Pure Mathematics 理论数学, 2011, 1, 189-197
http://dx.doi.org/10.12677/pm.2011.13037 Published Online October 2011 (http://www.hanspub.org/journal/pm/)

A Sort of New Solution for the Conjecture of Binary Matrix Equation

Qingcan Xiao, Zhilian Zeng
School of Mathematics and Information Science, Guangzhou University, Guangzhou
Email: qcxiao@21cn.com; zhilianzeng@gmail.com
Received: Jul. 13th, 2011; revised: Aug. 20th, 2011; accepted: Aug. 21st, 2011.

Abstract: In this paper, we give four general solutions satisfying the requirement of the conjecture for binary matrix equation $|E - 2\boldsymbol{A}| = q$. Many distinct solutions can be derived from the base solution, and the lower bound of the number of solutions can be determined, given the integer q. Furthermore, we study the properties of these base solutions, and find most of the solutions. We extend the result of François Arnault's paper [1], and solve the conjecture proposed by François Arnault proposed in [2].

Keywords: 2-adic Ring; FCSRs; ℓ-Sequences; Determinant

关于二进制矩阵方程猜想的一类新解

肖卿灿，曾志廉
广州大学数学与信息科学学院，广州
Email: qcxiao@21cn.com; zhilianzeng@gmail.com
收稿日期：2011 年 7 月 13 日；修回日期：2011 年 8 月 20 日；录用日期：2011 年 8 月 21 日

摘　要：本文给出了二进制矩阵方程$|E - 2\boldsymbol{A}| = q$满足猜想要求的四个通解，由此基础解衍生出不同的解，根据具体的q就能确定出不同的解个数的下限，在此基础上进一步研究解的性质，进而求出大部分的解。我们的结论推广了 François Arnault 等人在文[1]的结果，解决了 François Arnault 在文[2]中提出的猜想问题。

关键词：2-adic 环；FCSRs；ℓ序列；行列式

1. 引言

关于代数攻击和具有移位寄存器的反馈(FCSRs)问题很多人进行了研究，如 François Arnault 及 Thierry P. Berger[3]等人，在密码学和伪随机序列产生时使用，设计者不希望攻击者容易猜测到寄存器的内容，这要求内部状态有高熵。密码学中的矩阵方法是近两年来时兴的研究方法，为了增加破解难度，François Arnault 通过构造每行或每列至多有两个元素不为零的二进制矩阵 $\boldsymbol{A}$ 加以解决，他们构造了具有 FCSRs 的两个转移矩阵如下(其中 $\boldsymbol{A}$ 是$|E-2\boldsymbol{A}| = q$ 的解，q 为负奇数，$h = [\log_2(-q)]$，$n = h + 1$ 或 h，$\boldsymbol{A}$ 的元素 $\in \{-1,0,1\}$)：

$$\boldsymbol{A}_{G1} = \begin{pmatrix} r_0 & 1 & & & & \\ r_2 & 0 & 1 & & (0) & \\ r_3 & & 0 & 1 & & \\ \vdots & & & \ddots & \ddots & \\ r_{n-1} & & (0) & & 0 & 1 \\ 1 & & & & & 0 \end{pmatrix} \quad \boldsymbol{A}_{Fn} = \begin{pmatrix} 0 & 1 & & & & \\ & 0 & \ddots & & (0) & \\ & & \ddots & 1 & & \\ & (0) & & 0 & 1 & \\ & & & & 0 & 1 \\ 1 & r_{n-1} & \cdots & r_3 & r_2 & r_0 \end{pmatrix}$$

$$\left|E-2\boldsymbol{A}\right|=-2n-\sum_{j=2}^{n-1}r_j2^j+d_0,\quad r_0=\frac{1-\left(-1\right)^{\frac{1-q}{2}}}{2},\quad d_0=\left(-1\right)^{\frac{1-q}{2}}$$

François Arnault 在文[2]中猜测对于任意的负奇数 q 存在着在 $\boldsymbol{A}_{G_0}$ 或 $\boldsymbol{A}_{F_0}$ 基础上每行或每列至多只添加进一个非零元素的情况，使得在每行或每列至多有两个元素不为零的情况下，转移矩阵 $\boldsymbol{A}$ 满足$|E-2\boldsymbol{A}|=q$。

$$\boldsymbol{A}_{G_0}=\begin{pmatrix}r_0 & 1 & & & & \\ 0 & 0 & 1 & & (0) & \\ 0 & & 0 & 1 & & \\ \vdots & & & \ddots & \ddots & \\ 0 & & (0) & & 0 & 1 \\ 1 & & & & & 0\end{pmatrix}\quad \boldsymbol{A}_{F_0}=\begin{pmatrix}0 & 1 & & & & \\ & 0 & 1 & & (0) & \\ & & 0 & 1 & & \\ & (0) & & \ddots & \ddots & \\ & & & & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 & r_0\end{pmatrix} \tag{1}$$

本文给出了完整的存在性证明，在 $\boldsymbol{A}\neq\boldsymbol{A}_{G_0}$ 或 $\boldsymbol{A}_{F_0}$ 时，对于给定的 q，至少有四个 $\boldsymbol{A}$ 同时满足$|E-2\boldsymbol{A}|=q$，并给出 $\boldsymbol{A}$ 的四个通项公式。

下面先回顾一下行列式的定义，假设

$$\boldsymbol{D}=\begin{vmatrix}a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn}\end{vmatrix}$$

是由排成 n 阶方阵形式的 n^2 个数 $a_{ij}\left(i,j=1,2,\cdots,n\right)$ 确定的一个数，其值为 $n!$ 项之和 $\boldsymbol{D}=\sum\left(-1\right)^{\eta}a_{1\eta_1}a_{2\eta_2}\cdots a_{n\eta_n}$ 式中 $\eta_1,\eta_2,\cdots,\eta_n$ 是将序列1,2,$\cdots$,n 的元素次序交换 η 次所得到的一个序列，∑号表示对 $\eta_1,\eta_2,\cdots,\eta_n$ 取遍1,2,$\cdots$,n 的一切排列求和，那么数 $\boldsymbol{D}$ 称为 n 阶方阵相应的行列式。

2. 引理及定理证明

引理 1 设 x 为正整数，令 $h=[\log_2(x)]$，则对于任意一个正整数 x 均可化成两两不相邻的 2^i 的幂级数形式，其系数 $C\in\left\{-1,0,1\right\}^{h+1}$，其项数$\leq\left[n/2\right]+1$。

证明 当 x 为正偶数时，令 $x=2^{j_0}k_0$，$(2,k_0)=1$,若 $k_0=1$，则命题成立；若 $k_0>1$，不失一般性，只须证明 x 为正奇数的情形。由于对于任意的正奇数 x 均可表成 $4k\pm1$ 的形式，取 $c_0=\pm1$，则 $x=4k+c_0=2^{2+i_1}k_1+c_0$，(2, k_1) = 1,若 $k_1=1$，则命题成立；若 $k_1>1$，则 k_1 同样可表成 $4k_2\pm1$ 的形式，即 $k_1=4k_2\pm1$，同样取 $c_1=\pm1$，则 $k_1=4k_2\pm1=2^{2+i_2}k_3+\mathrm{c}_1$，$(2,k_3)=1$ 此时 $x=4k+c_0=2^{2+i_1}k_1+c_0=2^{4+i_1+i_2}k_3+c_12^{2+i_1}+c_0$

若 $k_3=1$，则命题成立；若 $k_3>1$，则 $k_3=4k_4\pm1$，同样地取 $c_2=\pm1$，则 $k_3=2^{2+i_3}k_5+c_2$，$(2,k_5)=1$，此时 $x=2^{6+i_1+i_2+i_3}k_5+c_22^{4+i_1+i_2}+c_12^{2+i_1}+c_0$

若 $k_5=1$，则命题成立；若 $k_5>1$，则这个过程不断地继续下去，经过有限次之后，最后总存在正整数 s 使得 $k_s=1$。令 $j_t=\sum_{e=1}^{t}i_e$，则

$$x=\sum_{l=0}^{m}c_l2^{2l+j_l} \tag{2}$$

其中 $j_0=0$，$c_m=1$，$n=2m+j_m$，由构造性证明过程易知其系数不为零的项数 $m+1\frac{n-j_m}{2}+1\leq\left[\frac{n}{2}\right]+1$ 证毕。

一般情况下，当 $2^h+2^{h-2}<x<2^{h+1}$ 时，取次数 $n=h+1$，当 $2^h<x<2^h+2^{h-2}$，取次数 $n=h$。参考文献[1]和[2]的方法我们容易证明引理 2。

引理 2 设 q 为负奇数，$r_0=\frac{1-\left(-1\right)^{\frac{1-q}{2}}}{2}$，$d_0=\left(-1\right)^{\frac{1-q}{2}}$，$y_i$ 为实数，$1\leq i\leq n$，令

$$\hat{\mathrm{A}}=\begin{pmatrix} d_0 & -2 & & & & \\ & 1 & -2 & & (0) & \\ & & 1 & -2 & & \\ & & & \ddots & \ddots & \\ & & (0) & & 1 & -2 \\ y_n & y_{n-1} & \cdots & y_3 & y_2 & y_1 \end{pmatrix},\ \text{则}\left|\hat{\mathrm{A}}\right|=y_n 2^{n-1}+d_0\sum_{i=1}^{n-1}y_i 2^{i-1} \tag{3}$$

定理 1 设 q 为负奇数，$r_0=\dfrac{1-(-1)^{\frac{1-q}{2}}}{2}$，$d_0=(-1)^{\frac{1-q}{2}}$，取 $h=[\log_2(-q)]$，令 $n=h+1$ 或 h，构造 n 阶方阵 $\boldsymbol{A}$：首先 $a_{n,1}=1$，$a_{i,i+1}=1,\ i=1,\cdots,n-1$，在此基础上添加元素，方阵 $\boldsymbol{A}_{G_0}$ 添加 $a_{1,1}=r_0$，方阵 $\boldsymbol{A}_{F_0}$ 添加 $a_{n,n}=r_0$，$\boldsymbol{A}_G$ 和 $\boldsymbol{A}_F$ 的具体构造如下：

1) 方阵 $\boldsymbol{A}_G$ 的构造

在 $\boldsymbol{A}_{G_0}$ 基础上添加 $a_{n-j,1+j}=r_{n-2j},\ a_{n-j-1,1+j}=r_{n-2j-1}$，第 $\left[\dfrac{n+3}{2}\right]$ 行第 $\left[\dfrac{n-1}{2}\right]$ 列中的元素为 r_3，第 $\left[\dfrac{n+2}{2}\right]$ 行第 $\left[\dfrac{n}{2}\right]$ 列中的元素为 r_2，其余都为零。

$$\boldsymbol{A}_G=\begin{pmatrix} r_0 & 1 & & & & & & & & \\ & 0 & 1 & & & & & & & \\ & & 0 & \ddots & & & & & & \\ & & & \ddots & 1 & & & & & \\ & & & & 0 & 1 & & & & \\ & & & & & 0 & 1 & & & \\ & & & & r_3 & r_2 & 0 & 1 & & \\ & & & \iddots & r_4 & & & 0 & 1 & \\ & & r_{n-5} & \iddots & & & & & 0 & \ddots \\ & r_{n-3} & r_{n-4} & & & & & & \ddots & 1 \\ 0 & r_{n-2} & & & & & & & & 0 \\ 1 & & & & & & & & & 0 \end{pmatrix}\text{或}\begin{pmatrix} r_0 & 1 & & & & & & & & \\ & 0 & 1 & & & & & & & \\ & & \ddots & \ddots & & & & & & \\ & & & & 0 & 1 & & & & \\ & & & & & 0 & 1 & & & \\ & & & & & r_2 & 0 & 1 & & \\ & & & & r_4 & r_3 & & 0 & 1 & \\ & & & \iddots & \iddots & & & & \ddots & \ddots \\ & & r_{n-3} & r_{n-4} & & & & & 0 & 1 \\ & 0 & r_{n-2} & & & & & & & 0 \\ 1 & & & & & & & & & 0 \end{pmatrix} \tag{4}$$

n 为偶数　　n 为奇数

另外 $\boldsymbol{A}_G$ 还有第二种构造方法：在 $\boldsymbol{A}_{G_0}$ 基础上添加 $a_{n-j,1+j}=r_{n-2j},\ a_{n-j,2+j}=r_{n-2j-1}$，第 $\left[\dfrac{n+5}{2}\right]$ 行第 $\left[\dfrac{n+1}{2}\right]$ 列中的元素为 r_3，第 $\left[\dfrac{n+4}{2}\right]$ 行第 $\left[\dfrac{n+2}{2}\right]$ 列中的元素为 r_2，其余都为零。

$$\boldsymbol{A}_G=\begin{pmatrix} r_0 & 1 & & & & & & & & \\ & 0 & 1 & & & & & & & \\ & & \ddots & \ddots & & & & & & \\ & & & 0 & 1 & & & & & \\ & & & & 0 & 1 & & & & \\ & & & & & 0 & 1 & & & \\ & & & & r_3 & r_2 & 0 & 1 & & \\ & & & \iddots & \iddots & & & \ddots & \ddots & \\ & & r_{n-3} & r_{n-4} & & & & & 0 & 1 \\ 1 & 0 & r_{n-2} & & & & & & & 0 \end{pmatrix}\text{或}\begin{pmatrix} r_0 & 1 & & & & & & & & \\ & 0 & 1 & & & & & & & \\ & & \ddots & \ddots & & & & & & \\ & & & & 0 & 1 & & & & \\ & & & & & 0 & 1 & & & \\ & & & & & r_2 & 0 & 1 & & \\ & & & & r_4 & r_3 & & \ddots & \ddots & \\ & & & \iddots & \iddots & & & & 0 & 1 \\ & & r_{n-3} & r_{n-4} & & & & & & 0 \\ 1 & 0 & r_{n-2} & & & & & & & 0 \end{pmatrix} \tag{5}$$

n 为偶数　　n 为奇数

2) 对于 $\boldsymbol{A}_F$ 而言，构造如下：在 $\boldsymbol{A}_{F_0}$ 基础上添加 $a_{n-j-2,j}=r_{n-2j}$，$a_{n-j-3,j}=r_{n-2j-1}$，第 $\left[\frac{n+1}{2}\right]$ 行第 $\left[\frac{n-3}{2}\right]$ 列中的元素为 r_3，第 $\left[\frac{n}{2}\right]$ 行第 $\left[\frac{n-2}{2}\right]$ 列中的元素为 r_2，其余都为零(详见(6)式)。

$$\boldsymbol{A}_F=\begin{pmatrix}
0 & 1 & & & & & & & & & & & & \\
 & 0 & 1 & & & & & & & & & & & \\
 & & 0 & \ddots & & & & & & & & & & \\
 & & & \ddots & 1 & & & & & & & & & \\
 & & & & 0 & 1 & & & & & & & & \\
 & & & r_3 & r_2 & 0 & 1 & & & & & & & \\
 & & \iddots & r_4 & & & 0 & 1 & & & & & & \\
 & r_{n-5} & \iddots & & & & & 0 & 1 & & & & & \\
r_{n-3} & r_{n-4} & & & & & & & 0 & \ddots & & & & \\
r_{n-2} & & & & & & & & & \ddots & 1 & & & \\
0 & & & & & & & & & & 0 & 1 & & \\
1 & & & & & & & & & & & & r_0
\end{pmatrix}$$

或

$$\begin{pmatrix}
0 & 1 & & & & & & & & & & & & \\
 & 0 & 1 & & & & & & & & & & & \\
 & & \ddots & \ddots & & & & & & & & & & \\
 & & & & 0 & 1 & & & & & & & & \\
 & & & & r_2 & 0 & 1 & & & & & & & \\
 & & & r_4 & r_3 & & 0 & 1 & & & & & & \\
 & \iddots & \iddots & & & & & 0 & 1 & & & & & \\
r_{n-3} & r_{n-4} & & & & & & & \ddots & \ddots & & & & \\
r_{n-2} & & & & & & & & & 0 & 1 & & & \\
0 & & & & & & & & & & 0 & 1 & & \\
1 & & & & & & & & & & & & r_0
\end{pmatrix}$$

(6)

n 为偶数　　n 为奇数

$$\boldsymbol{A}_F=\begin{pmatrix}
0 & 1 & & & & & & & & & & & & \\
 & 0 & 1 & & & & & & & & & & & \\
 & & 0 & \ddots & & & & & & & & & & \\
 & & & \ddots & 1 & & & & & & & & & \\
 & & & & 0 & 1 & & & & & & & & \\
 & & & & & 0 & 1 & & & & & & & \\
 & & & r_3 & r_2 & 0 & 1 & & & & & & & \\
 & & \iddots & r_4 & & & 0 & 1 & & & & & & \\
 & r_{n-5} & \iddots & & & & & 0 & \ddots & & & & & \\
 & r_{n-3} & r_{n-4} & & & & & & \ddots & 1 & & & & \\
0 & r_{n-2} & & & & & & & & 0 & 1 & & & \\
1 & & & & & & & & & & & & r_0
\end{pmatrix}$$

或

$$\begin{pmatrix}
0 & 1 & & & & & & & & & & & & \\
 & 0 & 1 & & & & & & & & & & & \\
 & & \ddots & \ddots & & & & & & & & & & \\
 & & & & 0 & 1 & & & & & & & & \\
 & & & & & 0 & 1 & & & & & & & \\
 & & & & r_2 & 0 & 1 & & & & & & & \\
 & & & r_4 & r_3 & & 0 & 1 & & & & & & \\
 & & \iddots & \iddots & & & & \ddots & \ddots & & & & & \\
 & r_{n-3} & r_{n-4} & & & & & & & 0 & 1 & & & \\
0 & r_{n-2} & & & & & & & & & 0 & 1 & & \\
1 & & & & & & & & & & & & r_0
\end{pmatrix}$$

(7)

n 为偶数　　n 为奇数

另外 $\boldsymbol{A}_F$ 还有第二种构造方法：在 $\boldsymbol{A}_{F_0}$ 基础上添加 $a_{n-j-2,j}=r_{n-2j}$，$a_{n-j-2,j+1}=r_{n-2j-1}$，第 $\left[\frac{n+3}{2}\right]$ 行第 $\left[\frac{n-1}{2}\right]$ 列中的元素为 r_3，第 $\left[\frac{n+2}{2}\right]$ 行第 $\left[\frac{n}{2}\right]$ 列中的元素为 r_2，其余都为零(详见(7)式)。

则对于以上八个行列式皆有

$$\left|E-2\boldsymbol{A}\right|=-2^n-d_0\left(r_{n-2}2^{n-2}+r_{n-3}2^{n-3}+\cdots r_{n-3}2^{n-3}+r_3 2^3+r_2 2^2\right)+d_0 \tag{8}$$

证明 我们先对(4)式的第一式计算$|E-2\boldsymbol{A}|$

$$\left|E-2\boldsymbol{A}_G\right|=\begin{vmatrix} d_0 & -2 & & & & & & & & & & & \\ & 1 & -2 & & & & & & & & & & \\ & & 1 & \ddots & & & & & & & & & \\ & & & \ddots & -2 & & & & & & & & \\ & & & & 1 & -2 & & & & & & & \\ & & & & & 1 & -2 & & & & & & \\ & & & & -2r_3 & -2r_2 & 1 & -2 & & & & & \\ & & & \iddots & -2r_4 & & & 1 & -2 & & & & \\ & & -2r_{n-5} & \iddots & & & & & \ddots & \ddots & & & \\ & -2r_{n-3} & -2r_{n-4} & & & & & & & 1 & -2 & & \\ & -2r_{n-2} & & & & & & & & & 1 & -2 & \\ -2 & & & & & & & & & & & 1 & \end{vmatrix} \tag{9}$$

第 n 行乘以 2 加到第 $n-1$ 行，第 $n-1$ 行乘以 2 加到第 $n-2$ 行，…，第$\left[\frac{n}{2}\right]$乘以 2 加到第$\left[\frac{n+2}{2}\right]$行，取 $\upsilon = \left[\frac{n+2}{2}\right]$，这样第 $\upsilon+1$ 列至第 n 列除主对角线上的元素为 1 外，其余均为 0。(υ,υ)位置上的元素为 1，则第 υ 行变为

$$\begin{pmatrix} -2^{\upsilon} & -2^{\upsilon-2}\left(2r_{n-2}+r_{n-3}\right) & -2^{\upsilon-3}\left(2r_{n-4}+r_{n-5}\right) & L & -2\left(2r_4+r_3\right) & -2r_2 & 1 & 0 & L & 0 \end{pmatrix}$$

由(1,1) - (υ,υ)位置所组成的行列式为引理 2 中(3)式的形式，把 $y_n=-2^{\upsilon}$，$y_{n-1}=-2^{\upsilon-2}(2r_{n-2}+r_{n-3})$，…，$y_3=-2(2r_4+r_3)$，$y_2=-2r_2$，$y_1=1$ 代入(3)式结合引理 2 可得

$$\begin{aligned}\left|E-2\boldsymbol{A}_G\right| &= -2^{\upsilon}2^{n-\upsilon}-2^{\upsilon-2}\left(2r_{n-2}+r_{n-3}\right)2^{n-\upsilon-1}d_0-\cdots-2\left(2r_4+r_3\right)d_0 2^2-2\cdot 2r_2+d_0 \\ &= -2^n-d_0\left(r_{n-2}2^{n-2}+r_{n-3}2^{n-3}+\cdots+r_{n-3}2^{n-3}+r_3 2^3+r_2 2^2\right)+d_0\end{aligned}$$

方法二：令 $\Gamma=E-2\boldsymbol{A}$，当$|\Gamma|=2^n\pm 1$ 时，命题显然成立，不失一般性，不妨设 r_j 不全为零($j=2,\cdots,n-2$)，Γ 在$(n,1)$位置上的代数余子式为$(-1)^{n+1}((-2)^{n-1})=2^{n-1}$，在$(n,n)$位置上的代数余子式为$(-1)^{n+n}\beta_1=\beta_1$，利用拉普拉斯展开定理我们有

$$|\Gamma|=-2\cdot 2^{n-1}+\beta_1=-2^n+\beta_1$$

对于 $n-1$ 阶行列式 β_1 在$(n-1,2)$位置上的余子式为主对角线上除第一个元素为 d_0 外其余元素均为–2 的下三角形，其代数余子式为$(-1)^{n-1+2}((-2)^{n-2-1}d_0)=2^{n-3}d_0$，在$(n-1,n-1)$位置上的代数余子式为 β_2，同样用拉普拉斯展开定理我们有

$$\beta_1=-2r_{n-2}(2^{n-3}d_0)+\beta_2=-d_0r_{n-2}2^{n-2}+\beta_2$$

若 $r_{n-2}\neq 0$，其余的均为零，则有 $\beta_2=d_0$，否则 β_2 在$(n-2,2)$位置上的余子式为主对角线上除第一个元素为 d_0 外其余元素均为–2 的下三角形，其代数余子式为$(-1)^{n-2+2}((-2)^{n-3-1}d_0)=2^{n-4}d_0$；$\beta_2$ 在$(n-2,3)$位置上的余子式为主对角线上除第一个元素为 d_0 和第二个元素为 1 外其余元素均为–2 的下三角形，其代数余子式为$(-1)^{n-2+3}((-2)^{n-3-2}d_0)=2^{n-5}d_0$，在$(n-2,n-2)$位置上的代数余子式为 β_3，同样用拉普拉斯展开定理我们有

$$\beta_2=-2r_{n-3}(2^{n-4}d_0)-2r_{n-4}(2^{n-5}d_0)+\beta_3=-d_0r_{n-3}2^{n-3}-d_0r_{n-4}2^{n-4}+\beta_3$$

若其余的均为零，则有 $\beta_3=d_0$，否则这个过程不断地继续下去，经过有限次之后(此种情形存在正整数 $s\leq \mathrm{INT}(n/2)$使得 $\beta_s=d_0$)，最后有

$$|E-2\boldsymbol{A}|=|\Gamma|=-2^n-d_0(r_{n-2}2^{n-2}+r_{n-3}2^{n-3}+\cdots+r_{n-3}2^{n-3}+r_3 2^3+r_2 2^2)+d_0$$

计算其余七个$|E-2\boldsymbol{A}|$可得出同样的结论。

当 $r_0 = 0$ 时 $d_0 = 1$，此时上面四种情形的矩阵 $\boldsymbol{A}$ 有两种是相同的，为此我们必须再构造一种情形，在 $\boldsymbol{A}_{G_0}$ 基础上添加 $a_{i,n-i} = r_{2i+1}, a_{i,n-i+1} = r_{2i}$，第 $\left\lceil \frac{n-3}{2} \right\rceil$ 行第 $\left\lceil \frac{n+4}{2} \right\rceil$ 列中的元素为 $r_{2\left\lceil \frac{n-1}{2} \right\rceil - 1}$，第 $\left\lceil \frac{n-2}{2} \right\rceil$ 行第 $\left\lceil \frac{n+5}{2} \right\rceil$ 列中的元素为 $r_{2\left\lceil \frac{n-2}{2} \right\rceil}$，至此我们完成 $\boldsymbol{A}_1$ 的构造。

$$\boldsymbol{A}_1 = \begin{vmatrix} 0 & 1 & & & & & & & r_3 & r_2 \\ & 0 & 1 & & & & & & \ddots & r_4 \\ & & \ddots & \ddots & & & & r_{n-3} & \ddots & \\ & & & 0 & 1 & & & r_{n-2} & & \\ & & & & 0 & 1 & & & & \\ & & & & & 0 & 1 & & & \\ & & & & & & \ddots & \ddots & & \\ & & & & & & & 0 & 1 & \\ & & & & & & & & 0 & 1 \\ 1 & & & & & & & & & 0 \end{vmatrix} \text{或} \begin{vmatrix} 0 & 1 & & & & & & & r_3 & r_2 \\ & 0 & 1 & & & & & & r_5 & r_4 \\ & & \ddots & \ddots & & & & \iddots & \iddots & \\ & & & 0 & 1 & & r_{n-2} & r_{n-3} & & \\ & & & & 0 & 1 & & & & \\ & & & & & 0 & 1 & & & \\ & & & & & & 0 & 1 & & \\ & & & & & & & \ddots & \ddots & \\ & & & & & & & & 0 & 1 \\ 1 & & & & & & & & & 0 \end{vmatrix} \tag{10}$$

n 为偶数　　n 为奇数

定理 2 设 $\boldsymbol{A}_1$ 为形如(10)式的 n 阶方阵，$r_i \in \{-1,0,1\}$，$i = 2,\cdots,n-2$，则

$$|E - 2\boldsymbol{A}_1| = -2^n - r_{n-2}2^{n-2} - r_{n-3}2^{n-3} - \cdots - r_3 2^3 - r_2 2^2 + 1$$

证明 我们先考察 $n-1$ 阶行列式 Ψ：

$$\Psi = \begin{vmatrix} -2 & & & & & & & & -2r_3 & -2r_2 \\ 1 & -2 & & & & & & & -2r_4 & \\ & 1 & \ddots & & & & & -2r_{n-3} & \ddots & \\ & & \ddots & -2 & & & & -2r_{n-2} & & \\ & & & 1 & -2 & & & & & \\ & & & & 1 & -2 & & & & \\ & & & & & \ddots & \ddots & & & \\ & & & & & & 1 & -2 & & \\ & & & & & & & 1 & -2 & \end{vmatrix} \text{或} \begin{vmatrix} -2 & & & & & & & & -2r_3 & -2r_2 \\ 1 & -2 & & & & & & & -2r_4 & \\ & 1 & \ddots & & & & & -2r_{n-4} & \ddots & \\ & & \ddots & -2 & & & -2r_{n-2} & -2r_{n-3} & & \\ & & & 1 & -2 & & & & & \\ & & & & 1 & -2 & & & & \\ & & & & & 1 & -2 & & & \\ & & & & & & \ddots & \ddots & & \\ & & & & & & & 1 & -2 & \\ & & & & & & & & 1 & -2 \end{vmatrix}$$

根据拉普拉斯行列式展开定理，Ψ 按第一行展开后有

$$\Psi = (-1)^{1+1}(-2)\alpha_1 + (-1)^{1+n-2}(-2r_3)(-2) + (-1)^{1+n-1}(-2r_2) = -2\alpha_1 + (-1)^{n+1}r_3 2^2 + 2(-1)^{n+1}r_2$$

同样对 α_1 根据拉普拉斯行列式展开定理，按第一行展开后有

$$\alpha_1 = (-2)\alpha_2 + (-1)^{1+n-4}(-2r_5)(-2)^2 + (-1)^{1+n-3}(-2r_2)(-2) = -2\alpha_2 + (-1)^n r_5 2^3 + (-1)^n r_4 2^2$$

此时 $\Psi = \alpha_2(-2)^2 + (-1)^{n+1}r_5 2^4 + (-1)^{n+1}r_4 2^3 + (-1)^{n+1}r_3 2^2 + 2(-1)^{n+1}r_2$

仿前可证，$\Psi = (-2)^{n-1} + (-1)^{n+1}(r_{n-2}2^{n-3} + r_{n-3}2^{n-4} + \cdots + r_3 2^2 + 2r_2)$

此时$|E - 2\boldsymbol{A}_1|$根据拉普拉斯行列式展开定理按第 n 行展开后有

$$|E - 2\boldsymbol{A}_1| = (-1)^{n+1}(-2)\Psi + 1 = -2^n - r_{n-2}2^{n-2} - r_{n-3}2^{n-3} - \cdots - r_3 2^3 - r_2 2^2 + 1$$

仍然为定理 1 的形式。

3. 结论

首先把负奇数 q 化成如下形式

$$q=-2^n-\sum_{j=2}^{n-2}b_j2^j+d_0 \tag{11}$$

$b_j\in\{-1,0,1\}$，取 $r_j=(-1)^{\frac{1-q}{2}}\quad b_j=d_0b_j$，$j=2,\cdots,n-2$

则前面所构造的方阵 $\boldsymbol{A}$ 都是$|E-2\boldsymbol{A}|=q$ 的解，根据引理 1，q 可化成

$$q=-2^n-\sum_{l=1}^{m-1}c_l2^{2l+j_l}+d_0,\quad i_l\geq 0,\quad 1\leq l\leq m,\quad j_t=\sum_{e=1}^{t}i_e,\quad n=2m+j_{m-1}+i_m \tag{12}$$

在此种情况下，b_j不为零的项两两不相邻，故利用 $r_j=d_0b_j$可知 r_j不为零的项也两两不相邻。这样我们就证明了对于任意一个负奇数 q，取 $h=[\log_2(-q)]$，令 $n=h+1$ 或 h，则存在着每行和每列至多有两个元素不为零的 n 阶方阵 $\boldsymbol{A}$ 满足$|E-2\boldsymbol{A}|=q$。

结合定理 1 和合定理 2 我们可得出更强的结论：

对于任意一个负奇数 q，取 $h=[\log_2(-q)]$，令 $n=h+1$ 或 h，n 的值可由$-q$ 表成(2)的形式唯一确定，当 $m\geq 1$，$n>8$ 时至少存在着 4 个每行和每列至多有两个元素不为零的 n 阶方阵 $\boldsymbol{A}$ 满足$|E-2\boldsymbol{A}|=q$。

4. 讨论及推广

其实当 $m=1$，$n=4$ 时，我们已经找到 4 个不同的解 $\boldsymbol{A}$，所以可把条件放宽至 $m\geq 1$，$n\geq 4$。当中间项即有奇数项又有偶数项时，(4)式和(7)式以副对角线作对称移动 r_j，$|\boldsymbol{A}-2E|$值不变。

我们在 $\boldsymbol{A}_{G_0}$ 基础上进一步考察在由$(n,1)$ - $(u+1,u)$位置所形成的矩形框内添加元素 $a_{i,j}$(其中 $a_{n,1}=1$，$1\leq j\leq u$, $u,1\leq i\leq n$)的情形(对于 $\boldsymbol{A}_{F_0}$ 的情形可类似处理)。令 $\upsilon=n-u$，$\Gamma=E-2\boldsymbol{A}$

$$\mathrm{B}=\begin{pmatrix}1&2&2^2&\cdots&2^{\upsilon-2}&2^{\upsilon-1}\\&1&\ddots&\ddots&\vdots&\vdots\\&&\ddots&2&2^2&2^3\\&&&1&2&2^2\\&&&&1&2\\&&&&&1\end{pmatrix},\ \mathrm{H}=\begin{pmatrix}1&&&&&\\2^{-1}d_0&1&&&&\\2^{-2}&2^{-1}&1&&&\\\vdots&\ddots&\ddots&\ddots&&\\2^{-u}&\cdots&2^{-2}&2^{-1}&1&\\2^{-u}&\cdots&2^{-3}&2^{-2}&2^{-1}&1\end{pmatrix},\ \mathrm{P}=\begin{pmatrix}\mathrm{E}_u&\\&\mathrm{B}\end{pmatrix},\ \mathrm{Q}=\begin{pmatrix}\mathrm{H}&\\&\mathrm{E}_{\upsilon-1}\end{pmatrix} \tag{13}$$

则有$|\mathrm{P}|=|\mathrm{Q}|=1$，$|E-2\boldsymbol{A}|=|\Gamma|=|\mathrm{P}|\cdot|\Gamma|=|\mathrm{P}\Gamma|=|\mathrm{P}\Gamma|\cdot|Q|=|\mathrm{P}\Gamma Q|$，先对 Γ 施行左乘 P 运算，运算后得到 $\mathrm{P}\Gamma$ 的第 $u+2$ 列至第 n 列元素除主对角线元素为 1 外，其余均为零。$(u+1,u+1)$位置上的元素为 1，此时 $\mathrm{P}\Gamma$ 的第 $u+1$ 行的前 u 个元素分别为

$$-2\sum_{i=1}^{\upsilon}a_{u+i,j}2^{i-1}=-\sum_{i=1}^{\upsilon}a_{u+i,j}2^i,\quad 1\leq j\leq u$$

由$(1,1)$ - $(u+1,u+1)$位置所组成的行列式为引理 2 中(3)式的形式，把 $y_{(u+1)-j+1}=-\sum_{i=1}^{\upsilon}a_{u+i,j}2^i$，$1\leq j\leq u$，$y_1=1$ 代入(3)式结合据引理 2 可得

$$\left|E-2\boldsymbol{A}\right|=\left|\mathrm{P}\Gamma\right|=-2^u\sum_{i=1}^{\upsilon}a_{u+i,1}2^i-d_0\sum_{j=2}^{u}2^{u+1-j}\sum_{i=1}^{\upsilon}a_{u+i,j}2^i+\mathrm{d}_0,\quad \upsilon=\mathrm{n}-u \tag{14}$$

若对 $\mathrm{P}\Gamma$ 再进行右乘 Q 运算，则 $\mathrm{P}\Gamma\mathrm{Q}$ 的第 1 行至第 u 行除$(u+1,u+2)$位置上的元素为-2 外，其余的均为 0，

这样就可对|PΓQ|运用行列式定义直接算出结果，其结果仍为(14)式。

对于 $\boldsymbol{A}_{F_0}$ 的情形，我们有

$$\left|E-2\boldsymbol{A}\right|=-2^{\upsilon}\sum_{j=1}^{u}a_{n,j}2^{j}-d_0\sum_{i=2}^{\upsilon}2^{\upsilon+1-i}\sum_{j=1}^{u}a_{u+i,j}2^{j}+\mathrm{d}_0,\quad \upsilon=n-u \tag{15}$$

当 $u=1$(参见(14)式)或 $\upsilon=1$(参见(15)式)即为 François Arnault 在文[1]中的结果。当 $u>1$ 时，令 $a_{n,1}=1, b_{i,1}=a_{i,1}$，$b_{i,j}=d_0a_{i,j}$，$u+1\le i\le n$，$1<j\le u$，则(14)可写成

$$\left|E-2\boldsymbol{A}\right|=\left|P\Gamma\right|=-2^{n}-\sum_{t=1}^{n-2}2^{n-t}\sum_{j\in\tau}b_{n-t+j-1,j}+d_0,\ \tau=\{\mathrm{j}:1\le t\le n-2, t+2-\upsilon\le j\le t+1, j\le u\} \tag{16}$$

若要满足猜想条件必须添加 $a_{1,1}=1$ 时 $j\ne 1$, $a_{n,n}=1$ 时 $j\ne t+1$，此时 τ 也可写成

$$\tau_u=\{j:2\le i\le \mathrm{n}-1,\ u+1\le i+j-1\le n, 1\le j\le u;\ a_{1,1}=1\text{ 时 }j\ne 1,\ a_{n,n}=1\text{ 时 }j\ne n+1-i\} \tag{17}$$

在$(n,1)$ - $(u+1,u)$位置所形成的矩形框内添加元素，每行每列至多只添加进一个非零元素，故有 2^{n-t} 的系数只能在$-\mathrm{b}_{n-t+j-1,j}$之中，也就是说 2^t 的系数$(1<t<n)$只出现在$(t+j-1,j)$位置上。对于 $a_{1,1}=1$ 时第 1 列不添加元素，对于 $a_{n,n}=1$ 时第 n 行不添加元素。

设 $a_\zeta(1<\zeta<n)$是满足猜想条件的一组解，a_ζ全部落在$(n,1)$ - $(u+1,u)$位置所形成的矩形框内，令 $h_\zeta=d_0a_\zeta$，利用(16)可知在$(n,1)$ - $(u+1,u)$位置所形成的矩形框内 h_t在$(t+j-1,j)$位置上$(2\le t\le\zeta)$任意移动都不会改变行列式 $|E-2\boldsymbol{A}|$的值，只要移动的结果满足猜想条件都是由此衍生的解。当 n 为偶数时最大的矩形框为 $n/2\times n/2$，n 为奇数时最大的矩形框为 $(n+1)/2\times(n-1)/2$ 和 $(n-1)/2\times(n+1)/2$，设 $m-1$ 为 a_ζ 中不为零的个数 $(m\le \mathrm{INT}(n/2))$，$a_{n,n}\ne 1$ 的情形其矩形框的最小高度为 $m-1$，从最小高度为 $m-1$ 的矩形框到最大的矩形框，再到最小宽度为 $m-1$ 的矩形框，依次在各矩形框内在$(t+j-1,j)$位置上移动各 h_t，得到满足猜想条件的不同解。

当中间项较少且 n 较大时，如 $m<n/4$，$n>30$ 时，(16)式中将出现较多空项，若在$(t+j-1,j)$位置上多填上一对符号相反的虚拟对 h_ζ，则$|E-2\boldsymbol{A}|$的值仍不变。对于给定的 q，找出满足猜想条件的虚拟对，重复以上步骤，找出符合条件的解。

同理对于上三角部分($d_0=-1$ 时，r_2 必须为零才可行)，在$(u,u+2)$ - $(1,n)$位置所形成的矩形框内添加元素 r_t，利用 $r_t=d_0b_t$，$2\le t$，2^t 的系数$(1<t<n)$只出现在$(\mathrm{i},n+1-t+i)$位置上。仿前可得出上三角部分的大部分解。

至此，对于每个给定的 q，我们能够求出大部分的解。为了防止虚拟对的出现我们只须把猜测的条件加强至：对于每个 t，最多只有一个落$(t+j-1,j)$位置上，或者最多只有一个出现在$(i,n+1-t+\mathrm{i})$位置上。特别强调填数的时候必须在同一矩形框内进行，若超出矩形框的范围就容易出错。例如：

$$\begin{vmatrix}
1 & -2 & & & & & & & & \\
 & 1 & -2 & & & & & & & \\
 & & 1 & -2 & & & & & & \\
 & & & 1 & -2 & & & & & \\
 & & & & 1 & -2 & & & & \\
0 & 0 & 0 & 0 & 2 & 1 & -2 & & & \\
0 & 0 & 0 & 2 & 0 & & 1 & -2 & & \\
0 & 0 & 2 & 0 & 0 & & & 1 & -2 & \\
0 & 0 & 0 & 0 & 0 & & & & 1 & -2 \\
-2 & & & & & & & & & -1
\end{vmatrix}=-1109
\qquad
\begin{vmatrix}
1 & -2 & & & & & & & & \\
 & 1 & -2 & & & & & & & \\
 & & 1 & -2 & & & & & & \\
0 & 0 & 2 & 1 & -2 & & & & & \\
0 & 0 & 0 & 0 & 1 & -2 & & & & \\
0 & 0 & 0 & & 0 & 1 & -2 & & & \\
0 & 2 & 0 & 0 & & & 1 & -2 & & \\
0 & 0 & 0 & & 0 & & & 1 & -2 & \\
0 & 0 & 0 & & & 2 & & & 1 & -2 \\
-2 & & & & & & & & & -1
\end{vmatrix}=-1173$$

第二式中 $r2$ 和 $r4$ 的移动超出了矩形框的范围，故出错。

5. 构造方法

设 q 为负奇数，$r_0=\frac{1-(-1)^{\frac{1-q}{2}}}{2}$，$d_0=(-1)^{\frac{1-q}{2}}$，根据引理 1，$q$ 可化成(12)式的形式，补齐系数为 0 的项，把它写成(11)式的形式。利用 $r_t=d_0b_t, 2\le t\le n-2$ 考察在$(n,1)$ - $(u+1,u)$位置所形成的矩形框内添加元素 r_t，每行每列至多只添加进一个非零元素，使得在每行或每列至多有两个元素不为零的情形。由上面的结论知 r_t 只能填在$(t+j-1,j)$位置上，据(17)式 j 必须满足 $j\in\tau_u$，利同(12)式可知，在$(n-(2+i_m)+j-1,j)$位置上 $rn-(2+i_m)$ 仅有 $3-r_0+i_m$ 种选法，上面我们已经构造满足猜想条件的 A(参见(4)~(7)及(10)式)，在此基础上沿着与主对角线平行的方向作平移变换，变换后若 $rn-(2+i_m)$的位置未越出边界，则仍为其解；当中间项即有奇数项又有偶数项时，(4)式和(7)式以副对角线作对称移动 r_j，$|\boldsymbol{A}-2E|$值不变，(5)式和(6)式作类似的变换，变换后若 $rn-(2+i_m)$ 的位置未越出边界，则$|\boldsymbol{A}-2E|$值不变。对于上三角的情形必须满足 $r2+i_1$ 未超出边界。

利同(12)式可知，在$(n-(2+i_m)+j-1,j)$位置上 $rn-(2+i_m)$仅有 $3-r_0+i_m$ 种选法，在$(n-(4+i_m+i_{m-1})+j-1,j)$位置上 $rn-(4+i_m+i_{m-1})$可能有 $3-r_0+i_m+i_{m-1}$ 种选法，令 $p_i=j_m-j_{m-i}$，$j_0=0$，对于在 $\boldsymbol{A}_{G_0}$ 基础上添加 $m-1$ 个不为零的元素($m\le \mathrm{INT}(n/2)$)，位于下三角位不同行不同列至多各添加一个元素使得每行和每列至多有两个元素不为零的情形。首先 $rn-(2+i_m)$填在$(n-(2+i_m),1)$位置上，接着 $rn-(4+i_m+i_{m-1})$ 填在$(n-(4+i_m+i_{m-1})+1,2)$位置上，$rn-(2j+p_i)$ 填在$(n-(2j+p_i)+j-1,j)$位置上，$r(2+i_1)$填在$(2+i_1+j-1,j)$位置上，若 i_l 全为零则仅有 $3-r_0$ 种填法$(1\le l\le m-1)$(定理 1 已给出)。若 i_l 不全为零，当 $m\ge 4$ 时 $rn-(4+i_m+i_{m-1})$ 填在$(n-(4+i_m+i_{m-1})+1,2)$位置上有 $3-r_0+i_m+i_{m-1}$ 种填法，则从最小高度为 $m-1$ 矩形框$((n,1)$ - $(n-m+2, n-m+1)$(开始出发扩大高度，沿着与主对角线平行的方向向左上角方向作平移变换 $2-r_0+i_m$ 次，在高度为 m 矩形框沿着与主对角线平行的方向在$(n-(2j+p_i)+j-1,j)$位置上移动部分 $rn-(2j+p_i)$位置得出满足条件的不同解，扩大矩形框的高度至 $m+1$，重复上述步骤，从最小高度为 $m-1$ 的矩形框到最大的矩形框(当 n 为偶数时最大的矩形框为 $n/2\times n/2$，n 为奇数时最大的矩形框为 $(n+1)/2\times(n-1)/2$ 和 $(n-1)/2\times(n+1)/2$，$a_{n,n}\ne 1$ 的情形其矩形框的最小高度为 $m-1$)，再到最小宽度为 $m-1$ 的矩形框，依次在各矩形框内在$(t+j-1,j)$位置上移动各 r_t，得到满足猜想条件的不同解。

同理对于上三角部分($d_0=-1$ 时，r_2 必须为零才可行)，在$(u,u+2)$ - $(1,n)$位置所形成的矩形框内添加元素 r_t，利用 $r_t=d_0b_t, 2\le t, 2^t$ 的系数$(1<t<n)$只出现在$(i,n+1-t+i)$位置上。仿前可得出上三角部分的大部分解。

6. 猜测

设 σ 为 $\mathrm{Max}\{\mathrm{Min}\{3-r_0+p_l,1+j_{m-l}-i_1\}:1\le l\le m-1\}$下标中最小的一个，我们猜测在下三角部可能有 $(1+r_0)\prod_{l=1}^{\sigma}(3-r_0+p_l)\prod_{l=1}^{m-2-\sigma}(1+j_{l+1}-i_1)$ 种填法；设 σ_1 为 $\mathrm{Max}\{\mathrm{Min}\{1-r_0+j_l, 1+p_{m-l}-i_m\}:1\le l\le m-1\}$下标中最小的一个，我们猜测在上三角部可能有 $(1+r_0)\prod_{l=1}^{\sigma_1}(1-r_0+j_l)\prod_{l=1}^{m-2-\sigma_1}(1+p_{l+1}-i_m)$ 种填法。

参考文献 (References)

[1] F. Arnault, T. P. Berger, C. Lauradoux, M. Minier and B. Pousse. A new approach for FCSRs. In: M. J. J. V. Rijmen Jr., R. Safavi-Naini (Eds.), Selected areas in cryptography. New York: Springer, 2009, 5867: 433-448.

[2] F. Arnault, T. P. Berger and B. Pousse. A matrix approach for FCSR automata. Cryptography and Communications, Springer Science + Business Media, 2011, 3(2): 109-139.

[3] T. P. Berger, M. Minier and B. Pousse. Software oriented stream ciphers based upon FCSRs in diversified mode. In: B. Roy, N. Sendrier (Eds.), INDOCRYPT 2009, Lecture notes in computer science. New York: Springer, 2009, 5922: 119-135.

