_h \mid \text{各} 1 \leqq i \leqq h \text{について} \bar{v}_i \in C_i \} \tag{33}$$

以下，C_1，C_2，…，C_hをCのコンポーネント符号と呼ぶ．Xを集合とするとき，記号$|X|$を集合Xの要素の個数とする．集合Cについて，次式が成立する．

$$|C| = \prod_{i=1}^{h} |C_i| \tag{34}$$

また，各コンポーネント符号C_iの情報ビット数をk_iとするとき，次式で定義されるkはCの次元と呼ばれる．

$$k = \sum_{i=1}^{h} k_i \tag{35}$$

つまり，kはCの情報ビット数である．

XをA^nの部分集合とし，$s, s' \in A$とするとき，$g(s, s')$をA^2から実数への写像とする（例えば，$d(\cdot, \cdot)$や$\underline{d}(\cdot, \cdot)$はこの条件を満たす写像である）．このとき，$D[g, X]$を次式で定義する．

$$D[g, X] \triangleq \min\{ g^{(n)}(\bar{s}, \bar{s}') \mid \bar{s}, \bar{s}' \in X \text{ かつ } \bar{s} \neq \bar{s}' \} \quad (36)$$

このとき，$D[d, C]$は，符号Cの最小2乗ユークリッド距離である．以下，XをA^nの部分集合とするとき，$D[d, X]$，$D[\underline{d}, X]$を，記号$D[X]$，$\underline{D}[X]$で表す．

$D[X]$，$\underline{D}[X]$について，明らかに，次式が成立する．

$$D[C] \geqq \underline{D}[C] \quad (37)$$

$D[g, C]$について次の下界が成立する（証明は付録Fに示す）．

$$D[g, C] \geqq \min_{1 \leqq i \leqq h} D[g_{\bar{B}_i}, C_i] \quad (38)$$

但し，$g(\cdot, \cdot)$をA^2から実数への写像，w, w'を$\bar{B}_i$の要素とするとき，$(\bar{B}_i)^2$から実数への写像である$g_{\bar{B}_i}(w, w')$は，次式で定義されるものとする．

$$\begin{aligned} g_{\bar{B}_i}(w, w') \triangleq \min\{ & g(s, s') \mid \text{各} u \in B_1 + \cdots + B_{j_i - 1}, \\ & v, v' \in B_{j_{i+1}} + \cdots + B_q \text{について} \\ & s = uwv,\ s' = uw'v' \} \end{aligned} \quad (39)$$

以下，XをA^{n}の部分集合とするとき，$D[d_{\overline{B}_i}, X]$，$D[\underline{d}_{\overline{B}_i}, X]$を，記号$D_{\overline{B}_i}[X]$，$\underline{D}_{\overline{B}_i}[X]$で表す．

ところで，Cの各コンポーネント符号C_1，C_2，…，C_hの構成法については，いくつかの方法がある[19]．ここでは，次の2通りの方法を考える．

［構成法1］

第1の方法は，j_iが次の条件を満たしている場合である．

$$j_{i+1} = j_i + 1 \tag{40}$$

従って，次の様な場合である．

$$\overline{B}_i = B_{j_i} \tag{41}$$

である．また，C_iは最小ハミング距離δ_iの2元符号とする．このとき，式(37)から，次の式が成立する．

$$D_{\overline{B}_i}[C_i] = \delta_i d_{j_i} \tag{42}$$

［構成法1おわり］

構成法1を用いた，最も単純な変調符号Cの構成法は，$h = q$，各iについて，$j_i = i$とした場合である．このとき，各$1 \leq i \leq q$について，$\overline{B}_i = B_i$となる．この符号の構成法を基本多レベル符号構成法という．各$\overline{B}_i = \{0, 2^{i-1}\}$上の符号$C_i$は，同じ符号長，最小ハミング距離をもつ2元符号$C_{bi}$から，符号ベクトルの中の1を$2^{i-1}$と置き換えることによって構成可能である．以下，$C_i$を$2^{i-1}C_{bi}$と表す．

このとき，直和

$$C = C_{b1} + 2C_{b2} + \cdots + 2^{q-1}C_{bq} \tag{43}$$

は，加法群Aの上の線形符号を表す．各C_{bi}は2元コンポーネント符号と呼ばれる．C_{bi}を，最小距離δ_iの2元(n, k_{bi})符号とすると$|C|$は次式で表される．

$$|C| = 2^{\sum_{i=1}^{q} k_{bi}} \tag{44}$$

ここで，Cの次元kは次の式で表される．

$$k = \sum_{i=1}^{q} k_{bi} \tag{45}$$

また，Cの最小2乗ユークリッド距離は式(38)より，次の下界式で表される．

$$D[C] \geqq \min_{1 \leqq i \leqq q} \delta_i d_i = \min_{1 \leqq i \leqq q} 4\delta_i \sin^2(2^{i-1-q}\pi) \tag{46}$$

Cの各符号ベクトル$\bar{v}$を2^q値PSK信号点集合の点に写像することにより2^q値PSKブロック変調符号を得る．Cの実効レートR[C]は次の式で与えられる．

$$R[C] = \frac{1}{2n} \sum_{i=1}^{q} k_{bi} \tag{47}$$

つまり，R[C]は，符号Cで（信号点空間の）1次元当り送信される情報ビットの数である．Cの，符号化しない4値PSKに対する漸近的な符号化利得γ[C]は次の式で表される．

$$\gamma[C] = 10\log_{10}\frac{R[C]D[C]}{2} \tag{48}$$

ここで述べた基本多レベル符号構成法によるブロック変調符号の構成法はImai, Hirakawa(10)によって最初に提案され，次いでGinzburg(12)によって提案されたものである．その後，構成法の拡張についての研究が，いくつか行われている(13,15,16,17,18,19)．

ここで述べた方法によって構成された4値，8値，16値PSK用ブロック変調符号を表6に示す．但し，表中の(1)V_nは，2元(n,n)符号（$\{0,1\}^n$），(2)P_nは2元線形(n,n-1)偶パリティ符号，(3)$P_n^{\perp}$はP_nの双対符号である，(n,1)繰り返し符号，(4)$RM_{i,j}$は符号長2^iのj次のリードマラー符号，(5)s-$RM_{i,j}$は符号長2^iのj次のリードマラー符号の短縮符号，(6)G_eはゴーレイ符号の偶部分符号である．表6の符号は符号長が短く，長い最小2乗ユークリッド距離をもち，符号化しない4値PSK変調に対して3から7.2dBの符号化利得をもつ．また，それらのどの符号も，トレリス構造をもつ．ここで述べた方法で構成されたブロック変調符号Cのトレリス構造は，各コンポーネント符号C_{bi}がトレリス構造をもつならば，それらの直積をとることによって構成可能である．

［構成法2］

第2のコンポーネント符号C_iの構成法は，j_iを次の条件が成立するように選ぶ．

表6　基本多レベル符号構成法によるいくつかのM値ＰＳＫ用ブロック変調符号

	Length n	D[C]	R[C]	γ[C] (dB)	No. of states of trellis	Binary component codes C_{b1}	C_{b2}	C_{b3}	C_{b4}
4-PSK									
C_1	16	8	13/16	5.12	2^4	$RM_{4,2}$	P_{16}		
C_2	16	16	1/2	6.0	2^6	$RM_{4,1}$	$RM_{4,2}$		
C_3	32	16	21/32	7.2	2^8	$RM_{5,2}$	$RM_{5,3}$		
8-PSK									
C_4	8	4	1	3.0	2^2	$P_8^{\perp}$	P_8	V_8	
C_5	15	4	16/15	3.3	2^4	s-$RM_{4,1}$	$P_7 \times P_8$	V_{15}	
C_6	16	4	9/8	3.5	2^4	$RM_{4,1}$	P_{16}	V_{16}	
C_7	23	4	28/23	3.8	2^7	G_e	P_{23}	V_{23}	
C_8	32	8	63/64	5.8	2^9	$RM_{5,1}$	$RM_{5,3}$	P_{32}	
C_9	$4h+3$ $4 \le h \le 7$	8	$\frac{4h}{4h+3}$	$10\log_{10}\frac{16h}{4h+3}$	2^6	$P_{4h+3}^{\perp}$	s–$RM_{5,3}$	P_{4h+3}	
16-PSK									
C_{10}	32	4	5/4	3.9	2^8	$P_{32}^{\perp}$	$RM_{5,2}$	P_{32}	V_{32}

$$j_{i+1} = j_i + 2 \tag{49}$$

この場合，$\bar{B}i$は次の式を満たす．

$$\bar{B}_i = B_{j_i} + B_{j_i+1} \tag{50}$$

以下，この構成法２の説明中では，$\bar{B}_i$，B_{j_i}，B_{j_i+1}，d_{j_i}，d_{j_i+1}，2^{j_i}，2^{j_i+1}を，それぞれ，$\bar{B}$，B，B'，d，d'，1，2と表す．

C_{b1}を，ハミング距離δ_{b1}の２元線形(n, k_{b1})符号とする．C_{bi}は，0のｎ字組のみを符号語とする符号でもよい．そのとき，δ_{b1}は無限大と定義する．また，C_{b2}を，２元線形(n, k_{b1})符号とする．ｆをC_{b2}から，集合$(\{0,1\}^n - C_{b1}) \cup \{\bar{0}\}$への線形写像とする．また，写像ｆは，各$\bar{u}$，$\bar{v} \in C_{b2}$について，$f(\bar{u} \oplus \bar{v}) = f(\bar{u}) \oplus f(\bar{v})$とする（但し，記号$\oplus$は２を法とする加法を表す）．このとき，符号長ｎの$\bar{B}$上へのブロック符号を次の式で定義する．

$$F(C_{b1}, f, C_{b2}) \triangleq \{(\bar{u} \oplus f(\bar{v})) + 2\bar{v} \mid \bar{u} \in C_{b1},\ \bar{v} \in C_{b2}\} \tag{51}$$

明らかに，$F(C_{b1}, f, C_{b2})$の情報ビット数は$k_{b1}+k_{b2}$である．

ここで，$F(C_{b1}, f, C_{b2})$の最小距離について考える．まず，C_{b2}の部分符号$C_{b2,0}$を次式で定義する．

$$C_{b2,0} \triangleq \{\ \bar{v} \in C_{b2} \mid f(\bar{v}) = \bar{0}\ \} \tag{52}$$

$\delta_{2,0}$を$C_{b2,0}$の最小ハミング距離とする．また，$F(C_{b1}, f, C_{b2})$の部分符号C'を次式で定義する．

$$C' \triangleq \{(\bar{u} \oplus f(\bar{v})) + 2\bar{v} \mid \bar{u} \in C_{b1},\ \bar{v} \in C_{b2} - C_{b2,0}\} \tag{53}$$

$F(C_{b1}, f, C_{b2}) - C' = C_{b1} + C_{b2,0}$（但し，演算記号+は直和を表す）であるから，式(38)より，次式が成立する．

$$\underline{D}_{\bar{B}}[F(C_{b1}, f, C_{b2})] = \min\{\delta_1 d, \delta_{2,0} d', \underline{D}_{\bar{B}}[C']\} \tag{54}$$

ここで，2元n字組の集合$f[C_{b2}]$を次式で定義する．

$$f[C_{b2}] \triangleq \{f(\bar{v}) \mid \bar{v} \in C_{b2}\} \tag{55}$$

Xを2元ベクトルの集合とするとき$\delta[X]$を集合Xの最小非零ハミング重みとする．また，$(\bar{u} \oplus f(\bar{v})) + 2\bar{v}$を$C'$の要素とすると，$\bar{v} \notin C_{b2,0}$より，$f(\bar{v}) \neq \bar{0}$であり，$\bar{u} \in C_{b1}$かつ，$C_{b1} \cap f[C_{b2}] = \{\bar{0}\}$より，$\bar{u} \oplus f(\bar{v}) \neq \bar{0}$である．従って，$\underline{D}_{\bar{B}}[C']$について，次の下界式が成立する．

$$\underline{D}_{\bar{B}}[C'] \geqq \delta[C_{b1} \oplus f[C_{b2}]]d \tag{56}$$

但し，$C_{b1} \oplus f[C_{b2}]$は，次の式で定義される．

$$C_{b1} \oplus f[C_{b2}] \triangleq \{\bar{u} \oplus \bar{v} \mid \bar{u} \in C_{b1},\ \bar{v} \in f[C_{b2}]\} \tag{57}$$

$\delta_1 \geqq \delta[C_{b1} \oplus f[C_{b2}]]$と式(54)，(56)より，次の下界式が得られる．

$$\underline{D}_{\bar{B}}[F(C_{b1}, f, C_{b2})] \geqq \min\{\delta_{2,0}d', \delta[C_{b1} \oplus f[C_{b2}]]d\} \quad (58)$$

［構成法２おわり］

ここで，構成法２によって構成されたコンポーネント符号を用いた変調符号の構成例を示す．

［例１］

$q=3$，つまり，８値ＰＳＫ変調とする．また，$h=2$とし，$\bar{B}_1=B_1+B_2$，$\bar{B}_2=B_3$とする．符号長$n=8$とする．$C_{b1}=\{\bar{0}\}$，$C_{b2}=\{0,1\}^8$とする．$\bar{g}$を次式で定義される２元８字組とする．

$$\bar{g} \triangleq (1, 0, 0, \cdots, 0) \quad (59)$$

写像ｆを次の様に定義する．

$$\begin{cases} f(\sigma^i \bar{g}) \triangleq (0,0,0,0,1,1,1,1) & 0 \leqq i \leqq 3 \text{のとき} \\ f(\sigma^i \bar{g}) \triangleq (1,1,1,1,0,0,0,0) & 4 \leqq i \leqq 7 \text{のとき} \end{cases} \quad (60)$$

但し，$\sigma^i \bar{g}$は，$\bar{g}$をｉ回右に巡回シフトして得られる８字組である．

このとき，$\bar{B}_1$上の符号$[F(C_{b1}, f, C_{b2})]$を次の様に定義する．

$$[F(C_{b1}, f, C_{b2})] \triangleq \{ f(\bar{v}) + 2\bar{v} \mid \bar{v} \in C_{b2}\} \quad (61)$$

また，２元符号C_{b3}を$C_{b3} \triangleq \{0,1\}^8$とする．そのとき，８値ＰＳＫ変調用ブロック符号Ｃを次式で定義する．

$$C \triangleq [F(C_{b1}, f, C_{b2})] + 4C_{b3} \tag{62}$$

この符号は，情報ビット数k=16，実効レートR[C]=1，最小2乗ユークリッド距離D[C]=4である．また，この符号は8区間4状態のトレリスダイアグラムをもつ．

□

2．2　ブロック変調符号の符号化法と復号法

符号長nの2^q値PSKブロック変調符号Cの符号化法は次の様に行われる．kを式(35)で表されるCの次元とするとき，kビットの通報u（以下，第1章の第1節同様，セグメントと呼ぶ）を，h個のサブセグメントに分割する．i番目のサブセグメントは，長さk_{bi}ビットの通報からなる．各$1 \leq i \leq h$についてi番目のサブセグメントをCのi番目のコンポーネント符号C_{bi}で符号化し，符号ベクトル$\bar{v}_i$を得る．Aの上のn字組$\bar{v}$を次の式で表される直和とする．

$$\bar{v} = \bar{v}_1 + 2^{j2-1}\bar{v}_2 + \cdots + 2^{jh-1}\bar{v}_h \tag{63}$$

$$= (s_1, s_2, \cdots, s_n) \tag{64}$$

この$\bar{v}$が通報uに対するCの符号語である．この符号語$\bar{v}$を第1章の第1節と同様フレームと呼ぶ．$\bar{v}$の各要素s_1，s_2，…，s_qは2^q値PSKの信号点に写像し送信する．つまり，kビットの通報がn個の2^q値PSK変調の信号点の系列に符号化されたことになる．

M値PSK変調符号の軟判定最尤復号は次の様に行われる．加法

群 $A = \{0, 1, \cdots, 2^q-1\}$ の各元 s に対して，$X(s)$，$Y(s)$ を次の様に定義する．

$$X(s) = \cos(2^{q-1}\pi s), \quad Y(s) = \sin(2^{q-1}\pi s) \tag{65}$$

このとき，A の任意の 2 つの元 s，s' について，次の式が成立する．

$$d(s, s') = (X(s)-X(s'))^2 + (Y(s)-Y(s'))^2 \tag{66}$$

各 $1 \leqq j \leqq n$ について，(x_j, y_j) を受信フレームの j 番目の信号に対する復調器の出力とする．従って，受信フレーム $\bar{z}$ は 2n 字組 $(x_1, y_1, x_2, y_2, \cdots, x_n, y_n)$ で表される．送信符号語 $\bar{v}=(s_1, s_2, \cdots, s_n)$ と受信フレーム $\bar{z}$ について，$|\bar{z}, \bar{v}|^2$ を次式で定義する．

$$|\bar{z}, \bar{v}|^2 = \sum_{j=1}^{n} (x_j-X(s_j))^2+(y_j-Y(s_j))^2 \tag{67}$$

いま，通信路を加法的白色ガウス雑音をもつ通信路と仮定する．信号 s が送信されたとき，復調器の出力 (x, y) は，次の同時確率密度関数 $p(x, y)$ で表される分布となる．

$$p(x, y) = \frac{1}{2\pi\sigma^2} \exp\{-[(x_j-X(s_j))^2+(y_j-Y(s_j))^2]/2\sigma^2\} \tag{68}$$

但し，$\sigma^2 = 1/2\rho$，ρ は信号シンボル当りの S N 比である[21]．

このとき，受信フレーム $\bar{z}$ に対して，$|\bar{z}, \bar{v}|^2$ が最小となる $\bar{v} \in C$ を復号結果とする復号法は最尤復号となっている．$\bar{v}$ に対応するセグ

メントが受信セグメントである．Cが状態数の比較的少ないトレリスダイアグラムをもつならば，ヴィタビ復号法により，最尤復号が実現できる．

2^q値ＰＳＫ変調符号の誤り解析を行うためには，その符号の完全重み分布を求める必要がある．$\bar{v}=(s_1, s_2, \cdots, s_n)$を加法群Ａ上のｎ字組とする．$\bar{v}$の重み構成comp($\bar{v}$)は，次の$2^q$字組$\bar{t}$で表される．

$$\bar{t} = (t_0, t_1, \cdots, t_{2^q-1}) \tag{69}$$

但し，t_iは$\bar{v}$中の要素s_jのうち，Ａの要素ｉに等しいもの個数である．W($\bar{t}$)をcomp($\bar{v}$)=$\bar{t}$であるような符号Ｃに属する符号語$\bar{v}$の数とする．Ｔを次式で定義される集合とする．

$$T \triangleq \{ (t_0, t_1, \cdots, t_{2^q-1}) \mid \text{各} 0 \leqq i \leqq 2^q-1 \text{について，} 0 \leqq t_i \leqq n \} \tag{70}$$

このとき，{W($\bar{t}$) | t∈T}がＣの完全重み分布である．W($\bar{t}$)はＣの各コンポーネント符号C_{b1}, C_{b2}, …, C_{bh}の２元重み分布の結合重み分布[7]より求めることができる．第４節では，Ｃの完全重み分布を利用して，Ｃを加法的白色ガウス雑音をもつ通信路で使用したときの誤り特性を解析する方法を示している．文献(15,16,19)では，表６に示した符号の完全重み分布を示している．

3．変調符号を内部符号に用いた縦接符号化方式の符号化法と復号法

この節では，ここで取り上げる縦接符号化法の符号化法と復号法について述べる．内部符号C_1は，第２節で述べた符号長n_1，コンポーネント符号C_{b1}，C_{b2}，…，C_{bh}の2^q値ＰＳＫブロック変調符号を用いる．但し，各C_{bi}は２元線形(n_1, k_{bi})符号とする．C_1の情報ビット数k_1は次の式で表される．

$$k_1 = \sum_{i=1}^{h} k_{bi} \tag{71}$$

外部符号C_2は有限体$GF(2^\ell)$上の最小距離d_2の(n_2, k_2)リードソロモン符号，または，その短縮符号とする．C_2は最大距離分離符号であるから，$d_2=n_2-k_2+1$である．

n_2，k_1，ℓの間には，第１章と同様，式(1)の関係（$k_1=m_1\ell$）が成立しているものとする．

符号化は第１章と同じく，以下に示す２段階で行う．

(1)　第１段階では$k_2\times k_1(=k_2m_1\ell)$ビットの通報を図２に示す様に縦$k_2$，横$m_1\ell$の格子状に配置する．$k_2$個の各行それぞれを$m_1$個の長さ$\ell$のビット列に分割する．各$\ell$ビットを$GF(2^\ell)$の元とみなし，縦方向$k_2$個のシンボル列（セクション）それぞれを外部符号$C_2$で符号化する．

(2)　第２段階では第１段階で得られたn_2個の長さ$m_1\ell$の各行ベクトルを（それぞれの行を第１章同様，セグメントと呼ぶ）２．２節で述べた方法を用いて内部符号C_1で符号化する．符号化の結果，n_1個の2^q-ＰＳＫ変調の信号点の系列が符号語として得られる．内部

符号の符号語に対応する長さn_1の行ベクトルを第1章同様，フレームと呼ぶ．得られたn_2個のフレームを順に送信する．このn_2個のフレームの系列をブロック（図3参照）と呼ぶ．

データブロックの復号法も基本的には第1章で述べた縦接符号化法の復号法と同様，以下に述べる2段階で行われる．

(1) 第1段階では，まず受信された各フレームについて2．2節で述べた方法を用いて内部符号に基づいて復号を行う．各フレームの復号結果は外部符号の復号バッファに送られる．

(2) 第2段階では外部符号に基づき，シンボル誤りの訂正を行う．予め，$(d_2-1)/2$以下の非負整数t_2が定められているとする．ブロックの各セクション毎に外部符号に基づいてシンドロームを計算する．それらが，t_2個以下のセグメントの誤りに対応するものならば，それらの訂正を行い（復号に成功したという），ブロックを受理する．そうでなければ，ブロック全体を消去する（または，再送を要求する）．

4．誤り特性の解析

この節では，第3節で述べた縦接符号化法を加法的白色ガウス雑音をもつ通信路で用いたときの誤り特性の解析法について述べる．ここでは，内部符号の各符号語は等確率で送信されるものと仮定する．

$P_c^{(1)}$，$P_{ic}^{(1)}$をそれぞれ受信フレームが正しく復号される確率，誤って復号される確率とする．内部符号C_1は，コンポーネント毎の2^qを法とする加法について閉じているので，一般性を失うことなく，コンポーネントがすべて0の符号語$\bar{0}$を送信すると仮定する．各受信フレーム$\bar{z}$に対して，$\bar{z}$が正しく復号されるための条件は，C_1のすべての符号語$\bar{v}\neq\bar{0}$に対して，次式が成立することである．

$$|\bar{z},\bar{v}|^2 > |\bar{z},\bar{0}|^2 \tag{72}$$

但し，$|\bar{z},\bar{v}|^2=|\bar{z},\bar{0}|^2$となる確率は0とする．

式(67)より，式(72)は次の様に書き換えられる．

$$2\sum_{j=1}^{n_1}(X(s_j)-1)(x_j-1)+Y(s_j)y_j <$$

$$\sum_{j=1}^{n_1}(X(s_j)-1)^2+Y(s_j)^2 = d^{(n)}(\bar{v},\bar{0}) \tag{73}$$

但し，$\bar{z}=(x_1,y_1,x_2,y_2,\cdots,x_{n_1},y_{n_1})$，$\bar{v}=(s_1,\ s_2,\ \cdots,\ s_{n_1})$とする．

$Q(\bar{v})$を式(73)の不等式を満たす$2n_1$字組$(x_1,y_1,x_2,y_2,\cdots,x_{n_1},y_{n_1})$の集合とする．集合$Q_c$を次式で定義する．

$$Q_c \triangleq \bigcap_{\bar{v} \in C_1 - \{\bar{0}\}} Q(\bar{v}) \tag{74}$$

このとき，式(68)から次式が成立する．

$$P_c^{(1)} = \frac{1}{(2\pi\sigma)^{n_1}} \int \cdots \int_{Q_c} \exp\{-[\sum_{j=1}^{n_1}((x_j-1)^2+y_j^2)/2\sigma^2\}$$

$$dx_1 dy_1 \cdots dx_{n_1} dy_{n_1} \tag{75}$$

但し，式(75)中の積分はQ_cの全範囲について行う．

Sを次の条件を満たす$C_1-\{\bar{0}\}$の部分集合とする．

$$\bigcap_{\bar{v} \in C_1 - \{\bar{0}\}} Q(\bar{v}) = \bigcap_{\bar{v} \in S} Q(\bar{v}) \tag{76}$$

式(76)を満足する集合Sを，以下，$C_1-\{\bar{0}\}$の代表集合と呼ぶ．

C_1の$\bar{0}$以外の各符号語$\bar{v}$に対して，$P_e^{(1)}(\bar{v})$を，受信フレーム$\bar{z}$が次の不等式を満たす確率とする．

$$|\bar{z},\bar{v}|^2 < |\bar{z},\bar{0}|^2 \tag{77}$$

式(77)は，次式の様に書き換えることができる．

$$2\sum_{j=1}^{n_1}(X(s_j)-1)(x_j-1)+Y(s_j)y_j \geq |\bar{v}|^2 \tag{78}$$

但し，$|\bar{v}|^2 \triangleq d^{(n)}(\bar{v},\bar{0})$とする．確率変数：

$$2\sum_{j=1}^{n_1}(X(s_j)-1)(x_j-1)+Y(s_j)y_j$$

は平均0，分散$4\sigma^2|\bar{v}|^2$の正規分布に従う．従って，$P_e^{(1)}(\bar{v})$について，次式が成立する．

$$P_e^{(1)}(\bar{v}) = \int_{|\bar{v}|^2}^{\infty} \frac{1}{2\sqrt{2\pi}\,\sigma\,|\bar{v}|} \exp\{-\frac{x^2}{8\sigma^2|\bar{v}|^2}\}dx$$

$$= \frac{1}{2}\,\mathrm{erfc}(\frac{|\bar{v}|}{2\sqrt{2}\sigma}) = \frac{1}{2}\,\mathrm{erfc}(\frac{\sqrt{\rho}\,|\bar{v}|}{2}) \qquad (79)$$

但し，erfc(x)はガウスの補誤差関数であり，次の式で定義される．

$$\mathrm{erfc}(x) = \frac{2}{\sqrt{\pi}}\int_x^{\infty} e^{-t^2}dt \qquad (80)$$

また，ρはシンボル当りのSN比である[21]．

$\bar{Q}_c$，$\bar{Q}(\bar{v})$を，それぞれ，Q_c，$Q(\bar{v})$の補集合とする．そのとき，式(74)，(76)から，次式が成立する．

$$\bar{Q}_c = \bigcap_{\bar{v}\in S}\bar{Q}(\bar{v}) \qquad (81)$$

以上の議論より，$P_{ic}^{(1)}$について，次の上界式が成立する．

$$P_{ic}^{(1)} = 1 - P_c^{(1)} \leqq \sum_{\bar{v}\in S} P_e^{(1)}(\bar{v}) \qquad (82)$$

実数の集合Δを，任意のC_1の$\bar{0}$以外の各符号語$\bar{v}$について，$d = d^{(n)}(\bar{v},\bar{0})$ならば，$d\in\Delta$，であるような集合とする．$A_d[S]$を，$d = d^{(n)}(\bar{v},\bar{0})$を満たす，Sに属する$C_1$の符号語$\bar{v}$の個数とする．式(53)，(56)から，次の不等式が成立する．

$$P_{ic}^{(1)} \leqq \frac{1}{2} \sum_{d \in \Delta} A_d[S] \ \mathrm{erfc}\left(\frac{\sqrt{d\rho}}{2}\right) \tag{83}$$

集合$A_d[C_1-\{\bar{0}\}]$はC_1の完全重み分布より求めることができる．$C_1-\{\bar{0}\}$の代表集合Sを小さく選ぶことができれば，$A_d[S]$は，dの値がC_1の最小2乗ユークリッド距離に近いところを除いて，$A_d[C_1-\{\bar{0}\}]$と比較して，かなり少なくすることができる．

次に，縦接符号全体の誤り特性の解析法について述べる．

P_c，P_{es}，P_{er}を，それぞれ，ブロック全体が正しく復号される確率，消去される確率，誤って復号される確率とする．P_c，P_{es}，P_{er}について，次の式が成立する．

$$1 - P_c = P_{es} + P_{er} = \sum_{i=t_2+1}^{n_2} \binom{n_2}{i} [P_{ic}^{(1)}]^i [1-P_{ic}^{(1)}]^{n_2-i} \tag{84}$$

$\bar{P}_{ic}^{(1)}$を$P_{ic}^{(1)}$の上界（例えば，式(82)の右辺）とする．そのとき，式(84)から，P_cについて，次の下界式が成立する．

$$P_c \geqq 1 - \sum_{i=t_2+1}^{n_2} \binom{n_2}{i} g_{n_2,i}(\bar{P}_{ic}^{(1)}) \tag{85}$$

但し，

$$g_{n_2,i}(x) = \begin{cases} x^i(1-x)^{n_2-i} & 0 \leqq x \leqq i/n_2 \text{のとき} \\ (i/n_2)^i(1-i/n_2)^{n_2-i} & \text{それ以外のとき} \end{cases} \tag{86}$$

$p_e(\bar{u})$を内部符号C_1による復号の結果得られた復号後のセグメントの誤りパターンが$\bar{u}$である確率とする．非負整数iについて，Q_i

を次式の集合から，その要素を大きいものから順に i 個選び，その和をとったものとする．

$$\{\ p_e(\bar{u})^i \mid \bar{u} \in [GF(2^{\ell})^{m_1}]-\{\bar{0}\}\ \} \tag{87}$$

このとき，付録Eと同様の議論から，P_{er}について，次の上界式が成立する．

$$P_{er} \leqq \sum_{w=d_2}^{n_2-i} \binom{n_2}{w} \sum_{h=0}^{\min\{t_2,\, n_2-w\}} \binom{n_2-w}{h} \sum_{j=w+h-t_2}^{w} \binom{w}{j} \bar{P}(w,h,j) \tag{88}$$

但し，$\bar{P}(w,h,j)$は次の式で定義される．

$$\bar{P}(w,h,j) \triangleq [P_{ic}^{(1)}]^{w+h-d_2}\ [1-P_{ic}^{(1)}]^{n_2-w-h}\, Q_{j+d_2-w} \tag{89}$$

式(85)，(88)の右辺をそれぞれ$\underline{P}_c$，$\bar{P}_{er}$で表す．$\underline{P}_c$，$\bar{P}_{er}$は，それぞれ，P_cの下界，P_{er}の上界となっている．確率$1-\underline{P}_c$は，ブロックが復号に失敗する確率と誤って復号される確率の和の上界となっている．

5．変調符号を内部符号に用いた縦接符号化方式の具体例

この節では，第3節で述べた縦接符号化方式のいくつかの具体例について述べ，それらの誤り特性と，符号化しない4値ＰＳＫに対する符号化利得を示す．どの具体例も外部符号は$GF(2^8)$上のＮＡＳＡ標準(255,223)リードソロモン符号を用いる．また，内部符号はすべて8値ＰＳＫ上のブロック変調符号である．

5．1　具体例1

具体例1の内部符号は，表6の符号C_4である．この符号は，符号長$n_1=8$，情報ビット数$k_1=16$，最小2乗ユークリッド距離$D[C]=4$，実効レート$R[C]=1$である．従って，式(48)より，この符号の漸近的な符号化利得$\gamma[C]$は3ｄＢである．この符号は8区間4状態のトレリスダイアグラムをもつ．従って，容易に軟判定ヴィタビ復号可能である．また，この符号の重要な特徴は45°の位相回転について閉じていることである[19]．従って，キャリア位相の再同期化を高速に行うことが可能である．

この符号の完全重み分布は次の式で表される．

各整数i,j,h，但しiは偶数，かつ，$0 \leqq j \leqq i \leqq 8$，$0 \leqq h \leqq 8-i$について

$$W((h,0,j,0,8-i-h,0,i-j,0))$$

$$= W((0,h,0,j,0,8-i-h,0,i-j))$$

$$= \binom{8}{i}\binom{i}{j}\binom{8-i}{h} \tag{90}$$

上記以外の$\bar{t}=(t_0, t_1, \cdots, t_7)$については，$W(\bar{t})=0$である．

$C_1-\{\bar{0}\}$の代表集合を求めることにより，次式で示される上界式が得られる．

$$P_{ic}^{(1)} \leqq 60\mathrm{erfc}(\sqrt{\rho}) + 64\mathrm{erfc}(\sqrt{2(2-\sqrt{2})\rho}) + 512\mathrm{erfc}\left(\frac{\sqrt{2(8-3\sqrt{2})\rho}}{2}\right) \tag{91}$$

式(91)の右辺を$\bar{P}_{ic}^{(1)}(C_{1,4})$と表す．図10に，この符号の誤って復号される確率の上界$\bar{P}_{ic}^{(1)}(C_{1,4})$と$P_{ic}^{(1)}$に関するシミュレーション結果（以下，記号$P_{ic,s}^{(1)}$で表す），及び，符号化しない4値ＰＳＫの誤り特性を示す．図より，この符号は符号化しない4値ＰＳＫに対して，誤って復号される確率が10^{-5}となる点で2.31dB，10^{-6}となる点で2.42dBの符号化利得があることがわかる．

次に，縦接符号全体の誤り特性について示す．$k_1=16$より，$m_1=2$，つまり，インターリービングの度数は２である．また，縦接符号全体の実効レートは(223/255)=0.875である．外部符号の復号では，１６セグメントまでの誤り訂正を行う．つまり，$t_2=16$である．そのときの，ブロックが復号に失敗する確率と誤って復号される確率の和の上界$1-\underline{P}_c$（式(85)の右辺）と，ブロックが誤って復号される確率の上界$\bar{P}_{er}$（式(88)の右辺）を，それぞれ，図11と12に示す．それらの図では，式(59)及び(62)の中の$P_{ic}^{(1)}$，Q_iの代わりにシミュレーションの結果$P_{ic,s}^{(1)}$，$Q_{i,s}$を用いて計算を行った結果（それぞれ，記号$1-P_{c,s}$，$\bar{P}_{er,s}$と表す．）を示す．Q_iに関するシミュレー

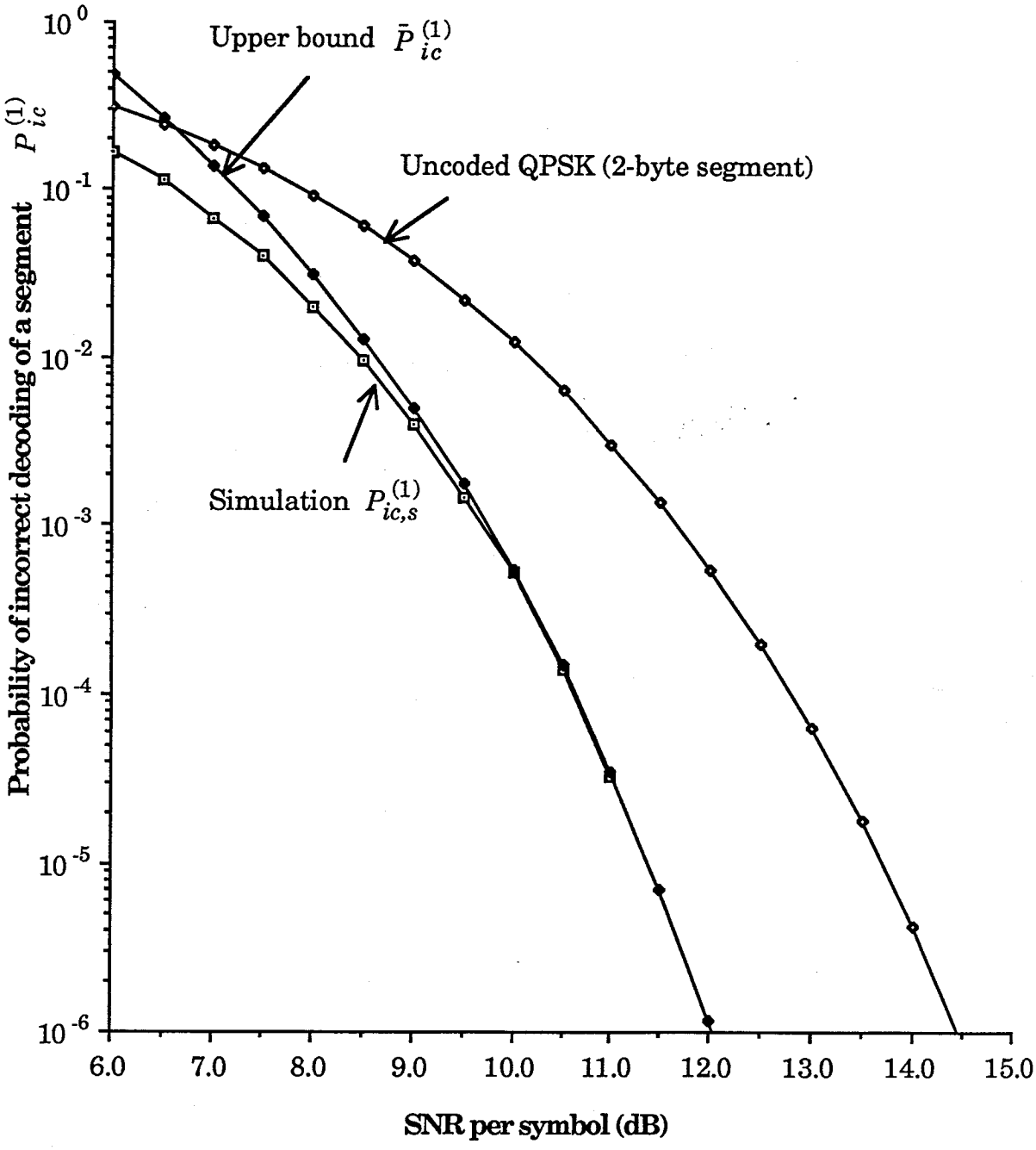

図10　８値ＰＳＫ変調符号（表６のC_4）の誤って復号される確率の上界の値とシミュレーション結果，及び，16ビットの通報を符号化しない４値ＰＳＫで送信したとき誤って受信される確率

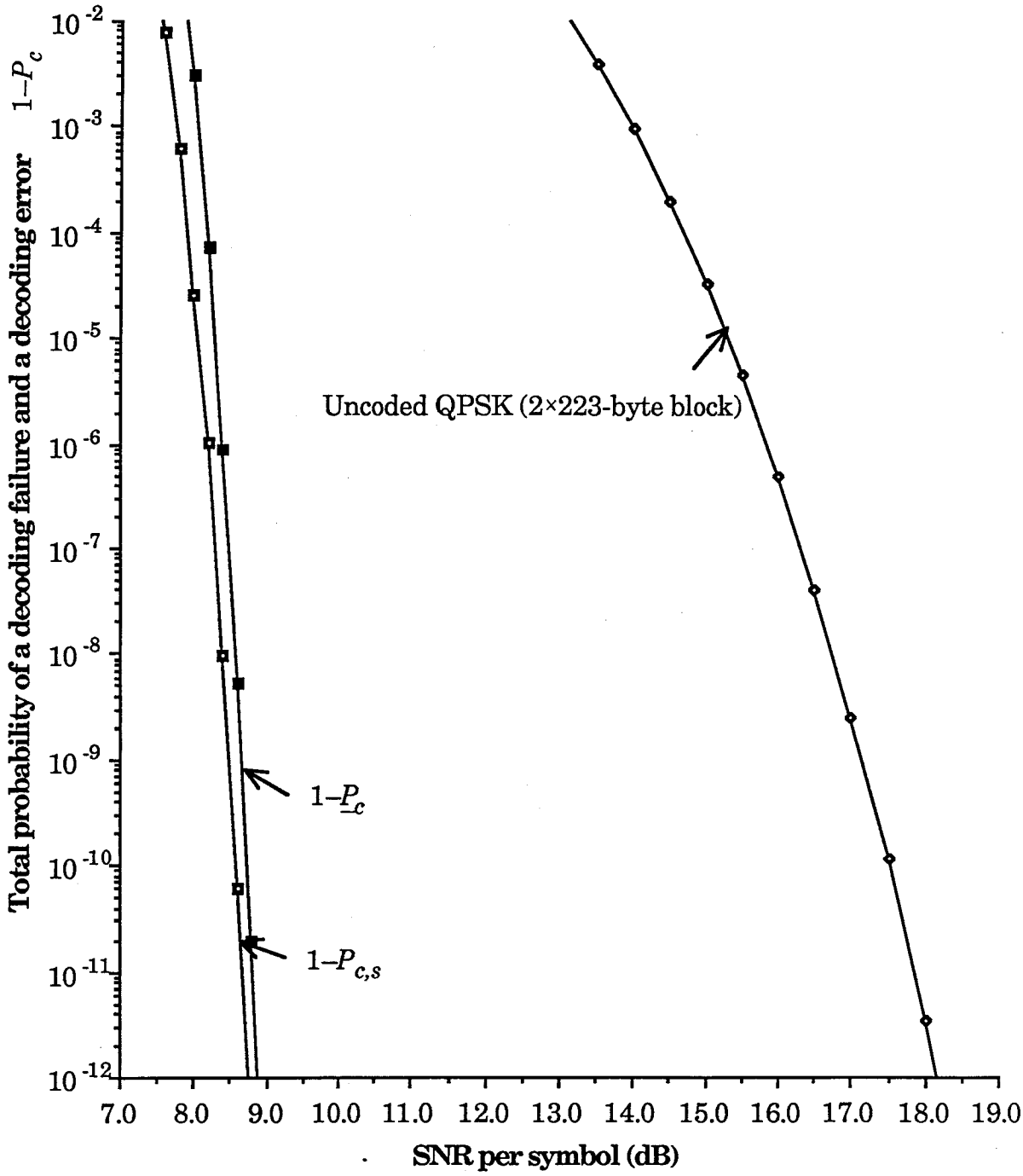

図11　内部符号に表６のC_4，外部符号に(255, 223)ＲＳ符号を用いた縦接符号の復号に失敗する確率と誤って復号される確率の和，及び，2×223ビットの通報を符号化しない４値ＰＳＫで送信したとき誤って受信される確率

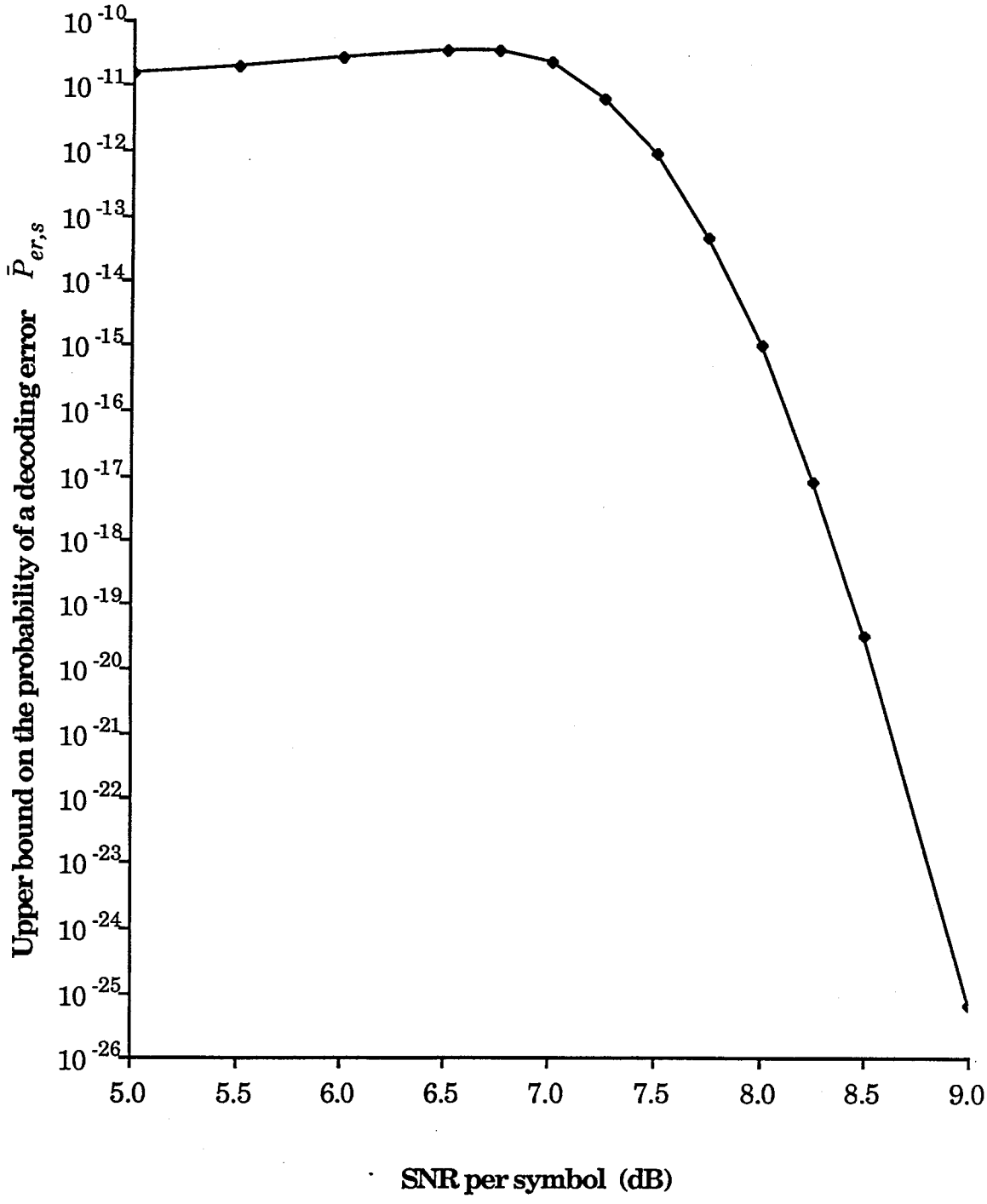

図12　内部符号に表６のC_4，外部符号に(255, 223)ＲＳ符号を用いた縦接符号の誤って復号される確率の上界の値

ション結果$Q_{i,s}$の信頼性向上のために，以下の事実を用いている．

(1) 内部符号による復号後のフレームの誤りパターン$\bar{v}$の重み構成を$(t_0, t_1, \cdots, t_7)$とするとき，復号後のフレームで特定の誤りパターン$\bar{v}$が起こる確率は次の式で表される5字組の値のみに依存する．

$$(t_0, t_1+t_7, t_2+t_6, t_3+t_5, t_4) \tag{92}$$

(2) 復号後のフレームから，復号後のセグメントが一意に定まる．

図11，12から，具体例1は，非常に高い信頼性と高いスループットをもつことがわかる．例えば，シンボルあたりのＳＮ比が9dBのとき，誤って復号される確率は，高々10^{-24}である．また，復号に失敗する確率は高々4.95×10^{-16}（内部符号の誤り特性の評価にシミュレーションを用いたとき）である．また，図11から，ブロックの復号失敗確率を評価基準としたときの符号化しない4値ＰＳＫに対する符号化利得は，ブロックの復号失敗確率が10^{-7}，10^{-10}の点で，それぞれ，8dB，9dBである．

誤り制御通信方式を，ファイル転送に応用する場合であれば，誤り特性の評価は，ブロックの復号失敗確率や誤って復号される確率によるべきであるが，それ以外の応用では，通常，復号後のビット誤り率による評価が用いられている．以下，復号後のビット誤り率について，２種類の評価法を考える．

第１の評価法P_{b1}は，ブロックの誤って復号される確率P_{er}から，次の換算式を用いて得られる概算値である．

$$P_{b1} \triangleq \frac{d_2}{2n_2} P_{er} \tag{93}$$

ブロックが復号に失敗したとき，再送が許される応用では，復号後のビット誤り率は式(93)が１つの評価値となる．図13に具体例１のP_{b1}の上界の値と符号化しない４値ＰＳＫのビット誤り率を示す．具体例１のP_{b1}を評価基準としたときの符号化しない４値ＰＳＫに対する符号化利得は，P_{b1}が10^{-12}の点で，9.8dBである．

第２の評価法P_{b2}は，ブロックが復号に失敗する確率と誤って復号される確率の和$1-P_c$から，次の換算式を用いて得られる概算値である．

$$P_{b2} \triangleq \frac{d_2}{2n_2}(1-P_c) \tag{94}$$

ブロックが復号に失敗したとき，再送が許されない応用では，復号後のビット誤り率は式(94)が１つの評価値となる．図14に具体例１のP_{b2}の値と符号化しない４値ＰＳＫのビット誤り率を示す．具体例１について，P_{b2}を評価基準としたときの符号化しない４値ＰＳＫに対する符号化利得は，P_{b2}が10^{-6}，10^{-10}の点で，それぞれ，5.52dB，7.60dBである．

５．２　具体例２

具体例２の内部符号は，表６のC_5である．この符号は，符号長n_1=16，次元（情報ビット数）36，最小２乗ユークリッド距離D[C]=4，実効レートR[C]=9/8である．従って，式(48)より，この符号の漸近的な符号化利得γ[C]は3.52ｄＢである．この符号は４区間16状態のトレリスダイアグラムをもつ．従って，具体例１よりも大きな復

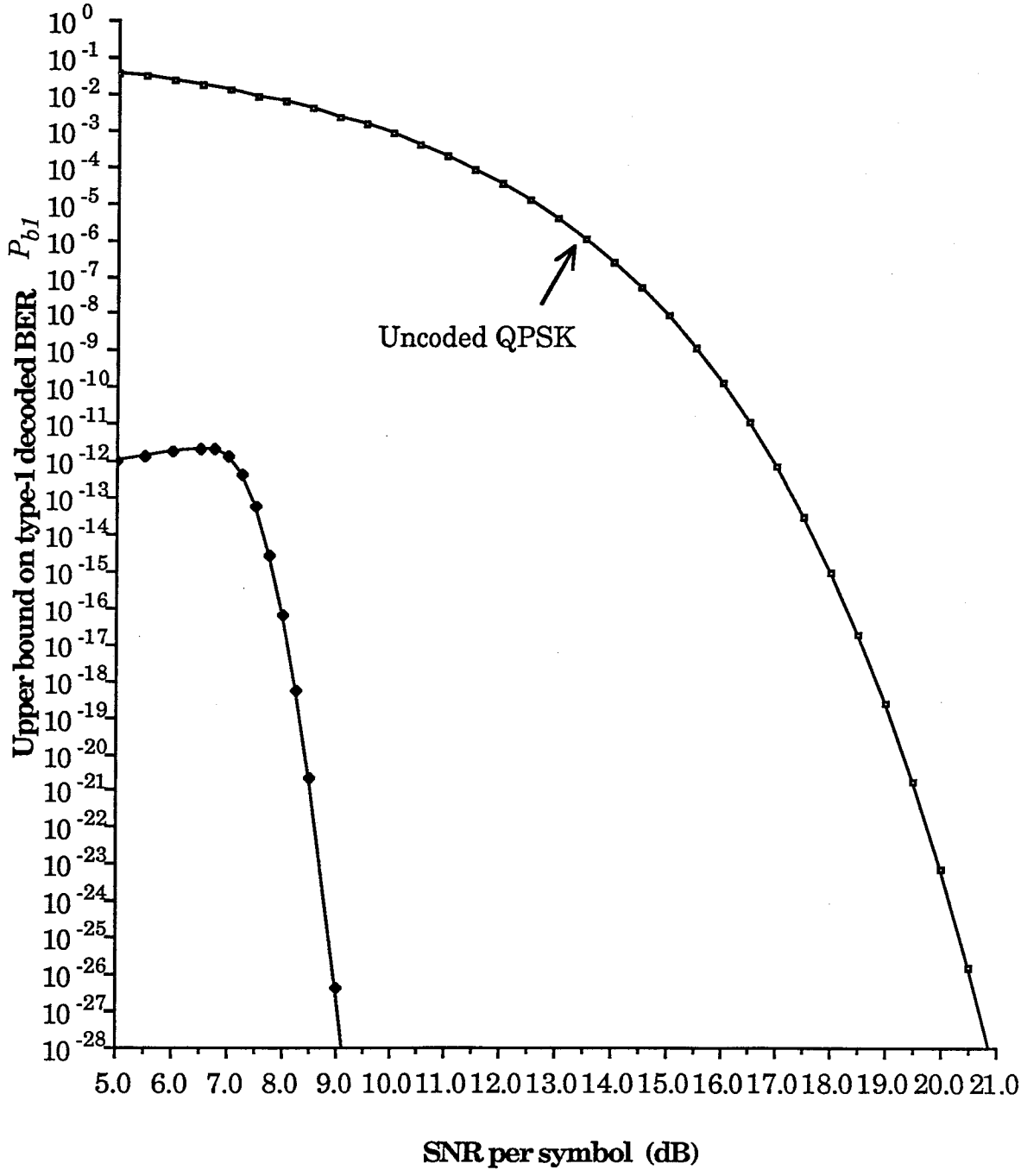

図13　内部符号に表６のC_4，外部符号に(255,223)ＲＳ符号を用いた縦接符号の復号後のビット誤り率の評価値P_{b1}の上界値，及び，符号化しない４値ＰＳＫの誤り確率

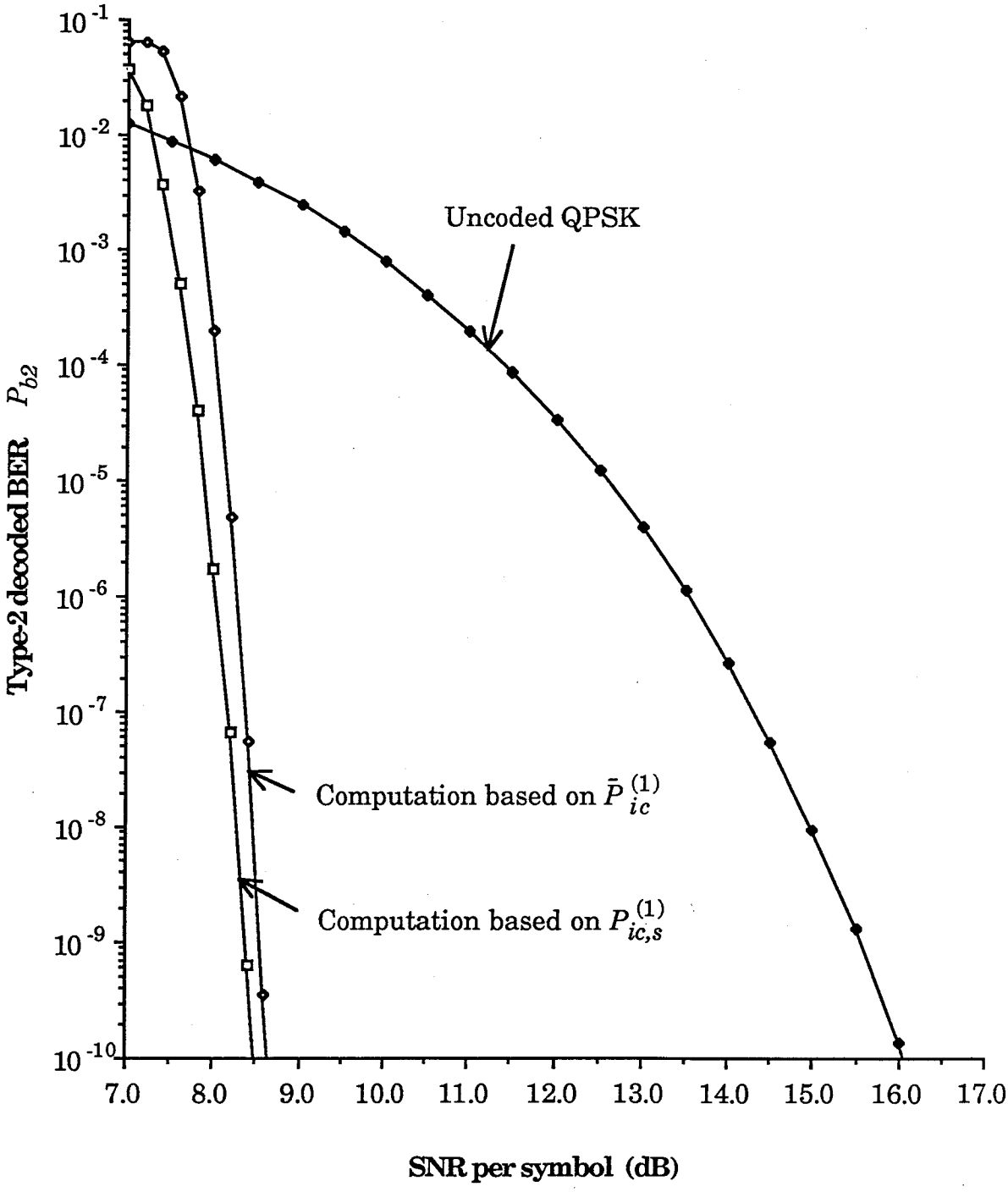

図14　内部符号に表６のC_4，外部符号に(255, 223)ＲＳ符号を用いた縦接符号の復号後のビット誤り率の評価値P_{b2}，及び符号化しない４値ＰＳＫの誤り確率

号複雑度をもつ．また，この符号も45°の位相回転について閉じている[19]．

この符号の完全重み分布は次の式で表される．

各整数$i, j, h, k_0, k_1, k_2, k_3$，但し$j$は偶数，かつ，

$0 \leqq i \leqq 16$，$0 \leqq j \leqq 16$，$0 \leqq h \leqq 16-j$，$0 \leqq k_0 \leqq h$，

$0 \leqq k_1 \leqq 16-j-h$，$0 \leqq k_2 \leqq 16-i-h$，$0 \leqq k_3 \leqq i+j+h-16$について

$$W((k_0, k_1, k_2, k_3, h-k_0, 16-j-h-k_1, 16-i-h-k_2, i+j+h-16-k_3))$$

$$= BW(i) \binom{16}{j} \binom{16-j}{h} \binom{h}{k_0} \binom{16-j-h}{k_1} \binom{16-i-h}{k_2} \binom{i+j+h-16}{k_3} \tag{95}$$

但し，$BW(i)$は，符号長16の1次のリードマラー符号の重みiの符号語数である．上記以外の$\bar{t}=(t_0, t_1, \cdots, t_7)$については，$W(\bar{t})=0$である．

$C_1-\{\bar{0}\}$の代表集合を求めることにより，次式で示される上界式が得られる．

$$P_{ic}^{(1)} \leqq 248\mathrm{erfc}(\sqrt{\rho}) + 1920\mathrm{erfc}(\sqrt{2(2-\sqrt{2})\rho})$$

$$+ 30720\mathrm{erfc}\left(\frac{\sqrt{2(9-4\sqrt{2})\rho}}{2}\right) + 15360\mathrm{erfc}\left(\frac{\sqrt{2(8-3\sqrt{2})\rho}}{2}\right)$$

$$+ 16384\mathrm{erfc}(2\sqrt{(2-\sqrt{2})\rho}) + 245760\mathrm{erfc}\left(\frac{\sqrt{3(8-3\sqrt{2})\rho}}{2}\right)$$

$$+ 262144\mathrm{erfc}\left(\frac{\sqrt{2(16-7\sqrt{2})\rho}}{2}\right) \qquad (96)$$

式(96)の右辺を$\bar{P}_{ic}^{(1)}(C_{1,5})$と表す．図15に，この符号の誤って復号される確率の上界$\bar{P}_{ic}^{(1)}(C_{1,5})$と$P_{ic}^{(1)}$に関するシミュレーション結果$P_{ic,s}^{(1)}$，及び，符号化しない4値ＰＳＫの誤り特性を示す．図より，この符号は符号化しない4値ＰＳＫに対して，誤って復号される確率が10^{-6}となる点で2.26dBの符号化利得があることがわかる．

次に，縦接符号全体の誤り特性について示す．C_5の情報ビット数は36であり，８の倍数ではないので，内部符号を２つ連接することにより，情報ビット数k_1=72とし，m_1=9とする．つまり，インターリービングの度数は９である．また，縦接符号全体の実効レートは(9/8)(223/255)=0.9838である．つまり，具体例２では，帯域幅の拡大はほとんど起こらない．外部符号の復号では，１６セグメントまでの誤り訂正を行う．つまり，t_2=16である．そのときの，ブロックが復号に失敗する確率と誤って復号される確率の和の上界$1-\underline{P}_c$（式(85)の右辺）と，ブロックが誤って復号される確率の上界$\bar{P}_{er}$（式(88)の右辺）を，それぞれ，図16と17に示す．それらの図では，具体例１同様，内部符号の誤り特性評価にシミュレーションによる結果$P_{ic,s}^{(1)}$，$Q_{i,s}$を用いて計算を行った結果$1-P_{c,s}$，$\bar{P}_{er,s}$を示す．

図16，17から，具体例２も，非常に高い信頼性と高いスループットをもつことがわかる．例えば，シンボルあたりのＳＮ比が10dBのとき，誤って復号される確率は，高々10^{-40}である．また，復号に失敗する確率は高々2.08×10^{-12}（内部符号の誤り特性の評価にシミュレーションを用いたとき）である．また，図16から，ブロックの復号失敗確率を評価基準としたときの符号化しない4値ＰＳＫに対する符号化利得は，ブロックの復号失敗確率が10^{-7}，10^{-10}の点

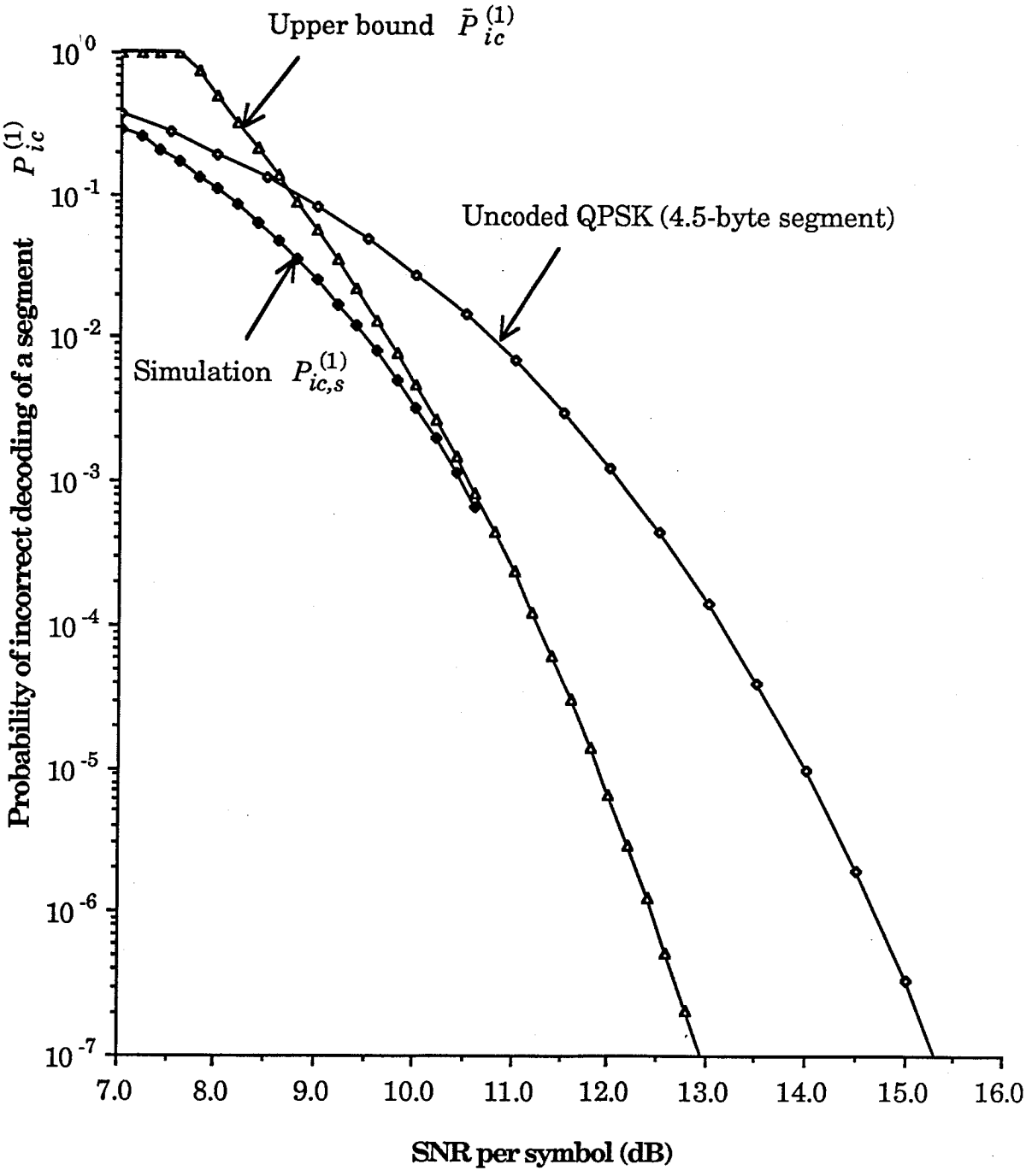

図15　８値ＰＳＫ変調符号（表６のC_5）の誤って復号される確率の上界の値とシミュレーション結果，及び，36ビットの通報を符号化しない４値ＰＳＫで送信したとき誤って受信される確率

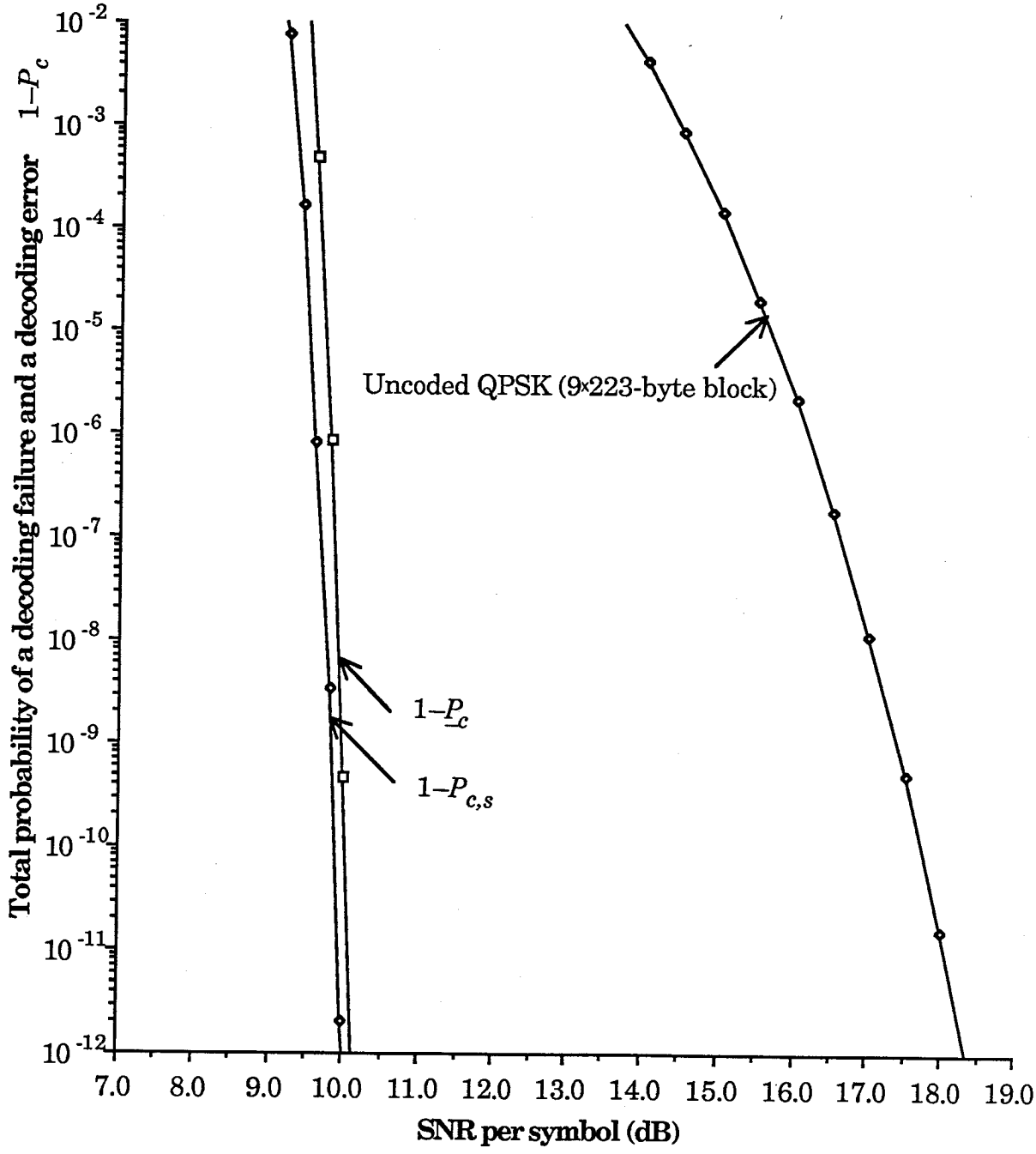

図16　内部符号に表６のC_5，外部符号に(255, 223)ＲＳ符号を用いた縦接符号の復号に失敗する確率と誤って復号される確率の和，及び，9×223ビットの通報を符号化しない４値ＰＳＫで送信したとき誤って受信される確率

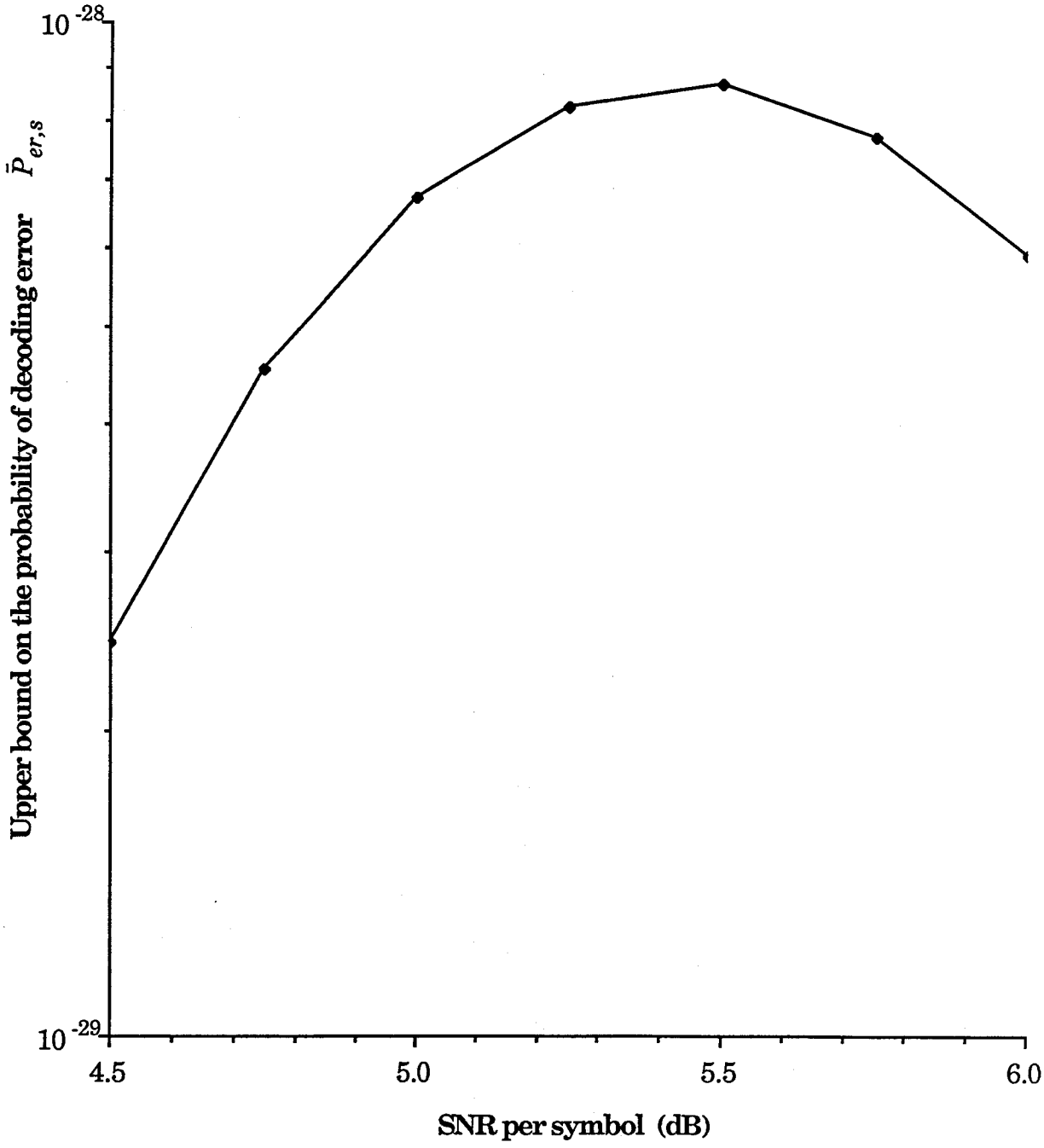

図17　内部符号に表６のC_5，外部符号に(255, 223)ＲＳ符号を用いた縦接符号の誤って復号される確率の上界の値

で，それぞれ，7dB，8dBである．

また，図18，19に具体例2の復号後のビット誤り率P_{b1}の上界値，及び，P_{b2}の値と符号化しない4値PSKのビット誤り率を示す．具体例2のP_{b1}を評価基準としたときの符号化しない4値PSKに対する符号化利得は，P_{b1}が10^{-31}の点で，15dBである．P_{b2}を評価基準としたときの符号化しない4値PSKに対する符号化利得は，P_{b2}が10^{-6}，10^{-10}の点で，それぞれ，4.05dB，6.26dBである．

5．3　具体例3

具体例3の内部符号は，第2節の例1で述べた符号である．この符号は，符号長$n_1=8$，情報ビット数$k_1=16$，最小2乗ユークリッド距離$D[C]=4$，実効レート$R[C]=1$である．従って，式(48)より，この符号の漸近的な符号化利得$\gamma[C]$は3dBである．この符号は8区間4状態のトレリスダイアグラムをもつ．従って，容易に軟判定ヴィタビ復号可能である．また，この符号は90°の位相回転について閉じている(19)．従って，キャリア位相の再同期化を高速に行うことが可能である．

この符号の完全重み分布は次の式で表される．

各整数$i_f, j_f, h_f, i_b, j_b, h_b$，但し$0 \leqq j_f \leqq i_f \leqq 4$，$0 \leqq j_b \leqq i_b \leqq 4$，$0 \leqq h_f \leqq 4-i_f$，$0 \leqq h_b \leqq 4-i_b$，また，$i_b$が偶数ならば$i_f$は偶数，について

1）i_f，i_bともに偶数のとき

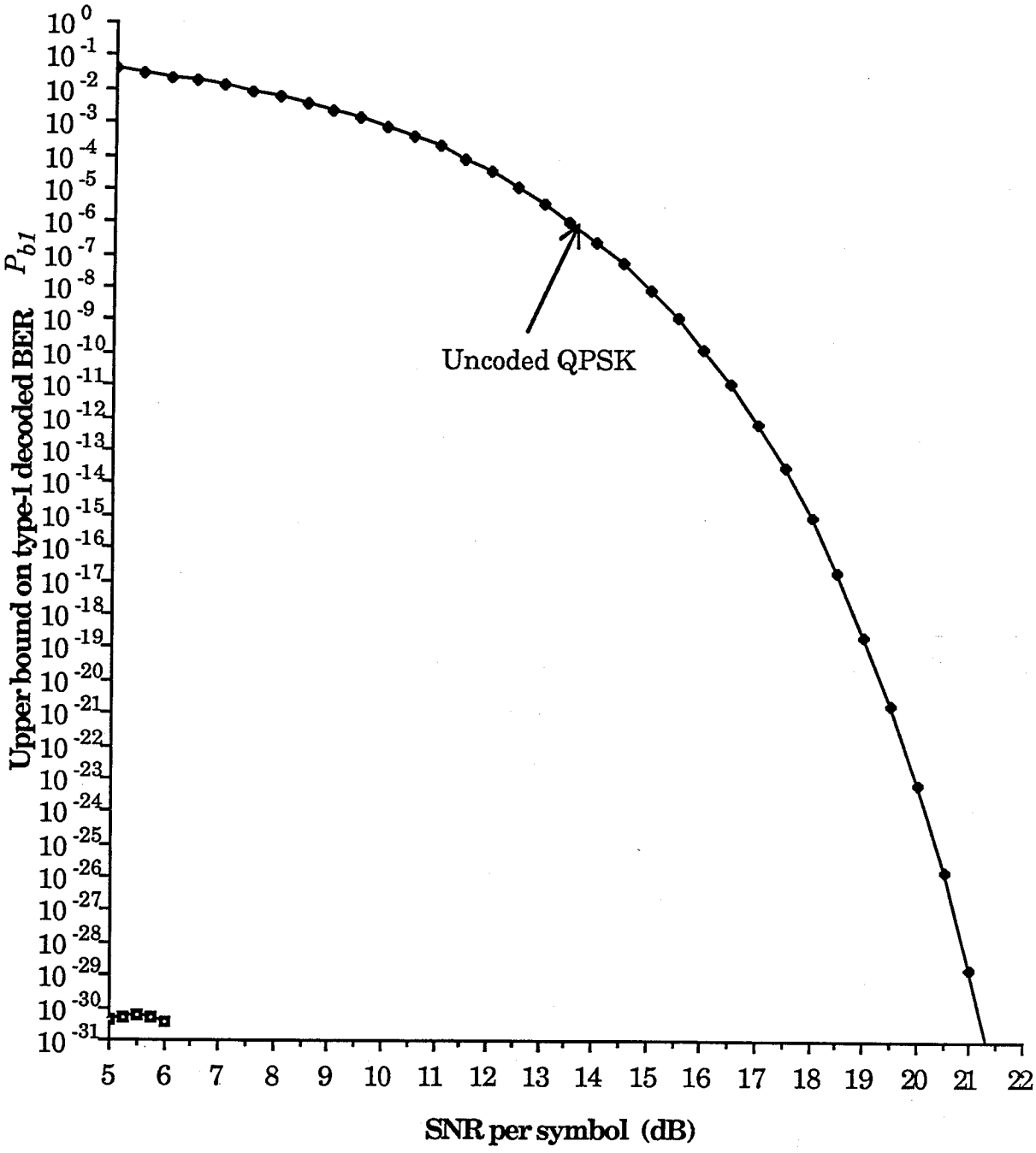

図18　内部符号に表６のC_5，外部符号に(255, 223)ＲＳ符号を用いた縦接符号の復号後のビット誤り率の評価値P_{b1}の上界値，及び，符号化しない４値ＰＳＫの誤り確率

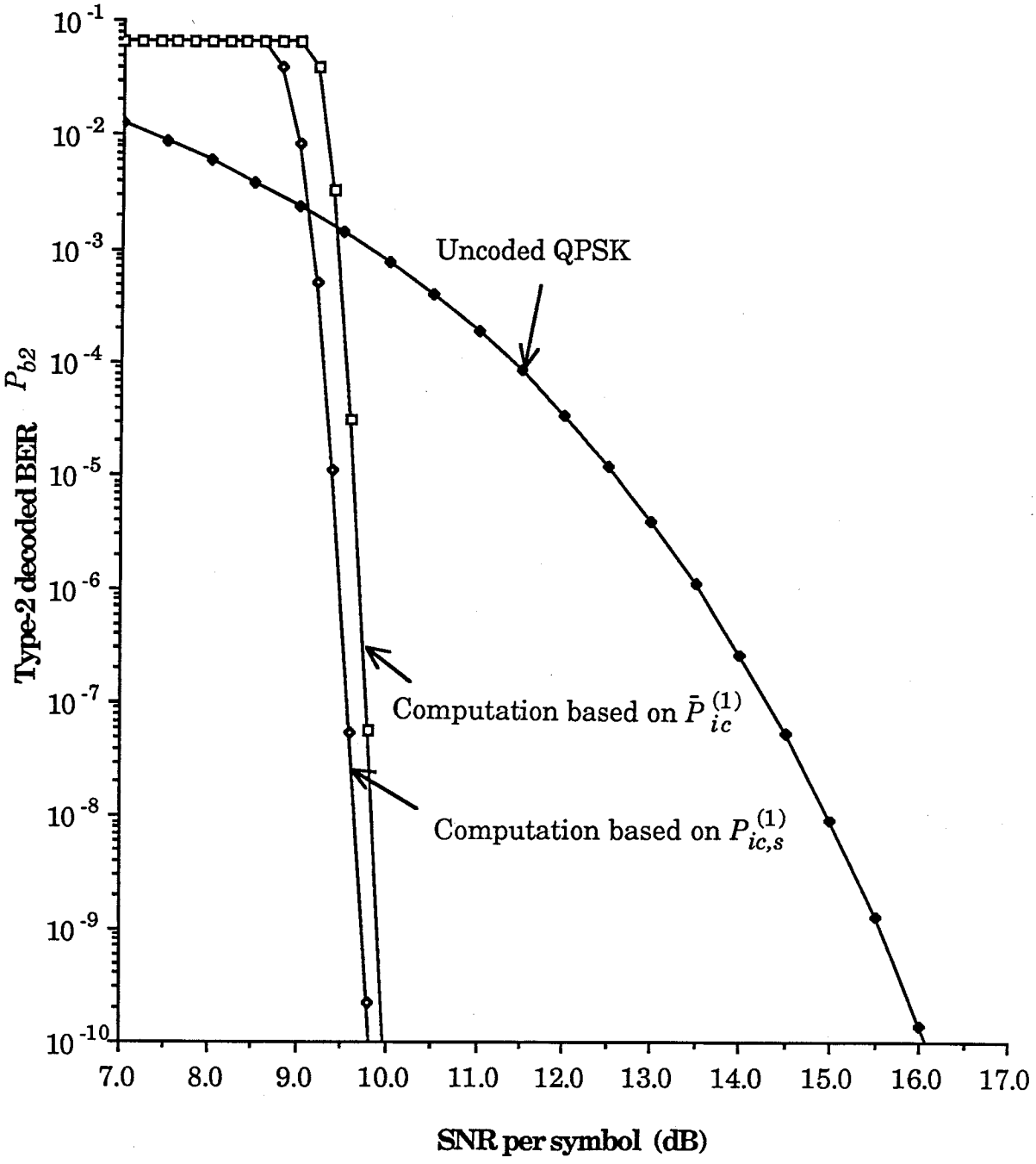

図19　内部符号に表６のC_5，外部符号に(255, 223)ＲＳ符号を用いた縦接符号の復号後のビット誤り率の評価値P_{b2}，及び符号化しない４値ＰＳＫの誤り確率

$$W((8-i_f-i_b-h_f-h_b, 0, i_f+i_b-j_f-j_b, 0, h_f+h_b, 0, j_f+j_b, 0))$$

$$= \quad Wg(i_f, j_f, h_f, i_b, j_b, h_b) \tag{97}$$

2) i_fが偶数，i_bが奇数のとき

$$W((4-i_b-h_b, 4-i_f-h_f, i_b-j_b, i_f-j_f, h_b, h_f, j_b, j_f))$$

$$= \quad W((4-i_f-h_f, 4-i_b-h_b, i_f-j_f, i_b-j_b, h_f, h_b, j_f, j_b))$$

$$= \quad 2Wg(i_f, j_f, h_f, i_b, j_b, h_b) \tag{98}$$

3) i_f，i_bともに奇数のとき

$$W((0, 8-i_f-i_b-h_f-h_b, 0, i_f+i_b-j_f-j_b, 0, h_f+h_b, 0, j_f+j_b))$$

$$= \quad Wg(i_f, j_f, h_f, i_b, j_b, h_b) \tag{99}$$

但し，$Wg(i_f, j_f, h_f, i_b, j_b, h_b)$は次式で定義される．

$$Wg(i_f, j_f, h_f, i_b, j_b, h_b) \triangleq$$

$$\binom{4}{i_f} \binom{i_f}{j_f} \binom{4-i_f}{h_f} \binom{4}{i_b} \binom{i_b}{j_b} \binom{4-i_b}{h_b} \tag{100}$$

上記以外の$\bar{t}=(t_0, t_1, \cdots, t_7)$については，$W(\bar{t})=0$である．

具体例３の内部符号は符号長，最小２乗ユークリッド距離，実効レート，トレリスダイアグラムの状態数の値が具体例１の内部符号と同一である．ここで，式(90)と式(96)-(100)を計算することにより，具体例１の符号の最小距離（D[C]=4）の符号語数が120であるのに対して，この具体例３の符号の最小距離（D[C]=4）の符号語数は56と少ないことがわかる．

$C_1-\{\bar{0}\}$の代表集合を求めることにより，次式で示される上界式が得られる．

$$P_{ic}^{(1)} \leq 28\mathrm{erfc}(\sqrt{\rho}) + 64\mathrm{erfc}\left(\frac{\sqrt{2(5-2\sqrt{2})\rho}}{2}\right)$$

$$+ 32\mathrm{erfc}(\sqrt{2(2-\sqrt{2})\rho}) + 128\mathrm{erfc}\left(\frac{\sqrt{2(5-\sqrt{2})\rho}}{2}\right)$$

$$+ 128\mathrm{erfc}\left(\frac{\sqrt{2(8-3\sqrt{2})\rho}}{2}\right) + 128\mathrm{erfc}(\sqrt{(4-\sqrt{2})\rho}) \quad (101)$$

式(101)の右辺を$\bar{P}_{ic}^{(1)}(C_{1,EX1})$と表す．図20に，この符号の誤って復号される確率の上界$\bar{P}_{ic}^{(1)}(C_{1,EX1})$と$P_{ic}^{(1)}$に関するシミュレーション結果（以下，記号$P_{ic,s}^{(1)}$で表す），及び，符号化しない４値ＰＳＫの誤り特性を示す．図より，この符号は符号化しない４値ＰＳＫに対して，誤って復号される確率が10^{-5}となる点で2.4dB，10^{-6}となる点で2.5dBの符号化利得があることがわかる．

次に，縦接符号全体の誤り特性について示す．k_1=16より，m_1=2，つまり，インターリービングの度数は２である．また，縦接符号全体の実効レートは(223/255)=0.875である．外部符号の復号では，１６セグメントまでの誤り訂正を行う．つまり，t_2=16である．そのときの，ブロックが復号に失敗する確率と誤って復号される確率

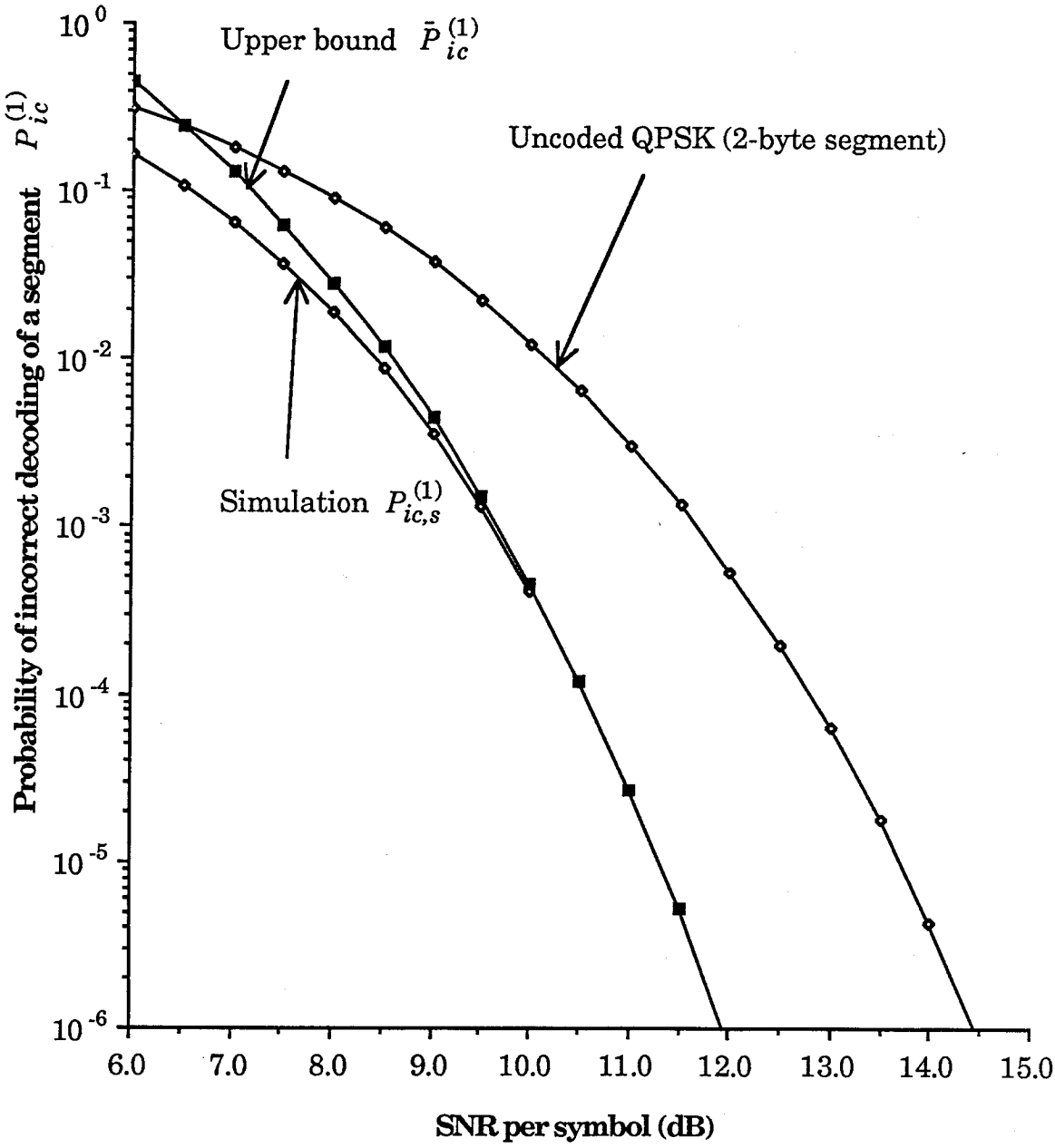

図20　８値ＰＳＫ変調符号（第２節例１の符号）の誤って復号される確率の上界の値とシミュレーション結果，及び，16ビットの通報を符号化しない４値ＰＳＫで送信したとき誤って受信される確率

の和の上界$1-\underline{P}_c$（式(85)の右辺）と，ブロックが誤って復号される確率の上界$\bar{P}_{er}$（式(88)の右辺）を，それぞれ，図21と22に示す．それらの図では，具体例１，２同様，内部符号の誤り特性評価にシミュレーションによる結果$P^{(1)}_{ic,s}$，$Q_{i,s}$を用いて計算を行った結果$1-P_{c,s}$，$\bar{P}_{er,s}$をあわせて示す．　図21，22から，具体例３も，非常に高い信頼性と高いスループットをもつことがわかる．例えば，シンボルあたりのＳＮ比が8.5dBのとき，誤って復号される確率は，高々10^{-19}である．また，復号に失敗する確率は高々10^{-9}（内部符号の誤り特性の評価にシミュレーションを用いたとき）である．また，図21から，ブロックの復号失敗確率を評価基準としたときの符号化しない４値ＰＳＫに対する符号化利得は，ブロックの復号失敗確率が10^{-7}，10^{-10}の点で，それぞれ，8.0dB，9.1dBである．

また，図23，24に具体例３の復号後のビット誤り率P_{b1}の上界値，及び，P_{b2}の値と符号化しない４値ＰＳＫのビット誤り率を示す．具体例３のP_{b1}を評価基準としたときの符号化しない４値ＰＳＫに対する符号化利得は，P_{b1}が10^{-12}の点で，9.8dBである．P_{b2}を評価基準としたときの符号化しない４値ＰＳＫに対する符号化利得は，P_{b2}が10^{-6}，10^{-10}の点で，それぞれ，5.6dB，7.7dBである．

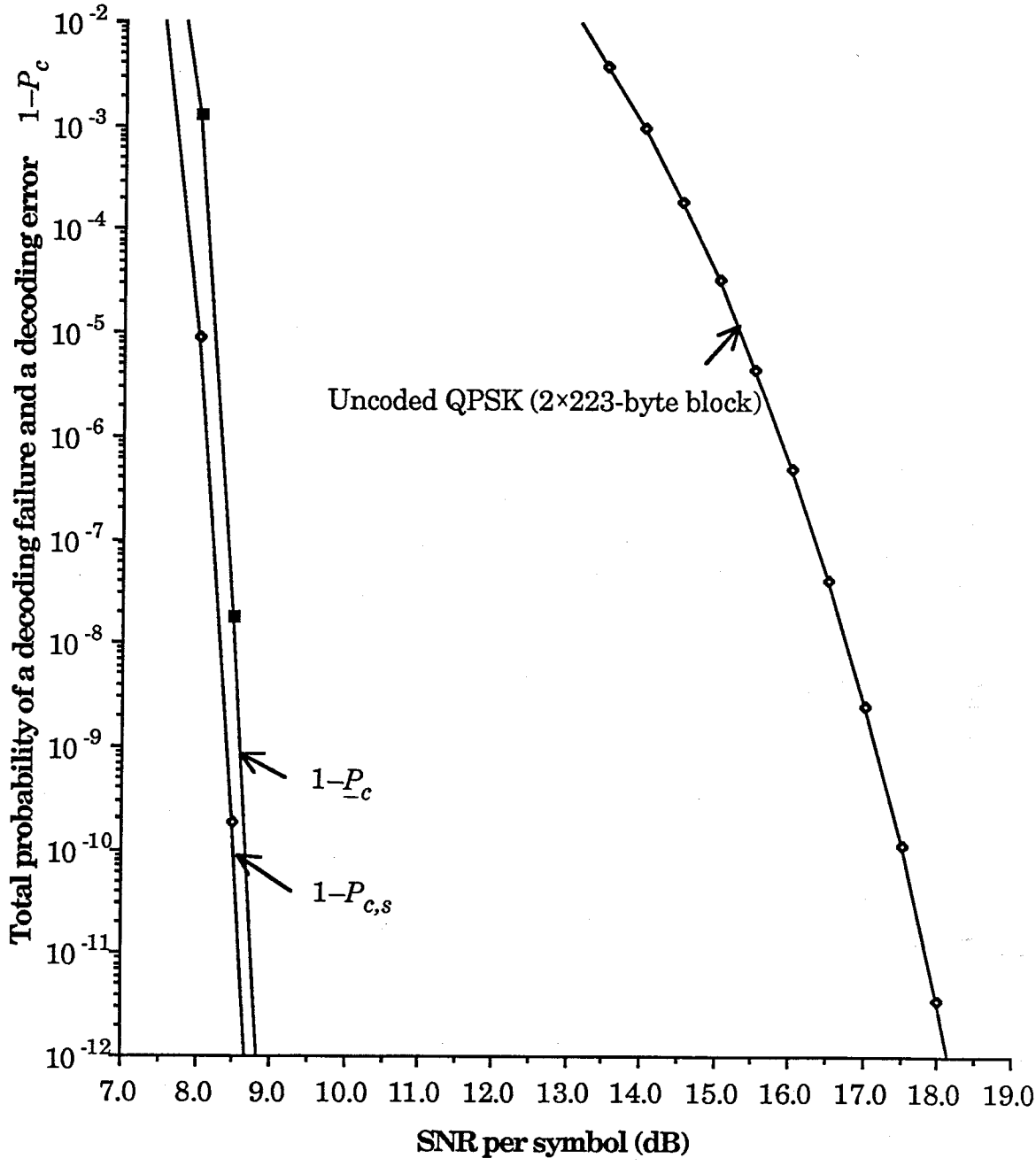

図21　内部符号に第２節例１の符号，外部符号に(255, 223)ＲＳ符号を用いた縦接符号の復号に失敗する確率と誤って復号される確率の和，及び，2×223ビットの通報を符号化しない４値ＰＳＫで送信したとき誤って受信される確率

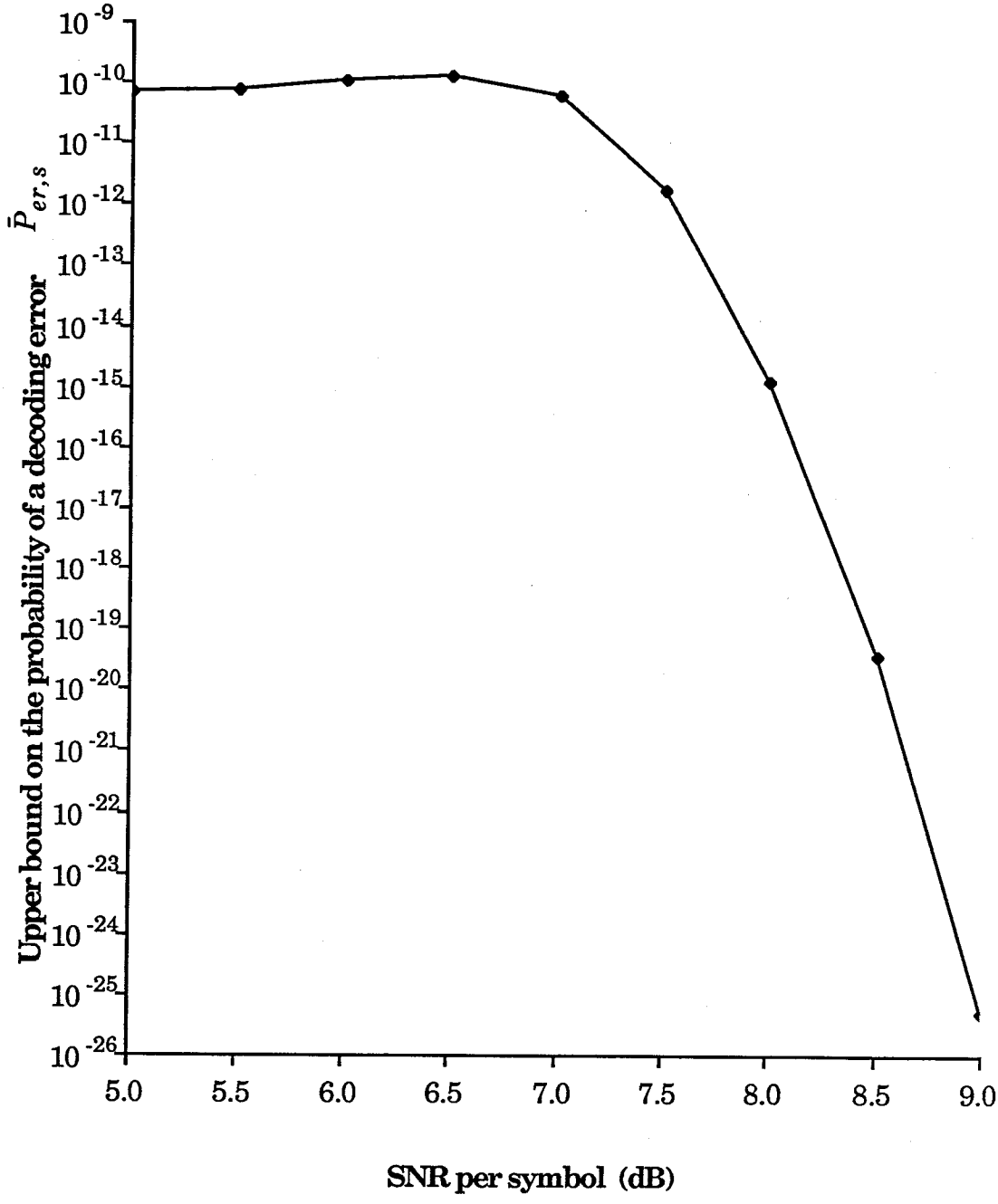

図22　内部符号に第２節例１の符号，外部符号に(255, 223)ＲＳ符号を用いた縦接符号の誤って復号される確率の上界の値

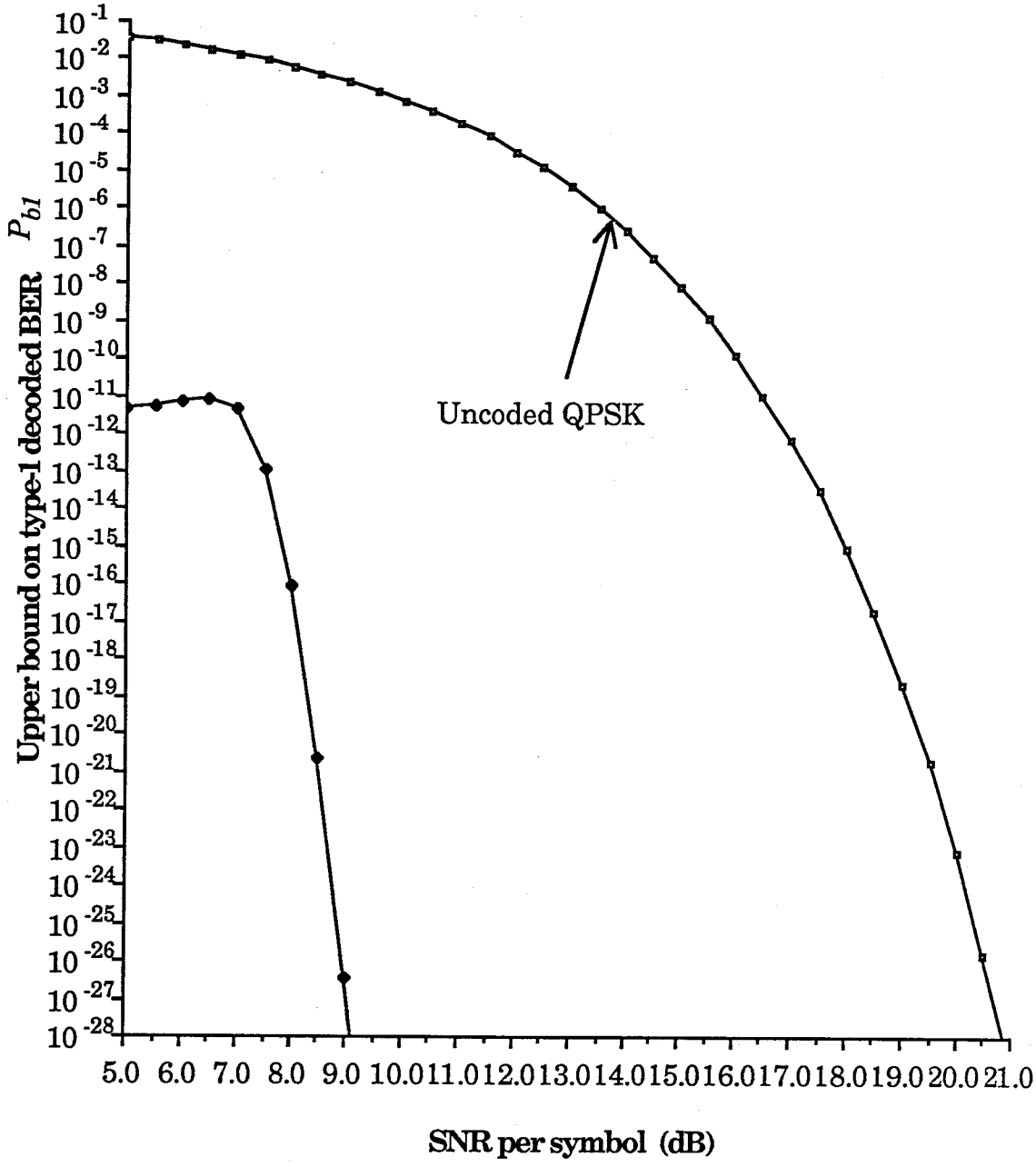

図23　内部符号に第２節例１の符号，外部符号に(255,223)ＲＳ符号を用いた縦接符号の復号後のビット誤り率の評価値P_{b1}の上界値，及び，符号化しない４値ＰＳＫの誤り確率

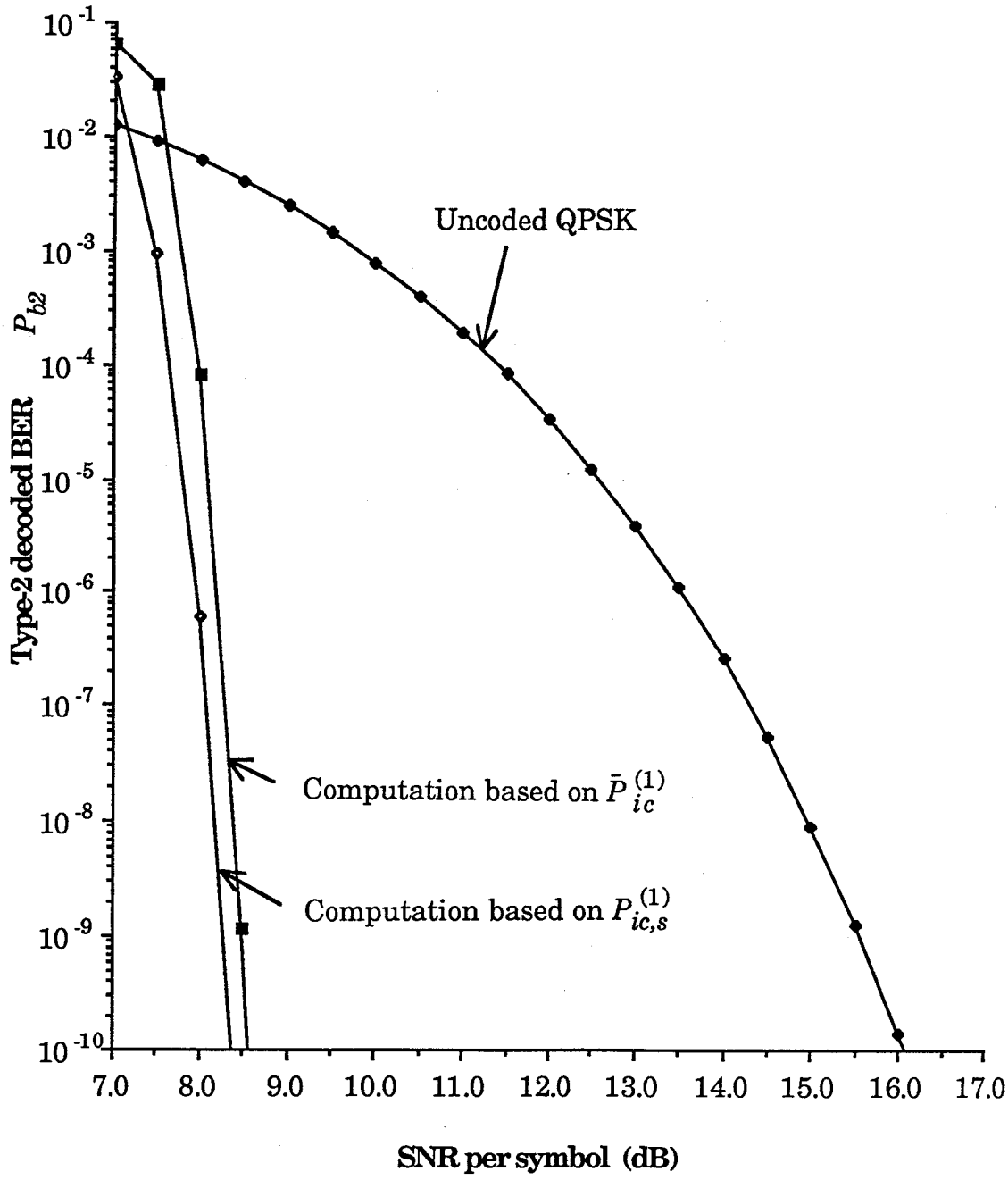

図24　内部符号に第２節例１の符号，外部符号に(255, 223)ＲＳ符号を用いた縦接符号の復号後のビット誤り率の評価値P_{b2}，及び符号化しない４値ＰＳＫの誤り確率

6．結言

この章では，縦接符号の内部符号に適したM値ＰＳＫブロック変調符号の構成法と，その方法によって構成された符号を内部符号に用いた縦接符号化法の構成法，及び，その縦接符号を加法的白色ガウス雑音をもつ通信路で用いたときの誤り特性の解析法を示した．ここで示した構成法による，いくつかの縦接符号の具体例を提案し，それらの誤り特性の解析を行った．それらの具体例では，外部符号にGF(2^8)上のＮＡＳＡ標準(255,223)リードソロモン符号を用いる．内部符号に符号長が最も長いものでも16と短く，状態数の少ないトレリスダイアグラムをもつ（最も多いものでも高々16状態）８値ＰＳＫブロック変調符号を用いる．従って，内部符号の復号は軟判定最尤復号法を用いた高速な復号器が利用可能である．また，バースト誤り訂正能力を高めるために外部符号でインターリービングを行っている．

具体例に対する解析結果から，ここで述べた縦接符号化法は，高い信頼性と低い復号複雑度と帯域幅の効率的な使用の３点を同時に満足することがわかった．ここで述べた具体例は，高い信頼性を必要とする衛星通信に適していることがわかった．

第３章　縦接符号化法を誤り訂正に用いたある誤り制御通信方式

１．序言

この章では，縦接符号化方式を用いた誤り制御通信方式の一つについて論じる．ここで取り上げる通信方式は，縦接符号化方式を用いた誤り訂正（Forward Error Correction：以下，ＦＥＣと略す）と，最初に送信したブロックが復号に失敗したときに，より強力な誤り訂正を行うための検査シンボルの再送とを組み合わせたタイプ２ハイブリッドＡＲＱ方式[22]の一種である．

ここでの縦接符号化方式の内部符号C_1は２元線形ブロック符号とブロック変調符号の両方を考える．内部符号に２元線形ブロック符号を用いた場合は第１章で述べた縦接符号化方式となり，ブロック変調符号を用いた場合には第２章で述べた縦接符号化方式となる．内部符号では誤りの訂正と検出をおこなうものとする．外部符号は第１章で述べたものと同じ有限体$GF(2^{\ell})$上の最小距離d_2の(n_2, k_2)線形符号であり，消去，誤りシンボルの訂正，及び，誤りの検出を行うものとする．但し，この章で取り上げる外部符号は最大距離分離符号，またはその短縮符号とする．外部符号は第１，２章と同様，バースト誤り訂正能力を高めるためにインターリービングが施される．

この通信方式では，検査シンボルの再送のために第三の符号C_rが用いられる．この符号は外部符号C_2を短縮して得られる$(2n_2-2k_2, n_2-k_2)$符号である．この符号はレート1/2であり，後述する反転操

作[22]が可能であるという性質をもつ．また，外部符号の短縮符号であることから復号器を外部符号と共用できるという利点をもつ．

以下，第２節では，ここで取り上げる通信方式のＦＥＣ方式について示す．第３節では，再送方式について述べる．第４節では，ここで取り上げる通信方式の誤り特性とスループット（伝送効率）特性の解析方法について述べる．第５節では，ここで取り上げる通信方式に基づく，いくつかの具体例を提案し，加法的白色ガウス雑音をもつ通信路でそれらの具体例を用いたときの誤り特性とスループット特性の解析を行なう．それらの具体例はＳＮ比が比較的低い通信路においても，高い信頼性とスループットを達成している．それらの具体例は通信路の雑音の状態が変動する衛星通信における高レートのファイル転送に適している．

2．誤り訂正方式

2．1　ＦＥＣ方式で用いられる誤り訂正符号

ＦＥＣ（誤り訂正）方式は第１章で論じた縦接符号化方式を用いる．ここでは，内部符号C_1には，２元線形ブロック符号とブロック変調符号の２つを考える．内部符号に２元線形ブロック符号を用いる場合，第１章の場合と同様，最小距離d_1の(n_1, k_1)符号とし，t_1個以下の誤り訂正とλ_1（但し，$\lambda_1 \geqq t_1$，$t_1+\lambda_1+1 \leqq d_1$）個以下の誤り検出を行うことができるものとする．内部符号にブロック変調符号を用いる場合，信号点数n_1，情報ビット数k_1とする．

外部符号C_2は有限体$GF(2^{\ell})$上の最大距離分離可能巡回符号，または，その短縮符号とする．C_2は最小距離d_2の(n_2, k_2)符号とする．

C_2は最大距離分離符号であるから，次の式が成立する．

$$d_2 - 1 = n_2 - k_2 \tag{102}$$

ここで(102)式の左辺をr_2と定義する．つまり，r_2はC_2の検査シンボル数である．ここで，n_2，r_2，k_1，ℓの間に，第１章の式(1)（$k_1=m_1\ell$）及び，次の条件が成立するものとする．

$$n_2 = m_2 r_2 \tag{103}$$

但し，m_2は，$m_2 \geqq 2$を満たす整数とする．

更に，この方式ではパリティ再送用に第３の符号C_rを用いる．C_rは外部符号C_2を短縮することによって得られる最小距離d_2の$(2r_2,$

r_2)最大距離分離可能符号である．C_rは，C_2の短縮符号であるから，C_2と同じ符号化器と復号器で符号化，復号が可能である．C_rは反転操作が可能であるという重要な性質をもつ(22)．つまり，$\bar{u}$を有限体GF(2^ℓ)の上のr_2字組とする．$R_r(\bar{u})$を$\bar{u}$をC_rによって符号化することによって得られる符号語の検査シンボルの系列とする．$R_r(\bar{u})$もGF(2^ℓ)の上のr_2字組である．このとき，$\bar{u}$と$R_r(\bar{u})$の間に1対1の対応関係が成立する．従って，C_rの符号語のr_2個の検査シンボルがすべてわかれば，文献(22)に述べられている反転操作により，対応するr_2個の情報シンボルが一意に定めることができる．

GF(2^ℓ)上のn_2字組$\bar{v}_i$をC_2の符号語とする（第1章のセクションに相当する）．式(103)よりn_2はr_2の倍数である．$\bar{v}_i$をm_2個に分割することにより得られる長さr_2の部分列を，それぞれ$\bar{v}_{i1}$，$\bar{v}_{i2}$，…，$\bar{v}_{i,m_2}$とする．以下，それらの部分列をサブセクションと呼ぶ．各$1 \leq j \leq m_2$について，$R_r(\bar{v}_{i,j})$を$\bar{v}_{i,j}$をC_rによって符号化することによって得られる符号語の検査シンボル部分の系列とする．そのとき，GF(2^ℓ)上のn_2字組$R(\bar{v}_i)$を，各サブセクション毎の$R_r(\bar{v}_{i,j})$を順に連接したものとする．つまり，次の式で定義されるものする．

$$R(\bar{v}_i) \triangleq (R_r(\bar{v}_{i1}), R_r(\bar{v}_{i2}), \cdots, R_r(\bar{v}_{i,m_2})) \qquad (104)$$

このとき，$\bar{v}_i$同様，$R(\bar{v}_i)$もC_2の符号語となる（証明は付録Gに示す）．

2．2　符号化法

符号化は第1章と同じく，以下に示す2段階で行う．

(1)　第1段階では$k_2 \times k_1 (=k_2 m_1 \ell)$ビットの通報を図2に示す様に縦$k_2$，横$m_1 \ell$の格子状に配置する．$k_2$個の各行それぞれを$m_1$個の長さ$\ell$のビット列に分割する．各$\ell$ビットを$GF(2^{\ell})$の元（シンボル）とみなし，縦方向$k_2$個のシンボル列（以下，データセクションと呼ぶ）それぞれを外部符号C_2で符号化する．各データセクションの内容は再送要求が行われたときのためにバッファに保管しておく．

(2)　第2段階では第1段階で得られたn_2個の長さ$m_1 \ell$の各行ベクトルを（それぞれの行をセグメントと呼び，セグメント中のm_1個のシンボルを左から順に1番目，2番目，…，m_1番目のシンボルという）内部符号C_1で符号化する．内部符号に2元線形ブロック符号を用いる場合，長さn_1の2元ベクトルが内部符号の符号語として得られる．内部符号にブロック変調符号を用いた場合，n_1個の変調信号点集合（例えば，8値ＰＳＫ変調信号点集合）の要素の系列が符号語として得られる．内部符号の符号語に対応する長さn_1の行ベクトルをフレームと呼ぶ．得られたn_2個のフレームを順に送信する．このn_2個のフレームの系列をデータブロック（図3参照）と呼ぶ．

2．3　データブロックの復号法

データブロックの復号法も基本的には第1章で述べた縦接符号化法の復号法と同様，以下に述べる2段階で行われる．

(1)　第1段階では，まず受信された各フレームについて内部符号に基づいて復号を行う．もし内部符号が2元線形ブロック符号ならば，シンドロームを計算し，次のいずれかを行なう．

(1.1) シンドロームがt_1個以下の誤りパターンeに対応するものならば，受信されたフレームにその誤りパターンeを加えることにより誤りを訂正し，その情報ビットの部分（以下，復号後のセグメントと呼ぶ）を，外部符号のデータブロック用復号バッファに送る．この場合，正しく訂正したか否かにかかわらず，そのフレームは復号に成功したという．復号に成功したフレームのセグメントをマークのないセグメントと呼ぶ．

(1.2) シンドロームが，t_1個を越える誤りパターンに対応する場合，そのフレームは復号に失敗したといい，そのセグメントを消去する．そのセグメントでt_1個を越える誤りが発生したことを外部符号の復号器に伝達する．

もし内部符号がブロック変調符号ならば，なんらかの復号アルゴリズム（例えば最尤復号法）に基づいて誤り訂正を行ない，復号結果を外部符号の復号バッファに送る．

(2) 第2段階では外部符号に基づき，シンボル誤りとシンボル消去の訂正を行う．予め，d_2-1以下の非負整数T_{es}と，各$0 \leq i \leq T_{es}$に対して，$(d_2-1-i)/2$以下の非負整数$t_2(i)$が定められているとする．

(2.1) 消去されたセグメントの個数iが，T_{es}を越えるときには，ブロックの再送を要求する．

(2.2) (2.1)以外のとき，ブロックの各セクション毎に外部符号に基づいて計算したシンドロームが，i個のシンボル消去と$t_2(i)$個以下のシンボル誤りに対応するならば，それらの訂正を行い，データブロックを受理する．そうでなければ，ブロックの再送を要求する．

3．再送方式

この節ではここで取り上げる通信方式の再送方式について述べる．

データブロック$\bar{v}$が送信されたとき，$\hat{v}$というブロックが受信されたとする．$\hat{v}$の復号に失敗したとき，受信側は外部符号の復号バッファの内容を保存し，送信側に再送を要求する．送信側は，以下の2段階で再送を行う．

(1)　各$1 \leqq i \leqq m_1$に対して，$\bar{v}_i$を$\bar{v}$のi番目のデータセクションとする．2．1節で述べた方法を用いて，各$\bar{v}_i$をサブセクション$\bar{v}_{ij}$（$1 \leqq j \leqq m_2$，以下これらのサブセクションをデータサブセクションと呼ぶ．）に分割する．各データサブセクションをC_rで符号化し，その検査シンボル部分の系列$R_r(\bar{v}_{ij})$（以下，パリティサブセクションと呼ぶ．）を得る．一つのデータセクション$\bar{v}$に対応するパリティサブセクションを連接し，

$$R(\bar{v}_i) \quad = \quad (R_r(\bar{v}_{i1}), R_r(\bar{v}_{i2}), \cdots, R_r(\bar{v}_{i,m_2}))$$

を構成する．以下，$R_r(\bar{v}_i)$をパリティセクションと呼ぶ．得られたm_1個のパリティセクションを1回目の送信のときと同様に格子状に配置する．

(2)　第二段階も，1回目の送信のときと同様，第一段階で得られたn_2個の行ベクトルを行方向に内部符号C_1で符号化を行い，得られたフレームを順に送信する．パリティセクションから作られたn_2個のフレームの系列をパリティブロックと呼び，$P(\bar{v})$で表す．

次に，受信側の動作について述べる．今，送信された$P(\bar{v})$に対して，$\hat{P}(\bar{v})$が受信されたとする．$\hat{P}(\bar{v})$の復号は1回目のときと同様，

2段階の手続きで行われる．内部符号の復号は1回目のときと同じである．内部符号の復号結果はパリティセクション復号用の復号バッファもしも，m_1個のパリティセクションの復号がすべて成功したら，各パリティセクション毎に2．1節で述べた反転操作を施し，もとのデータセクションを得る．もし$\hat{P}(\bar{v})$の復号に失敗したならば，各$1 \leqq i \leqq m_1$について，1回目の受信により得られたデータセクション用復号バッファの内容$\hat{v}_i$と，今回の受信により得られたパリティセクション用復号バッファの内容$\hat{P}(\bar{v}_i)$を，それぞれサブセクション単位に分割し，対応するデータサブセクション$\hat{v}_{ij}$と，パリティサブセクション$\hat{R}_r(\bar{v}_{ij})$を組合せ，C_rに基づいて復号する．すべての$1 \leqq i \leqq m_1$，$1 \leqq j \leqq m_2$について，（$\hat{v}_{ij}$，$\hat{R}_r(\bar{v}_{ij})$）の組がC_rの復号に成功し，（$\bar{v}^*_{ij}$，$R^*_r(\bar{v}_{ij})$）という復号結果を得たとする．そのとき，各$1 \leqq i \leqq m_1$について，以下の式で定義される$\bar{v}^*_i$を求める．

$$\bar{v}^*_i = (\bar{v}^*_{i1}, \bar{v}^*_{i2}, \cdots, \bar{v}^*_{i,m_2}) \tag{105}$$

つまり，$\bar{v}^*_i$は，C_rによる復号結果のi番目のデータセクションに対応する部分を連接したものである．受信側は，各$\bar{v}^*_i$に対してC_2に基づいて誤り検出を行う．すべての$\bar{v}^*_i$，$1 \leqq i \leqq m_1$がC_2の符号語ならば（誤りが検出されなかったならば）それらを受理する．もし，どれか1個所でもC_rの復号に失敗するか，$\bar{v}^*_i$に誤りが検出されたならば，$\hat{P}(\bar{v}_i)$の内容をバッファに保管し，再度再送を要求する．

2回目の再送はデータブロック$\bar{v}$，3回目の再送はパリティブロック$P(\bar{v})$という様に，以下，ブロックが受理されるまで，データブロックとパリティブロックを交互に再送する（図25参照）．

この誤り制御方式の大きな利点は，誤り訂正のための余分な検査

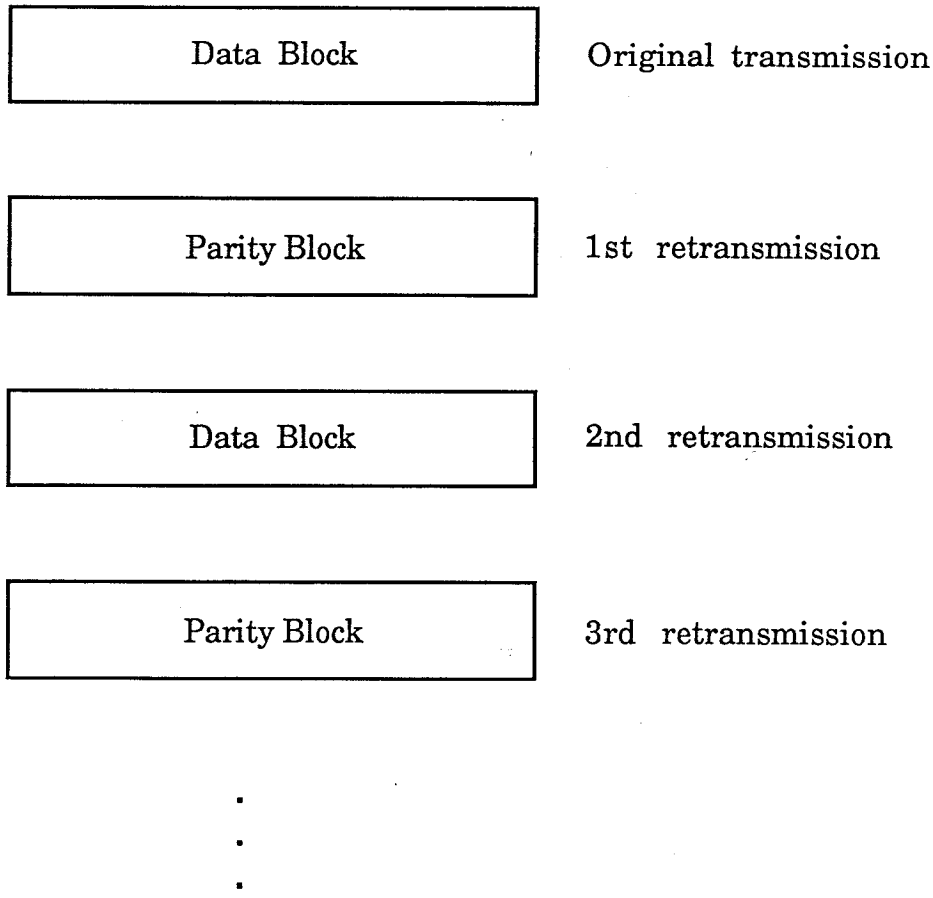

図25　データブロックとパリティブロックの交互再送

シンボルは，必要なときにのみ送信されるという所である．その余分な検査シンボルは，もとの縦接符号と同じレートで送られる．もし，C_rの誤り訂正能力が十分強力ならば（C_rのレートは１／２である），高々１回の再送で通報を復元できる．その場合，システム全体のスループットはもとの縦接符号のレートの半分となる．比較的雑音の少ない通信路ならば，縦接符号の訂正能力で通報の復元が可能であるから，システム全体のスループットは縦接符号のレートとなる．

また，この方式は，C_rがC_2の短縮符号であることから，C_rの復号器とC_2の復号器を兼用できるという利点をもつ．

4．性能解析

この節では，前節までで述べた誤り制御通信方式の性能の解析を行う．本方式を加法的白色ガウス雑音をもつ通信路で用いたときの誤り確率の上界とスループットの下界を示す．

4．1　ＦＥＣ方式の解析

それぞれの送信（再送を含む）では，まず，受信されたデータブロック，パリティブロックに対してC_1とC_2に基づく復号が行われる．P_c，P_{er}，P_{es}を，それぞれ，C_1とC_2に基づく復号によってブロックが正しく誤って復号される確率，復号に失敗する確率，誤って復号される上界とする．第１章の第２，３節では，P_{er}の上界の計算法（式(20)）と，P_cの計算法（式(22)）を示している．

4．2　C_rの復号の誤り解析

次に，C_rに基づく復号の誤り解析を行う．各$1 \leqq u \leqq m_1$について，$P_{er}^{(r)}(u)$，$P_{df}^{(r)}(u)$を，それぞれ，u番目のセクションのデーターパリティサブセクション対をC_rに基づいて復号を行ったときに，誤って復号する確率，復号に失敗する確率とする．

内部符号の復号に関する確率の定義を行う．$P_{es}^{(1)}$を受信セグメントが消去される確率とする．消去操作を行わない場合には，$P_{es}^{(1)}=0$である．αを$GF(2^{\ell})$の元とし，$1 \leqq u \leqq m_1$とするとき，$p_e(u, \alpha)$を，

あるセグメントが復号に成功し，かつ，そのセグメントのu番目のシンボル位置の誤りシンボルがαとなる確率とする．$\bar{P}_e(u)$を復号に成功したセグメントのu番目のシンボルが誤りである確率とする．内部符号に2元線形ブロック符号を用いたときのそれらの確率の計算方法が第1章の第2節に述べられている．第1章の付録B及び，文献(9)の5．1節と同様の議論により，$P_{er}^{(r)}(u)$，$P_{df}^{(r)}(u)$について次の式が成立する．

$$P_{df}^{(r)}(u)+P_{er}^{(r)}(u) =$$

$$\sum_{i=0}^{d_2-1}\binom{n_r}{i}[P_{es}^{(1)}]^i \sum_{j=\lfloor\frac{n_r-i-1}{2}\rfloor+1}^{n_r-i}\binom{n_r-i}{j}$$

$$[\bar{p}_e(u)]^j[1-P_{es}^{(1)}-\bar{p}_e(u)]^{n_r-i-j}$$

$$+\sum_{i=d_2}^{n_r}\binom{n_r}{i}[P_{es}^{(1)}]^i[1-P_{es}^{(1)}]^{n_r-i} \qquad (106)$$

$$P_{er}^{(r)}(u) \leqq$$

$$\sum_{i=0}^{d_2-1}\binom{n_r}{i}\sum_{w=d_2-i}^{n_r-i}\binom{n_r-i}{w}\sum_{h=0}^{\min\{\lfloor\frac{n_r-i-1}{2}\rfloor,\,n_r-i-w\}}$$

$$\binom{n_r-i-w}{h}\sum_{j=w+h-\lfloor\frac{n_r-i-1}{2}\rfloor}\binom{w}{j}\bar{P}_e(u,i,w,h,j) \qquad (107)$$

但し，$n_r \triangleq 2r_2$，つまり，C_rの符号長であり，また，$\bar{P}_e(u,i,w,h,j)$は次の式で定義される．

$$\bar{P}_e(u,i,w,h,j) \triangleq$$

$$[P_{es}^{(1)}]^{i}[\bar{p}_e(u)]^{i+w+h-d_2}[\bar{p}_e(u,0)]^{n_r-i-w-h}$$

$$[1-P_{es}^{(1)}]^{n_r-i}\sum_{q=0}^{2^{\ell}-2}[\bar{p}_e(u,\gamma^{q})]^{j+d_2-i-w} \qquad (108)$$

但し，γはGF(2^{ℓ})の原始元とする．式(107)の右辺を$\bar{P}_{er}^{(r)}(u)$と定義する．$P_{er}^{(all)}$および$P_{df}^{(all)}$を，それぞれ，ブロック全体が誤って復号される確率と復号に失敗する確率とする．それらの確率について次の不等式が成立する．

$$P_{er}^{(all)}+P_{df}^{(all)} \leqq$$

$$\max\{\sum_{u=1}^{m_1}[1-[1-(P_{df}^{(r)}(u)+P_{er}^{(r)}(u))]^{m_2}],1\} \qquad (109)$$

あるセクションが誤って復号されるための条件は，そのセクションを構成するm_2個のサブセクションのいくつかがC_rに基づく復号で誤って復号され，かつ，セクションがC_2の符号語となっていることである．C_2は最小距離r_2+1の$(m_2r_2,(m_2-1)r_2)$符号，C_rはC_2を短縮した$(2r_2,r_2)$符号である．これらのことから，あるセクションのm_2-1個のサブセクションでC_rに基づいて復号されたとき，そのセクションがC_2の符号語となるため様な残り1つのサブセクションの復号結果はm_2-1個のサブセクションの復号結果から一意に定まる．u番目のセクションのC_rの復号によって特定のエラーパターンが起こる確率を$P_{ep}(u)$で表す．$P_{ep}(u)$について次の不等式が成立する（証明は付録Hに示す）．

$$P_{ep}(u) \leqq$$

$$\sum_{i_1=0}^{r_2} \binom{d_2}{i_1} \sum_{i_2=0}^{r_2-i_1} \binom{n_r-d_2}{i_2} [P_{es}^{(1)}]^{i_1+i_2}$$

$$\sum_{h=0}^{\min\{\lfloor\frac{r_2-(i_1+i_2)}{2}\rfloor,\, n_r-i_2-d_2\}} \binom{n_r-i_2-d_2}{h}$$

$$[\bar{p}_e(u)]^h [\bar{p}_e(u,0)]^{n_r-d_2-i_2-h} \sum_{j=d_2-i_1+h-\lfloor\frac{r_2-(i_1+i_2)}{2}\rfloor}^{d_2-i_1}$$

$$\binom{d_2-i_1}{j} [\max_{\alpha\neq 0}\{\bar{p}_e(u,\alpha)\}]^j [1-P_{es}^{(1)}]^{d_2-i_1-j} \qquad (110)$$

(110)式の右辺を$\bar{P}_{ep}^{(max)}(u)$で表す．(110)式から次の式が成立する．

$$P_{er}^{(all)} \leqq \sum_{u=1}^{m_1} \{ \bar{P}_{ep}^{(max)}(u) \sum_{j=1}^{m_2-1} \sum_{i=1}^{j} \binom{j-1}{i}$$

$$[P_{er}^{(r)}(u)]^i [1-(P_{df}^{(r)}(u)+P_{er}^{(r)}(u)]^{m_2-i-1}\} \qquad (111)$$

(111)式の右辺を$\bar{P}_{er}^{(all)}$で表す．(111)式はブロックが誤って復号される確率の上界となっている．

4．3　システムの誤り特性とスループット特性

$P_{df}^{(h)}$，$P_{er}^{(h)}$を，それぞれ，高々h-1回までの再送を行ったと仮定したときのシステムの復号失敗確率と誤って復号する確率とする．$P_{df}^{(2)}$，$P_{er}^{(2)}$について次の式が成立する．

$$P_{er}^{(2)} \leqq P_{er} + P_{es}P_{er} + P_{er}^{(all)}$$

$$\leqq \bar{P}_{er} + (P_{er}+P_{es})\bar{P}_{er} + \bar{P}_{er}^{(all)} \tag{112}$$

$$P_{df}^{(2)} \leqq P_{df}^{(all)} \leqq P_{er}^{(all)} + P_{df}^{(all)} \tag{113}$$

(112), (113)式の右辺をそれぞれ$\bar{P}_{er}^{(2)}$, $\bar{P}_{df}^{(2)}$と表す．スループットは次の式で表される．

$$\zeta^{(2)} = \frac{k_1(n_2-d_2+1)}{n_1 n_2(1+P_{es})} \geqq \frac{k_1(n_2-d_2+1)}{n_1 n_2(1+P_{er}+P_{es})} \tag{114}$$

(114)式の右辺を$\underline{\zeta}^{(2)}$と表す．

次に，$P_{df}^{(3)}$, $P_{er}^{(3)}$の上界について考察する．$1 \leqq u \leqq m_1$について，$P_{c,c}^{(3)}(u)$（または$P_{f,c}^{(3)}(u)$）を，u番目のセクションの特定のサブセクションの位置で，データブロック（1回目送信）とパリティブロック（再送1回目）のサブセクション対をC_rによって復号をおこなった結果正しく復号し（または復号に失敗するか誤って復号し），パリティブロック（再送1回目）とデータブロック（再送2回目）のサブセクション対を正しく復号する確率とする．$P_{c,c}^{(3)}(u)$, $P_{f,c}^{(3)}(u)$について次の等式が成立する．

$$P_{c,c}^{(3)}(u) =$$

$$\sum_{i_1=0}^{d_2-1} \binom{k_r}{i_1} \sum_{i_2=0}^{d_2-1-i_1} \binom{k_r}{i_2} \sum_{i_3=0}^{d_2-1-i_2} \binom{k_r}{i_3} [P_{es}^{(1)}]^{i_1+i_2+i_3}$$

$$\sum_{j_1=0}^{\left\lfloor \frac{d_2-i_1-i_2}{2} \right\rfloor} \binom{k_r-i_1}{j_1} \sum_{j_2=0}^{\min\left\{\left\lfloor \frac{d_2-i_1-i_2}{2} \right\rfloor - j_1,\ \left\lfloor \frac{d_2-i_2-i_3}{2} \right\rfloor\right\}}$$

$$\binom{k_r-i_2}{j_2} \sum_{j_3=0}^{\left\lfloor \frac{d_2-i_2-i_3}{2} \right\rfloor - j_2} \binom{k_r-i_3}{j_3}$$

$$[\bar{p}_e(u)]^{j_1+j_2+j_3}[1-P_{es}^{(1)}-\bar{p}_e(u)]^{3k_r-(i_1+i_2+i_3)-(j_1+j_2+j_3)}$$

(115)

$$P_{f,c}^{(3)}(u) =$$

$$\sum_{i_1=0}^{d_2-1}\binom{k_r}{i_1}\sum_{i_2=0}^{d_2-1-i_1}\binom{k_r}{i_2}\sum_{i_3=0}^{d_2-1-i_2}\binom{k_r}{i_3}[P_{es}^{(1)}]^{i_1+i_2+i_3}$$

$$\sum_{j_1=0}^{k_r-i_1}\binom{k_r-i_1}{j_1}\sum_{j_2=\max\{0,\lfloor\frac{d_2-i_1-i_2}{2}\rfloor+1-j_1\}}^{k_r-i_2}$$

$$\binom{k_r-i_2}{j_2}\sum_{j_3=0}^{\lfloor\frac{d_2-i_2-i_3}{2}\rfloor-j_2}\binom{k_r-i_3}{j_3}$$

$$[\bar{p}_e(u)]^{j_1+j_2+j_3}[1-P_{es}^{(1)}-\bar{p}_e(u)]^{3k_r-(i_1+i_2+i_3)-(j_1+j_2+j_3)}$$

$$+\sum_{i_1=0}^{k_r}\binom{k_r}{i_1}[1-P_{es}^{(1)}]^{k_r-i_1}\sum_{i_2=\max\{0,d_2-i_1+1\}}^{k_r}\binom{k_r}{i_2}$$

$$\sum_{i_3=0}^{d_2-1-i_2}\binom{k_r}{i_3}[P_{es}^{(1)}]^{i_1+i_2+i_3}$$

$$\sum_{j_2=0}^{\lfloor\frac{d_2-i_2-i_3}{2}\rfloor}\binom{k_r-i_2}{j_2}\sum_{j_3=0}^{\lfloor\frac{d_2-i_2-i_3}{2}\rfloor-j_2}\binom{k_r-i_3}{j_3}$$

$$[\bar{p}_e(u)]^{j_2+j_3}[1-P_{es}^{(1)}-\bar{p}_e(u)]^{2k_r-(i_2+i_3)-(j_2+j_3)} \quad (116)$$

但し，k_rはC_rの情報点数である．すなわち，$k_r=r_2$である．

$P_{df}^{(3)}$，$P_{er}^{(3)}$について次の不等式が成立する．

$$P_{df}^{(3)} \leqq \max\{\sum_{u=1}^{m_1}\{1-\sum_{j=1}^{m_2}\binom{m_2}{j}[P_{f,c}^{(3)}(u)]^j[P_{c,c}^{(3)}(u)]^{m_2-j}$$

$$- \left[1-(P_{df}^{(r)}(u)+P_{er}^{(r)}(u)\right]^{m_2} \},\ 1\} \tag{117}$$

$$P_{er}^{(3)} \leqq P_{er}^{(2)} + P_{df}^{(2)}(P_{er}+P_{er}^{(all)})$$

$$\leqq \bar{P}_{er}^{(2)} + \bar{P}_{df}^{(2)}(\bar{P}_{er}+\bar{P}_{er}^{(all)}) \tag{118}$$

(117), (118)式の右辺をそれぞれ$\bar{P}_{er}^{(3)}$, $\bar{P}_{df}^{(3)}$と表す．スループットは次の式で表される．

$$\zeta^{(3)} = \frac{k_1(n_2-d_2+1)}{n_1 n_2(1+P_{es}+P_{df}^{(2)})} \geqq \frac{k_1(n_2-d_2+1)}{n_1 n_2(1+P_{er}+P_{es}\bar{P}_{df}^{(2)})} \tag{119}$$

(119)式の右辺を$\underline{\zeta}^{(3)}$と表す．

5．いくつかの具体例の特性解析

この節では，ここで取り上げた通信方式の３つの具体例について，第４節で述べた解析方法を用いて，それらの具体例を加法的白色ガウス雑音をもつ通信路で用いたときの，誤り特性とスループット特性について解析を行う．

［例１］第１の例では，内部符号を用いない．$n_1=k_1=\ell=8$とする．外部符号C_2は，有限体$GF(2^8)$上の短縮(224,192)リードソロモン符号を用いる．この符号はNASAの標準(255,223)リードソロモン符号を31シンボル短縮することによって得られる符号である．この符号の最小距離d_2は33であり，消去，誤りシンボルの数をそれぞれe，tとすれば，$2t+e\leqq 32$までのシンボル消去とシンボル誤りが訂正可能である．C_rは外部符号C_2を短縮して得られる(64,32)符号であり，C_2と同じ訂正能力をもつ．この縦接符号のレートは0.857である．

$t_2=7$としたときの誤り特性とスループット特性を表７と図26，27，28，29に示す．

それらの解析では変調方式は符号化を行わない４値ＰＳＫ変調を用いて行った．シンボルあたりのＳＮ比がρの加法的白色ガウス雑音を持つ通信路と符号化を行わない４値ＰＳＫ変調の組合せは，等価的に２元対称通信路とみなすことができ，そのときのビット誤り率εは次の式で与えられる[21]．

$$\varepsilon = \frac{1}{2}\ \mathrm{erfc}\left(\sqrt{\frac{\rho}{2}}\right) \tag{120}$$

但し，erfc(x)はガウスの補誤差関数（第２章，式(80)）である．

表7　具体例1（内部符号を用いない）の誤り特性とスループット特性

SNR per symbol (dB)	Bit-error rate (%)	$P_{er}+P_{es}$	$\bar{P}_{er}$	$\bar{P}_{er}^{(3)}$	$\bar{P}_{df}^{(2)}$	$\bar{P}_{df}^{(3)}$	$\underline{\zeta}^{(3)}$
4.32	5.00	1.00E+00	1.36E-12	4.07E-12	1.00E+00	1.00E+00	0.285
4.59	4.50	1.00E+00	2.23E-12	6.68E-12	1.00E+00	1.00E+00	0.285
4.86	4.00	1.00E+00	3.63E-12	1.09E-11	1.00E+00	9.99E-01	0.285
5.16	3.50	1.00E+00	5.87E-12	1.75E-11	9.78E-01	9.58E-01	0.287
5.49	3.00	1.00E+00	9.42E-12	2.64E-11	8.03E-01	6.72E-01	0.305
5.56	2.90	1.00E+00	1.04E-11	2.83E-11	7.33E-01	5.73E-01	0.313
5.63	2.80	1.00E+00	1.14E-11	3.01E-11	6.52E-01	4.69E-01	0.323
5.70	2.70	1.00E+00	1.25E-11	3.20E-11	5.64E-01	3.67E-01	0.334
5.77	2.60	1.00E+00	1.37E-11	3.38E-11	4.72E-01	2.73E-01	0.346
5.85	2.50	1.00E+00	1.50E-11	3.56E-11	3.83E-01	1.93E-01	0.359
5.92	2.40	1.00E+00	1.63E-11	3.75E-11	2.99E-01	1.30E-01	0.372
6.00	2.30	1.00E+00	1.77E-11	3.94E-11	2.26E-01	8.20E-02	0.385
6.08	2.20	1.00E+00	1.91E-11	4.13E-11	1.63E-01	4.92E-02	0.396
6.17	2.10	1.00E+00	2.04E-11	4.31E-11	1.14E-01	2.80E-02	0.405
6.25	2.00	1.00E+00	2.14E-11	4.44E-11	7.51E-02	1.50E-02	0.413
6.34	1.90	1.00E+00	2.20E-11	4.50E-11	4.77E-02	7.62E-03	0.418
6.43	1.80	1.00E+00	2.18E-11	4.42E-11	2.88E-02	3.65E-03	0.422
6.53	1.70	1.00E+00	2.07E-11	4.17E-11	1.64E-02	1.65E-03	0.425
6.63	1.60	1.00E+00	1.84E-11	3.72E-11	8.82E-03	6.92E-04	0.426
6.73	1.50	1.00E+00	1.54E-11	3.09E-11	4.44E-03	2.71E-04	0.427
6.84	1.40	1.00E+00	1.18E-11	2.35E-11	2.07E-03	9.71E-05	0.428
6.95	1.30	1.00E+00	7.97E-12	1.60E-11	8.83E-04	3.16E-05	0.428
7.07	1.20	1.00E+00	4.74E-12	9.47E-12	3.41E-04	9.09E-06	0.428
7.20	1.10	9.99E-01	2.39E-12	4.77E-12	1.18E-04	2.28E-06	0.428
7.33	1.00	9.97E-01	9.80E-13	1.96E-12	3.50E-05	4.81E-07	0.429
7.48	0.90	9.90E-01	3.14E-13	6.25E-13	8.80E-06	8.28E-08	0.430
7.64	0.80	9.72E-01	7.35E-14	1.45E-13	1.80E-06	1.11E-08	0.434
7.81	0.70	9.27E-01	1.16E-14	2.22E-14	2.80E-07	1.08E-09	0.444
8.00	0.60	8.31E-01	1.07E-15	1.95E-15	3.08E-08	6.90E-11	0.468
8.22	0.50	6.58E-01	4.76E-17	7.88E-17	2.10E-09	2.53E-12	0.517
8.34	0.45	5.41E-01	6.97E-18	1.08E-17	4.30E-10	3.65E-13	0.556
8.47	0.40	4.12E-01	7.39E-19	1.05E-18	7.13E-11	4.13E-14	0.607
8.62	0.35	2.82E-01	5.22E-20	6.69E-20	9.06E-12	3.44E-15	0.668
8.78	0.30	1.67E-01	2.16E-21	2.52E-21	8.11E-13	1.93E-16	0.734
8.97	0.25	7.98E-02	4.29E-23	4.63E-23	4.50E-14	6.27E-18	0.793
9.18	0.20	2.80E-02	2.95E-25	3.03E-25	1.25E-15	9.42E-20	0.833
9.45	0.15	5.93E-03	3.80E-28	3.82E-28	1.16E-17	4.22E-22	0.852
9.80	0.10	4.95E-04	2.29E-32	2.29E-32	1.44E-20	2.14E-25	0.856
10.35	0.05	4.17E-06	7.78E-40	7.78E-40	1.35E-25	5.86E-31	0.857

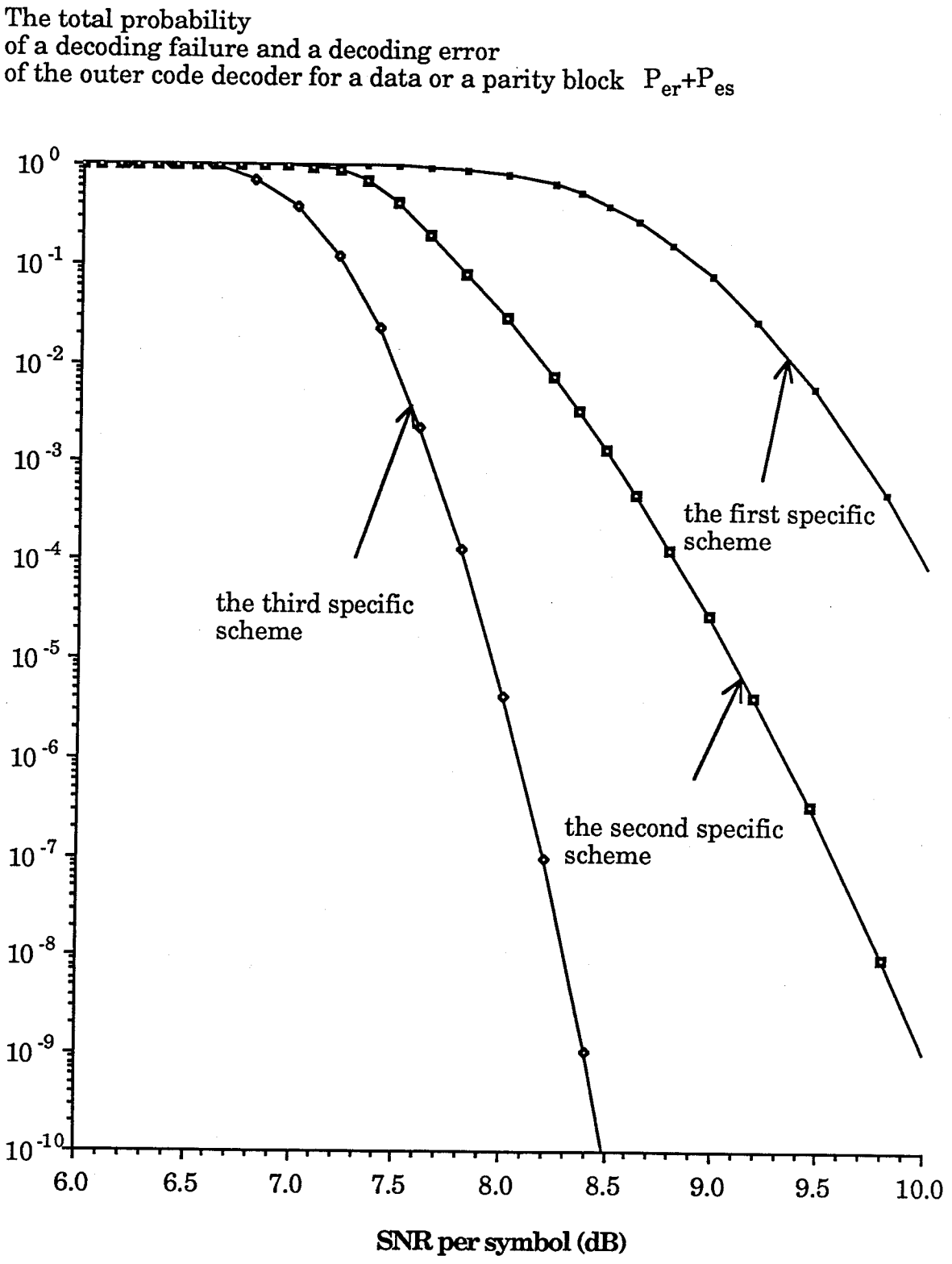

図26　3つの具体例における，データブロック（または，パリティブロック）が復号に失敗する確率と誤って復号される確率の和 $P_{es}+P_{er}$

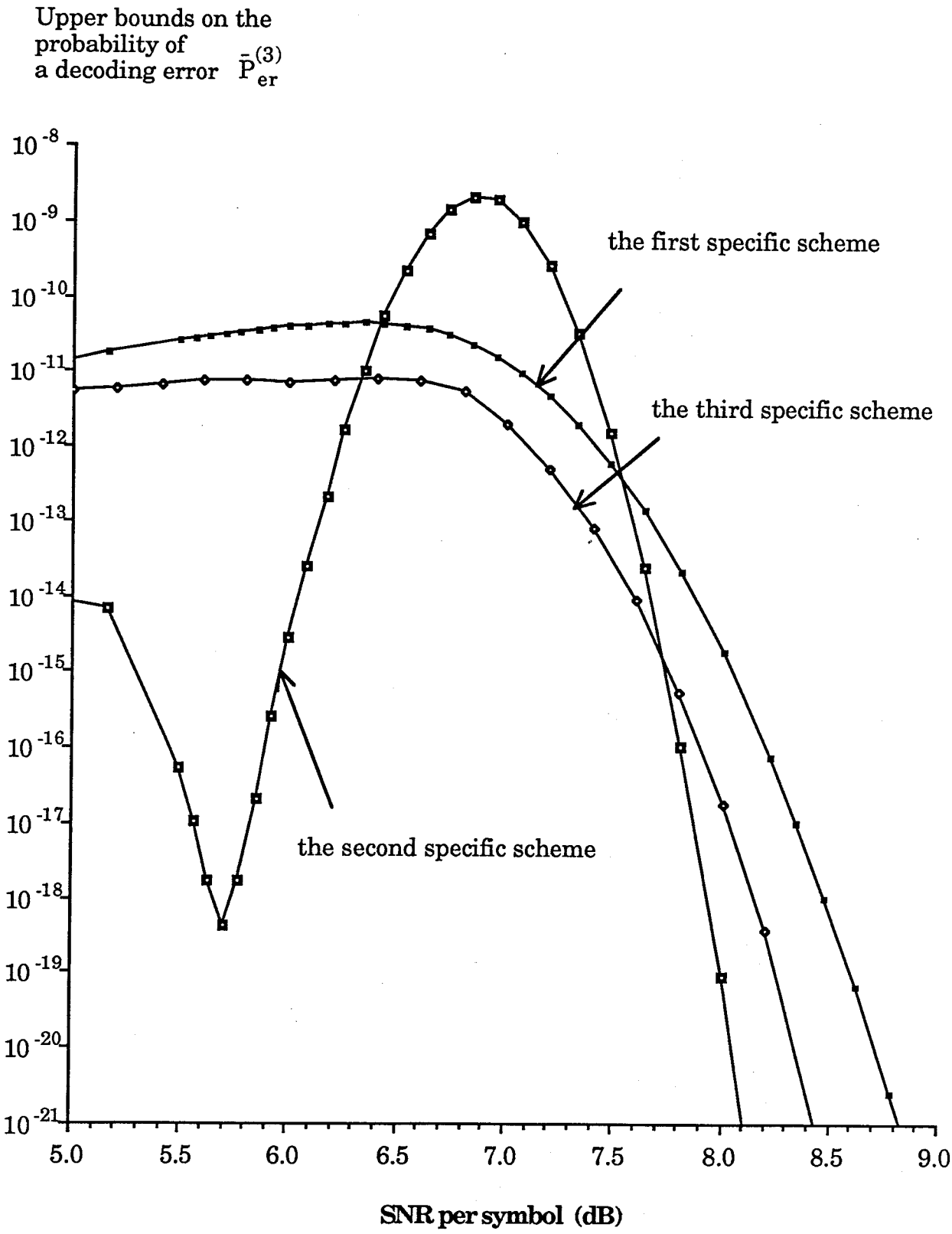

図27　3つの具体例における，高々2回迄の再送を行ったときのブロックが誤って復号される確率の上界 $\bar{P}_{er}^{(3)}$

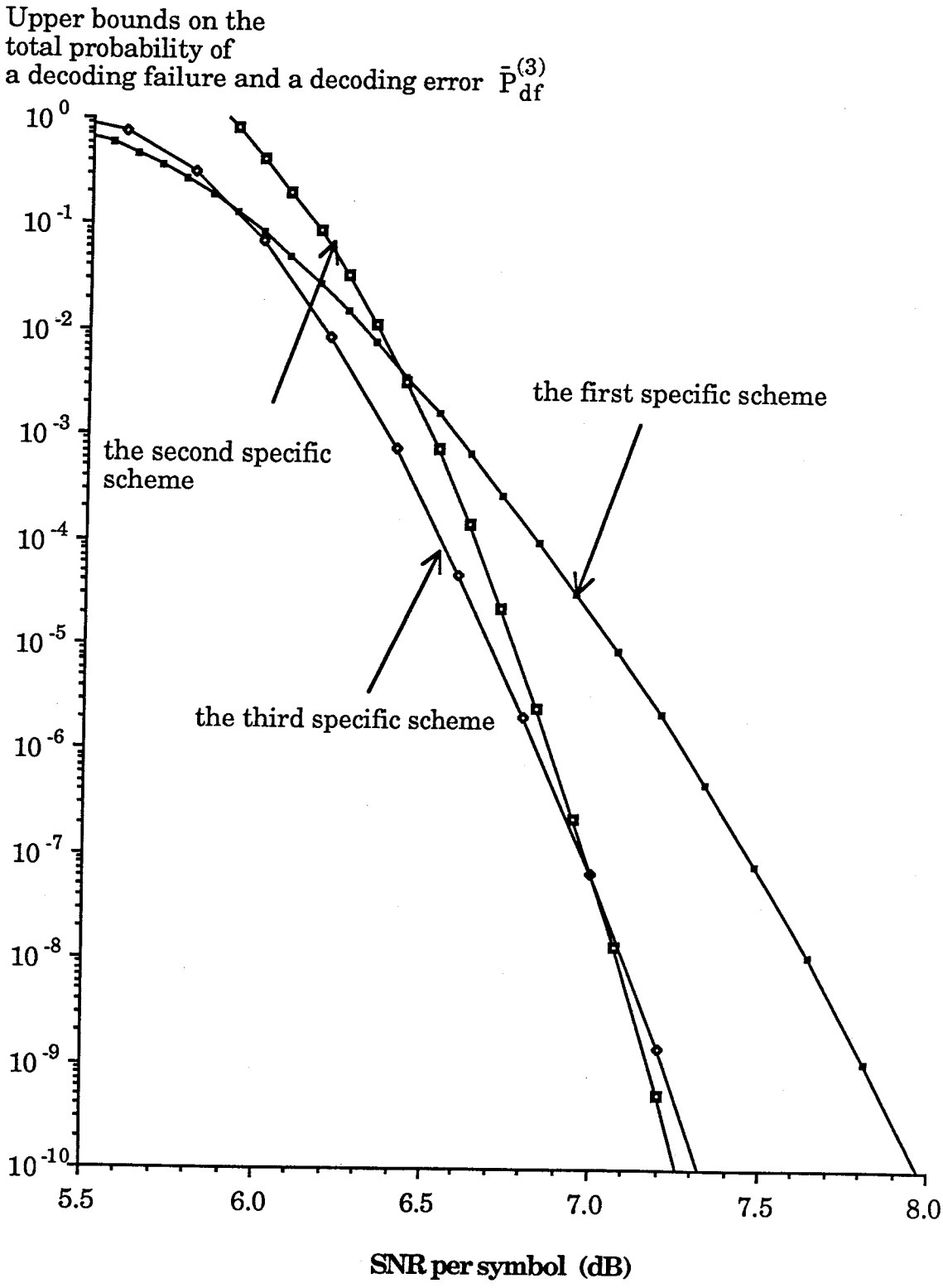

図28　3つの具体例における，高々2回迄の再送を行ったときのブロックが復号に失敗する確率と誤って復号される確率の和の上界 $\bar{P}_{df}^{(3)}$

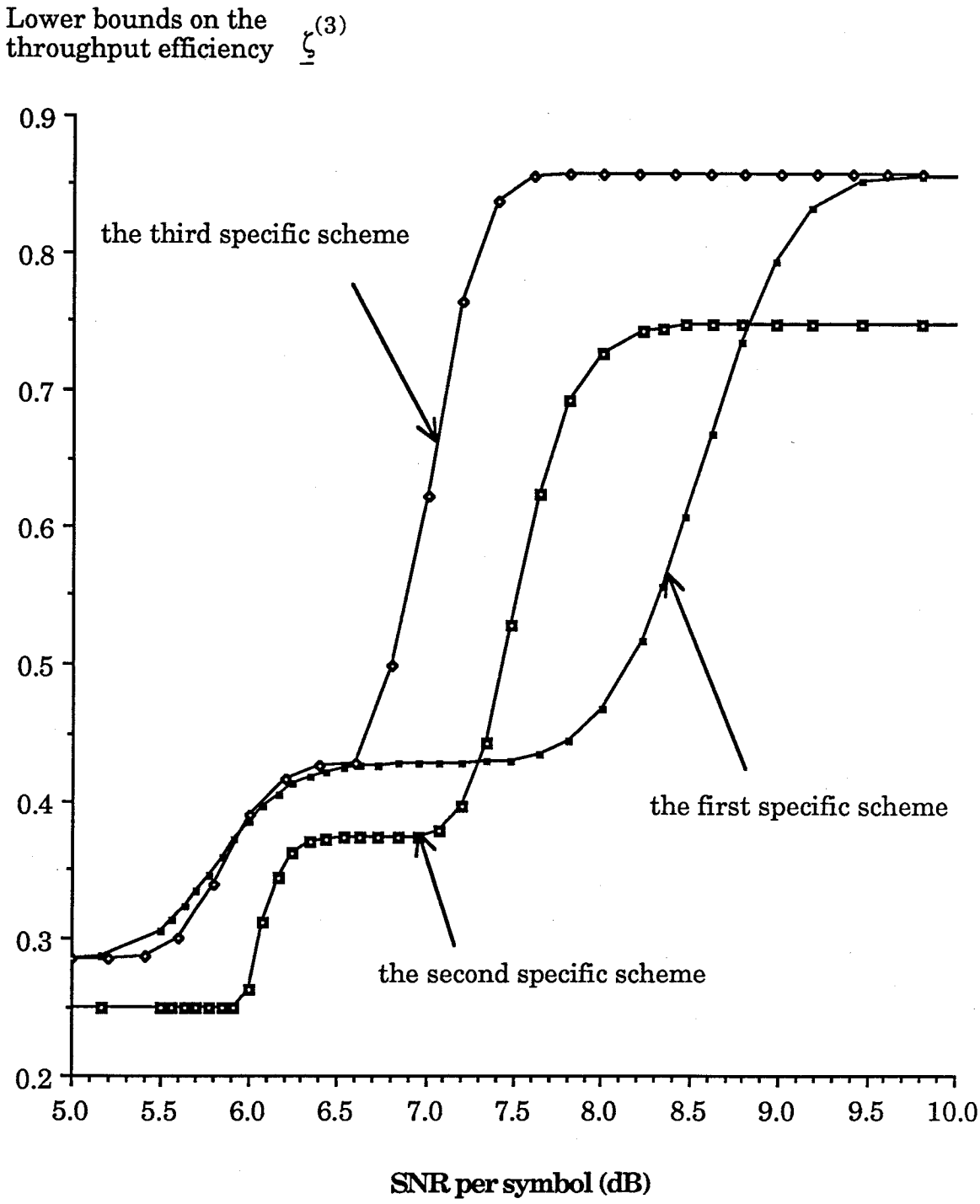

図29　3つの具体例における，高々2回迄の再送を行ったときのスループットの下界 $\underline{\zeta}^{(3)}$

この節の以下の解析では，(120)式の関係を用いてシンボルあたりのＳＮ比とビット誤り率の換算をおこなっている．

表７から，ビット誤り率が0.1%（シンボルあたりのＳＮ比が9.8dB）のとき，高々２回までの再送で復号に失敗する確率は2.14×10^{-25}，誤って復号する確率は10^{-31}以下であり，スループットは縦接符号のレートである0.856である．従って，例１では，ビット誤り率が0.1%以下ならば，実用上ほとんど誤りや再送を考慮に入れることなく通信可能である．

［例２］第２の例では内部符号C_1に第１章の表１の$C_1(1)$を用いる．この符号を内部符号に用いた縦接符号の具体例を２元対称通信路で用いたときの誤り特性の解析結果が，第１章の表３に示されている（但し，ここで取り上げる例とは外部符号の符号長が異なる）．この符号は次式で示される生成多項式：

$$g(x) = (1+x)(1+x+x^6) \tag{121}$$

をもつ符号長56のハミング符号を1ビット短縮した符号である．内部符号のパラメータは$n_1=55$，$k_1=48$，$t_1=1$である．また，$m_1=6$，つまり，外部符号は６重にインターリービングされる．外部符号C_2，C_r，変調方式は例１と同じものを用いる．この縦接符号のレートは0.748である．

$T_{es}=22$，$t_2=2$としたときの誤り特性とスループット特性を表８と図26，27，28，29に示す．表８から，ビット誤り率が0.5%（シンボルあたりのＳＮ比が8.22dB）のとき，高々２回までの再送で復号に失敗する確率は2.19×10^{-25}，誤って復号する確率は10^{-23}以下であ

表８　具体例２（内部符号に表１のC_1（２元線形符号）を用いる）の誤り特性とスループット特性

SNR per symbol (dB)	Bit-error rate (%)	$P_{er}+P_{es}$	$\bar{P}_{er}$	$\bar{P}_{er}^{(3)}$	$\bar{P}_{df}^{(2)}$	$\bar{P}_{df}^{(3)}$	$\underline{\zeta}^{(3)}$
4.32	5.00	1.00E+00	4.73E-41	8.56E-17	1.00E+00	1.00E+00	0.249
4.59	4.50	1.00E+00	1.41E-37	1.37E-15	1.00E+00	1.00E+00	0.249
4.86	4.00	1.00E+00	1.84E-33	9.14E-15	1.00E+00	1.00E+00	0.249
5.16	3.50	1.00E+00	1.03E-28	6.70E-15	1.00E+00	1.00E+00	0.249
5.49	3.00	1.00E+00	1.97E-23	5.49E-17	1.00E+00	1.00E+00	0.249
5.56	2.90	1.00E+00	2.50E-22	1.04E-17	1.00E+00	1.00E+00	0.249
5.63	2.80	1.00E+00	3.24E-21	1.75E-18	1.00E+00	1.00E+00	0.249
5.70	2.70	1.00E+00	4.25E-20	4.47E-19	1.00E+00	1.00E+00	0.249
5.77	2.60	1.00E+00	5.56E-19	1.75E-18	1.00E+00	1.00E+00	0.249
5.85	2.50	1.00E+00	7.11E-18	2.14E-17	1.00E+00	1.00E+00	0.249
5.92	2.40	1.00E+00	8.77E-17	2.63E-16	1.00E+00	8.14E-01	0.249
6.00	2.30	1.00E+00	1.01E-15	2.87E-15	8.34E-01	4.27E-01	0.263
6.08	2.20	1.00E+00	1.06E-14	2.55E-14	4.05E-01	2.05E-01	0.311
6.17	2.10	1.00E+00	9.84E-14	2.14E-13	1.73E-01	8.83E-02	0.344
6.25	2.00	1.00E+00	7.84E-13	1.62E-12	6.41E-02	3.38E-02	0.362
6.34	1.90	1.00E+00	5.18E-12	1.05E-11	2.06E-02	1.13E-02	0.370
6.43	1.80	1.00E+00	2.75E-11	5.50E-11	5.58E-03	3.21E-03	0.372
6.53	1.70	1.00E+00	1.13E-10	2.25E-10	1.27E-03	7.62E-04	0.373
6.63	1.60	1.00E+00	3.41E-10	6.82E-10	2.33E-04	1.48E-04	0.373
6.73	1.50	1.00E+00	7.31E-10	1.47E-09	3.39E-05	2.25E-05	0.373
6.84	1.40	1.00E+00	1.06E-09	2.11E-09	3.78E-06	2.62E-06	0.374
6.95	1.30	9.96E-01	9.56E-10	1.91E-09	3.09E-07	2.24E-07	0.374
7.07	1.20	9.73E-01	5.07E-10	1.00E-09	1.77E-08	1.33E-08	0.379
7.20	1.10	8.86E-01	1.44E-10	2.71E-10	6.60E-10	5.16E-10	0.396
7.33	1.00	6.86E-01	1.94E-11	3.26E-11	1.50E-11	1.22E-11	0.443
7.48	0.90	4.16E-01	1.08E-12	1.52E-12	1.86E-13	1.56E-13	0.528
7.64	0.80	2.00E-01	2.03E-14	2.43E-14	1.10E-15	9.45E-16	0.623
7.81	0.70	8.24E-02	9.93E-17	1.08E-16	2.54E-18	2.26E-18	0.691
8.00	0.60	2.91E-02	8.72E-20	8.98E-20	1.75E-21	1.60E-21	0.726
8.22	0.50	7.79E-03	7.72E-24	7.78E-24	2.35E-25	2.19E-25	0.742
8.34	0.45	3.49E-03	2.34E-26	2.35E-26	1.21E-27	1.14E-27	0.745
8.47	0.40	1.38E-03	2.68E-29	2.68E-29	3.04E-30	2.89E-30	0.747
8.62	0.35	4.69E-04	9.05E-33	9.05E-33	3.16E-33	3.04E-33	0.747
8.78	0.30	1.31E-04	6.34E-37	6.34E-37	******	******	0.747
8.97	0.25	2.82E-05	5.31E-42	5.31E-42	******	******	0.748
9.18	0.20	4.16E-06	2.13E-48	2.13E-48	******	******	0.748
9.45	0.15	3.41E-07	7.32E-57	7.32E-57	******	******	0.748
9.80	0.10	9.64E-09	4.66E-69	4.66E-69	******	******	0.748
10.35	0.05	2.04E-11	2.65E-90	2.65E-90	******	******	0.748

(*) 表中の記号“******”は，その欄の値が10^{-34}以下であることを表す．

り，スループットは0.742である．

［例３］第３の例では，内部符号C_1に第２章の表６の８値ＰＳＫブロック変調符号C_4を用いる．この符号は，また，第２章第５節の具体例１の内部符号としても用いられている（但し，ここで取り上げる例とは外部符号の符号長が異なる）．この符号は$n_1=8$，$k_1=16$である．この符号は，１信号点あたり２ビット，つまり符号化しない４値ＰＳＫ変調と同じ数の情報ビットを送信可能である．従って，例３の内部符号のレートは例１のものと同じである．この符号は４状態のトレリスダイアグラムをもつため，軟判定ヴィタビ復号法で容易に復号可能である．更に，この符号は45°の位相回転について閉じている．

外部符号と，C_rは例１，２と同じものを用いる．また，$m_1=2$，つまり，外部符号は２重にインターリービングされる．この縦接符号のレートは例１と同じ0.857である．

内部符号の復号で軟判定最尤復号法により誤り訂正を行ない，$t_2=16$としたときの誤り特性とスループット特性を表９と図26，27，28，29に示す．それらの解析では，内部符号の復号時の誤り確率$P_{ic}^{(1)}$，$\bar{p}_e(u,\alpha)$はシミュレーションによって求めている．

表９から，ビット誤り率が0.6%（シンボルあたりのＳＮ比が8.00 dB）のとき，高々２回までの再送で復号に失敗する確率は1.12×10^{-17}，誤って復号する確率は10^{-18}以下であり，スループットは0.857である．例３では，ビット誤り率が0.7%以下ならば，実用上ほとんど誤りや再送を考慮に入れることなく通信可能である．

次に，３つの具体例の比較をおこなう．図26，27，28，29は，３つの具体例の解析結果を併せて示している．図29から，例２は，シ

表９　具体例３（内部符号に表６のC_4（８値ＰＳＫ変調符号）を用いる）の
誤り特性とスループット特性

SNR per symbol (dB)	Bit-error rate (%)	$P_{er}+P_{es}$	$\bar{P}_{er}$	$\bar{P}_{er}^{(3)}$	$\bar{P}_{df}^{(2)}$	$\bar{P}_{df}^{(3)}$	$\underline{\zeta}^{(3)}$
5.0	3.77	1.00E+00	1.80E-12	5.39E-12	1.00E+00	1.00E+00	0.285
5.2	3.44	1.00E+00	1.99E-12	5.96E-12	1.00E+00	1.00E+00	0.285
5.4	3.13	1.00E+00	2.27E-12	6.77E-12	9.84E-01	9.69E-01	0.287
5.6	2.84	1.00E+00	2.65E-12	7.56E-12	8.55E-01	7.51E-01	0.300
5.8	2.56	1.00E+00	2.90E-12	7.29E-12	5.17E-01	3.18E-01	0.340
6.0	2.30	1.00E+00	3.22E-12	7.08E-12	2.01E-01	6.84E-02	0.390
6.2	2.06	1.00E+00	3.56E-12	7.29E-12	5.13E-02	8.48E-03	0.417
6.4	1.83	1.00E+00	3.85E-12	7.72E-12	9.48E-03	7.64E-04	0.426
6.6	1.63	1.00E+00	3.63E-12	7.26E-12	1.21E-03	4.75E-05	0.428
6.8	1.43	7.17E-01	3.08E-12	5.29E-12	1.10E-04	2.09E-06	0.499
7.0	1.26	3.77E-01	1.47E-12	2.02E-12	7.36E-06	6.61E-08	0.622
7.2	1.10	1.21E-01	4.58E-13	5.13E-13	3.61E-07	1.48E-09	0.764
7.4	0.95	2.25E-02	8.24E-14	8.42E-14	1.16E-08	2.06E-11	0.838
7.6	0.82	2.23E-03	9.25E-15	9.27E-15	3.22E-10	2.57E-13	0.855
7.8	0.71	1.30E-04	5.45E-16	5.45E-16	5.48E-12	1.88E-15	0.857
8.0	0.60	4.30E-06	1.92E-17	1.92E-17	7.35E-14	1.12E-17	0.857

ンボルあたりのＳＮ比が8.78dBと7.33dBの間では，例１より高いスループットで通信可能であり，例３は，シンボルあたりのＳＮ比のほぼ全区間にわたって例１，２より高いスループットで通信可能であることがわかる．しかし，例２の内部符号はシンドロームから誤り位置を表引き操作によって求める高速な復号法が存在するのに対して，例３の内部符号の復号法は，軟判定ヴィタビ復号法という，比較的時間がかかり，複雑な復号器を必要とする復号法である．しかし，優れた特性は，それらの点を補って余りあるものと思われる．

6．結言

この章では，縦接符号化方式によるＦＥＣ（誤り訂正）と，ブロックが復号に失敗したときにより強力な誤り訂正を行なうための検査シンボルの再送とを組み合わせた，新しい誤り制御通信方式について，その誤り特性とスループット特性の計算法を示した．この方式では，検査シンボルは，必要が生じたときのみ送信され，もとのブロックと同じ情報量を有する．検査シンボルは反転操作可能なレート１／２の強力な誤り訂正能力を持つ符号によって作られる．

この方式は，通信路が比較的雑音の少ないときには，縦接符号のレートと等しいスループットを有する．通信路が比較的雑音の多いとき，例えば，この章で述べたいくつかの具体例では，シンボルあたりのＳＮ比が6.5dBのときでも，高々１回の再送で通信可能で，そのとき，縦接符号の１／２のレートのスループットを有する．

３つの具体例について，誤り特性とスループット特性を示した．そのうちの１つは，内部符号に第２章の具体例で用いたものと同じ８値ＰＳＫブロック変調符号を用い，軟判定最尤復号を行う．その例は他の２つの例と比較して高いスループットを有する．また，どの例も雑音の多い通信路においても高い信頼性をもつ．３つの例すべて，(255,223)ＮＡＳＡ標準リードソロモン符号を短縮した，(224,192)符号を用いている．

それらの具体例は，通信路のＳＮ比が変動する衛星通信における高レートのファイル転送に適している．

結　論

本論文では，縦接符号化法による符号の構成法と，その符号を2元対称通信路（内部符号に2元線形符号を用いた場合）や加法的白色ガウス雑音をもつ通信路（内部符号にブロック変調符号を用いた場合）で用いたときの，誤って復号される確率や正しく復号される確率の計算法，及び，縦接符号によるＦＥＣと検査シンボルの再送を組み合わせた誤り制御通信方式と，その誤り特性やスループット特性の解析法について述べた．

ここでは，縦接符号化法を用いた誤り制御通信方式，および，その誤り確率の計算法について，残された課題，及び今後の展望について述べる．

本論文で取り上げた縦接符号化法のうち，内部符号にブロック変調符号を用いたのでは，内部符号の復号時に，軟判定最尤復号法による誤り訂正を行なうものと仮定したが，ここで，

1．誤り訂正と共に誤り検出をおこない，外部符号の復号時に内部符号で検出された誤りを訂正する方法，

2．内部符号による復号時に最尤復号法よりも，より簡単，かつ，高速な復号法の採用，

等が考えられる．それらの場合の誤って復号される確率や復号に失敗する確率がどうなるか検討することは興味深い問題である．また，現在，内部符号による復号時の誤訂正確率や復号によって生じる誤りパターンに関するいくつかの確率については，シミュレーションによる評価の方が上界式に基づく評価よりも，かなりよい結果が得られている．しかし，一般にシミュレーションによる評価では，統計的な誤差の問題が残り，かつ，シミュレーションに要する計算時

間も膨大なものとなる．そこで今後，内部符号に用いる変調符号のより詳細な幾何学的，代数学的構造に着目した上界式の改良が重要な問題である．また，内部符号に適したブロック変調符号の新しい構成法の開発は，たいへん重要な問題である．

また，内部符号に２元線形符号を用いたＦＥＣと検査シンボルの再送を組み合わせた誤り制御通信方式では，サブセクション対の復号に用いるレート１／２符号の誤り訂正能力が強力であることから，内部符号の復号に失敗したときに，消去操作を行なわないで，マーク付け操作を行なった方が，ブロックの復号に失敗する確率が低くなる可能性が高い．しかし，その場合の誤り特性やスループット特性の解析は困難な問題であろう．

謝　　辞

本研究に関して，常日頃より直接理解ある御指導を賜り，励ましていただいた嵩忠雄教授に深謝いたします．

大学学部，大学院を通じて御指導，御教示いただいた情報工学科の故藤澤俊男教授，都倉信樹教授，故高島堅助教授，鳥居宏次教授，谷口健一教授，産業科学研究所の豊田順一教授，北橋忠宏教授，角所収教授ならびに大型計算機センターの宮原秀夫教授に心から感謝いたします．

また，研究の詳細に至るまで，熱心に御指導，御助言いただいたハワイ大学のＳｈｕ　Ｌｉｎ教授，嵩研究室の藤原融助手に心から感謝いたします．

種々の面で御助言，御援助いただいた，藤井護助教授，伊藤実助教授，井上克郎助手，東野輝夫助手，関浩之助手，大阪大学医学部の田村進一教授，岡山大学工学部の杉山裕二教授に心から感謝いたします．

更に，筆者の在学中，御討論，御助力いただいた嵩研究室の方々，とくに，プログラム作成などに御協力いただいた院生宇治田聡氏，学生西永誠司氏に感謝いたします．

文　献

(1) G.D. Forney, Jr.: "Concatenated Codes", M.I.T. Press, Cambridge, MA (1966).

(2) M. Kasahara, Y. Sugiyama, S. Hirasawa and T. Namekawa: "New Classes of Binary Codes Constructed on the Basis of Concatenated Codes and Product Codes", IEEE Transactions on Information Theory, Vol. **IT-22**, pp. 462-468 (July 1976).

(3) S. Hirasawa, M. Kasahara, Y. Sugiyama and T. Namekawa: "Modified Product Codes", IEEE Transactions on Information Theory, Vol. **IT-30**, pp. 299-306 (March 1984).

(4) 今井，須田，矢代："２重符号化方式の適応的復号法"，電子通信学会論文誌(A), Vol. **J67-A**, No. 10, pp. 943-950 (1984年10月).

(5) T. Kasami, S. Lin and T. Fujiwara: "A Concatenated Coding Scheme for Error Control", IEEE Transactions on Communications, Vol. **COM-34**, No. 5, pp. 481-488, (May 1986).

(6) J. MacWilliams: "A Theorem on the Distribution of Weights in a Systematic Code", Bell System Techchnical Journal, No. 42, pp.79-94 (1963).

(7) F. J. MacWilliams and N. J. A. Sloane: "The Theory of Error-Correcting Codes", North-Holland, Amsterdam (1977).

(8) T. Kasami, T. Fujiwara, T. Takata and S. Lin: "A

Cascaded Coding Scheme for Error Control and its Performance Analysis", IEEE Transactions on Information Theory, Vol. **IT-34**, No. 3, pp.448-462 (May 1988).

(9) 高田:"縦接符号化法の正しく復号される確率，誤り見逃し確率と復号失敗確率"，大阪大学修士学位論文 (1986年2月).

(10) H. Imai and S. Hirakawa: "A New Multilevel Coding Method Using Error Correcting Codes", IEEE Transactions on Information Theory, Vol. **IT-23**, No. 2, pp.371-376 (May 1977).

(11) G. Ungerboeck: "Channel Coding with Multilevel/Phase Signals", IEEE Transactions on Information Theory, Vol. **IT-28**, pp. 55-67 (January 1982).

(12) V. V. Ginzburg: "Multidimensional Signal for a Continuous Channel", Problemy Peredachi Informatsii, Vol. **20**, No. 1, pp. 28-46 (1984).

(13) S. I. Sayegh: "A Class of Optimum Block Codes in Signal Space", IEEE Transactions on Communications, Vol. **COM-34**, No. 10, pp. 1043-1045 (October 1986).

(14) R. H. Deng and D. J. Costello, Jr.: "High Rate Concatenated Coding System with Bandwidth Efficient Inner Codes", presented at the 1986 IEEE International Symposium on Information Theory, Ann Arbor, October 6-9, 1986 and also submitted to IEEE Transactions on Communications (1987).

(15) T. Kasami, T. Takata, T. Fujiwara and S. Lin: "Error Control Systems with Combined Block Coding and M-ary

PSK Modulations", 第10回情報理論とその応用シンポジウム予稿集, Vol. 1, pp.393-398, (1987年11月).

(16) 嵩, 高田, 藤原, Lin: "符号化変調におけるブロック符号構成法について", 電子情報通信学会技術報告, **IT87-126**, pp. 49-54 (1988年3月).

(17) T. Kasami and S. Lin: "Bandwidth Efficient Block Codes for M-ary PSK Modulation", Technical Report to NASA Goddard Space Flight Center, Greenbelt, MD. (December 1988).

(18) S. Lin, T. Kasami, T. Fujiwara and T. Takata: "Cascaded Coding Schemes for Error Control in Space and Satellite Communications", Proceedings of 1988 International Forum on Information and its Applications, Tokyo, Japan June 27-30, 1988.

(19) T. Kasami, T. Takata, T. Fujiwara and S. Lin: "On Construction of Bandwidth Efficient Block Codes", IEEE Transactions on Information Theory (投稿中).

(20) A. J. Viterbi: "Error Bounds for Convolutional Codes and an Asymptotically Optimum Decoding Algorithm", IEEE Transactions on Information Theory, Vol. **IT-13**, pp. 260-269 (April 1967).

(21) J. C. Proakis: "Digital Communications", McGraw-Hill, New York (1983).

(22) S. Lin and D. J. Costello, Jr.: "Error Control Coding: Fundamentals and Applications", Prentice-Hall, New Jersey (1983).

付　　録

A．式(7)の証明

一般の場合のMacWilliamsの等式[7]より，$A_i^{(1)}(u,\beta)$と$B_h^{(1)}(u,\gamma)$について次の式が成立する．

$$A_i^{(1)}(u,\beta) = 2^{-r_1} \sum_{h=0}^{n_1-\ell} \sum_{\gamma \in GF(2^\ell)} B_h^{(1)}(u,\gamma)$$

$$P_i(h, n_1-\ell) \prod_{f=1}^{\ell} P_{\beta_f}(\gamma_f, 1) \qquad (A\cdot1)$$

但し，β_fはβを2進表現したときのf番目のビットを表す．

文献(7)のp.151より，次の2つの式が成立する．

$$\prod_{f=1}^{\ell} P_{\beta_f}(\gamma_f, 1) = (-1)^{(|\beta|+|\gamma|-|\beta+\gamma|)/2} \qquad (A\cdot2)$$

$$\sum_{i=0}^{n_1-\ell} P_i(h, n_1-\ell)\ (1+XY)^{n_1-\ell-i}(X+Y)^i$$

$$= (1+X)^{n_1-\ell-h}(1-X)^h(1+Y)^{n_1-\ell-h}(1-Y)^h \qquad (A\cdot3)$$

また，$W_{j,s}^{(i)}(n)$の生成関数は次式で表される．

$$W_{j,s}^{(i)}(n)X^jY^s = (1+XY)^{n-i}(X+Y)^i \qquad (A\cdot4)$$

式(A・1)，(A・2)，(A・3)と(A・4)より次式が成立する．

$$\sum_{i=0}^{n_1-\ell} \sum_{\substack{\beta \in GF(2^\ell) \\ |\alpha-\beta| \leq t_1}} A_i^{(1)}(u,\beta) \sum_{j=0}^{n_1-\ell} \sum_{s=0}^{n_1-\ell} W_{j,s}^{(i)}(n_1-\ell) X^j Y^s$$

$$= 2^{-r_1} \sum_{h=0}^{n_1-\ell} \sum_{\gamma \in GF(2^\ell)} B_h^{(1)}(u,\gamma) \sum_{\beta \in GF(2^\ell)}$$

$$(-1)^{(|\alpha|+|\beta|-|\alpha+\beta|)/2}$$

$$(1+X)^{n_1-\ell-h}(1-X)^h(1+Y)^{n_1-\ell-h}(1-Y)^h \qquad (A\cdot5)$$

式(A・5)をYについての多項式とみなし，両辺それぞれYの0次から$t_1-|\alpha-\beta|$次の項までの和をとった式のXに$\varepsilon/(1-\varepsilon)$，Yに1をそれぞれ代入して，両辺を$(1-\varepsilon)^{n_1}$倍することにより次式を得る．

$$\sum_{i=0}^{n_1-\ell} \sum_{\substack{\beta \in GF(2^\ell) \\ |\alpha-\beta| \leq t_1}} A_i^{(1)}(u,\beta) \sum_{j=0}^{n_1-\ell}$$

$$\sum_{s=0}^{t_1-|\alpha-\beta|} W_{j,s}^{(i)}(n_1-\ell)\ \varepsilon^j\ (1-\varepsilon)^{n_1-j}$$

$$= 2^{-r_1} \sum_{h=0}^{n_1-\ell} \sum_{\gamma \in GF(2^\ell)} B_h^{(1)}(u,\gamma)$$

$$\sum_{\substack{\beta \in GF(2^\ell) \\ |\alpha-\beta| \leq t_1}} (-1)^{(|\beta|+|\gamma|-|\beta+\gamma|)/2}$$

$$(1-\varepsilon)^\ell (1-2\varepsilon)^h \sum_{s=0}^{t_1-|\alpha-\beta|} P_s(h, n_1-\ell) \qquad (A\cdot6)$$

式(A・6)を式(6)に代入することにより式(7)を得る．　（証明終）

B．式(9)の証明

付録Aの式(A・1)，(A・2)，(A・3)，(A・4)から，次式が成立する．

$$\sum_{i=0}^{n_1-\ell} A_i^{(1)}(u,\beta)\left[\sum_{j=0}^{n_1-\ell}\sum_{s=0}^{n_1-\ell} W_{j,s}^{(i)}(n_1-\ell)X^jY^s\right]$$

$$\left[\sum_{j'=0}^{n_1-\ell}\sum_{s'=0}^{n_1-\ell} W_{j',s'}^{(|\alpha|)}(\ell)\,X^{j'}Y^{s'}\right]$$

$$= 2^{-r_1}(1+XY)^{\ell-|\alpha|}(X+Y)^{|\alpha|}\sum_{h=0}^{n_1-\ell}$$

$$\sum_{\beta\in GF(2^\ell)} B_h^{(1)}(u,\beta)\,(-1)^{(|\beta|+|\gamma|-|\beta+\gamma|)/2}$$

$$(1+X)^{n_1-\ell-h}(1-X)^h\,(1+Y)^{n_1-\ell-h}(1-Y)^h \qquad (B\cdot1)$$

式(B・1)をYについての多項式とみなし，両辺それぞれYの0次からt_1次の項までの和をとった式のXに$\varepsilon/(1-\varepsilon)$，Yに1をそれぞれ代入して，両辺を$(1-\varepsilon)^{n_1}$倍して得られる式を式(8)に代入することにより，式(9)を得る．　（証明終）

C．式(13)の証明

$F(X_1, X_2, \cdots, X_{m_1+1}, Y)$を次式で定義する．

$$F(X_1, X_2, \cdots, X_{m_1+1}, Y) = \sum_{i_1=0}^{\ell} \cdots \sum_{i_{m_1}=0}^{\ell} \sum_{i_{m_1+1}=0}^{r_1} A^{(1)}_{i_1, i_2, \cdots, i_{m_1+1}}$$

$$\left[\prod_{h=1}^{m_1} \sum_{j_h=0}^{\ell} \sum_{s_h=0}^{\ell} W^{(i_h)}_{j_h, s_h}(\ell)\, X^{j_h}\, Y^{s_h} \right]$$

$$\left[\sum_{j_{m_1+1}=0}^{r_1} \sum_{s_{m_1+1}=0}^{r_1} W^{(i_{m_1+1})}_{j_{m_1+1}, s_{m_1+1}}(r_1)\, X^{j_{m_1+1}}\, Y^{s_{m_1+1}} \right] \tag{C・1}$$

式(A・4)と一般の場合のMacWilliamsの等式[7, p. 151]より

$$F(X_1, X_2, \cdots, X_{m_1+1}, Y) = \sum_{i_1=0}^{\ell} \cdots \sum_{i_{m_1}=0}^{\ell} \sum_{i_{m_1+1}=0}^{r_1} A^{(1)}_{i_1, i_2, \cdots, i_{m_1+1}}$$

$$\prod_{h=1}^{m_1} (1+X_h Y)^{\ell - i_h} (X_h+Y)^{i_h} (1+X_{m_1+1} Y)^{r_1 - i_{m_1+1}} (X_{m_1+1}+Y)^{i_{m_1+1}}$$

$$= 2^{-r_1} \sum_{i_1=0}^{\ell} \cdots \sum_{i_{m_1}=0}^{\ell} \sum_{i_{m_1+1}=0}^{r_1} B^{(1)}_{i_1, i_2, \cdots, i_{m_1+1}}$$

$$\left[\prod_{h=1}^{m_1} (1+X_h)^{\ell - i_h} (1-X_h)^{i_h} \right] (1+X_{m_1+1})^{r_1 - i_{m_1+1}} (1-X_{m_1+1})^{i_{m_1+1}}$$

$$(1+Y)^{n_1 - \sum_{h=1}^{m_1+1} i_h} \quad (1-Y)^{\sum_{h=1}^{m_1+1} i_h} \tag{C・2}$$

$H=\{i \mid a_i=1 (1 \leqq i \leqq m_1)\}$とするとき，$F_{H, t_1}(X_1, X_2, \cdots, X_{m_1+1}, Y)$を，$F(X_1, X_2, \cdots, X_{m_1+1}, Y)$の項のうち，$h \in H$を満たす$h$について$X_h$の次数が非零，$h \in \{1, 2, \cdots, m_1\}-H$を満たす$h$について$X_h$の次数が零，かつ，$Y$の次数が$t_1$以下であるような項の和とする．式(C・2)より，次式が成立する．

$$F_{H,t_1}(X_1, X_2, \cdots, X_{m_1+1}, Y) =$$

$$2^{-r_1} \sum_{i_1=0}^{\ell} \cdots \sum_{i_{m_1}=0}^{\ell} \sum_{i_{m_1+1}=0}^{r_1} B^{(1)}_{i_1, i_2, \cdots, i_{m_1+1}}$$

$$\left[\sum_{s=0}^{t_1} P_s\left(\prod_{h=1}^{m_1} i_h,\ n_1\right) \right] \left[\prod_{h=1}^{m_1} (1+X_h)^{\ell - i_h} (1-X_h)^{i_h} \right]$$

$$(1+X_{m_1+1})^{r_1 - i_{m_1+1}} (1-X_{m_1+1})^{i_{m_1+1}} \qquad (C\cdot 3)$$

Krawtchoukの多項式の定義から次の式が成立する[7, p.153].

$$\sum_{s=0}^{t} P_s(i, n) = P_t(i-1, n-1) \qquad (C\cdot 4)$$

式(C・3)の各X_h, $1 \leqq h \leqq m_1+1$に$\varepsilon/(1-\varepsilon)$を代入し，Yに1を代入し，両辺を$(1-\varepsilon)^{n_1}$倍して得られる式と式(C・4)を式(12)に代入することにより，式(13)を得る．　（証明終）

D．式(18)の証明

式(A・4)から，次式が成立する．

$$\sum_{(i_1,\cdots,i_{m_1+1})\in I(H)} A^{(1)}_{i_1,i_2,\cdots,i_{m_1+1}}$$

$$\left[\prod_{h=1}^{m_1}\sum_{j_h=0}^{\ell}\sum_{s_h=0}^{\ell} W^{(i_h)}_{j_h,s_h}(\ell)\ X^{j_h}\ Y^{s_h}\right]$$

$$\left[\sum_{j_{m_1+1}=0}^{r_1}\sum_{s_{m_1+1}=0}^{r_1} W^{(i_{m_1+1})}_{j_{m_1+1},s_{m_1+1}}(r_1)\ X^{j_{m_1+1}}\ Y^{s_{m_1+1}}\right]$$

$$=\sum_{(i_1,\cdots,i_{m_1+1})\in I(H)} A^{(1)}_{i_1,i_2,\cdots,i_{m_1+1}}$$

$$(1+XY)^{n_1-\sum_{h=1}^{m_1+1} i_h}\ (X+Y)^{\sum_{h=1}^{m_1+1} i_h}$$

$$=\ (1+XY)^{\ell\,|H|}\sum_{(i_1,\cdots,i_{m_1+1})\in I(H)} A^{(1)}_{i_1,i_2,\cdots,i_{m_1+1}}$$

$$(1+XY)^{n_1-\ell\,|H|-\sum_{h=1}^{m_1+1} i_h}\ (X+Y)^{\sum_{h=1}^{m_1+1} i_h} \qquad (D\cdot 1)$$

$C_1(H)'$を次式で定義されるC_1の部分符号とする．

$C_1(H)' = \{\bar{v}\in C_1 \mid$ 各$h\in H$について，$\bar{v}$のh番目のシンボルの重みは0$\}$

$C_1(H)$を$C_1(H)'$の各元から，各$h\in H$について，h番目のシンボル位置のビットを取り除くことによって得られる$(n_1-\ell\,|H|, k_1-\ell\,|H|)$符号とする．

$A^{(1)}_i(H)$を$C_1(H)$の重みiの符号語数とする．$I(H)$の定義（式(19)）

から，式(D・1)の右辺は次のように書き直すことができる．

$$(1+XY)^{\ell|H|}\sum_{i=0}^{n_1-\ell|H|}A_i^{(1)}(H)\ (1+XY)^{n_1-\ell|H|-i}(X+Y)^i \tag{D・2}$$

$B_i^{(1)}(H)$を$C_1(H)$の双対符号の重み i の符号語数とする．Mac-Williamsの等式[7]から式(D・2)は次のように書き直すことができる．

$$2^{-r_1}(1+XY)^{\ell|H|}\sum_{i=0}^{n_1-\ell|H|}B_i^{(1)}(H)$$

$$(1+X)^{n_1-\ell|H|-i}(1-X)^i(1+Y)^{n_1-\ell|H|-i}(1-Y)^i \tag{D・3}$$

式(D・1)，(D・3)から，次の式が成立する．

$$\sum_{(i_1,\cdots,i_{m_1+1})\in I(H)}A^{(1)}_{i_1,i_2,\cdots,i_{m_1+1}}$$

$$\left[\prod_{h=1}^{m_1}\sum_{j_h=0}^{\ell}\sum_{s_h=0}^{\ell}W^{(i_h)}_{j_h,s_h}(\ell)\ X^{j_h}Y^{s_h}\right]$$

$$\left[\sum_{j_{m_1+1}=0}^{r_1}\sum_{s_{m_1+1}=0}^{r_1}W^{(i_{m_1+1})}_{j_{m_1+1},s_{m_1+1}}(r_1)\ X^{j_{m_1+1}}\ Y^{s_{m_1+1}}\right]$$

$$=\ 2^{-r_1}(1+XY)^{\ell|H|}\sum_{i=0}^{n_1-\ell|H|}B_i^{(1)}(H)\ (1+X)^{n_1-\ell|H|-i}(1-X)^i$$

$$\sum_{j=0}^{s}X^j\binom{\ell|H|}{j}\ P_{s-j}(i,n_1-\ell|H|) \tag{D・4}$$

式(D・4)をYについての多項式とみなし，両辺それぞれYの0次からt_1次の項までの和をとった式のYに1を代入すると次式を得る．

$$\sum_{(i_1,\cdots,i_{m_1+1})\in I(H)} A^{(1)}_{i_1,i_2,\cdots,i_{m_1+1}} \sum_{j_1=0}^{\ell} \cdots \sum_{j_{m_1}=0}^{\ell}$$

$$\sum_{j_{m_1+1}=0}^{r_1} \sum_{(s_1,s_2,\cdots,s_{m_1+1})\in S(t_1)} \left[\prod_{h=1}^{m_1} W^{(i_h)}_{j_h,s_h}(\ell) \right]$$

$$W^{(i_{m_1+1})}_{j_{m_1+1},s_{m_1+1}}(r_1)\ X^{\sum_{h=1}^{m_1+1} j_h} \qquad (D\cdot 5)$$

式(D・5)の各Xに$\varepsilon/(1-\varepsilon)$を代入し，両辺を$(1-\varepsilon)^{n_1}$倍した式を式(17)に代入することにより，次式を得る．

$$P_e^{(1)}(H) = 2^{-r_1} \sum_{i=0}^{n_1-\ell|H|} B_i^{(1)}(H)\ (1-2\varepsilon)^i (1-\varepsilon)^{\ell|H|}$$

$$\sum_{s=0}^{t_1} (\varepsilon/(1-\varepsilon))^{n_1-\ell|H|} \sum_{j=0}^{s} \binom{\ell|H|}{j} P_{s-j}(i, n_1-\ell|H|) \qquad (D\cdot 6)$$

$C_1(H)$の双対符号の生成行列は，C_1の検査行列の$h\in H$番目のシンボルに対応する列をとりのぞいたものであるから，$B_i^{(1)}(H)$について次式が成立する．

$$B_i^{(1)}(H) = \sum_{I_i(H)} B^{(1)}_{i_1,i_2,\cdots,i_{m_1+1}} \qquad (D\cdot 7)$$

但し，集合$I_i(H)$は次式で定義される．

$$I_i(H) = \{(i_1,\cdots,i_{m_1+1}) \mid \text{各}1\leqq h\leqq m_1\text{について}0\leqq i_h\leqq \ell,\ 0\leqq i_{m_1+1}\leqq r_1,\ \text{かつ},\ \sum_{h\in H} i_h = i\} \qquad (D\cdot 8)$$

式(D・7)に式(D・8)を代入することにより，式(18)を得る．

（証明終）

E．式(20)の証明

n_2個の復号後のセグメントにそれぞれ1，2，…，n_2の番号を付け，集合Nを，$N=\{1,2,\cdots,n_2\}$とする．いま消去されたセグメントの数がT_{es}以下であったと仮定する．集合E_sを消去されたセグメントの番号の集合とする．$N-E_s$の各元fについて，$e_f(u)$をf番目の復号後のセグメントのu番目の誤りシンボルとする．送信されたブロックのu番目のセクションの外部符号の符号語を$\bar{v}_c$とし，外部符号の復号段階においてu番目のセクションに誤りパターン$\bar{v}$（$\bar{v}$も外部符号の符号語）が起ったものとする．すなわち，外部符号の復号によって得られる復号結果は$\bar{v}_c+\bar{v}$である．v_fを$\bar{v}$のf番目のシンボルとし，$W(\bar{v})$，$H(\bar{v})$，$J(\bar{v})$を次の様に定義する．

$$W(\bar{v}) = \{f \mid v_f \neq 0,\ f \notin E_s\}$$

$$H(\bar{v}) = \{f \mid e_f(u) \neq 0,\ v_f = 0,\ f \notin E_s\}$$

$$J(\bar{v}) = \{f \mid e_f(u) = v_f \neq 0,\ f \notin E_s\}$$

t_2個以下のシンボル誤りとT_{es}個以下のシンボル消去が訂正されることから，次の不等式が成立する．

$$|H(\bar{v})|+|W(\bar{v})|-|J(\bar{v})| \leqq t_2$$

各$\bar{v} \in C_2$，$E_s \subseteq N$について，Nの部分集合H，J，J_2，S_2，Z_2を，$H \cap (E_s \cup W(\bar{v})) = \phi$，$J \subseteq W(\bar{v})$，$H_2 \subseteq H$，$J_2 \subseteq J$，$S_2 \subseteq W(\bar{v})-J$，$Z_2 \subseteq N-E_s-H$かつ$|H|+|W(\bar{v})|-|J| \leqq t_2$を満たす任意の集合とする．各u（$1 \leqq u \leqq$

m_1) について$P(u, E_s, \bar{v}, H, J, H_2, J_2, S_2, Z_2)$を$H(\bar{v})=H$, $J(\bar{v})=J$, 集合H, J, $W(\bar{v})-J$, $N-E_s-W(\bar{v})-H$の中のマーク付きセグメントの集合がそれぞれH_2, J_2, S_2, Z_2である誤りパターンが内部符号による復号の結果発生する確率とする.

$P(u, E_s, \bar{v}, H, J, H_2, J_2, S_2, Z_2)$は次の式で表される.

$$P(u, E_s, \bar{v}, H, J, H_2, J_2, S_2, Z_2) =$$

$$[P_{es}^{(1)}]^i [\bar{P}_e(u)]^{h-h_2} [\bar{P}_{e\ell}(u)]^{h_2} [P_e(u,0)]^{n_2-i-w-h-z_2}$$

$$[P_{e\ell}(u,0)]^{z_2} \prod_{f \in J-J_2} p_e(u, v_f) \prod_{f \in J_2} p_{e\ell}(u, v_f)$$

$$\prod_{f \in W(\bar{v})-J-S_2} (1-P_{es}^{(1)}-P_{e\ell}^{(1)}-p_e(u, v_f)) \prod_{f \in S_2} (P_{e\ell}^{(1)}-p_{e\ell}(u, v_f))$$

但し, $i=|E_s|$, $w=|W(\bar{v})|$, $h=|H|$, $h_2=|H_2|$, $z_2=|Z_2|$とする.

集合Wを$W \supseteq J$, $d_2-i \leqq |W|$, $|W|+h-j \leqq t_2$を満たす$N-E_s-H$の部分集合とし, $C_2(E_s, W)$を次の条件を満たすC_2の符号語の部分集合とする.

$$C_2(E_s, W) = \{(v_1, v_2, \cdots, v_{n_2}) \in C_2 \mid f \in W \text{のとき} v_f \neq 0,$$
$$f \notin W \cup E_s \text{のとき} v_f = 0\}$$

明らかに$\bar{v} \in C_2(E_s, W)$ならば$W(\bar{v})=W$である. 以下,

$\sum_{C_2(E_s, W)} P(u, E_s, \bar{v}, H, J, H_2, J_2, S_2, Z_2)$の上界式を考える.

$i \leqq T_{es}$, $t_2 \leqq (d_2-1-T_{es})/2$より次式が成立する.

$$d_2 \geqq i+2t_2+1$$

また，$w=|W|$とすれば$d_2 \leqq w+i$かつ$h+w-j \leqq t_2$であるから次式が成立する．

$$j \geqq i+w-d_2 \geqq 0$$

J'を$|J'|=i+w-d_2$を満たすJの部分集合とする．

$f \in J'$であるような各$a_f \in GF(2^{\ell})-\{0\}$について$v_f=v'_f=a_f$を満たす様な$C_2(E_s, W)$の異なる２つの符号語$\bar{v}=(v_1, v_2, \cdots, v_{n_2})$と$\bar{v}'=(v'_1, v'_2, \cdots, v'_{n_2})$を考える．$\bar{v}-\bar{v}'$の重みは少なくとも$d_2$であるから次の式が成立する．

$$f \in E_s \cup W-J' \text{について} \quad v_f \neq v'_f$$

相加相乗平均に関する不等式より次式が成立する．

$$\sum_{\bar{v} \in \{\bar{v} \in C_2(E_s, W) \mid f \in J' \text{について} v_f=a_f\}}$$

$$\prod_{f \in J-J_2} p_e(u, v_f) \quad \prod_{f \in J_2} p_{e\ell}(u, v_f)$$

$$\leqq \prod_{f \in J'-J_2} p_e(u, a_f) \quad \prod_{f \in J' \cap J_2} p_{e\ell}(u, a_f)$$

$$\sum_{q=0}^{2^{\ell}-2} [p_e(u, \gamma^q)]^b \sum_{q=0}^{2^{\ell}-2} [p_{e\ell}(u, \gamma^q)]^{j+d_2-i-w-b}$$

但し，$\max\{0, d_2-i-w+j-j_2\} \leqq b \leqq \min\{j-j_2, d_2-i-w+j\}$，$j_2=|J_2|$である．従って，次の不等式が成立する．

$$\sum_{\bar{v}\in C_2(E_s,W)} \prod_{f\in J-J_2} p_e(u,v_f) \prod_{f\in J_2} p_{e\ell}(u,v_f) \leqq$$

$$[\bar{p}_e(u)]^{j-j_2-b} [\bar{p}_{e\ell}(u)]^{j_2-d_2+i+w-j+b}$$

$$\sum_{q=0}^{2^{\ell}-2} [p_e(u,\gamma^q)]^b \sum_{q=0}^{2^{\ell}-2} [p_{e\ell}(u,\gamma^q)]^{j+d_2-i-w-b}$$

従って，次の不等式が成立する．

$$\sum_{\bar{v}\in C_2(E_s,W)} P(u,E_s,\bar{v},H,J,H_2,J_2,S_2,Z_2) \leqq$$

$$[P_{es}^{(1)}]^i [\bar{p}_e(u)]^{j-j_2-b+h-h_2} [\bar{p}_{e\ell}(u)]^{j_2-d_2+i+w-j+b}$$

$$[P_e(u,0)]^{n_2-i-w-h-z_2} [P_{e\ell}(u,0)]^{z_2} (1-P_{es}^{(1)}-P_{e\ell}^{(1)})^{w-j-f_2}$$

$$[P_{e\ell}^{(1)}]^{f_2} \sum_{q=0}^{2^{\ell}-2} [p_e(u,\gamma^q)]^b \sum_{q=0}^{2^{\ell}-2} [p_{e\ell}(u,\gamma^q)]^{j+d_2-i-w-b}$$

上式の左辺を$\bar{P}(u,E_s,\bar{v},H,J,H_2,J_2,S_2,Z_2)$と表す．

$P_{er}(u)$はすべてのE_s，H，J，W，H_2，J_2，S_2，Z_2の組合せについて

$\sum_{\bar{v}\in C_2(E_s,W)} P(u,E_s,\bar{v},H,J,H_2,J_2,S_2,Z_2)$の和をとったものであるから，式(20)が成立する．　（証明終）

F．式(38)の証明

Cの異なる2つの符号語を$\bar{v}=(s_1, s_2, \cdots, s_n)$，$\bar{v}'=(s_1', s_2', \cdots, s_n')$とするとき，$\bar{v}$，$\bar{v}'$は次の式で表すことができる．

$$\bar{v} = \bar{v}_1 + 2^{j_2-1}\bar{v}_2 + \cdots + 2^{j_h-1}\bar{v}_h \qquad (F\cdot1)$$

$$\bar{v}' = \bar{v}_1' + 2^{j_2-1}\bar{v}_2' + \cdots + 2^{j_h-1}\bar{v}_h' \qquad (F\cdot2)$$

但し，$\bar{v}_i$，$\bar{v}_i'$は，Cのコンポーネント符号C_iの符号語である．各$1 \leqq i \leqq h$，$1 \leqq j \leqq n$について，$\bar{v}_i$，$\bar{v}_i'$，s_j，s_j'は，次の式で表される．

$$\bar{v}_i = (v_{1i}, v_{2i}, \cdots, v_{ni}), \quad v_{ji} \in \bar{B}_i \qquad (F\cdot3)$$

$$\bar{v}_i' = (v_{1i}', v_{2i}', \cdots, v_{ni}'), \quad v_{ji}' \in \bar{B}_i \qquad (F\cdot4)$$

$$\bar{s}_j = \bar{v}_{j1} + 2^{j_2-1}\bar{v}_{j2} + \cdots + 2^{j_h-1}\bar{v}_{jh} \qquad (F\cdot5)$$

$$\bar{s}_j' = \bar{v}_{j1}' + 2^{j_2-1}\bar{v}_{j2}' + \cdots + 2^{j_h-1}\bar{v}_{jh}' \qquad (F\cdot6)$$

ここで，mを次の条件が成り立つ最小の添字の値とする．

$$\bar{v}_m \neq \bar{v}_m' \qquad (F\cdot7)$$

そのとき，$1 \leqq i \leqq m$，$1 \leqq j \leqq n$について，$v_{ji}=v_{ji}'$であるから，式(39)より，次式が成立する．

$$g(s_j, s_j^{'})$$

$$= g(\bar{v}_{j1}+2^{j2-1}\bar{v}_{j2}+\cdots+2^{jh-1}\bar{v}_{jh}, \bar{v}_{j1}^{'}+2^{j2-1}\bar{v}_{j2}^{'}+\cdots+2^{jh-1}\bar{v}_{jh}^{'})$$

$$\geqq g_{\bar{B}_m}(2^{jm-1}v_{jm}, 2^{jm-1}v_{jm}^{'}) \qquad (F\cdot 8)$$

従って，式(30)と(36)，(F・8)より，次式が成立する．

$$g^{(n)}(\bar{v}, \bar{v}^{'}) \geqq g_{\bar{B}_m}(2^{jm-1}\bar{v}_m, 2^{jm-1}\bar{v}_m^{'}) \geqq D[g_{\bar{B}_m}, C_m] \qquad (F\cdot 9)$$

従って，式(38)が成立する．　　（証明終）

G．$R(\bar{v}_i)$（式(104)）がC_2の符号語であることの証明

$\bar{g}_2(X)$を外部符号C_2の生成多項式とする．$\bar{g}_2(X)$の次数は$n_2-k_2=d_2-1$である．$\bar{v}(X)$をC_2の符号多項式とする．$\bar{v}_1(X)$，$\bar{v}_2(X)$，…，$\bar{v}_{m_2}(X)$を$\bar{v}(X)$のm_2個のサブセクションとする．$\bar{v}(X)$と$\bar{v}_1(X)$，$\bar{v}_2(X)$，…，$\bar{v}_{m_2}(X)$の間に次の式が成立する．

$$\bar{v}(X) = \bar{v}_1(X)+\bar{v}_2(X)X^{r_2}+ \cdots +\bar{v}_{m_2}(X)^{(m_2-1)r_2} \qquad (G\cdot1)$$

C_rはC_2の短縮符号であるから，C_rの生成多項式も$\bar{g}_2(X)$である．従って，$\bar{v}(X)$のｉ番目のサブセクション$\bar{v}_i(X)$をC_rで符号化して得られる符号多項式の検査シンボル部分の多項式$R_r[\bar{v}_i(X)]$は，$X^{r_2}\bar{v}_i(X)$を$\bar{g}_2(X)$で除算を行ったときの剰余多項式となる．従って，次の式が成立する．

$$X^{r_2}\bar{v}_i(X) = \bar{a}_i(X)\bar{g}_2(X) + R_r[\bar{v}_i(X)] \qquad (G\cdot2)$$

ここで，$R_r[\bar{v}_i(X)]$の次数はr_2-1以下である．式(104)は次の多項式で表される．

$$R[\bar{v}(X)] = R_r[\bar{v}_1(X)]+R_r[\bar{v}_2(X)]X^{r_2}+\cdots+R_r[\bar{v}_{m_2}(X)]X^{(m_2-1)r_2} \qquad (G\cdot3)$$

式(G･1)及び式(G･2)を式(G･3)に代入することにより次式を得る．

$$R[\bar{v}(X)] = \{ \bar{a}_1(X)+\bar{a}_2(X)X^{r_2}+ \cdots +\bar{a}_{m_2}(X)X^{(m_2-1)r_2}\}\bar{g}_2(X) + \bar{v}(X)X^{r_2} \qquad (G\cdot4)$$

$\bar{v}(X)$はC_2の符号多項式であるから，$\bar{g}_2(X)$で整除する．従って，式(G・4)より，$R[\bar{v}(X)]$は，$\bar{g}_2(X)$で整除する．$R[\bar{v}(X)]$の次数は$m_2r_2-1=n_2-1$次以下であるから，$R[\bar{v}(X)]$は，C_2の符号多項式である．

（証明終）

H．式(110)の証明

$P_{er}(u;w)$をC_rによる復号の結果，あるサブセクションに重みwの誤りパターンが発生する確率とする．式(20)の導出法と同じ議論から（付録Eを参照），次の不等式が成立する．

$$P_{er}(u;w) \leqq$$

$$\sum_{i_1=0}^{r_2} \binom{w}{i_1} \sum_{i_2=0}^{r_2-i_1} \binom{n_r-w}{i_2} [P_{es}^{(1)}]^{i_1+i_2}$$

$$\sum_{h=0}^{\min\{\lfloor \frac{r_2-(i_1+i_2)}{2} \rfloor, n_r-i_2-w\}} \binom{n_r-i_2-w}{h}$$

$$[\bar{p}_e(u)]^h [\bar{p}_e(u,0)]^{n_r-w-i_2-h} \sum_{j=w-i_1+h-\lfloor \frac{r_2-(i_1+i_2)}{2} \rfloor}^{w-i_1}$$

$$\binom{w-i_1}{j} [\max_{\alpha\neq 0}\{\bar{p}_e(u,\alpha)\}]^j [1-P_{es}^{(1)}]^{w-i_1-j} \qquad (H\cdot 1)$$

式(H・1)の右辺を$\bar{P}_{er}(u;w)$と定義する．次に，条件：

$$\frac{\max_{\alpha\neq 0}\{\bar{p}_e(u,\alpha)\}}{\bar{p}_e(u,0)} \leqq \frac{2}{d_2+1} \qquad (H\cdot 2)$$

が成立するならば，すべての$1 \leqq u \leqq m_1$，$d_2 \leqq w \leqq n_r$について，次の関係式：

$$\bar{P}(u;d_2) \geqq \bar{P}(u;w) \qquad (H\cdot 3)$$

が成立することを示す．式(H・1)より次式が成立する．

$$P_{er}(u;w+1) \leqq$$

$$\sum_{i_1=0}^{r_2} \binom{w+1}{i_1} \sum_{i_2=0}^{r_2-i_1} \binom{n_r-w-1}{i_2} [P_{es}^{(1)}]^{i_1+i_2}$$

$$\sum_{h=0}^{\min\{\lfloor \frac{r_2-(i_1+i_2)}{2} \rfloor, n_r-i_2-w-1\}} \binom{n_r-i_2-w-1}{h}$$

$$[\bar{p}_e(u)]^h [\bar{p}_e(u,0)]^{n_r-w-1-i_2-h} \sum_{j=w-i_1+h-\lfloor \frac{r_2-(i_1+i_2)}{2} \rfloor}^{w-i_1}$$

$$\binom{w-i_1}{j+1} [\max_{\alpha \neq 0}\{\bar{p}_e(u,\alpha)\}]^{j+1} [1-P_{es}^{(1)}]^{w-i_1-j} \qquad (H\cdot 4)$$

式(H・1)の右辺と式(H・4)の右辺を比較することにより，式(H・3)が成立するための条件は，次の条件が成立することである．

各 $d_2 \leqq w < n_r$, $0 \leqq i_1+i_2 \leqq r_2$,

$0 \leqq h \leqq \min\{\lfloor (d_2-(i_1+i_2)-1)/2 \rfloor, n_r-w\}$,

かつ，$w-i_1+h-\lfloor (d_2-(i_1+i_2)-1)/2 \rfloor \leqq j \leqq w$ に対して，

$$\frac{\binom{w+1}{i_1}\binom{n_r-w-1}{i_2}\binom{n_r-i_2-w-1}{h}\binom{w+1-i_1}{j+1}\max_{\alpha \neq 0}\{\bar{p}_e(u,\alpha)\}}{\binom{w}{i_1}\binom{n_r-w}{i_2}\binom{n_r-i_2-w}{h}\binom{w-i_1}{j}\bar{p}_e(u,0)}$$

$$\leqq 1 \qquad (H\cdot 5)$$

式(H・5)は次の様に書き直すことができる．

$$\frac{\max_{\alpha \neq 0}\{\bar{p}_e(u,\alpha)\}}{\bar{p}_e(u,0)} \leqq \frac{(n_r-w)(j+1)}{(n_r-i_2-w-h)(w+1)} \qquad (H\cdot 6)$$

条件(H・2)が成立するならば，各$d_2 \leqq w < n_r$，$0 \leqq i_1+i_2 \leqq r_2$，$0 \leqq h \leqq \min\{\lfloor(d_2-(i_1+i_2)-1)/2\rfloor, n_r-w\}$，かつ，$w-i_1+h-\lfloor(d_2-(i_1+i_2)-1)/2\rfloor \leqq j \leqq w$に対して，式(H・6)が成立する．そのとき，$\bar{P}_{ep}^{(max)}(u)$は，$C_r$による復号の結果，与えられた特定の誤りパターンが発生する確率の上界となっている．第5節の具体例で用いた内部符号と外部符号では，ビット誤り率$\varepsilon \leqq 0.2$の範囲で条件(H・2)を満足する．従って，それらのビット誤り率の範囲では式(110)を満足する．

（証明終）