

高速衛星通信に適した誤り訂正符号 その1

名古屋工業大学
岡本英二

1. まえがき

衛星通信はその広域性と地上災害などに対する高安定性により、放送も含め幅広く用いられている。近年の有線・無線通信の大容量化に伴い、衛星通信においても高速化が進んでいる[1,2]。一方、衛星通信を含む宇宙通信では、長い通信距離に伴う減衰を補うことを理由として見通し通信を行うことが前提であるため、直進性の強い周波数帯を用いることによる不都合は大きくなく、従来よりマイクロ波、ミリ波帯などが用いられており、光を用いた通信も研究開発なされている[3]。宇宙通信の主な形態は深宇宙を含めた衛星間通信、地上一衛星間通信であるが、地上無線と比べると長距離通信に伴う減衰が非常に大きい。また地上一衛星通信においては、大気の揺らぎ、準マイクロ波帯以上の雨・雲による減衰、移動体通信の場合にはさらに建物、樹木などによるシャドウイング、マルチパス受信によるフェージングが発生し、受信電力に変動が生じてしまい瞬時的な変動と共に、時にはバースト的な受信電力の落ち込みとして表れる。

これらの変動による復号品質の劣化を防ぐために、宇宙通信では通信路符号化(前方誤り訂正, forward error correction: FEC)の適用が必須である。一般的に伝送品質を上げるための技術としては前方誤り訂正と自動再送要求(automatic repeat request: ARQ)の組み合わせが強力に作用するが、衛星のように広域性を持ち、伝搬距離が長い場合には再送要求の輻輳と再送遅延が大きくなり有効に機能しなくなるため、衛星通信においては ARQ は必ずしも用いられず、前方誤り訂正が広く適用されている。従来から衛星通信では通信路符号化としてビタビ復号を適用した畳み込み符号[4]や、Reed-Solomon 符号[5]が用いられてきたが、近年強い符号としてターボ符号[6]や Low-density parity-check (LDPC) 符号[7]が実用化され、衛星デジタルテレビ放送 (DVB-S2)、IEEE802.16e、第 3 世代携帯電話など、地上系衛星系を問わず放送、通信規格として採用されている。一般的に特に地上系のシステムでは、これらの符号の復号には訂正能力を上げるために、軟値を用いて再帰的な繰返し演算を行う手法も用いられている。しかし伝送速度の高速化に伴い、この軟値再帰的復号では計算量が多く次第に復号遅延が無視できないようになってきた。また無線伝送においては、同じ長さのバースト的電力落ち込みでも、高速化によりその間のビット数が増加するため相対的にバースト長が長くなってしまふ。この計算遅延と長バースト長に対応するためには高速信号処理と長符号が必要となり、復号の回路規模などの所要能力を極めて高くしてしまう。そのためシンプルな符号化、復号化が行え、かつ性能のよい長い符号が求められているところであった。これらは必ずしも物理レイヤである必要はなく、上位レイヤでの構造を持つもので実現することが高速処理には望ましいとの検討がなされている[8]。

現在そのような符号として、消失通信路に対する Rateless 符号[9,10]や LDPC 符号の一種である Low-density generator matrix (LDGM) 符号[11]が提案されている。消失通信路とは、通信路を通った信号が 2 値的な変動を受け、正しく受信されるか消失するかに分けられるものである。また消失した位置は受信側で受信電力測定などにより正しく把握できると仮定される。これらの符号は消失通信路に対して高い

誤り訂正能力を持ち、かつ線形演算で復号が行えるため、高速な宇宙通信に有効であると考えられている。

そこで本号及び次号の2号で、消失通信路に対する Rateless 符号と LDGM 符号の構成について説明を行う。また一般的モデルである AWGN 通信路に対する LDPC 符号とその復号についても述べ、違いを明らかにする。まず本号「その1」では AWGN と消失通信路のモデルについて簡単に述べ、LDPC 符号と軟値再帰的演算を行う Sum-product 復号について説明し、高速衛星通信において必要な誤り訂正符号の構成条件を述べる。次号の「その2」では Rateless 符号と LDGM 符号を紹介し、最後にまとめを述べる。

2. 通信路モデル

通信路符号化では伝搬路で受けるひずみや雑音により最適な符号設計が変化するが、最も基本的な物理層の伝搬路モデルは付加的白色ガウス雑音 (additive white Gaussian noise: AWGN) 通信路である。図1に等価低域系における離散時間モデルを示す。

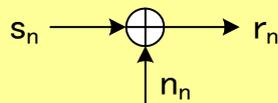


図1 AWGN 通信路の離散時間モデル

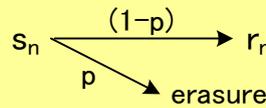


図2 消失通信路の離散時間モデル

等価低域系では複素ベクトルにより送受信信号を表すことができ、 n を時刻、送信シンボルを s_n 、受信シンボルを r_n 、ガウス雑音シンボルを n_n としたとき、 $r_n = s_n + n_n$ で表すことができる。この通信路をもう少し単純化したモデルとして図2に示すようなランダム消失通信路 (erasure channel: EC. 2元入力の場合 binary erasure channel: BEC という) がある。離散送信シンボルはランダムな確率 p で消失し、 $(1-p)$ の確率で正しく受信される。つまり受信された場合は正しく、他のシンボルに誤ることは無いというモデルである。以降ではこの2つの伝搬路モデルを対象として考える。

3. LDPC 符号と Sum-product 復号

LDPC 符号は 1962 年に R. Gallager により提案された通信路符号化手法[7]で、提案当初は当時の計算能力から実現性に乏しいとして注目を集めなかったが、1990 年代に再発見され、その強力な誤り訂正能力から種々のシステムに用いられるようになった。LDPC 符号は非常に疎な、すなわち行列内の非零要素の数が非常に少ない検査行列により定義される線形ブロック符号である。LDPC 符号と sum-product 復号法と呼ばれる復号法の組み合わせにより得られる AWGN 通信路でのビット誤り率特性は、ターボ符号に匹敵するか、もしくは符号長の長い場合にはそれを上回り、シャノン限界に非常に近づくということが知られている。なお LDPC は線形符号でありガロア体上の多次元で構成できるが、以下は簡単のため GF(2) 上の2元 LDPC について述べる。

LDPC 符号の構成には正則と非正則がある。正則 LDPC とは検査行列の行数を M 、列数を N 、行列中の各列、各行の1の数(重み)をそれぞれ j 、 k ($j \ll N, k \ll N, j < k$) としたとき、

$$jN = kM \tag{1}$$

を満たす構成であり、そうでなければ非正則である。一般に正則 LDPC の方が構築が簡単であるが、適切な構造の非正則 LDPC の方が誤り率特性は良い。ここでは正則 LDPC の構成について説明する。図3に Gallager の正則 LDPC の検査行列 \mathbf{H} の構成例を示す。

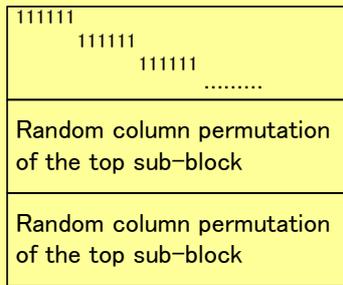


図3 Gallager による検査行列 \mathbf{H} の構成法の例, $j = 3, k = 6$.

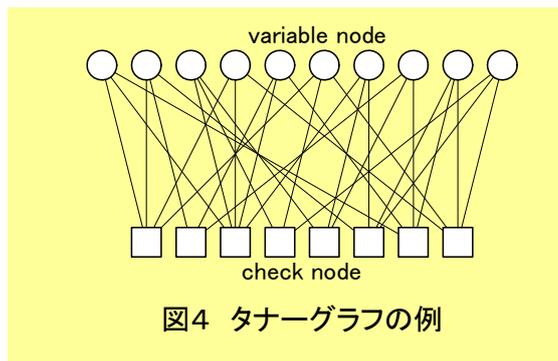
図のように検査行列を行方向のサブブロックに分ける. そのブロック数は列重み j に一致し, 1段目は行重み k に沿って規則的に階段状に1を配置し, 2段目以降はその列をランダムに入れ替えて配置する. このように情報ビットとパリティビットにランダムで疎な拘束条件を設け長い符号を構成することで, 強い誤り訂正能力を得る.

LDPC 符号の生成行列 \mathbf{G} は検査行列 \mathbf{H} より作成する. 線形符号では \mathbf{P} を情報・検査ビット関連行列としたとき, 生成行列と検査行列に

$$\mathbf{GH}^T = \mathbf{0}, \quad \mathbf{H} = [\mathbf{P}, \mathbf{I}], \quad \mathbf{G} = [\mathbf{I}, \mathbf{P}^T] \quad (2)$$

の関係があるため, 図3のようにして生成された検査行列 \mathbf{H} に対し基本行操作を行い, (2) 式のような既約台形正準形の形に変形することによって \mathbf{P} を得, 生成行列 \mathbf{G} を作成することができる. なお基本行操作とは 1) 行ベクトルを入れ替える, 2) 任意の行ベクトルを他の行に加える, の操作のことである. 基本行操作だけで既約台形正準形への変換ができない場合には列の入れ替えを行い, 変換する. ただし列操作を行った場合は, 図3の検査行列 \mathbf{H} の対応列も入れ替える必要がある. こうして得られた生成行列 \mathbf{G} に情報ビット列 \mathbf{m} を左から乗算することで $\mathbf{c} = \mathbf{m}^T \mathbf{G}$ として符号語 \mathbf{c} を得る.

LDPC の復号アルゴリズムはいくつか存在するが, Sum-product 復号法が最も能力の高い手法として知られている. ここでは対数を用いた Sum-product 復号について述べる. 図4に復号の際に用いるタナーグラフと呼ばれる2部グラフの例を示す.



タナーグラフの上部は変数ノード(variable node)といい, 検査行列の列数 N に等しいノード数を持ち, ノード n は第 n 列目に相当する. 同様に下部はチェックノード(check node)といい, 行数 M に等しく, ノード m は第 m 行目に相当する. そして検査行列 \mathbf{H} の第 m 行 n 列の要素 $H_{mn} = 1$ に対応する変数ノード n とチェックノード m 間が接続される. このグラフを用いて再帰的計算を行い, 復号特性を向上させる. タナーグラフで伝達される媒体はビットの対数尤度比(log-likelihood ratio: LLR)である. 2値入力 AWGN 通信路において, 受信値を r_n とし, 情報ビット $\{0,1\}$ をそれぞれ $\{1,-1\}$ として変調した場合, 受信 LLR 値 λ_n は以下のように得られる.

$$\lambda_n = \ln \frac{P(r_n | s_n = 1)}{P(r_n | s_n = -1)} = \frac{2}{\sigma^2} r_n \quad (3)$$

ここで σ^2 はガウス雑音の分散である。そして、検査行列の第 m 行の列番号部分集合 $N_m = \{n : H_{mn} = 1\}$, 第 n 列の行番号部分集合 $M_n = \{m : H_{mn} = 1\}$ を用い、繰返し l 回目における事前 LLR 値を $u_{mn}^{(l)}$, 外部 LLR 値を $v_{mn}^{(l)}$ として以下の Sum-product アルゴリズムにより復号演算を行う。

S1) 初期化 :

初回演算では繰返し復号による事前情報は与えられていないため, $H_{mn} = 1$ を満たすすべての (m, n) に対する事前 LLR, 外部 LLR 値を $u_{mn}^{(1)} = v_{mn}^{(1)} = 0$ とし, $l = 1$ とする。

S2) 行処理 (チェックノード処理) :

各チェックノードに対し, 接続されているすべての受信 LLR 値 λ_n , 事前 LLR 値 $u_{mn}^{(l)}$ を用いて次式のように外部 LLR 値 $v_{mn}^{(l)}$ を更新する。

$$v_{mn}^{(l)} = \left(\prod_{n' \in N_m \setminus n} \text{sign}(\lambda_{n'} + u_{mn'}^{(l)}) \right) f \left(\sum_{n' \in N_m \setminus n} f(|\lambda_{n'} + u_{mn'}^{(l)}|) \right) \quad (4)$$

ここで $N_m \setminus n$ は n を除く N_m の集合を表す。また式中の関数は

$$\text{sign}(x) = \begin{cases} 1, & x \geq 0 \\ -1, & x < 0 \end{cases} \quad (5)$$

$$f(x) = \ln \frac{e^x + 1}{e^x - 1} = -\ln \left[\tanh \left(\frac{x}{2} \right) \right] \quad (6)$$

である。(6) 式の $f(x)$ は Gallager の f 関数と呼ばれる。

S3) 列処理 (変数ノード処理) :

同様に各変数ノードに対し, 接続されているすべての外部 LLR 値 $v_{m'n}^{(l)}$ を用いて次式のように事前 LLR 値 $u_{mn}^{(l)}$ を更新する。

$$u_{mn}^{(l)} = \sum_{m' \in M_n \setminus m} v_{m'n}^{(l)} \quad (7)$$

S4) 一時推定語算出 :

得られた LLR を用いて

$$\hat{c}_n = \begin{cases} 0, & \text{if } \text{sign} \left(\lambda_n + \sum_{m \in M_n} v_{mn} \right) = 1 \\ 1, & \text{if } \text{sign} \left(\lambda_n + \sum_{m \in M_n} v_{mn} \right) = -1 \end{cases} \quad (8)$$

を計算し, 一時推定語 $\hat{\mathbf{c}} = \{\hat{c}_1, \dots, \hat{c}_n\}$ を算出する。

S5) パリティ検査 :

線形符号における符号語の必要十分条件

$$\hat{\mathbf{c}} \mathbf{H}^T = \mathbf{0} \quad (9)$$

が成り立つ場合は $\hat{\mathbf{c}}$ が符号語であるので復号結果として出力し, アルゴリズムを終了する。

S6) 繰返し :

もし $l < l_{\max}$ ならば $l = l + 1$ として S2 に戻る. そうでなければ最後の推定語を出力して終了する.

このように軟値である LLR を用いて再帰的復号を行うことにより, 優れた誤り訂正能力が得られる. 計算機シミュレーションにより LDPC 符号のビット誤り率特性を調べた. シミュレーション条件を表1に, 算出結果を図5に示す.

表1 AWGN 通信路における LDPC 符号伝送特性のシミュレーション条件

符号長	N=1032, 4128
パリティ長	M=514, 2062
重み(j,k)	(3,6)
符号化率	約 1/2
変調方式	BPSK
伝搬路	AWGN
復号方式	Sum-product
l_{\max}	40

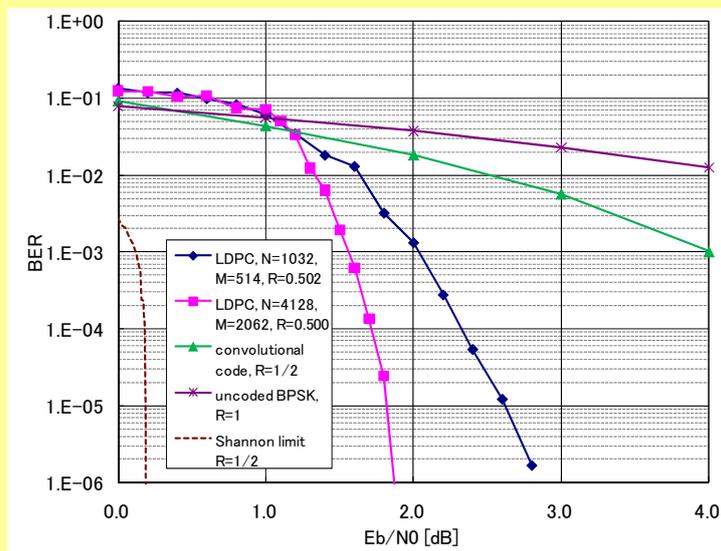


図5 LDPC 符号のビット誤り率特性

このように同じ符号化率の再帰的組織置み込み符号と比べて大きな符号化利得が得られており, シヤノン限界に近付いていることが分かる. また符号長の伸長により特性が改善されていることも示されている. 本例では基本的な検査行列生成法を用いたため必ずしも与えられた符号長に対して LDPC の能力が最大化されていないが, 検査行列の最適化を行うと誤り率特性はさらにシャノン限界に近づく. なお正確にいうと Gallager の生成法による正則 LDPC 符号では検査行列の階数が $(j-1)$ ランクが落ちるため, (1) 式は成り立たない. 本例の符号長設定のようにランクに沿ったものとするか, (1) 式を成り立たせるために従属行を加えて見かけ上成り立つようにする.

4. 高速衛星通信において必要な誤り訂正符号の構成条件

前節のように Sum-product アルゴリズムを用いる LDPC 復号では, AWGN 通信路における高い誤り訂正能力を提供するが, 軟値を用い数回から数十回の再帰的演算を行うため復号器の計算負荷がやや高

く、高速通信を行う際には計算遅延が無視できなくなってくる。また衛星通信においては、特に高い周波数を用いる場合には受信信号は伝搬路変動によってバースト的な電力低下が表れる。これは地上における大気の揺らぎ、受信側のポインティング、追尾機構の誤差、再同期獲得までの遅延、雲によるシャドウイングなどによって起こり[12]、周波数の高い空間光通信では数十～数百 ms の連続落ち込みが発生するといわれている[8]。しかも、同じ長さのバースト的電力落ち込みでも、高速伝送化よりその間のビット数が増加するため相対的にバースト長が長くなってしまふ。例えば 10ms のバースト落ち込みが発生した場合、2値伝送系 1Kbps 伝送のときは 10 ビットのバースト消失であるが、10Mbps 伝送のときは 10^5 ビットものバースト消失となってしまふ。この計算遅延と長バースト長に対応するためには高速信号処理、長符号が必要となり、軟値再帰的演算を行う場合は復号の回路規模などの所要能力を極めて高くしてしまふ。したがってシンプルな符号化、復号化が行え、かつ性能のよい長い符号が求められているところであった。そのためには L2 など上位レイヤにおけるパケット単位での符号化復号化処理、硬値を用いた線形復号が適切であると述べられている[8]。また高周波や光を用いた衛星通信では信号の直進性が高いため、受信信号は「良好」「劣悪」の2値的な状態とみなせる。これは復号誤りが起こらない「良好」の受信電力を閾値とすることにより伝搬路を消失通信路としてモデル化ができることを意味している。したがって高速衛星通信においては、バースト消失通信路に対して有効で、硬値線形復号が可能な符号が適しているといえる。その具体例については次号に続く。 ■

著者紹介

岡本英二 名古屋工業大学大学院工学研究科・准教授

平 7 京都大学大学院修士課程了。平 7-14 郵政省通信総合研究所（現・情報通信研究機構）。ETS-VI, COMETS の実験研究, ミリ波加入者系無線アクセスシステムの研究開発に従事。現在は無線通信システムに関する教育研究に従事。

謝辞： 本研究の一部は大幸財団の援助により行われました。深謝いたします。

参考文献

- [1] 超高速インターネット衛星「きずな」(WINDS). [Online]
http://www.jaxa.jp/projects/sat/winds/index_j.html
- [2] 高橋卓, “超高速インターネット衛星で用いられる再生交換中継システム,” 信学誌, vol. 91, no. 9, pp. 771-776, Sep. 2008.
- [3] 豊嶋守生, 高山佳久, “宇宙光通信の動向と今後の計画,” 月刊オプトロニクス, vol. 27, no. 11, pp. 141-148, Nov. 2008.
- [4] P. Elias, “Coding for noisy channels,” IRE Convention Record, Part IV, pp. 37-46, 1955.
- [5] I. S. Reed and G. Solomon, “Polynomial code over certain finite fields,” J. Soc. Ind. Appl. Math., No. 8, pp. 300-304, Jun. 1960.
- [6] C. Berrou and A. Glavieux, “Near optimum error correcting coding and decoding: Turbo-codes,” IEEE Trans. Commun., vol. 44, pp. 1261-1271, Oct. 1996.
- [7] R. G. Gallager, “Low-density parity-check codes,” IRE Trans. on Information Theory, vol. IT-8, no. 1, pp. 21-28, 1962.
- [8] H. Henniger, “Packet-layer forward error correction coding for fading mitigation,” Proceedings of SPIE Free-space laser communications VI, vol. 6304, pp. 630419.1 -630419.8, Sep. 2006.
- [9] M. Luby, “LT codes,” in Proc. 43rd Ann. IEEE Symp. Found. Comp. Sci., pp. 271-280, 2002.
- [10] A. Shokrollahi, “Raptor codes,” in Proc. IEEE Int. Symp. Inform. Theory, p. 36, 2004.
- [11] V. Roca and C. Neumann, “Design, Evaluation and Comparison of Four Large Block FEC Codecs, LDPC, LDGM, LDGM Staircase and LDGM Triangle, plus a Reed-Solomon Small Block FEC Codec”, INRIA Research Report RR-5225, June 2004.
- [12] M. Toyoshima, H. Takenaka, C. Schaefer, N. Miyashita, Y. Shoji, Y. Takayama, Y. Koyama, H. Kunimori, S. Yamakawa, and E. Okamoto, “Results from Phase-4 Kirari Optical Communication Demonstration Experiments with the NICT Optical Ground Station (KODEN),” Proc. AIAA Int'l Commun. Satellite Systems Conf., ICSSC2009- 3.4.2, CD-ROM 9 pages, Jun. 2009.