0-1 行列の疎行列直接解法向け番号変換

師岡 真成（早大），本山 義史（早大），後 保範（早大）

Ordering method for direct sparse solver of 0-1 matrix.

Masanari Morooka, Yoshifumi Motoyama, Yasunori Ushiro(Waseda)

概要：RSA 暗号解読で発生する大規模な 0-1 疎行列の線形計算を扱う。多数の解を求めるには反復解法より直接解法が向いている。疎行列直接解法では、行及び列の番号変換が性能を大きく作用する。ここでは、fill-in がより少ない番号変換方法を検討した。

1. はじめに

RSA 暗号は現在の情報社会において欠かせない技術である。RSA 暗号は多数桁の因数分解の困難性を利用し、解読はふるい法が使用されている。ふるい法ではふるいで得られたデータの基底のベキを偶数にして、平方の形にするため 0-1 行列の線形計算が必要となる。現在この計算には反復法が使用されている。ふるいは計算全体の約 9 割を占める。ふるいをより高速にするアルゴリズムの中には線形計算の解を多数必要とするものがある。反復法では求める解の数を増やすと、それに比例して計算量が増加する。一方、直接法はガウス消去法では求める解の数を増やしても、計算量はほとんど増加しない。そのため、大規模な 0-1 行列の疎行列直接解法を対象にする。疎行列直接解法の計算量とメモリー使用量は、行及び列番号の付け方に大きく依存する。ここでは、0-1 行列のガウス消去法による疎行列直接解法向け番号変換を取り上げる。

2. RSA 暗号解読における線形計算

ふるい法による RSA 暗号解読では、得られたデータ数を n とし、基底を m とすると n×m 次元の行列が得られる。行列の値は各基底の整数ベキ数である。データ数 n は m より多く求める。線形計算の目的は各基底のベキ数が偶数となるようなデータの組合せを見つけることである。そのため、線形計算に用いる行列はふるいで得られた行列要素に mod 2 の処理を行い、要素の値が 0 と 1 の行列になる。線形解も 0 と 1 の値になり、各基底のベキ数が偶数となるデータの組合せ(従属解、1 は採用、0 は不採用)を示している。行列のサイズは RSA-768(10 進 232 桁)の解読で約 2 億次元である。RSA-1024(10 進 309 桁)では百億次元程度と推定されている。しかし、1 要素の数は非常に少ない疎行列となる。各データ(行方向)は 1 要素が数百である。一方、基底(列方向)は 1 要素が 2 個/列から(m/2)個/列まで大きく変化し、大半は数個/列から十数個/列となる。n×m の行列を A とする。

反復法では少し横長の $A^Tx=0$ のゼロでない解 x を求める。反復法は通常 64 個の解 x をブロックランチョス法で計算する。直接法は行列 A にガウスの消去法を適用する。ガウス消去は疎行列の形のまま行う。

3. 0-1 疎行列の記憶方法

0-1 疎行列は、値を記憶する必要が無く非ゼロ(値が 1)の位置だけ記憶する。

0-1 疎行列の記憶方法については、図1に示すように各行毎に値が 1 の要素の列番号を記憶する。行列 A は 1 次元配列に順番に配置する。行列 A の k 行の最初の非ゼロの位置は PA[k]で示す。通常は PA[0]=0 とするが、ガウス消去過程では、1 の値が増加し消去前、消去後と二つ必要で、一方を配列の中間の値にする。

k	A(密行列)	PA: 0	A(疎行列)
0	0 1 0 1 0 0 0 0	2	1 3 <-1 の位置
1	0 1 0 0 0 0 0 1	4	1 7
2	0 1 0 1 0 1 1 0	8	1 3 5 6
3	0 1 1 0 0 1 1 1	13	1 2 5 6 7
4	1 0 1 0 0 0 0 1	16	0 2 7
5	0 1 1 1 0 0 0 1	20	1 2 3 7
6	0 0 1 0 0 0 0 1	22	2 7
7	1 0 0 0 0 0 0 1	24	0 7

図1. 0-1 疎行列記憶方法の例

4. ガウス消去結果と従属解の取り出し

図 2 に 13×9 次元の行列のガウス消去結果を示す。軸交換ベクトル VC と枢軸ベクトル VP も図 2 のように変換されている。消去後に 6 行残っているので、従属解は 6 個存在する。その中の1つ、k=7 の行より得られる解は「7,4,1,3,2,6,5」である。7 は VC の値で、4 以下は 7 行の A の値「0,1,2,3,5,7」を VP の対応位置の値で変換したものである。 同様に、k=8 から得られる解は「8,1,3,2,6,5」となる。

以下同様にして、k=9,10,11,12 から 4 個の解が得られる。

k	VC	PA	A					
7	7	6	0	1	2	3	5	7
8	8	11	1	2	3	5	7	
9	9	13	1	3				
10	0	15	5	7				
11	11	20	0	1	3	4	5	
12	12	23	1	2	5			

VP = 4 1 3 2 10 6 0 5 0

図 2.　ガウス消去結果

5. 番号変換で目指す疎行列の形

番号変換の狙いは 0-1 疎行列のガウス消去で演算量とメモリ使用量を減少させることである。今回扱うのは疎行列であるが、説明は密行列の形で行う。また、値 0 の部分は、スペースで表す。ここで、方針を下記に示す。

(1)　一部を密行列処理

0-1 疎行列において 1 の要素が多い部分を密行列として処理する。密行列は図 3 の斜線の部分で、行列の最後の位置を置く。

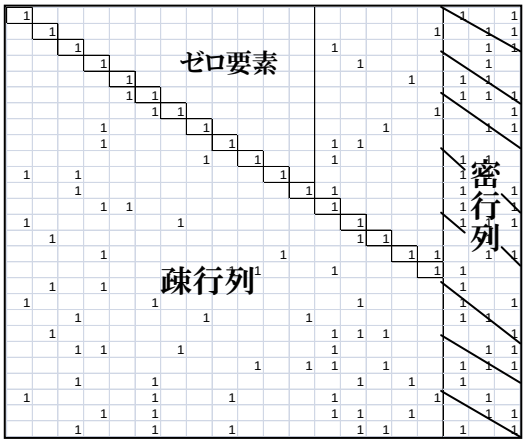

図 3.　目指す行列の形

(2)　対角に 1 の要素を並べる

疎行列部分の対角が 1 になるように行及び列番号を変換する。

(3) 上三角部分のゼロ要素拡大

疎行列部分の上三角のゼロ要素の範囲を可能な限り広げる。

6. 番号変換の手順

図 4 の入力行列を例に番号変換の手順を示す。5 章の 3 つの方針に沿って、番号変換の手順を説明する。

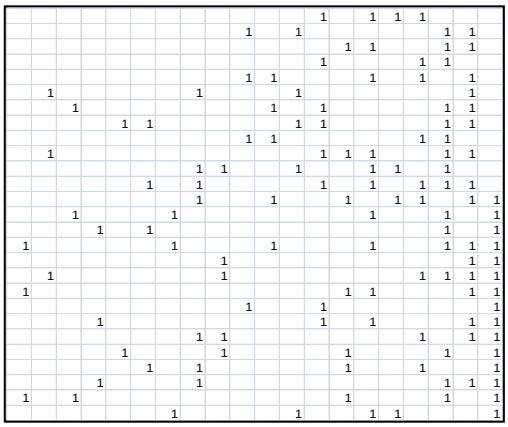

図4. 入力行列の例

6.1　一部を密行列処理

列番号変換を行い、行列の最後の部分を密行列として扱う。列番号変換は各列の値 1 の要素数が少ない順に並べる。図 5 の例では、15%(3 行)を密行列として扱う。

6.2 対角に 1 の要素を並べる

(1)　行番号変換

疎行列として扱う部分の各行の値 1 の要素数が少ない順に行を並べ替える。

(2)　対角要素選択

疎行列部分の対角の値が 1 になるように下記を行う。

(a) 行番号順に、値 1 の要素を 1 つ選ぶ
基本は先頭の列番号を選ぶ

(b) 選ぶ、列番号が既に選ばれていたら

(c) 次に列番号の小さい 1 を選択する。
もし選ぶ列番号が無い場合、この行は捨てて、次の行に移る。図 5 の□で囲われた 1 が選択した例である。

(d) 選択した1が対角になるように行と列番号を変更する。

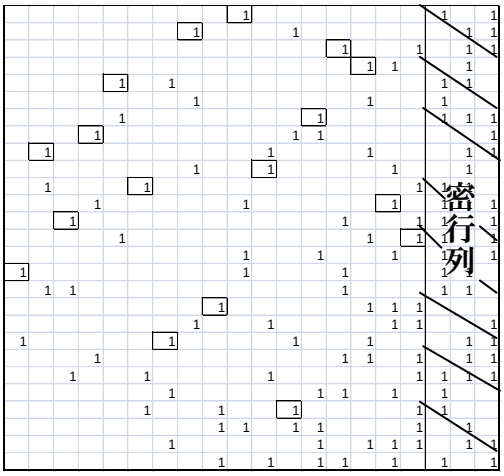

図 5. 疎行列と密行列の分離

6.3 上三角部分のゼロ要素拡大

図 6 に、対角に 1 の要素を並べた、疎行列部分を示す。この上三角部分に存在する値 1 の要素をできる限り、後の列に番号交換で移動させる。下記の番号変換は、上三角部分の値 1 が後に移せなくなるまで続ける。

(1)　移動させる1の選択

上三角部分において、列番号の小さい方から1がある位置(行番号と列番号)を選ぶ。この列を①列とする。選択例を図 6 の①に示す。

(2)　移動先の位置の選択

上三角部分において、列番号の大きい方から選んだ1がある列までを調べ、1がない列を 1 つ選ぶ。この列を②列とする。選択例を図6の②に示す

(3)　移動条件の確認、移動

(1) で選んだ1の列に対して、

(a) から(b)までの行間に 1 があるかを調べる。確認範囲例を図 6 の③に示す。

(a) 対角部分の一つ下の行

(b) (2)で選んだ列の対角部分の行

もし、なければ①列と②列の対角部分を入れ替える番号変換をする。

あれば(2)の作業に戻る。

詳細な処理は発表時に示す。

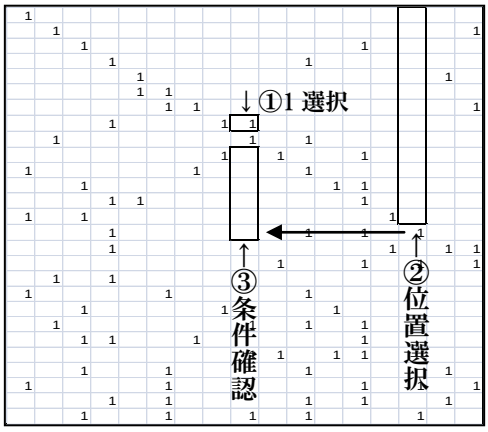

図6. 値 1 を対角にもつ疎行列部分

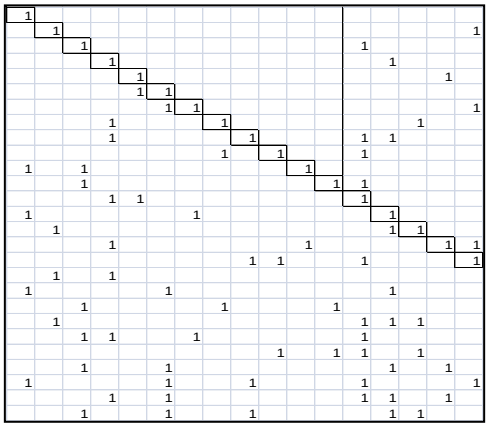

図 7.番号変換完了後の疎行列部分

7. 参考文献

[1] 木田 祐司, “数体ふるい法による素因数分解”, 2003 年, http://www.rkmath.rikkyo.ac.jp/~kida/nfs_intro.pdf

[2] 小国 力編, 行列計算ソフトウェア「疎行列用オーダリング法」“, 1991 年, 丸善

[3] Y. Ushiro, H. Hasegawa, “Acceleration of the Processing of Linear Equations in Characteristic 2 for RSA Decryption”, Annual Report of Earth Simulator Center, 165-170, 2013 年

[4] Y. Ushiro, H. Hasegawa, “Acceleration of the Processing of Linear Equations in Characteristic 2 for RSA Decryption”, Annual Report of Earth Simulator Center, 165-170, 2012 年

[4] Y. Ushiro, H. Hasegawa, “RSA Decryption using Earth Simulator”, Annual Report of Earth Simulator Center, 167-171, 2011 年

[6] 後保範,”ベクトル計算機による RSA 暗号ふるいの高速化”, 京大数理解析研講究録 1733, 101-117, 2011 年 3 月