テーマ４：平均時計算量の解析（その３）

本日の講義の目的

- 最尤推定問題の典型例：k-LIN 問題群
- 単純なメッセージ伝搬法：確率伝搬法→スペクトラル法→単純化→？

4.6. k-LIN 問題群

最尤推定問題の例として今回は（二値）線形連立方程式として表される問題群を考えよう．具体的には，二値（± 1 の値を取る）変数に対し，たとえば

$$x_1 \oplus x_3 \oplus x_{11} = +1$$

のような線形方程式を考える．ただし，$\oplus$ は通常の整数の掛け算（排他的論理輪和もしくは mod 2 での計算）とする．このような式を k-変数線形方程式（略して k-変数式）という．ただし，k は式に現われる変数の数である．

以下では $k \geq 2$ を一つ固定して考える（といっても授業では $k = 2$ に限定する）．変数の数 n，式の数 m に対し，k-変数線形連立方程式の集合を次のように定義する．

$$k\text{-LIN}(n, m) \;=\; \{\, \{eq_1, ..., eq_m\} \,|\, \text{各 } eq_i \text{ は } k\text{-変数式} \,\}.$$

式 eq_i に現われる変数を，以下では記号 $x_{i_1}, ..., x_{i_k}$ で，式 eq_i の右辺の値を b_i で表すことにする．なお，変数の添え字は小さい順 $i_1 \leq \cdots \leq i_k$ で考える．

最尤推定問題を考える場合，元となる解がある．つまり $\boldsymbol{x} = x_1, ..., x_n$ に対する値の割り当て $\boldsymbol{a} = (a_1, ..., a_n)$ である．これに対し，右辺の値が正しい値になっている式を（$\boldsymbol{a}$ に対し）無矛盾な式といい，その逆になっている式を誤った式と呼ぶことにする．

最尤推定問題の一つのパターンは，ある少ない割合で誤った式も含む線形方程式から元の割り当てを推定することである．そのような最尤推定問題の場合には，次のような式の確率モデル（つまり，連立方程式 L のランダムな生成法）が考えられる.（注：以下は変数の数 n と元の解（割り当て $\boldsymbol{a}$）が与えられた場合の生成法．パラメータとして P, Q_{+1}, Q_{-1} を用いる.）

すべての変数の k 個組 $(x_{i_1}, ..., x_{i_k})$ に対し，

1. その変数からなる式を確率 P で（i 番目の）左辺式として採用.
2. その右辺値 b を $\boldsymbol{a}$ に基づき計算.
3. 確率 $1 - Q_b$ で $b_i = b$ を確率 Q_b で $b_i = -b$ とし，式 $eq_i =$ “$x_{i_1} \oplus \cdots \oplus x_{i_k} = b$” を連立方程式 L の i 番目の式として加える.

このように生成された連立方程式の集合を（ランダムな生成方法も含め）k-LIN$(n, \boldsymbol{a}, P, Q_{+1}, Q_{-1})$ と書くことにする．たとえば "$L : k$-LIN$(n, \boldsymbol{a}, P, Q_{+1}, Q_{-1})$" と書くと，それは L を上記の方法でランダムに生成することを意味する．

先週説明した問題の多くは（ほぼ）この形式で定義することができる．

例１：ノイズ有り 2-LIN 問題（Perturbed-kLIN Problem)

レポートの課題の１つで配布したプログラムが対象としている問題．与えられた変数の数 n に対し，$\boldsymbol{a} = (+1, +1, ..., +1)$ で，$Q_{+1} = Q_{-1} = Q$ の場合を考えている．これを以下では k-LIN(n, P, Q) で表す．サンプルプログラムでは，$k = 2$ か $k = 3$ の場合を考えている．

例２：Bisection 問題

- もともとの問題の確率モデル（頂点が $V = \{1, ..., 2n\}$ の場合）：
  1. 答えとして想定している V の分割を V_1, V_2 とする．これはランダムに決めてもよい（ただし Bisection 問題の場合には $|V_1| = |V_2|$）．けれども，簡単のためここでは $V_1 = \{1, ..., n\}$, $V_2 = \{n + 1, ..., 2n\}$ と固定しておく．
  2. 同じ分割に所属する頂点同志は確率 p で，そうでない頂点同士は確率 r（ただし $r < p$）で辺を結ぶ．なお，後の議論を単純にするために同じ頂点同士をループで結ぶのも許すことにする．
  3. 問題は，このように作られたグラフから，最もらしい分割を求めることである．

- 対応する 2-LIN モデル：
  我々が連立方程式に直して問題を解く場合には元の解の情報は一切ない．つまりグラフのみから方程式を作る方法を考えるべきである．いくつか方法があるが，ここでは，すべての二変数に対して式を作り，辺があれば右辺を $+1$ に，なければ右辺を -1 とする，という方法をとる．その場合，対応する 2-LIN$(n, \boldsymbol{a}, P, Q_{+1}, Q_{-1})$ モデルは次のようになる．

$$\begin{aligned} \boldsymbol{a} &= (+1, +1, ..., +1, -1, -1, ..., -1) \\ P &= 1.0, \quad Q_{+1} = 1 - p, \quad Q_{-1} = r. \end{aligned}$$

例３：LDPC 復号問題

- もともとの問題の確率モデル（符号語長 n ビット，シンドローム長 m ビットの場合）：
  1. パリティチェック行列 A をランダムに作る．行ベクトルとして n 個の要素から成る 0,1-行ベクトルで，1 が k 個の立ったベクトルをランダムに（約）m 個集めてきて行列を作る．具体的には，各行ベクトルを確率 $P = m/\binom{n}{k}$ で行列に加える[1]．

[1] こうすると行数は平均で m になるが，実際にできる行列の行数がピッタリ m にならない場合もある．また，先週説明したような列の 1 の数も同じ行列にならない場合が多い．その点は今回は目をつぶってください！

2. 符号語を通信したときのノイズベクトル $\boldsymbol{n} = (a_1, ..., a_n)$ を，各 a_i を独立に確率 p で 1 に，確率 $1-p$ で 0 に定めることで作る．シンドロームを $\boldsymbol{c} = A\boldsymbol{a}$ で求める．
3. 問題は，このように作られた A と $\boldsymbol{c}$ から，最もらしいノイズベクトルを求めることである．

- 対応する k-LIN モデル：
  まさに $A\boldsymbol{x} = \boldsymbol{c}$ が解きたい連立方程式である．これを生成するには

$$\begin{aligned} \boldsymbol{a} &: \{\, \boldsymbol{n} = (a_1, ..., a_n) \,|\, \text{確率 } p \text{ で } a_i = +1,\ 1-p \text{ で } a_i = -1 \,\} \\ P &= m/\tbinom{n}{k},\ \ Q_{+1} = Q_{-1} = 0. \end{aligned}$$

4.7. メッセージ伝播アルゴリズム

上記のような問題に対しては，貪欲型ランダムウォーク局所探索アルゴリズムが比較的うまく働く場合が多い．一方，確率伝播法 (Belief Propagation) からもアルゴリズムが提案できる．先週，確率伝搬法を最大固有ベクトルを求める反復法とみなす導出を考えたが，そこで得た考え方をさらに単純化すると単純なメッセージ伝播アルゴリズムに行き着く．これも非常にうまく機能する．ここでは Perturbed-kLIN Problem（ノイズ有り kLIN 問題）の $k = 2$ もしくは $= 3$ の場合を対象に，メッセージ伝播アルゴリズムについてもう少し解説しよう．

アルゴリズムの概略（$k = 2$ の場合）は以下の通りである．

---

procedure Message Passing Algorithm for the Perturbed 2-LIN Problem
input $L = \{eq_1, ..., eq_m\}$;
  set $\mathtt{x} := +1$, and set the others all 0;
  repeat `MAXSTEP` times **do** {
    for all $\mathtt{x}_i$, $1 \le i \le n$, **in paralell do** {
      $\mathtt{x}_i := \sum_{eq \in E_i} m_{eq \to i}$; — $(*)$
    }
    if stabilized **then exit**;
  }
  output $(\mathrm{sign}(\mathtt{x}_1), ..., \mathrm{sign}(\mathtt{x}_n))$;
end-procedure

Remarks:

- E_i = the set of equations containing $\mathtt{x}_i$.
- $m_{eq \to i} \stackrel{\text{def}}{=} \mathtt{x}_j$ if $b = +1$, and $m_{eq \to i} \stackrel{\text{def}}{=} -\mathtt{x}_j$ if $b = -1$, where $eq =$ "$x_i \oplus x_j = b$".
- $\mathrm{sign}(z) = +1$ (resp., $= -1$) if $z > 0$ (resp., $z < 0$), and it is 0 if $z = 0$.

A simple message passing algorithm for the Perturbed 2-LIN Problem

---