統計数理(2013)
第 61 巻 第 1 号 123–134

特集「最適化技術に基づく統計的推論」
[総合報告]

最適化手法に基づく誤り訂正符号の復号アルゴリズムについて

和田山 正†

(受付 2012 年 6 月 28 日; 改訂 8 月 28 日; 採択 9 月 5 日)

要　　旨

近年，線形計画法などの連続最適化に基づく誤り訂正符号の復号法が登場し，符号理論研究者の注目を集めている．本稿では，著者の提案する内点法に基づく LDPC 符号(Low-Density Parity-Check 符号)の復号法の概要とその特徴を紹介する．この復号法(内点復号法)は，LDPC 符号の復号問題を凸計画問題として定式化し，バリア関数に基づく主パス追跡内点法により近似的にその凸計画問題を高速に解く，という考え方に基づいて構成されている．本復号アルゴリズムは，線形ベクトル通信路の範疇に入る定常無記憶通信路，シンボル間干渉通信路，MIMO 通信路，マルチプルアクセス通信路など様々な通信路に適用が可能であり，幅広い応用が期待されている．

キーワード： 内点法，凸計画問題，低密度パリティ検査符号.

1. 緒言

誤り訂正符号の復号法に最適化の考え方が導入されたのは比較的最近(2002 年頃)であり，その先駆的な仕事として Feldman ら線形計画法に基づく復号法(LP 復号法) (Feldman, 2003; Feldman et al., 2005)が挙げられる．Feldman らの仕事に刺激され，Vontobel and Koetter (2006)，Koetter and Vontobel (2003)，Burshtein (2008) などの線形計画復号法の改良，および理論的検討がなされてきており，それらは符号理論研究における新しい潮流となりつつある．

著者のグループでは，近年，凸最適化手法に基づく LDPC (Low-Density Parity-Check; 低密度パリティ検査)符号(Gallager, 1963)の内点復号法(Wadayama, 2010)を中心にして，主パス追跡内点法に基づく線形計画(LP)復号法(Wadayama, 2009)，2 次計画法に基づく CDMA 方式におけるマルチユーザ検出アルゴリズム(伊藤・和田山, 2011)，ニュートン法に基づく 2 次元シンボル間干渉通信路に適した等化アルゴリズムの開発など連続的最適化手法に基づく通信系の復号・検出アルゴリズムの開発と性能評価を進めている．特に研究の方針として重視しているのは，内点法やニュートン法といった連続最適化手法を通信系のアルゴリズムに適用するときに生じる諸問題について深い理解を得ること，そして，その理解に立脚して最適化の見地から高速かつ復号・推定性能の高い復号・信号検出アルゴリズムを開発することである．

本稿では，凸最適化問題に基づく LDPC 符号の復号法に関して，論文 Wadayama (2010)の概要を紹介するとともに，連続最適化技法の誤り訂正符号の復号アルゴリズムへの応用の可能性について論じる．

† 名古屋工業大学：〒466–8555 名古屋市昭和区御器所町

論文 Wadayama (2010) で提案された内点復号法は，凸計画問題に対する主パス追跡内点法に基づき構成された LDPC 符号の復号用アルゴリズムである．この復号アルゴリズムは，受信器の処理である等化 (equalization)，誤り訂正処理など全てをまとめて凸最適化問題として定式化し，内点法により一気にその最適化問題を解くことによって復号結果を得る．シンボル間干渉等化，MIMO 処理などを凸最適化 (2 次計画問題) として扱う手法に関する研究はすでにいくつかある．本研究の新規な点は，符号に関する凸多面体を導入し誤り訂正符号の復号も含めて最適化を行う点にある．

内点法の LDPC 符号の復号問題への応用には，著者らのグループによる研究以外にも Vontobel (2008) による内点法の応用 や Taghavi et al. (2008) による主双対内点法の研究 などがあり，これらの研究は最適化の見地から符号理論の研究を進める研究者の関心を集めている．

実数空間における最適化問題という視座から受信器における受信処理を統一的に眺めることにより，連続最適化に基づく推論計算がコンポーネントベースの受信器アルゴリズム設計に代わる新しい受信器の構成原理を与える可能性が見えてくる．復号問題に対する連続最適化アプローチの通信伝送分野における適用範囲は広く，線形ベクトル通信路の範疇に入る定常無記憶通信路，シンボル間干渉通信路，MIMO 通信路，マルチプルアクセス通信路など様々な通信路に適用が可能であり，幅広い応用が期待されている．

2. 基礎的事項

連続最適化に基づく復号法の原理である，緩和推定問題について解説したのち，本稿の以下の部分で必要とされる記法・定義などを導入する．

2.1 低密度パリティ検査 (LDPC) 符号

低密度パリティ検査符号，あるいは LDPC 符号は，1960 年代に R. Gallager により開発された線形符号である．この符号の大きな特徴は，疎な検査行列により定義される線形符号であり，sum-product 復号法 (または，loopy belief propagation) と呼ばれる確率推論アルゴリズムにより復号処理が効率良く実行できる点にある．その強力な誤り訂正能力から，LDPC 符号は，近年デジタル放送やハードディスクドライブ向けの誤り訂正符号として実用化されており，より強力な誤り訂正能力が求められる次世代の誤り訂正符号の主力として注目されている．

LDPC 符号は，非常に疎な検査行列に基づいて定義される 2 元線形符号である．また，同時に LDPC 符号は，疎な 2 部グラフに基づいて定義される符号と見ることもでき，疎グラフ上で定義される様々なメッセージパッシング型の復号アルゴリズムにより復号することができる．LDPC 符号の代表的な復号法である sum-product 復号法では，受信語から送信シンボルの周辺事後確率の効率の良い近似計算が行われる．

適切に設計された LDPC 符号と sum-product 復号法の組合せは非常に強力な誤り訂正能力を持つことが知られている．例えば，誤り訂正符号の性能限界として知られるシャノン限界に非常に近い復号性能を持つ LDPC 符号も構成されている．

2 元体 $\mathbb{F}_2$ 上の検査行列 $H \triangleq \{h_{i,j}\}(i \in [1,m], j \in [1,n])$ に対して，2 元線型符号 $C(H)$ を

$$C(H) \triangleq \{\boldsymbol{x} \in \mathbb{F}_2^n : H\boldsymbol{x} = 0^m\} \tag{2.1}$$

と定義する．なお，この定義の行列ベクトル積 $H\boldsymbol{x}$ は，2 元体 $\mathbb{F}_2$ 上の計算に従う．なお，2 元体 $\mathbb{F}_2$ は $\{0,1\}$ の元を有し，実数体と異なり加法について $1+1=0$ が成立する．記法 $[a,b]$ は，整数の集合 $\{a, a+1, \ldots, b-1, b\}$ を意味する．なお，本稿では，ボールド体の英文字は列ベクトルを表すものとする．また，0^m は，長さ n のゼロベクトルである．ここで，検査行列 H が疎行列である場合，$C(H)$ は LDPC 符号となる．疎行列の定義は文脈により異なるが，符号長

に対して検査行列中の列に含まれる 1 の個数が定数で押さえられる場合に疎行列と呼ぶことが一般的である．

2.2 2 元線形符号の復号問題

送信信号を確率変数 X で，受信信号を確率変数 Y で表すとき，定常無記憶通信路 S の確率的な振る舞いは，条件付き確率分布 $P_{Y|X}(y|x)$ により与えられる．いま，S を n 回利用して，$\boldsymbol{X}=(X_1,X_2,\ldots,X_n)^T$ を送信し，$\boldsymbol{Y}=(Y_1,Y_2,\ldots,Y_n)^T$ を受信するものとしよう．ここで，S の無記憶性より，n 回の S の利用に関わる条件付き確率分布は

$$P_{\boldsymbol{Y}|\boldsymbol{X}}(\boldsymbol{y}|\boldsymbol{x})=\prod_{i=1}^{n}P_{Y_i|X_i}(y_i|x_i) \tag{2.2}$$

となる．また定常性より，すべての $i\in[1,n]$ に対して $P_{Y_i|X_i}(y_i|x_i)$ は同一分布となる．

符号化通信システムは，符号化器と復号器の組から成っている．符号化器は，送信したいメッセージを 2 元線型符号 $C(H)$ の符号語に符号化するのが，その主たる役目である．一方，受信ベクトル $\boldsymbol{y}$ から，送信符号語を推定し推定語 $\hat{\boldsymbol{x}}$ を出力するのが復号器の役目である．

ブロック誤り率 $\Pr[\boldsymbol{x}\neq\hat{\boldsymbol{x}}]$ の最小化を考えるとき，ブロック単位最大事後確率を最大化する最大事後確率復号法が最適である．通信系の応用では，すべての符号語は等確率に選択されると仮定することが自然である．事前確率が等確率の場合，最大事後確率推定は最尤推定と一致する．

最尤推定に基づく復号則である最尤復号則は

$$\hat{\boldsymbol{x}}=\arg\max_{\boldsymbol{x}\in C(H)}P_{\boldsymbol{Y}|\boldsymbol{X}}(\boldsymbol{y}|\boldsymbol{x}) \tag{2.3}$$

と与えられる．ここで，$C(H)$ に含まれる符号語の個数は，符号長 n に対して指数関数的に増大することに注意したい．この最尤推定則を復号アルゴリズムとして単純に適用するならば，その復号アルゴリズムは指数時間アルゴリズムとなる．この計算量の壁を破るためには，符号または復号法に何らかの工夫が必要である．

2.3 緩和推定問題

具体的な例を挙げて，本稿で紹介する復号法の考え方について説明する．

検査行列 H により定義される線形符号 $C(H)$ のひとつの符号語 $\boldsymbol{x}\in C(H)$ が加法的白色ガウス通信路（AWGN 通信路）に送出されたものと仮定しよう．送信の際には，バイナリ $(0,1)$・バイポーラ $(+1,-1)$ 変換が行われるものとする．すなわち，受信ベクトル $\boldsymbol{r}$ は

$$\boldsymbol{r}=(\boldsymbol{1}-2\boldsymbol{x})+\boldsymbol{z} \tag{2.4}$$

と与えられる．ここで，$\boldsymbol{z}$ は白色ガウス雑音ベクトルであり，$\boldsymbol{1}$ はすべての要素が 1 であるベクトルである．

上述の通信系に対する最尤復号則は，

$$\hat{\boldsymbol{x}}=\arg\min_{\boldsymbol{x}'\in C(H)}||\boldsymbol{r}-(\boldsymbol{1}-2\boldsymbol{x}')||^2 \tag{2.5}$$

と与えられる．ここで，$\hat{\boldsymbol{x}}$ は推定ベクトルであり，$||\cdot||$ は，ユークリッドノルムである．この最尤復号則は，雑音項に関する多次元ガウス分布に対応する尤度関数の最大化と等価である．一般の 2 元線形符号の場合，この最尤復号則に基づく最尤復号アルゴリズムは符号長 n に関する指数時間アルゴリズムとなる．

この最尤推定則に基づく最尤復号問題は，一種の組み合わせ最適化問題と見なすことができる．元問題の実数緩和問題を考えるというアプローチは，計算量的に困難な組み合わせ最適化

問題に対する近似解法として組み合わせ最適化の分野でしばしば利用される Schrijver (2003). 上記の最尤推定則を緩和して得られる緩和推定則

$$\hat{\boldsymbol{x}} = \arg \min_{\boldsymbol{x}' \in Conv(C(H))} ||\boldsymbol{r} - (\boldsymbol{1} - 2\boldsymbol{x}')||^2 \tag{2.6}$$

を考えよう. ここで, $Conv(C(H))$ は, $\mathbb{F}_2$ の元 $(0,1)$ を実数の $(0,1)$ と見なした上での符号語の凸包である. この最適化問題の目的関数は 2 次関数であり, 実行可能領域は有界凸多面体 (符号語の凸包) であることから, この緩和最尤推定問題は 2 次計画問題となっている. したがって, この問題は, 実数体上の最小化問題となっており, 連続最適化手法により効率良く解くことができる可能性がある (Boyd and Vandenberghe, 2004).

2.4 基本多面体

2 元線形符号 $C(H)$ の凸包は, 符号長 n に対して指数的な数の面を持つため, そのまま最適化問題に利用するのは計算量の点で得策ではない. Feldman らは, LDPC 符号の線形計画復号の定式化 (Feldman, 2003; Feldman et al., 2005) において, 実行可能領域を基本多面体とすることにより, この問題を解決した.

基本多面体は 2 元線形符号 $C(H)$ の凸包を包含する緩和凸多面体であり, その頂点集合は $C(H)$ の符号語を包含する. 基本多面体の重要な性質として, LDPC 符号の場合には基本多面体の面の数は符号長 n に対して多項式的に増加することが知られている.

いま, $A_i \triangleq \{j \in [1,n] : h_{i,j} = 1\}$, $i \in [1,m]$ と定義する. また, $T_i (i \in [1,m])$ を A_i に含まれるすべての奇数サイズの部分集合とする. すなわち,

$$T_i \triangleq \{S \subset A_i : |S| \text{ is odd}\} \tag{2.7}$$

である. 実ベクトル $\boldsymbol{x} \in \mathbb{R}^n$ に関する制約

$$\forall i \in [1,m], \forall S \in T_i, \quad 1 + \sum_{t \in S} (x_t - 1) - \sum_{t \in A_i \setminus S} x_t \leq 0, \tag{2.8}$$

と

$$\forall j \in [1,n], \quad 0 \leq x_j \leq 1 \tag{2.9}$$

はそれぞれパリティ制約式 とボックス制約式と呼ばれる.

パリティ制約式は, 検査行列 H のパリティ検査式と関係している. この関係を例を用いて説明する. ひとつの A_i と $S \subset T_i$ を固定しよう. また, $\boldsymbol{x} = (x_1, \ldots, x_n)^T$ を

$$x_i = \begin{cases} 1, & i \in S \\ 0, & i \notin S \end{cases}$$

と定義する. いま, $\boldsymbol{x}$ を 2 元体 $\mathbb{F}_2$ の元であると考えると $H\boldsymbol{x} \neq 0^m$ となる. なぜならば, S のサイズが奇数であることと $\boldsymbol{x}$ の定義より

$$\sum_{j=1}^{n} h_{i,j} x_j = \sum_{j \in A_i} x_j = \sum_{j \in S} x_j + \sum_{k \in A_i \setminus S} x_k = 1$$

となるからである. なお, この式の和は, 2 元体上の和である. 一方, 今度は, $\boldsymbol{x}$ を実ベクトルと見なして, パリティ制約式の左辺の量を評価すると

$$1 + \sum_{t \in S} (x_t - 1) - \sum_{t \in A_i \setminus S} x_t = 1$$

となり，このベクトル $\boldsymbol{x}$ はパリティ制約式を満足しないことが分かる．すなわち，パリティ制約式は，2 元体上のパリティ検査式が排除する奇数重みの 2 元体系列を実数体上で排除する不等式条件となっている．

基本多面体 $\mathcal{P}(H)$ は

$$\mathcal{P}(H) \triangleq \{\boldsymbol{x} \in \mathbb{R}^n : \boldsymbol{x} \text{ satisfies constraints (2.8) and (2.9)}\} \tag{2.10}$$

と定義される多面体である（Koetter and Vontobel, 2003; Feldman et al., 2005）．基本多面体 $\mathcal{P}(H)$ の内部集合を $\mathcal{P}^*(H)$ と表記する．

LDPC 符号のひとつの検査シンボルに注目すると，その検査シンボルに関連するビットシンボルの集合は単一パリティ検査符号（偶重み符号）を構成していると見ることができる．基本多面体は，すべての検査シンボルに対応する単一パリティ検査符号の凸包の共通集合である．基本多面体の頂点は，符号語となっている 符号語頂点（整数頂点）と非整数成分を持つ非符号語頂点に分類される．

2.5 LP 復号法

本節では，Feldman らの提案した LP（線形計画）復号法の概略について説明する．この Feldman らの仕事は，連続最適化と復号問題を結びつけた最初の仕事である．本稿で後に述べられる内点復号法において直接的に LP 復号法が利用されるわけではないが，我々の研究の出発点となる復号法という意味で簡潔に説明を行う．

2 値入力対称出力（BIOS）通信路に関する条件付確率密度関数 $P_{Y_i|X_i}(y_i|x_i)(i \in [1,n])$ が与えられていると仮定する．例えば，AWGN 通信路は BIOS 通信路の一例である．確率変数 Y_i と X_i はそれぞれ，第 i 受信シンボルと i 送信シンボルを意味している．対数尤度比ベクトル $\boldsymbol{\lambda} \triangleq (\lambda_1, \lambda_2, \ldots, \lambda_n)^T$ は

$$\lambda_i \triangleq \ln \frac{P_{Y_i|X_i}(y_i|0)}{P_{Y_i|X_i}(y_i|1)}, \quad i \in [1,n] \tag{2.11}$$

と与えられる．Feldman らにより提案された LP 復号法は線形計画問題（Feldman et al., 2005）

$$\hat{\boldsymbol{x}} = \arg \min_{\boldsymbol{x} \in \mathcal{P}(H)} \sum_{i=1}^{n} \lambda_i x_i$$

として定義される．ここで，$\hat{\boldsymbol{x}}$ は推定語であり，これはこの線形計画問題の解となるため基本多面体の頂点となる．基本多面体は，上で述べたように非整数頂点（疑似符号語と呼ばれる）を持つ場合があるため，一般には，LP 復号則は最尤推定則とは同一ではなく，近似最尤復号則となっている．LDPC 符号の場合には，LP 復号法は経験的に比較的良好な復号結果を与えることが知られている．

2.6 線形干渉通信路

本稿で紹介する内点復号法の主たる対象となる線形干渉通信路を定義する．

送信者は，2 元線形符号 $C(H)$ の符号語 $\boldsymbol{x}$ を受信者に向けて送信する．受信者は受信語

$$\boldsymbol{r} = V\boldsymbol{x} + \boldsymbol{b} + \boldsymbol{z}, \tag{2.12}$$

を受け取る．ここで， V は正則な $n \times n$ 実行列（干渉行列），$\boldsymbol{b}$ は長さ n の実ベクトルである．これらの V と $\boldsymbol{b}$ は受信者にとって既知である．ベクトル $\boldsymbol{z} \in \mathbb{R}^n$ は雑音ベクトルである．この通信路モデルを線形ベクトル通信路モデルと呼ぶ．適切に V と $\boldsymbol{b}$ を定義することにより，シンボル間干渉のある通信路や MIMO 通信路は，この線形ベクトル通信路の一例と考えることができる．

上記の線形ベクトル通信路における最尤推定問題を緩和することにより，緩和最尤推定則

$$\hat{\boldsymbol{x}} = \arg \min_{\boldsymbol{x} \in \mathcal{P}(H)} f(V\boldsymbol{x} + \boldsymbol{b}, \boldsymbol{r}) \tag{2.13}$$

が得られる．ここで $f(\cdot,\cdot)$ は，雑音の統計的性質に基づいて決められた適切な距離関数である．ここで，距離関数 $d(\cdot,\cdot)$ は最尤推定において利用される負対数尤度関数に基づき決定される．例えば，雑音ベクトルが加法的白色ガウス雑音である場合には，この距離関数はユークリッド 2 乗距離関数となり，緩和最尤推定則は実数体上の 2 次計画問題

$$\hat{\boldsymbol{x}} = \arg \min_{\boldsymbol{x} \in \mathcal{P}(H)} ||\boldsymbol{r} - (V\boldsymbol{x} + \boldsymbol{b})||^2 \tag{2.14}$$

となる．

3. 内点復号法

本節では，内点復号法の考え方と概要について述べる．

3.1 内点法に基づく復号法

通信への連続最適化アルゴリズムの応用を考える場合に重要になるのが計算速度である．例えば， 多くの通信系応用分野において 1 つの復号問題は数マイクロ秒以下という非常に短い時間内に解く必要がある．そのため，復号に最適化技法を利用する場合には，通信伝送路の性質，LDPC 符号の特徴を十分に利用した高速な復号アルゴリズムを構成し，かつ並列実行可能なハードウェアとしての実現可能性を持つ方式を考案することが重要になる．

以下では，前述の緩和最尤推定則により与えられる 2 次計画問題を LDPC 符号の特徴を生かした主パス追跡内点法を利用して解くことを考える．

まず準備として，基本多面体に基づいて次のように対数バリア関数を

$$\begin{aligned} B(\boldsymbol{x}) \stackrel{\triangle}{=} & -\sum_{i \in [1,m]} \sum_{S \subset T_i} \ln \left[- \left(1 + \sum_{t \in S} (x_t - 1) - \sum_{t \in A_i \setminus S} x_t \right) \right] \\ & - \sum_{j \in [1,n]} \ln[-(-x_j)] - \sum_{j \in [1,n]} \ln[-(x_j - 1)] \end{aligned}$$

と定義する．

この対数バリア関数の第 1 項はパリティ制約に基づくバリア項であり，第 2，3 項はボックス制約に基づくバリア項である．このバリア関数は基本多面体の内部集合において定義される関数であり，$\boldsymbol{x}$ が基本多面体の境界に接近していくとバリア関数値は $+\infty$ に向けて増大していく．

緩和推定則における目的関数 $f(V\boldsymbol{x} + \boldsymbol{b}, \boldsymbol{r})$ とバリア関数に基づき，メリット関数を

$$\psi^{(t)}(\boldsymbol{x}) = tf(V\boldsymbol{x} + \boldsymbol{b}, \boldsymbol{r}) + B(\boldsymbol{x}) \tag{3.1}$$

と定義する．ここで，t は正実数のパラメータであり，スケールパラメータと呼ぶ．

内点復号法は，主パス追跡型内点法によりメリット関数 $\psi^{(t)}(\boldsymbol{x})$ を最小化することにより，緩和最尤推定問題の近似解を得るという考えに基づき構成されている．内点復号法の基本的な流れは次のとおりである．

(1) t の初期値を設定する．探索初期点を基本多面体の中心点 $\boldsymbol{x} = (1/2, 1/2, \ldots, 1/2)^T$ と設定する．
(2) 勾配降下法，またはニュートン法を利用して，$\psi^{(t)}(\boldsymbol{x})$ を最小化する (中心点の探索処理)．
(3) 探索点に対して，min-sum 復号法を適用し，一次推定語を作成する．

(4) $t := \alpha t$ (α は正の実数) として，t の値を増加させる．
(5) ステップ (2) に戻る．

内点復号法の各ステップは，符号長について線形時間で計算が終了するように設計されている．以下では，内点復号法の各ステップについて説明する．

3.2 メリット関数の勾配ベクトルとヘッセ行列

内点復号法のステップ (2) では，与えられたパラメータ t に対応する中心点を見いだすために勾配降下法，またはニュートン法を利用する．数値最適化の文脈では内点法の中心点探索部に勾配法が用いられることは無いが，文献 Wadayama (2010) では，計算量削減の観点から勾配降下法の利用も検討している．

勾配法を利用するためには，探索点におけるメリット関数の勾配ベクトルが，ニュートン法を利用するためには，勾配ベクトルとヘッセ行列の計算が必要となる．

メリット関数の勾配ベクトルは

$$\nabla\psi^{(t)}(\boldsymbol{x}) \triangleq \left(\frac{\partial}{\partial x_1}\psi^{(t)}(\boldsymbol{x}), \frac{\partial}{\partial x_2}\psi^{(t)}(\boldsymbol{x}), \ldots, \frac{\partial}{\partial x_n}\psi^{(t)}(\boldsymbol{x})\right)^T \tag{3.2}$$

と与えられる．第 k シンボルの導関数は

$$\begin{aligned}\frac{\partial}{\partial x_k}\psi^{(t)}(\boldsymbol{x}) &= t\frac{\partial}{\partial x_k}f(\boldsymbol{x}) + \frac{\partial}{\partial x_k}B(\boldsymbol{x}) \\ &= t\frac{\partial}{\partial x_k}f(\boldsymbol{x}) + \sum_{i\in[1,m]}\sum_{S\in T_i}\tau_k^{(i,S)}(\boldsymbol{x}) - \frac{1}{x_k} - \frac{1}{x_k-1}\end{aligned}$$

となる．ここで，

$$\tau_k^{(i,S)}(\boldsymbol{x}) \triangleq \frac{I[k\in A_i\backslash S] - I[k\in S]}{1+\sum_{l\in S}(x_l-1) - \sum_{l\in A_i\backslash S}x_l}, \tag{3.3}$$

($i\in[1,m], S\subset[1,n]$) である．記法 $I[condition]$ は，指標関数を表しており，もし，$condition$ が真ならば $I[condition]=1$ となり，一方，$condition$ が偽ならば，$I[condition]=0$ となる．

パリティ制約に関するバリア関数の偏導関数は $2^{w_r-1}m$ 個の項を含んでいる．したがって，$\nabla\psi^{(t)}(\boldsymbol{x})$ のナイーブな評価には，検査行列の行重み w_r について指数時間の計算が必要となる．もし，検査行列の行重みが大きいときには，この部分の計算量が内点復号法全体の計算量を支配することになる．全体の計算量削減のために，ここでは真の勾配ベクトルを正確に評価するのではなく，その近似値をより少ない計算量で評価するという方策を用いる．

近似勾配ベクトル $\boldsymbol{g} \triangleq (g_1,\ldots,g_n)^T$ は

$$g_k \triangleq t\frac{\partial}{\partial x_k}f(\boldsymbol{x}) + \sum_{i\in[1,m]}\tau_k^{(i,S^{(i)})}(\boldsymbol{x}) - \frac{1}{x_k} - \frac{1}{x_k-1}, \quad k\in[1,n],\ \boldsymbol{x}\in\mathcal{P}^*(H) \tag{3.4}$$

と定義される．ここで集合 $S^{(i)}$ は

$$S^{(i)} \triangleq \arg\max_{S\subset T_i}\left[1+\sum_{l\in S}(x_l-1) - \sum_{l\in A_i\backslash S}x_l\right], \quad i\in[1,m] \tag{3.5}$$

と定義される T_i の部分集合である．近似勾配ベクトルは，真の勾配ベクトルの中に現れる和に関する支配項のみを足して得られる近似量と見ることができる．論文 Wadayama (2010) では，動的計画法に基づく $S^{(i)}$ を求める効率の良い手法が提案されており，その手法を利用すれば $S^{(i)}$ は w_r に比例する時間で算出が可能である．すべてのチェックノードを考えると，近似

勾配ベクトルの評価計算量は $O(w_r m)$ となり，この計算量はナイーブな真の勾配ベクトルの評価に対して十分に高速である．

中心点の計算にニュートン法を用いる場合には，勾配ベクトルに加えて，探索点におけるヘッセ行列の算出が実行時の反復ごとに必要となる．LDPC 符号ではヘッセ行列が疎行列になること，近似勾配ベクトルの計算の際に利用した近似計算などを組み合わせることで，近似ヘッセ行列の高速計算が可能となる．近似ヘッセ行列の詳細は論文 Wadayama (2010) を参照されたい．

3.3 min-sum 復号法

内点復号法の目標は目的関数 $f(\boldsymbol{x})$ の最小値を正確に評価することではなく，推定ベクトル $\hat{\boldsymbol{x}}$ を高速に算出した上で十分に小さい誤り率を達成することにある．そこで，内点復号法のステップ (3) では，LDPC 符号の復号法として知られる min-sum 復号法を符号語の推定に利用する．

min-sum 復号法は，sum-product 復号法のチェックノードにおける更新式を計算がより容易な近似更新式に代えて得られる LDPC 符号の復号アルゴリズムで広く実用的に利用されている．近似チェックノード更新式は，加算・乗算・絶対値・最小要素選択の基本演算からなり，

$$\alpha_{c_i \to x_j} = \left(\prod_{k \in A_i \backslash j} \mathrm{sign}(\beta_{x_k \to c_i}) \right) \min_{k \in A_i \backslash j} |\beta_{x_k \to c_i}| \tag{3.6}$$

という形をしている．ここで，c_i は i 番目のチェックノードを表し，x_k は k 番目のビットノードを表す．また，$\alpha_{c_i \to x_j}$ はチェックノード c_i からビットノード x_j に送られるメッセージであり，$\beta_{x_k \to c_i}$ のビットノード x_k からチェックノード c_i に送られるメッセージである．図 1 に min-sum 復号法におけるビットノード処理とチェックノード処理を図示している．図中の B_i は

$$B_i \stackrel{\triangle}{=} \{j \in [1,m] : h_{i,j} = 1\},\ i \in [1,n]$$

と定義される．アルゴリズムの詳細については，例えば，和田山 (2010) を参照されたい．

min-sum 復号法は，tanh の計算など複雑な処理を含まないためハードウェア実装に向いている．min-sum 復号法の復号性能は，sum-product 復号法の復号性能に若干及ばないが復号中にメッセージのスケーリングを行うことにより，多くの場合，両者の性能差はほとんど無くなることが知られている．

緩和推定問題の最小解に十分に収束していない段階でも，min-sum 復号法を併用することにより送信符号語を正しく推定できる場合が多くある．そのため，min-sum 復号法の利用により内点復号法の反復処理 (ステップ (1) から (4)) の回数を大きく減らすことができる．

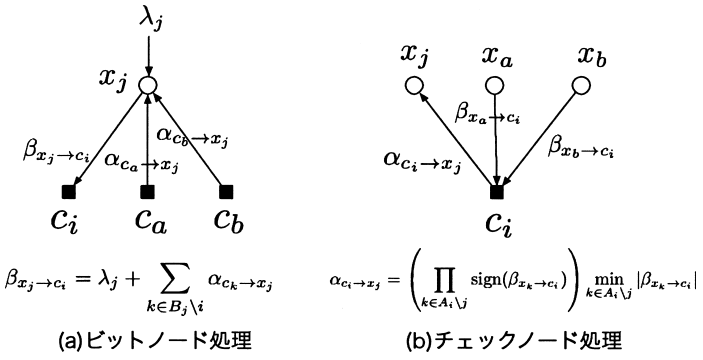

図 1. min-sum 復号法におけるビットノード処理とチェックノード処理.

3.4 ニュートン方程式の求解

内点復号法のステップ(2)において，ニュートン法を利用する場合には，ニュートン方程式 $G\boldsymbol{d}=\boldsymbol{g}$ を解く必要がある．ここで，G と $\boldsymbol{d}$ はそれぞれ探索点における近似ヘッセ行列と近似勾配ベクトルであり，$\boldsymbol{d}$ は探索ステップとして利用されるニュートンステップである．このニュートン方程式の求解が復号法全体の計算量に対して支配的な影響を与えるため，適切な求解手法を利用することが求められる．論文 Wadayama(2010)では，コレスキー分解と前進後退代入を組み合わせる求解手法，ならびにヤコビ法に基づく求解手法の検討が行われている．また，文献 Wadayama(2009)においては，前処理付共役勾配法の利用が検討されている．共役勾配法の前処理としては，単純なヘッセ行列の対角近似が利用されている．

LDPC 符号を定義する検査行列が疎であることから，ヘッセ行列 G も疎行列となる．LDPC 符号の復号問題に関しては，ヘッセ行列の疎性を容易に利用することのできる前処理付共役勾配法が計算量の点から，他の方法よりも有利である傾向にある(Wadayama, 2009)．

4. むすび

本稿では，論文 Wadayama(2010)にて提案された内点復号法において，そのアルゴリズムの考え方と概略を紹介した．復号アルゴリズムの性能や振る舞いの詳細については，同論文を参考にされたい．現時点で主流であるビリーフプロパゲーション(BP)に基づく結合メッセージパッシング復号器と比較して遜色のない復号性能が内点復号法により得られることが同論文で報告されている．

現在，符号理論の分野では，LDPC 符号など疎グラフに基づいて定義される符号を BP により復号するアプローチが最も標準的なアプローチとなっている．本稿で紹介した連続最適化技法に基づく復号手法は，その意味では非主流派のアプローチということになる．しかし，非主流派のアプローチにもいくつかの優れた点がある．

連続最適化技法に基づく復号手法の考え方は，組み合わせ最適化の緩和解法と共通する部分が多い．そのため，連続最適化アルゴリズムや組み合わせ最適化などの関連分野の優れた技術を復号性能向上のために利用できる可能性がある．特に組み合わせ最適化分野で利用されている整数計画問題に関する技法は復号性能改善のために重要である．例えば，LP 復号法の復号性能の改善のために，(1)混合整数計画法の利用，(2)制約条件の付加による基本多面体の緊密化といった工夫が近年提案されてきている．

Draper et al.(2007)では，LDPC 符号の LP 復号問題において，(1)の混合整数計画の利用に基づくアプローチにより BP 復号性能を上回る復号性能が得られることが報告されている．この手法の概要は次のとおりである．LP 復号の結果として非整数ベクトルが得られた場合に非整数要素の位置の変数が整数であるという制約を新たに導入する．そして，再び LP 問題を解き直すという処理を行う．2 回目の処理では，最初に得られた解とは異なる解が得られるため，整数解(すなわち符号語)が得られる可能性が生じる．2 回目の解が再び非整数解の場合，同様のプロセスを反復する．計算量は通常の LP 復号法よりも大きくなるものの，この反復により，符号語を発見できる可能性が高まることが計算機実験の結果として報告されている．

(2)の制約条件の付加による基本多面体の緊密化アプローチでは，実行可能領域である多面体に適切な線形制約条件(超平面)を追加することにより多面体緩和の緊密化を行う．緊密化された実行可能領域で最適化を行うことにより，元の場合と比べて質の良い解が得られる可能性が高まる．

例えば，切除平面法に基づく LDPC 符号の復号法(Tanatmis et al., 2009)では，復号中に得られた非整数解を削除する切除超平面を追加しながら線形計画問題を解き直すという復号プロセ

スを実行する．一方，我々のグループが開発した切除平面法に基づく検査行列改良手法(Miwa et al., 2009)は，符号の検査行列の行の線形結合として得られる冗長行の生成する切除超平面を利用する．復号結果に悪影響を与える基本多面体における非符号語頂点を切除することにより，LP 復号法の復号性能改善が得られることが示されている．緩和復号問題においては，組み合わせ最適化の緩和解法と同様に少ない計算量で整数解を得ることが特に重要であり，現在，著者のグループでは整数頂点を選好するペナルティ関数を利用した非線形最適化手法の検討を進めている．

本稿で扱った問題は，「情報通信の文脈において，連続最適化技法に基づき信頼性の高い推論を実現する」という問題であった．この問題は組み合わせ最適化や連続最適化，推論，符号理論にまたがる問題であり，学際的色彩の濃いものである．情報通信，信号処理，確率推論の世界における，特にリアルタイム性が要求される用途での連続最適化技法の応用には今後のさらなる進展の可能性があると考えられ，分野の枠を超えた研究の推進が求められている．

謝　辞

本研究の一部は，科学研究費 基盤 C No. 22560370 の支援を受けた．

参 考 文 献

Boyd, S. and Vandenberghe, L. (2004). *Convex Optimization*, Cambridge University Press, New York.

Burshtein, D. (2008). Iterative approximate linear programming decoding of LDPC codes with linear complexity, *Proceedings of IEEE International Symposium on Information Theory*, *Toronto*.

Draper, S. C., Yedidia, J. S. and Wang, Y. (2007). ML decoding via mixed-integer adaptive linear programming, *Proceedings of IEEE International Symposium on Information Theory*, *Nice*.

Feldman, J. (2003). Decoding error-correcting codes via linear programming, Ph.D. Thesis, Massachusetts Institute of Technology,

Feldman, J., Wainwright, M. J. and Karger, D. R. (2005). Using linear programming to decode binary linear codes, *IEEE Transactions on Information Theory*, **51**(3), 954–972.

Gallager, R. G. (1963). *Low Density Parity Check Codes*, MIT Press, Cambridge, Massachusetts.

伊藤慎吾，和田山正 (2011). 2 次計画法に基づく同期 CDMA マルチユーザ検出アルゴリズム，電子情報通信学会和文誌 A，**J94-A**(8), 649–656.

Koetter, R. and Vontobel, P. O. (2003). Graph covers and iterative decoding of finite-length codes, *Proceedings of 3rd International Symposium on Turbo Codes and Related Topics*, *Brest*.

Miwa, M., Wadayama, T. and Takumi, I. (2009). A cutting-plane method based on redundant rows for improving fractional distance, *IEEE Journal on Selected Areas in Communications*, **27**(6), 1005–1012.

Schrijver, A. (2003). *Combinatorial Optimization*: *Polyhedra and Efficiency*, Springer, Berlin.

Taghavi, M. H., Shokrollahi, A. and Siegel, P. H. (2008). Efficient implementation of linear programming decoding, *Forty-Sixth Annual Allerton Conference*, Allerton Park & Retreat Center, University of Illinois Monticello, Illinois.

Tanatmis, A., Ruzika, S., Hamacher, H., Punekar, M., Kienle, F. and Wehn, N. (2009). Valid inequalities for binary linear codes, *Proceedings of IEEE International Symposium on Information Theory*, *Seoul*.

Vontobel, P. O. (2008). Interior-point algorithms for linear-programming decoding, *Proceedings of Information Theory and Its Applications Workshop*, UC San Diego, La Jolla.

Vontobel P. O. and Koetter R. (2006). Towards low-complexity linear-programming decoding, *Pro-*

ceedings of 4th International Conference on Turbo Codes and Related Topics, *Munich*.

Wadayama, T. (2009). An LP decoding algorithm based on primal path-following interior point method, *Proceedings of IEEE International Symposium on Information Theory*, *Seoul*.

Wadayama, T. (2010). Interior point decoding for linear vector channels based on convex optimization, *IEEE Transactions on Information Theory*, **56**(10), 4905–4921.

和田山正 (2010). 『誤り訂正技術の基礎』, 森北出版, 東京.

A Review of Decoding Algorithm for LDPC Codes Based on Numerical Optimization Techniques

Tadashi Wadayama

Nagoya Institute of Technology

This paper reviews a decoding algorithm for low-density parity-check (LDPC) codes based on convex optimization according to the reference Wadayama (2010). The decoding algorithm, called *interior point decoding*, is designed for linear vector channels. The linear vector channels include many practically important channels such as inter-symbol interference channels and partial response channels. It is shown that the maximum likelihood decoding (MLD) rule for a linear vector channel can be relaxed to a convex optimization problem called a relaxed MLD problem. The decoding algorithm is based on the primal path-following interior point method with a barrier function. Approximate variations of the gradient descent and the Newton methods are used to solve the convex optimization problem.

Key words: Interior point method, convex optimization, low-density parity-check codes.