BN2002 · 2002
Seminer on Bayesian Networks (BN2002)
Tokyo, Japan, Sep 1-2, 2002.

# LDPC符号とBP復号アルゴリズム

和田山 正*
岡山県立大学 情報工学部

**Abstract:** LDPC 符号や疎なグラフに基づく誤り訂正符号 (ターボ符号など) と belief propagation に基づく復号アルゴリズムの組み合わせは、従来、達成できなかった驚くべき復号性能の実現を可能にしている。本稿では、LDPC 符号の特徴、LDPC 符号の研究の流れ、符号理論分野における sum-product アルゴリズムに関する研究の流れ、現在の研究動向などについて述べる。なお、この予稿はサーベイ的文書であり、講演で述べきれない部分を補完することを目的としている。

## 1 はじめに

誤り訂正符号の理論的な限界については、Shannon の通信路符号化定理により明確に知ることができる。しかし、通信路符号化定理が保証する性能に近い性能を持ち、かつ実時間で復号できる符号を構成できるか、もし構成できるならばどのようにしてそれを構成・復号するか、という問題を解く鍵をこの通信路符号化定理から見出すことは残念ながら容易ではない。

符号理論の 50 年の歩みは、言ってみれば Shannon により明らかにされた通信路容量を実現する現実的な符号化/復号アルゴリズムの開発を目指してきたと見ることもできる。この観点から見ると近年の低密度パリティ検査符号 (low density parity check code, 以下では LDPC 符号と略記する) の再評価 [18][28] には大きな意味がある。LDPC 符号は、非常に疎な検査行列により定義される線形符号であり、1960 年代に Gallager により提案された符号である [10]。LDPC 符号がシャノン限界に迫る性能を持つことが理論、実験の両面から再確認されたことから、LDPC 符号と sum-product 復号法の組み合わせが上記の目標、すなわち実時間復号アルゴリズムによりシャノン限界に迫るためのブレークスルーであるという認識が急速に広がりつつある。sum-product 復号法は、belief propagation(BP) の原理を符号に関連するグラフ (タナーグラフと呼ばれる) に適用して得られる復号アルゴリズムである。

LDPC 符号とその復号法である sum-product 復号法の組み合わせは極めて強力である。例えば、乱数に基づいて構成された符号長 1 万、符号化率 1/2 の正則 (regular)LDPC 符号により、ビット誤り率 $10^{-5}$ において白色ガウス通信路のシャノン限界から 1.3dB という復号特性が容易に得られる。さらに、うまくデザインされた非正則 (irregular)LDPC 符号はより優れたビット誤り率特性を発揮することが知られている。

このように LDPC 符号と sum-product 復号法により、無記憶通信路における符号化問題は肯定的解決への道筋が開けてきたと言えるだろう。また、実用的にもターボ符号 [4][5] と並んで、LDPC 符号の復号計算量と復号特性とのトレードオフは従来の連接符号に対しても優位に立ち、次世代の誤り訂正符号として有望視されている。

LDPC 符号を特徴付ける顕著な点として、この符号がランダムに構成される点が挙げられる。通信路符号化定理により保証されているように、符号長が十分に長い場合、ランダム符号アンサンブルから選び出された符号は、ほぼ確実に優れた最尤復号性能を持つ。しかし、ランダム符号は効率の良い復号を可能とする構造を持たないため、それを復号するには符号長に対して指数時間の計算時間が必要とされる。LDPC 符号のように検査行列が低密度である符号は、優れた最尤復号特性を保証するランダム性を保ちつつ、復号に適した構造、すなわち疎なグラフ構造を兼ね備えている。

sum-product 復号法は、グラフィカルモデル上における確率伝播アルゴリズムであり、隠れ変数 (送信情報シンボル) の事後確率分布を観測値 (受信信号系列) に基づいて計算する手法であり、BP の一つのインスタンスであると見ることができる。ただし、復号に利用するグラフは、通常のベイジアンネットワークとは異なり多数のループを含む。そのため、BP では正確な事後確率分布を計算はできずに近似計算となる。多くの実験結果より、グラフが疎な場合 (これは符号の検査行列が疎な場合に相当する) には、sum-product 復号法による送信情報シ

*〒 719-1197 岡山県総社市窪木 111 tel: 0866-94-2413, e-mail: wadayama@c.oka-pu.ac.jp, URL: http://vega.c.oka-pu.ac.jp/~wadayama/

ンボルの推定は非常に精度が良いことが知られている。

このように LDPC 符号に関する符号化技術は、大数の法則に基づく情報理論的手法とベイズ的手法との融合により生まれた新しい技術であり、従来の代数的符号理論に基づく誤り訂正符号とは一線を画している。

## 2 LDPC 符号に関する研究の流れ

現在、多くの符号理論研究者がこの分野に注目しており、研究の展開するスピードも速い。情報理論分野における最大のシンポジウムである ISIT(International Symposium on Information Theory) において、本年では全体の約 15%が疎グラフに基づく符号と反復復号関係 (ターボ符号なども含む) の発表であった。しかし、このような状況はターボ符号の登場、LDPC 符号の再評価以後のことであり、10 年前の状況は今とは全く異なっていた。

LDPC 符号は Gallager により、1960 年代初頭に提案された [10]。彼は、さらに符号アンサンブルに基づく最尤復号性能の解析、sum-product 復号法の提案も行っている。しかし、この先駆的な業績は、90 年代の LDPC 符号の再評価に至る 30 数年間に渡り、いくつかの論文で関連する議論が展開された以外はほぼ忘れられた存在となっていた。その理由として、当時はコンピュータ資源が高価であり、LDPC 符号の性能が特に顕著に発揮される符号長が十分に長い場合に関するシミュレーションが困難であったことが考えられる[1]。また、その当時 (60 年代から 70 年代にかけて) は、新しい符号と復号法、例えば、連接符号、代数的符号 (BCH 符号、Reed-Solomon 符号) とその復号法 (Berlekamp-Massy 復号法、Euclid 復号法)、畳み込み符号、Viterbi アルゴリズムなどの登場ラッシュが続いていたため、その影に隠れてしまったというのも一因だろう。

Gallager の論文がほとんど忘れられていたこの時期にも、LDPC 符号に関していくつかの重要な仕事がなされている。80 年代初頭に Tanner は、LDPC 符号の重要な拡張 (この拡張は、Spielman による expander 符号 [28] に引き継がれていく) を行い、また sum-product 復号法をグラフ上で動作するメッセージパッシングアルゴリズムとして明確に記述した [30]。Tanner により導入された 2 部グラフに基づく線形符号の表現は、今日、タナーグラフと呼ばれている。

また同時期に数学者の Margulis は、内径の大きいグラフの代数的構成法を示し、そのグラフを用いて正則 LDPC 符号を構成している [19]。最近、Rosenthal らにより、Margulis が構成した LDPC 符号の優れた復号性能がシミュレーションにより確認されている [24]。Margulis の仕事は、近年のラマヌジャングラフに基づく LDPC 符号の研究の出発点となっており、これも時代に先駆けた研究の 1 つである。

Zyablov と Pinsker は、論文 [33] において、符号長について一定の割合の誤りを訂正できる計算量 $O(n \log n)$ の復号アルゴリズムを持つ LDPC 符号が存在することを示した。彼らも 70 年代に LDPC 符号の可能性を見抜いていたものと思われる。

90 年代中頃の MacKay の論文 [18] は、LDPC 符号の再評価の契機となった。彼は、広いクラスの通信路モデルにおいて、シャノン限界に漸近できる LDPC 符号系列の存在を示した。また、LDPC 符号と sum-product 復号法の組み合わせに関する幅広いシミュレーション結果を示し、その優れた性能を明らかにした。彼のこの論文は、LDPC 符号の研究に新たな視点をもたらし、これ以後の研究に強い影響を与えている。

MacKay とは独立に Spielman らは expander グラフに基づく expander 符号と呼ばれる符号を提案し、それが構成的な漸近的に良い符号 (asymptotically good code)[2] であり、符号長について一定割合の誤りを必ず訂正できる線形時間復号アルゴリズムが存在することを示した [28]。この expander 符号は LDPC 符号の一種であり、Spielman らの仕事は LDPC 符号の潜在的可能性を示しているとともにタナーグラフの expansion 係数が重要なパラメータであることを明らかにした点でも興味深い。

最近の重要な研究成果としては、Richardson らによる非正則 LDPC 符号の設計法の確立 [23] が挙げられるだろう[3]。非正則 LDPC 符号とは、検査行列の行重み、列重みが一定でない LDPC 符号のことを意味している。検査行列の行重み、列重み分布は、その符号の sum-product 復号法による復号特性を決める重要な設計パラメータである。Richardson らは、反復閾値 (iterative threshold) と呼ばれる反復復号法における SN 限界値を最適化パラメータとして最適な行重み、列重みの分布を導出する手法を開発した。また同時に、反復閾値を計算する density evolution という手法を提案した。彼らの構成した非正則 LDPC 符号の復号特性は極めて優れていることが復号シミュレーションによって示されている。彼らの提案した density evolution は、現在、様々な反復復号系の復号性能の解析に利用されており、LDPC 符号以外の符

[1] それでも、Gallager は当時、符号長 1000 程度までのシュミレーションは実際に行っている。

[2] 符号化率 $R$ の符号 (系列) で符号長 $n$ を無限大とするとき、相対最小距離 $d/n$ が正になる符号 (系列) を漸近的に良い符号と呼ぶ。例えば、構成的な漸近的に良い符号として Justesen 符号が知られている (ただし、Justesen 符号の復号は線形時間ではできない)。

[3] 彼らはこの仕事の業績により、本年の IEEE 情報理論ソサイェティの paper award を受賞している。

号の設計にも有用であることが分かってきている。

このように反復復号を利用する場合の性能解析は、density evolution が有効である。一方、LDPC 符号の最尤復号時の復号特性の解析法として Miller らの手法 [21] が知られている。この論文 [21] では、LDPC 符号のアンサンブル重み分布 [10][14] に基づいて復号性能の上界が導かれている。

# 3 sum-product アルゴリズムに関する研究の流れ

LDPC 符号の復号法として利用される sum-product 復号法は、より一般的な sum-product アルゴリズム (BP と等価なアルゴリズム) のひとつのインスタンスである。sum-product アルゴリズムは、復号アルゴリズムとしてだけではなく、デジタル通信、信号処理、人工知能などの分野においてさまざまな形で利用されている。例えば、隠れマルコフモデルに対する前向き後ろ向きアルゴリズム (BCJR アルゴリズム)、Viterbi アルゴリズム、ターボ復号法、カルマンフィルタなどが挙げられる [1][12][20]。このように様々な一見異なるアルゴリズムが同じアルゴリズム原理に基づいているということが明らかになってきたのは比較的最近のことである。

Gallager は彼の博士論文 [10] の中で、sum-product 復号法を LDPC 符号の復号法として完全な形で述べている。Tanner は線形符号を定義するグラフとその復号法に関する議論を展開した [30]。Wiberg は、タナーグラフに状態ノードを追加することを考案した [32]。このアイデアにより、線形符号の最簡トレリス、畳み込み符号のトレリスに基づく BCJR アルゴリズムと Viterbi アルゴリズムが sum-product アルゴリズムのインスタンスであることが明確になった。また、同時に彼は、sum-product アルゴリズムの抽象化を行った。

Aji と McEliece は、Wiberg のアイデアを発展させるとともに、sum-product アルゴリズムが、因子分解される目的関数の計算を分配則 (一般化分配則と彼らは呼んでいる) に基づいて効率的に行うアルゴリズムであること明らかにした [1]。Kschishang と Frey はファクターグラフ [12] を導入し、目的関数の因子分解をグラフ化することにより sum-product アルゴリズムが見通しよく理解できることを示した。彼らはさらに、基礎となるグラフィカルモデルを変えることにより、"sum-product アルゴリズム原理" から FFT など数多くの既知のアルゴリズムが自然に導かれることを明らかにした。最近、符号理論コミュニティでは、ファクターグラフが反復復号系を議論する際の基本的な道具の一つとなりつつある。

# 4 最近の研究動向

符号理論分野において、反復復号系の現在の研究分野は多岐にわたるため、それをまとめるのは容易ではない。本節では、筆者の考える最近の研究動向を示す代表的なトピックスについて述べる。

## 4.1 density evolution

反復復号アルゴリズムを外部値 (extrinsic value) を交換する 2 つのサブ復号器からなるものと見る。サブ復号器 1 は入力された事前値 $(A_1^{(1)}, A_2^{(1)}, \ldots, A_N^{(1)})$ から外部値 $(E_1^{(1)}, E_2^{(1)}, \ldots, E_N^{(1)})$ を計算する SISO(Soft-In Soft-Out) 復号器である。サブ復号器 1 から出力された外部値 $(E_1^{(1)}, E_2^{(1)}, \ldots, E_N^{(1)})$ は次にサブ復号器 2 に事前値として入力される。そして、サブ復号器 2 は外部値 $(E_1^{(2)}, E_2^{(2)}, \ldots, E_N^{(2)})$ を出力する。この外部値は、次に事前値としてサブ復号器 1 に入力される。これらの操作が繰り返されて反復復号が進んでいく。この復号モデルは、LDPC 符号の復号法である sum-product 復号法だけではなく、ターボ符号、シリアル連接ターボ符号の復号器などにも適用できる。

復号器で受信される受信語は、確率変数であるため、これらの事前値・外部値も確率変数となる。反復復号の各反復において変化していく事前値・外部値の確率密度関数を評価できれば反復復号系の誤り率を解析することが可能となる。density evolution は、反復ごとの事前値、外部値の確率密度関数を計算する手法であり、もともと sum-product 復号法の性能解析手段として提案された [22][23]。最近では、ターボ符号などの性能解析にも利用されるようになってきている。この場合は、モンテカルロ法を利用して外部値の確率密度関数を計算している。

## 4.2 EXIT チャートによる収束解析

イレギュラー LDPC 符号の設計などにおいて、反復閾値の正確な計算が必要な場合、density evolution は非常に有用なテクニックである。しかし、計算量が多く、数値計算上の不安定性が出やすいため、より計算のしやすい density evolution の近似法が考えられている。そのひとつとして、ガウス分布により外部値の確率密度関数を近似し計算を進めるガウス近似法 (Gaussian approximation) が知られている [7]。

最近、注目されているのが ten Brink による EXIT (EXtrinsic Infomation Transfer) チャートを利用した収束解析である [31]。EXIT チャートは、サブ復号器の入力における事前値の相互情報量と出力の外部値の相互情

報量の関係 (伝達特性) を図示したものである。その図に描かれた 2 本伝達関数曲線 (サブ復号器 1,2 にそれぞれ対応する) に基づいて、復号器の収束過程が導かれる。ここでいう相互情報量は、入力が 2 値 $(+1, -1)$ で出力が事前値/外部値の確率分布を持つ実数値であるような仮想的な通信路の相互情報量を意味している。

EXIT チャート法のメリットとして、直感的に誤り率特性の収束特性を理解しやすい点、符号の設計に非常に使い易い点が挙げられる。また、少なくとも LDPC 符号、ターボ符号の復号系においては非常に精度の高い収束解析が可能であることが実験的に確かめられている。

### 4.3 符号長が有限長の場合の性能解析法

density evolution、ガウス近似法、EXIT チャート法の全ては符号長が無限大であるという仮定に基づいた議論であり、符号長が有限の場合 (特に符号長が数千以下のように短いとき) には正確な解析ができないという問題がある。実用的には、符号長が数千以下の符号を使う場合が圧倒的に多い。そのため、符号長が有限長の場合の復号性能の解析、符号の設計法の確立が強く求められいる。

### 4.4 組み合わせデザイン・代数的手法に基づく LDPC 符号の設計

sum-product 復号法により良い復号結果を得るためには、そのタナーグラフの内径 (girth) は可能な限り大きいほうが良いことが知られている。また、LDPC 符号においても他の線形符号と同様に与えられた符号長と次元において最小距離は可能な限り大きいほうが (特に SN 比が高い場合に) 望ましい。このような条件を満たす符号を代数的に構成する手法がいくつか知られている。

乱数に基づいて構成された LDPC 符号は、その検査行列を符号化器、復号器において保持する必要があり、符号長が大きい場合にはそれが実装上の問題となる場合がある。代数的に構成された LDPC 符号の場合は、その代数的構造を生かすことにより LDPC 符号の符号化器、復号器の実装を簡単化できる可能性がある。すなわち、確定的なルールにより検査行列を構成できる場合には、符号化器・復号器内に検査行列を保持しておく必要がなくなる。

このような代数的な LDPC 符号の構成法として、置換行列に基づく方法 [8]、ブロックデザインに基づく手法、ユークリッド幾何、射影幾何に基づく手法 [13]、ラマヌジャングラフなどの expander グラフに基づく手法 [28][19][24] が知られており、現在でも検討が進んでいる。

### 4.5 圧縮・多端子システムへの LDPC/ターボ符号系の適用

LDPC 符号のアンサンブルは、ランダム符号アンサンブルに近い性質を持っており、例えば、MacKay により、無記憶通信路の通信路容量を達成する (最尤復号法で復号した場合) 符号を含むことが示されている [18]。情報理論の多くの成果の証明は、ランダム符号化 (ランダム符号アンサンブルの性能解析) のアイデアに基づいている。

無記憶通信路の通信路容量以外の情報理論的限界値についても、ランダム符号アンサンブルの代りに LDPC 符号アンサンブルを利用して達成され得るか、達成されないならば LDPC 符号アンサンブルにおける限界値はいくらか、という問題が考えられる。LDPC 符号アンサンブルのインスタンスは、ランダム符号アンサンブルのインスタンスとは違い、実際に復号できることから、もしそのような証明ができれば、理論・実用の両面から興味深い。

情報源圧縮、多端子通信路での LDPC 符号やターボ符号の利用に関する議論は始まっており、これらは情報理論と符号理論の両方にまたがる問題として重要であると思われる。

### 4.6 記憶のある通信路への応用

現実の通信路では、通信路が記憶性を有する場合が多い。例えば、先に送信したシンボルの影響を後続の送信シンボルが受けるシンボル干渉通信路 (ISI 通信路) や誤りが連続して生じるバースト性通信路において良い性能を発揮する符号・復号法を見出すことは重要な課題である。

Arnold らは、2 値入力の ISI 通信路の相互情報量を計算する手法 (モンテカルロ法と BCJR アルゴリズムに基づく) を最近発表した [2]。この手法を基本として、Kavčić らは、与えられた ISI 通信路に対して相互情報量を最大化するマルコフ情報源を見出すアルゴリズム (有本・Bluhut アルゴリズムに類似している) を発表している。また、このアルゴリズムを利用して設計したトレリス符号とイレギュラー LDPC 符号をシリアル連接することにより ISI 通信路において非常に良好な復号性能が達成されることが示されている [17]。彼らの手法は、通信路容量の下界を求めるアルゴリズムが符号設計に利用できることを示している点でも興味深い。

## 参考文献


[1] S.M.Aji, R.J.McEliece, "The generalized distributive law," *IEEE Trans. Inform. Theory*, vol.46, pp.325–343 (2000).

[2] D. Arnold, H.A.Loeliger, "On the infomation rate of binary-input channels with memory,"

[3] L.R.Bahl, J.Cocke , F.Jelinek, J.Raviv, "Optimal decoding of linear codes for minimizing symbol error rate," *IEEE Trans. Inform. Theory*, vol.20,pp.284–287 (1974).

[4] C.Berrou, A.Glavieux, P.Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes," in *Proceedings of IEEE International Conference on Communications(ICC)*, Geneva, pp.1064–1070 (1993).

[5] C.Berrou, A.Glavieux, "Near optimum error correcting codes and decoding: turbo-codes," *IEEE Trans. Commun.*, vol.44, pp.1261–1271 (1996).

[6] S.Y.Chung, "On the construction of some capacity-approaching coding schemes," Ph.D dissertation, MIT (2000).

[7] S.Y.Chung, T.J.Richardson, R.L.Urbanke, "Analysis of sum-product decoding of low-density parity-check codes using a Gaussian approximation," *IEEE Trans. Inform. Theory*, vol.47, pp.657–686 (2001).

[8] J.L.Fan, "Constrained coding and soft iterative decoding," Kluwer Academic Publishers (2001).

[9] B.J.Frey, "Graphical models for machine learning and digital communication," MIT Press (1998).

[10] R.G.Gallager,"Low density parity check codes," in Research Monograph series. Cambridge, MIT Press (1963).

[11] R.G.Gallager, "Information theory and reliable communication," John Wiley & Sons (1968).

[12] F.R.Kschischang, B.J.Frey, H.A. Loeliger, "Factor graphs and the sum-product algorithm," *IEEE Trans. Inform. Theory*, vol.47, pp.498–519 (2001).

[13] Y.Kou, S.Lin, M.P.C. Fossorier, "Low density parity check codes based on finite geometries: a rediscovery and new results," *IEEE Trans. Inform. Theory*, vol.47, pp.2711–2736 (2001).

[14] S. Litsyn, V. Shevelev, "On ensembles of low-density parity check codes:asymptotic distance distributions," *IEEE Trans. Inform. Theory*, vol.48, pp.887–908 (2002).

[15] M.G.Luby, M.Mitzenmacher, M.A.Shokrollahi, D.A.Spielman, "Efficient erasure correcting codes," *IEEE Trans. Inform. Theory*, vol.47, pp.569–584 (2001).

[16] M.G.Luby, M.Mitzenmacher, M.A.Shokrollahi, D.A.Spielman, "Improved low-density parity-check codes using irregular graphs," *IEEE Trans. Inform. Theory*, vol.47, pp.585–598 (2001).

[17] X. Ma, N. Vanica, A. Kavčić, "Matched information rate codes for binary ISI channels," in *Proceedings of IEEE International Symposium on Information Theory(ISIT)* (2002).

[18] D.J.C.MacKay,"Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inform.Theory*, vol.45, pp.399–431 (1999).

[19] G. A.Margulis, "Explicit constructions of graphs without short cycles and low density codes," *Combinatorica*, vol.2, no.1 pp.71–78 (1982).

[20] R.J.McEliece, D.J.C.MacKay, J.F.Cheng, "Turbo decoding as an instance of Pearl's 'belief propagation' algorithm," *IEEE Journal on Selected Areas in Comm.*, vol.27, pp.140–152 (1998).

[21] G.Miller, D.Burshtein, "Bounds on the maximum-likelihood decoding error probability of low-density parity-check codes," *IEEE Trans. Inform.Theory*, vol.47, pp.2696–2710 (2001).

[22] T.J.Richardson, R.L.Urbanke, "The capacity of low-density parity check codes under message-passing decoding," *IEEE Trans. Inform.Theory*, vol.47, pp.599–618 (2001).

[23] T.J.Richardson, M.A.Shokrollahi, R.L.Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Trans. Inform.Theory*, vol.47, pp.619–637 (2001).

[24] J.Rosenthal, P.O.Vontobel, "Constructions of LDPC codes using Ramanujan graphs and ideas from Margulis," in Proceedings of *38th Alleton Conference Communications, Control and Computing*, pp.248–257 (2000).

[25] W.E.Ryan, "A turbo code tutorial," `http://www.ece.arizona.edu/~ryan/`

[26] W.E.Ryan, "An introduction to LDPC codes," `http://www.ece.arizona.edu/~ryan/`

[27] C.E.Shannon, "Claude Elwood Shannon: collected papers," IEEE Press (1993).

[28] M.Sipser, D.Spielman, "Expander codes," *IEEE Trans. Inform. Theory*, vol.42, pp.1710–1722 (1996).

[29] D.Spielman, "Linear-time encodable and decodable error-correcting codes," *IEEE Trans. Inform. Theory*, vol.42, pp.1723–1731 (1996).

[30] R.M.Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inform. Theory*, vol.27, pp.533–547 (1981).

[31] S. ten Brink, "Convergence behavior of iteratively decoded parallel concatenated codes," *IEEE Trans. Comm.*, vol.49, pp.1727–1737 (2001).

[32] N.Wiberg, "Codes and decoding on general graph," Ph.D thesis, Dept. of Electrical Engineering, Liköping University, Sweden (1996).

[33] V.Zyablov, M.Pinsker, "Estimation of error correction complexity of Gallager low-density codes," *Problems of information transmission*, vol.11, pp.18-28 (1976).