2001 年 ベイジアンネットチュートリアル
Tutorial on Bayesian Networks (BN2001)
Tokyo, Japan, July 29, 2001.

Turbo符号，LDPC符号の復号アルゴリズム

Posterior Probability Calculation and the Decoding Algorithms for Turbo codes and LDPC codes

松嶋 敏泰* Toshiyasu MATSUSHIMA
早稲田大学 理工学部 Waseda University

Abstract: 情報理論、符号理論の分野では，近年，Turbo 符号及び LDPC 符号が理論限界に非常に近い高い性能を保持していることが実験的に実証され，次世代の移動体通信の方式に採用されるなど注目を集めている．このような高性能が実現された背景には，これらの符号の潜在的性能の高さと共に，誤り率最小復号を近似的に実現する効率良い復号アルゴリズムの存在を見逃すことは出来ない．この復号アルゴリズムが Bayesian network の代表的確信度更新アルゴリズムである Belief Propagation と等価であることが最近明らかになった．これらの復号アルゴリズムと確信度更新アルゴリズムが処理している問題は事後確率の計算のと解釈され，その他の多くの分野でも重要な問題となっている．本稿ではこの事後確率計算の問題を，確率分布のグラフ表現と，そのグラフを用いた効率良い計算アルゴリズムの観点から整理し，誤り訂正符号とその復号問題に適用した場合を概説する．

1 はじめに

誤り訂正符号は情報化社会において情報伝送，蓄積の基盤技術として欠くことの出来ない技術となっている．誤り訂正符号の性能は復号誤り率，符号化率，計算量などで評価され，その代表的理論的限界には Shannon 限界がある．現在実用化されている符号の多くは Shannon 限界に遠く及んでいなかったが，近年，Shannon 限界に近づく符号として Turbo 符号 [3] [6] [7] や LDPC(Low Density Parity Check) 符号 [5] [16] が注目されている．これらの符号の符号自体の潜在的性能の高さは様々な研究から明らかになりつつあるが，それと共に，誤り率最小復号を近似的に実現する効率良い復号アルゴリズムについても注目が集まり，多くの研究成果がでてきている [11][14]．また，その概念は様々な符号の復号や復調，検出など伝送システム全般へと適用されつつある [10]．

誤り訂正符号の復号問題は受信系列から情報系列を推定する問題と考えることができ，その本質は受信系列を与えられたもとでの情報系列の事後確率の計算問題に帰着される．また，BN(Bayesian Network) を用いた知識表現の分野において，証拠 (evidence) が与えられたもとで各命題の確信度 (belief)[15][18] の更新を行うことは，ある確率変数の値が与えられたもとでのその他の確率変数の事後周辺確率を求めていることに他ならない．よって両者は共通の問題と考えることができ，近年 Turbo 復号アルゴリズムや LDPC 符号で用いられる sum-products アルゴリズムは BN の代表的推論アルゴリズムである BP(Belief Propagation) と等価であることが明らかになった．このような事後確率の計算問題は符号理論における復号問題や人工知能分野における不確実な知識を扱う問題のみならず，統計学をはじめ，統計力学の分野，学習理論の分野，パターン認識の分野など様々な分野において共通で重要な問題となっている．

本稿では，まず誤り訂正符号の復号問題を事後確率の計算問題として整理する．次に確率変数間の従属関係が部分的に存在する確率分布のグラフを用いた代表的表現法と，そのグラフ上で情報を伝搬させることにより効率的に事後確率を計算するアルゴリズムについて概観する．最後にこれらを踏まえて，誤り訂正符号の復号問題における，符号のグラフ表現とグラフ上の伝搬を用いた効率的で高性能な復号アルゴリズムについて説明する．

2 誤り訂正符号の復号と事後確率計算

誤り訂正符号 [8] を用いた通信，蓄積についてまず簡単に説明する．送信側ではまず送信したい情報系列

*〒 169-8555 東京都新宿区大久保 3-4-1, tel&fax: 03-5286-3301, e-mail: toshi@matsu.mgmt.waseda.ac.jp

$\mathbf{u} = (u_1, \cdots, u_K)$, $u_k \in A$ から符号化（関数）C により符号語 $C(\mathbf{u})$ を生成し，通信路を通して受信側へ送る．受信側では送信側から送られた符号語が雑音などの影響により一部のシンボルが異なってしまった受信系列を受け取ることになり，この受信系列を元の符号語または情報系列にもどすことを復号と呼ぶ．

この分野で中心的に研究されている符号はシンボル長 K の情報系列 $\mathbf{u}$ に $K \times N$ 生成行列 G をかけて[1] シンボル長 N の符号語を生成する線形符号のクラスである．

$$C(\mathbf{u}) = \mathbf{u}G.$$

生成行列の左側 $K \times K$ が単位行列であった場合，符号語は $(\mathbf{u}, \mathbf{x})$ となる．$\mathbf{x}$ をパリティと呼び，このような符号を組織符号と呼ぶ．

生成行列 G に対して $GH^T = 0$ を満たす行列 H を検査行列と呼び，すべての符号語が以下の性質を満たすことは符号語の生成過程より明らかであろう．

$$C(\mathbf{u})H^T = 0.$$

通信路で誤りが生じて符号語と異なってしまった場合の受信系列 $\mathbf{y}$ は，検査行列 H をかけても 0 にはならず，誤りが生じたことが受信側で検出される．この積をシンドロームと呼び，これを手がかりにある範囲内の誤りに対しては，ある種の方程式を解くことによって，誤りが生じたシンボルを求めることができる．このような代数的復号法が現在実用的には多く用いられている．この代数的復号法は計算量が少なく，訂正可能な領域が理論的に保証されているなどの利点を持っている．

結局この復号の問題は，受信系列を $\mathbf{y}$ としたもとで，受信系列 $\mathbf{y}$ から符号語 $C(\mathbf{u})$ または情報系列 $\mathbf{u}$ を推定する問題に帰着される．推定は情報系列全体 $\mathbf{u}$ をブロックとして推定する場合と各情報シンボル u_k を推定する場合に大別される．一般に推定の評価には誤り率が用いられ，前者に対するものをブロック誤り率，後者に対するものをシンボル誤り率と呼んでいる．

ブロック誤り率を最小化する推定 (復号) 法は受信系列を与えられたもとでの事後確率 $P(\mathbf{u}|\mathbf{y})$ を最大化する情報系列$\hat{\mathbf{u}}$を推定値とすることになる．これは $\mathbf{u}$ の事前確率が一様な場合は，尤度 $P(\mathbf{y}|\mathbf{u})$ を最大化する情報系列と一致し，通常これを最尤復号と呼んでいる．一方，シンボル誤り率を最小化する推定法は事後確率 $P(u_k|\mathbf{y})$ を最大化する情報シンボル$\hat{u}_k$を推定値とすることになる．通常これを MAP(Maximum a posteriori probability) 復号[2] または MPM(Maximum posterior marginal) 復号などと呼んでいる．

$\mathbf{u}$ を推定する場合も u_k を推定する場合もそれぞれの確率変数の事後確率を計算し，その最大値を探索するという意味で基本的には同じ手続きで復号は行われるが，計算の困難な部分は両者で異なっている．一般に情報系列全体の事後確率 $P(\mathbf{u}|\mathbf{y})$ は比較的容易に計算可能であるが，最大値をとる$\hat{\mathbf{u}}$を $|A|^K$ の候補から探索する問題は多くの計算量が必要とされる．この状況は尤度最大化の問題でも同様で，通信路復号化の多くの研究はこの最適な最尤復号に近い誤り率を，少ない計算量で実現する事に向けられてきた．例えば代数的復号だけでは最尤復号と比べ誤り率が高くなってしまうので，代数的復号を繰り返して用いることにより最尤復号またはそれに近い復号を実現するアルゴリズムが多く研究されている．

逆に，個々の情報シンボル u_k を推定する場合において，最大値を見つけることは $|A| - 1$ の比較で容易であるが，各情報シンボルの事後確率 $P(u_k|\mathbf{y})$ を計算することは，事後結合確率 $P(\mathbf{u}|\mathbf{y})$ から周辺確率を計算することに対応し，一般には $|A|^{K-1}$回の加算が必要となり指数オーダの計算量となる．この事後周辺確率計算を，少ない計算量で近似計算することに成功したある種の反復アルゴリズムが，Turbo 復号や LDPC 符号における sum-products アルゴリズムである．

先に述べたように，事後確率の値を求めることがその問題の主要な課題となっている問題は様々な分野で見ることができる．BN をはじめとする確率推論の分野おいて，証拠が与えられもとで各命題の確信度の更新を行うことは主要な問題であり，この問題はある確率変数の値が与えられたもとでのその他の確率変数の事後周辺確率を求めている上記の問題と同値の問題となっている．

3 確率変数間の相互関係のグラフによる表現

事後周辺確率の計算は一般に多くの計算量を必要とするが，確率変数間の相互の関連が部分的にのみ存在する確率分布においてはその計算が容易になる可能性がある．相互の関連が部分的とは，系全体の確率構造を表す結合確率が，確率変数の部分集合の関数の積で表される場合を指す．その関数としては，例えば条件付き確率やポテンシャル関数が用いられている．

このような条件が当てはまる確率分布として典型的なのはマルコフモデルであろう．隠れマルコフモデルなども含めたマルコフモデルは時系列解析，制御理論，信号処理，音声処理など様々な工学分野で用いられている．１次元の広がりの関連を扱ったマルコフモデルを一般化

[1] A は有限集合なのでこれらの演算は有限代数上の演算となる．

[2] 正確には情報シンボルに対する最大事後確率復号と呼び，情報系列 (ブロック) に対する最大事後確率復号と区別すべきであろうがここでは慣例に従う．

し，ある要素（確率変数）の確率が，近傍の要素が与えられたもとでの条件付き確率のみで決まるマルコフランダム場 (MRF) は，統計力学や画像処理の分野で使われている．人工知能の分野の不確実な知識処理の問題でも，確率事象や命題間の関係に条件付き独立が仮定される場合は多い．

これらの部分的に確率変数が関連を持つ分布の確率構造を表現するには，確率変数を節点に対応させ，関連のある確率変数の節点間を枝で結んだグラフを用いると分かりやすく表現できる．用いられるグラフ表現は分野によって様々であるが，まず無向グラフと有向グラフに大別される．前者としては MRF[11]，moral グラフ [13] 等があり，後者として代表的なのが BN である．BN は系全体の確率を条件付き確率の積で表し，条件付き確率を親節点から子節点への有向枝に対応させグラフ化している．正確には BN は cycle が無い有向グラフ (DAG: Directed Acyclic Graph) で定義され，知識処理の分野で広く用いられている．また，統計学の分野でも，多変量解析で求められた確率分布の確率変数間の関連を，グラフで表現するグラフィカルモデリングの研究が盛んに行われている．

符号理論の場合も情報系列 $\mathbf{U}$, パリティ$\mathbf{X}$, 受信系列 $\mathbf{Y}$ の各シンボルを確率変数としてとらえ全体の確率構造を考えると，各確率変数は部分的に関連をもつ構造となっている．符号のグラフ表現としては，白丸の節点で確率変数を表し，黒丸の節点で関連の有ることを表す Tanner グラフ [11] が従来から提案されていた．Tanner グラフは近年 factor グラフとして一般化されている [11]．また，畳み込み符号や一部の線形符号は，トレリス [19] によってその構造を簡素に表現可能であり，従来から広く用いられている．

このようなグラフ表現は，部分的に確率変数が関連を持つ分布の確率構造を視覚的に分かりやすくする為だけではなく，このグラフを用いて事後確率計算等を効率良く行うアルゴリズムを構成するために役立っている．例えば，符号理論で用いられるトレリスは，最尤復号を保証する効率よいアルゴリズムである Viterbi アルゴリズム [19] の計算プロセスを表していると考えることもできる．後で詳しく述べる BN の確信度更新アルゴリズムと Turbo 復号の同等性が明らかになつた最近では [11][14]，様々な符号が BN や factor グラフを用いて表現され，符号の性能や効率的復号法などの研究がなされている．図 1 は BN を用いて符号を表現した一例である．

4 事後確率の効率的計算アルゴリズム

隠れマルコフモデルにおいて，観測値が与えられたもとでの各時点の状態の事後確率を求める効率的アルゴリズムとして forward-backward アルゴリズム [2] がある．マルコフモデルの条件付き独立性をうまく利用し，時点順に計算する値と最終時点から時点を遡りながら計算する値を合わせるだけで事後確率を効率良く計算するアルゴリズムである．グラフ的な視点からアルゴリズムを見ると，状態遷移を表したトレリス上を順方向に流れる情報と逆方向に流れる情報が，それぞれの端点まで到達するとアルゴリズムは終了し，正しい事後確率を出力することになる．このアルゴリズムは隠れマルコフモデルが用いられる様々な分野で使用されており，応用分野の一例としはて音声認識の問題がある．

BN における確信度更新，つまり事後周辺確率の計算における効率的アルゴリズムはとしては BP が代表的である．BP では有向グラフの順方向へメッセージπと逆方向へのメッセージλを伝搬させることにより各節点の事後周辺確率を求めている．BP も事後周辺確率を部分的な確率計算の反復で行う効率的アルゴリズムと解釈することができる．BN は DAG として定義されているが，BP を用いることができるグラフは DAG の部分クラスである Polytree(一般木) と呼ばれる loop の無い DAG のクラスに限定されている [15]．BP が正しく事後周辺確率を計算できる保証はこの木構造上で条件付き独立の性質をうまく用いた点にあり，先に述べた forward-backward アルゴリズムとアルゴリズムの本質は同じである．

BP の性能が保証できるクラスはこの Polytree に限られるが，計算量は確率変数の数とアルファベットの大きさの多項式オーダとなる効率の良いアルゴリズムとなっている．Polytree より広いクラスの DAG に対しても正確さの保証のある計算アルゴリズムが幾つか提案されているが計算量は増加してしまう [15] [13]．この問題を計算量から考えると，DAG の一般的クラスにおける事後周辺確率計算問題は NP 困難となることが計算理論分野で有名な 3-SAT 問題を用いて証明されている [4]．

その他のグラフ表現として factor グラフにおいては効率的な事後周辺確率計算アルゴリズムとして sum-products アルゴリズムがある．グラフ上で 2 種類の情報を 2 種類の節点を通して流し計算をするアルゴリズムで，節点に集まってきた情報を和と積で計算することでこのように呼ばれる．BP と本質的には同じアルゴリズムであることが示されており，このアルゴリズムも fac-

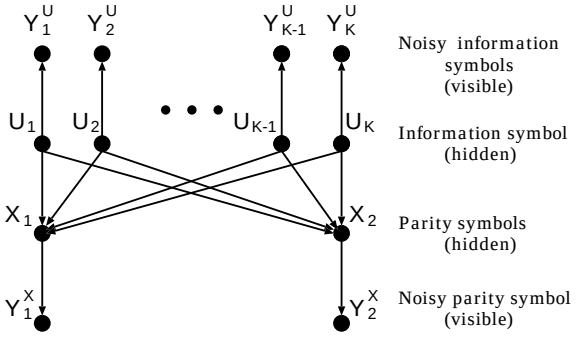

図 1: BN による符号の表現例

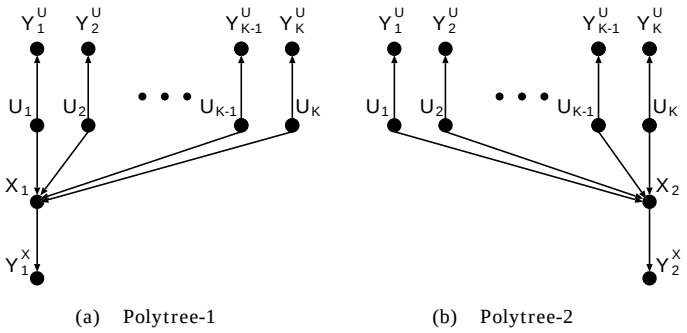

図 2: 図 1 の BN の部分グラフ

tor グラフに loop がない場合のみ正しい計算の保証がある．統計力学の分野では MRF 上での確率変数の事後期待値を効率よく計算する手法に平均場近似がある．平均場近似には様々な手法があるが，ある種の手法は BP や sum-products アルゴリズムと同等であることが知られている [12]．また，DAG よりさらに広い分布クラスに対して，与えられる情報も確率変数の値としてだけでなく確率として与えられる場合にも周辺事後確率計算が行えるアルゴリズムも提案されている [17]．

5 符号のグラフ表現と効率的復号アルゴリズム

符号のグラフ表現とその上での効率的な事後周辺確率計算アルゴリズムを眺めてみよう．例えば畳み込み符号を BN で表現すると Polytree で表現可能なため，BP アルゴリズムで正確な事後周辺確率が計算できることになる．トレリス符号に対し正確な MAP 復号を実現するアルゴリズムとして符号理論の分野では BCJR[1] アルゴリズムが有名であるが，これは forward-backward アルゴリズムそのものであることが知られている．畳み込み符号の MAP 復号は確率的には隠れマルコフモデルの状態推定と同等な問題であるので，2 つのアルゴリズムが一致することは当然の帰結といえる．さらに semi-ring 上の演算の定義を変えれば forward-backward アルゴリズムは先程述べた Viterbi アルゴリズムとも等価となる [7] [11]．これらのアルゴリズムはすべて BP の特殊形と解釈されるので，符号を BN で表現した場合に Polytree で表現可能であれば，その符号に対して BP と等価な効率よい復号アルゴリズムが構成できることになる．

しかし，オリジナルの Turbo 符号 (並列連接畳み込み符号) をはじめ多くの符号は DAG による表現は可能であるが Polytree で表現されないことが多い．例えば，図 1 の符号は loop があり Polytree とはなっていない．このような場合でも，BP をうまく用いることで，情報シンボルの事後確率の近似計算を行えないだろうか．図 1 をよく見ると，節点 X_1 に集まってくる枝に着目した部分グラフは図 2(a) のように Polytree になっていることに気づく．この部分グラフを Polytree-1 と呼び，節点 X_2 に着目した図 2(b) の部分グラフを Polytree-2 と呼ぶ．まず Polytree-1 上で BP により各節点の暫定的な事後確率計算を行う．Polytree-1 上で得られた情報系列 $\mathbf{U}$ に関する暫定的な事後確率を用いて Polytree-2 上でまた BP を行い，それを反復することで暫定事後確率の値を更新し収束させることを考える．実は BP をこのように用いた反復アルゴリズムが，Turbo 復号で行われている近似事後確率計算と同等であることが示される [14]．

オリジナルの Turbo 符号は，情報系列を一つの畳み込み符号で符号化した符号を送信し，それに並列して，その情報系列にインタリーバをかけ置換した新たな系列を，もう一つの畳み込み符号で符号化したパリティ部も送信するもので，並列連接畳み込み符号と考えられる．Turbo 符号全体の DAG を 2 つの畳み込み符号の DAG に分割すれば，それぞれは Polytree となり，BP と等価な BCJR アルゴリズムを交互に用い反復することにより，事後周辺確率の近似値が求まることになる．

また，Gallager により提案され最近再発見された LDPC (低密度パリティ検査) 符号 [5] [16] は，2 元符号で検査行列 H の各列の 1 の数を J 個と一定数に制限した符号である．J は 3 など比較的小さい数が用いられ，検査行列の 1 の密度が低いためこのように呼ばれる．この符号も DN や factor グラフで表現すると loop があるグラフとなってしまう．そこで，Turbo 復号と同様に符号を表現したグラフを幾つかの loop のない部分グラフに分解し BP または sum-products アルゴリズムで反復計算し復号を行っている．sum-products アルゴリズムを用いる場合，節点に集まってくる情報の数が J となることで和の計算の次元が J となり，効率的計算が可能となっている．統計力学のイジングスピンモデルにおける TAP

平均場近似は上記のアルゴリズムと等価であることが知られており，統計力学の分野からLDPC符号を考察した研究も行われている[12]．

このように一般のDAGにBPを無理やりに用いた場合の性能は保証されるのであろうか．残念ながら，一般的には正しい事後確率を計算することの保証どころか，収束性も保証されていない．そのためTurbo復号やLDPC符号におけるsum-productsアルゴリズムは，統計学や確率推論の研究者からは性能補償範囲を超えた強引な適用法として，必ずしも良い評価ばかりではない．しかし，これらの２つの符号をはじめいくつかの符号に対しては，復号誤り特性に関する多くのシミュレーションの結果から，これらの復号法の良好な性能が確認されている．理論的面からは，BPの演算を変換したBPと同質なアルゴリズム[3]については、いくつかの性質が保証されている。例えば、loopが一つでアルファベットが2元のDAGに対しアルゴリズムは収束し，収束結果は真の最大事後確率による推定と一致するという意味で正当性が示されている[20]．この結果を拡張して単一loopが複数存在するDAGに対しても，ある範囲内で正当性の保証が得られることが最近報告されている．また最近，情報幾何を用いてTurbo復号の収束性について考察する研究[9]も行われている．

6　まとめ

事後確率，事後期待値を求める問題は，知識処理，符号理論，統計学，情報理論，学習理論，統計力学，制御理論など様々な分野で重要な問題であり，グラフによる確率分布の表現法や計算アルゴリズムも多岐にわたっている．本稿では，BPを用いた符号理論における復号問題を中心にこれらの研究の関連についてほんの一部を垣間見た．今後，これらの各分野が益々相互に関連をもち，この問題に対しての研究がさらに盛んになることが期待されている．

参考文献

[1] L.R. Bahl, J. Cocke, F. Jelinek and J. Raviv, *Optimal decoding of linear codes for minimizing symbol error rate* IEEE Trans. IT, Vol.20, 1974.

[2] L.E. Baum and T. Petrie, *Statistical inference for probabilistic functions on finite state markov chains* Annals of Mathematical Statistics, Vol.37, 1966.

[3] C. Berrou, A. Glavieux and P. Thitimajshima, *Near Shannon limit error-correcting coding and decoding*, in Proc. IEEE Int. Conf. Commun., 1993.

[4] P. Dagum, *Approximating Probabilistic Inference in Bayesian belief networks is NP-hard* Artificial Intelligence, Vol.42, 1990.

[5] R.G. Gallager, *Low-Density Parity-Check Codes* MIT Press, Cambridge, 1963.

[6] J. Hagenauer, E. Offer and L. Papke, *Iterative decoding of binary block and convolutional codes*, IEEE Trans. IT, Vol.42, 1996.

[7] C. Heegard and S.B. Wicker, *Turbo coding* Kluwer Academic Publishers, 1999.

[8] 平澤茂一，西島利尚, 符号理論入門, 培風館, .

[9] 池田思朗，田中利幸, 甘利俊一, ターボ符号の情報幾何, IBIS2001, 2001.

[10] 井坂元彦, 今井秀樹, *Shannon*限界への道標*: "Parallel concatenated (Turbo) coding", "Turbo (Iterative) decoding"*とその周辺, 信学技報IT98-51, 1998.

[11] F.R. Kschischang and B.J. Frey, *Iterative decoding of compound codes by probability propagation in graphical models*, IEEE J. Sel. Areas Commun., Vol.16 No.2, 1998.

[12] Y. Kabashima and D. Sad, *Belief propagation vs. TAP for decoding corrupted messages*, Europhys. Lett. Vol.44, No.5, 1998.

[13] S.L. Lauritzen and D.J. Spiegelhalter, *Local computation with probabilities on graphical structures and their application to expert systems*, J.R. Statist. Soc., Vol.50, No.2, 1988.

[14] R.J. McElice, D.J.C. MacKay and J. Cheng, *Turbo decoding as an instance of Pearl's "Belief Propagation"*, IEEE J. Sel. Areas Commun., Vol.16, No.2, 1998.

[15] J. Pearl, *Probabilistic reasoning in intelligent systems* Morgan Kaufmann, 1988.

[16] D.J.C. MacKay, *Good Error-Correcting Codes Based on Very Sparse Matrices* , IEEE IT., Vol.45, No.2, 1999.

[3]本稿で中心的に述べた事後周辺確率を求めるのではなく、未知確率変数ベクトルの値を事後確率最大で推定することが目的のアルゴリズム

[17] T. Matsushima, T.K. Matsushima and S. Hirasawa, *An Iterative Calculation Algorithm for Posterior Probability*, Proc. the 23rd Symp. on Information Theory and Its Applications, 2000.

[18] 本村陽一, **ベイジアンネットワーク**, 電子情報通信学会誌, Vol.83, No.8, 2000

[19] A. Viterbi and J.K. Omura, *Principle of Digital Communication and Coding*, McGraw-Hill, New York, 1979.

[20] Y. Weiss, *Belief propagation and revision in networks with loop*, M.I.T A.I. Memo No.1616, 1997.