软件测试

1. 摘要

本报告对NTT和MSM的Matlab软件进行数据注入测试，主要测试软件算法执行结果的正确性。

1. 测试环境

Windows版本：windows 11。

Matlab版本：2017a。

1. 数据来源

数据来源为泰块科技公司提供的BLS12\_377椭圆曲线数据。数据为二进制，低位在前。

1. NTT算法软件测试

4.1 测试函数说明

主要测试的函数为BN\_NTT和BN\_parallelNTT。测试m文件为testNTT1024.m。

1. [s] = BN\_NTT( n,R,x,G,G\_inverse,N,N\_inverse,R2modN,nR\_inverse,type)

输入参数：

n：需要进行NTT变换的x中含有数据个数的2的幂次。

R:默认为2，表示二进制，暂时不用。

x：需要进行NTT变换的数据，二进制表示，元胞数据格式。

G：素数N的原根。

G\_inverse:原根的逆元。

N：有限域椭圆曲线的素数p。

N\_inverse：N对于R的逆元。其中R=2^256（区别于第二个参数R）。

R2modN：R^2对N的模。其中R=2^256（区别于第二个参数R）。

nR\_inverse：输入数据个数模N的逆元。

type：NTT变换的类型，1为NTT变换，-1为INTT变换。

输出参数：

s：NTT变换结果，元胞数据类型，二进制，低位在前。

1. [s]=BN\_parallelNTT( n1,n2,R,x,row,col,G,G\_inverse,N,N\_inverse,R2modN,

nR\_inverse1,nR\_inverse2,type)

输入参数：

n1：需要进行NTT变换的x分成矩阵的行数的2的幂次。

n2：需要进行NTT变换的x分成矩阵的列数的2的幂次。

R:默认为2，表示二进制，暂时不用。

x：需要进行NTT变换的数据，数据个数=n1\*n2，二进制表示，元胞数据格式。

row：需要进行NTT变换的x分成矩阵的行数，row=2^n1。

col：需要进行NTT变换的x分成矩阵的列数，col=2^n2。

G：素数N的原根。

G\_inverse:原根的逆元。

N：有限域椭圆曲线的素数p。

N\_inverse：N对于R的逆元。其中R=2^256（区别于第二个参数R）。

R2modN：R^2对N的模。其中R=2^256（区别于第二个参数R）。

nR\_inverse1：输入数据行数模N的逆元。

nR\_inverse2：输入数据列数模N的逆元。

type：NTT变换的类型，1为NTT变换，-1为INTT变换。

输出参数：

s：NTT变换结果，元胞数据类型，二进制，低位在前。

4.2 测试的m文件

testNTT1024.m为测试m文件。读入的数据包括以上两个测试函数的参数。parallelFlag为并行计算标志位，parallelFlag=1时，进行并行NTT计算；parallelFlag=0时，进行串行NTT计算。测试数据N位256位，包括3个补零位。即R=2^256。

1. NTT算法软件测试结果

测试数据大小位1024个。串并行运算测试结果均正确。给的NTT输入（变量名为inputdat\_mat）和输出数据(变量名为outputdata)Matlab部分截图如下图 1图 2所示。

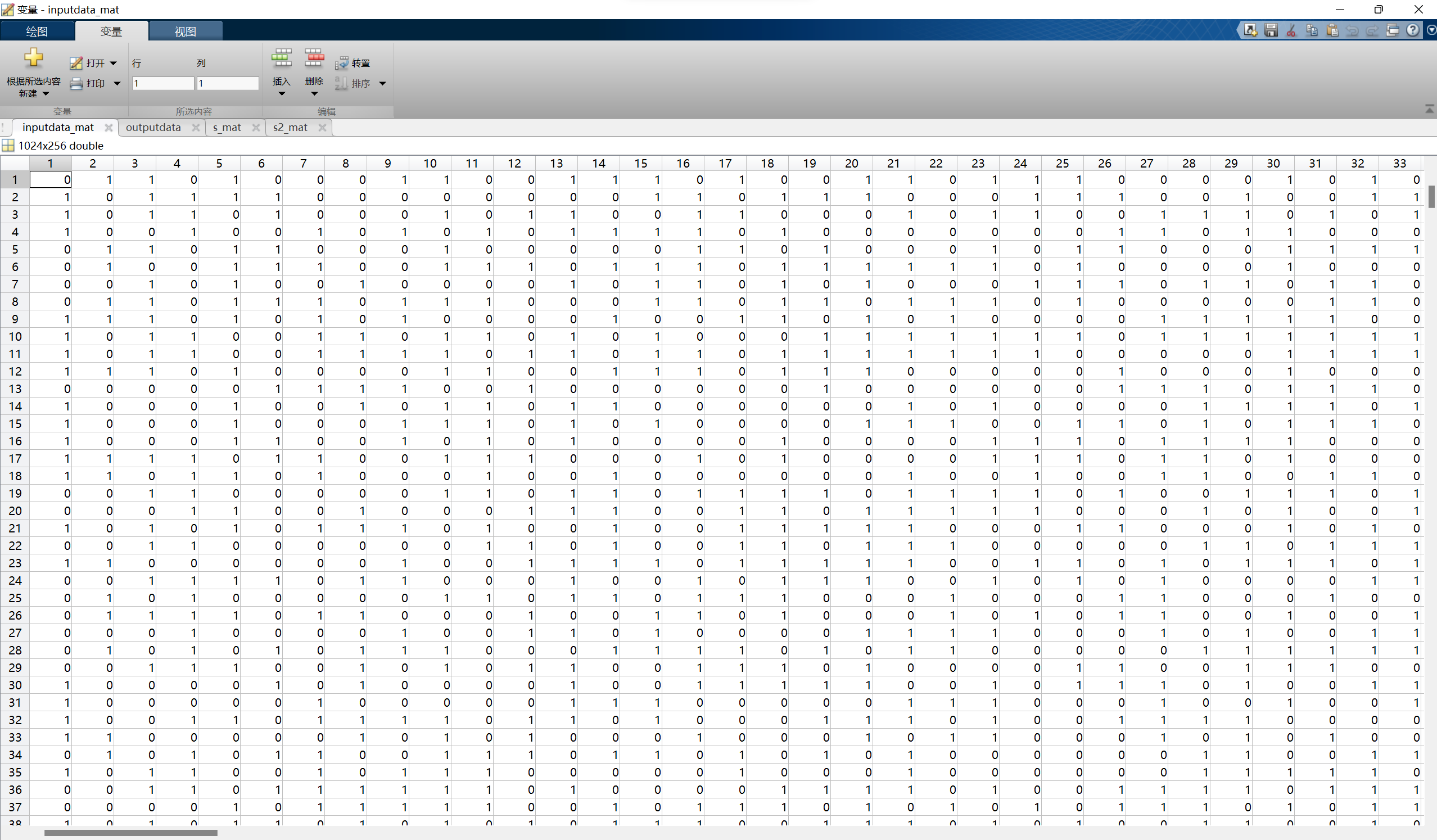


图 1 给的NTT输入数据

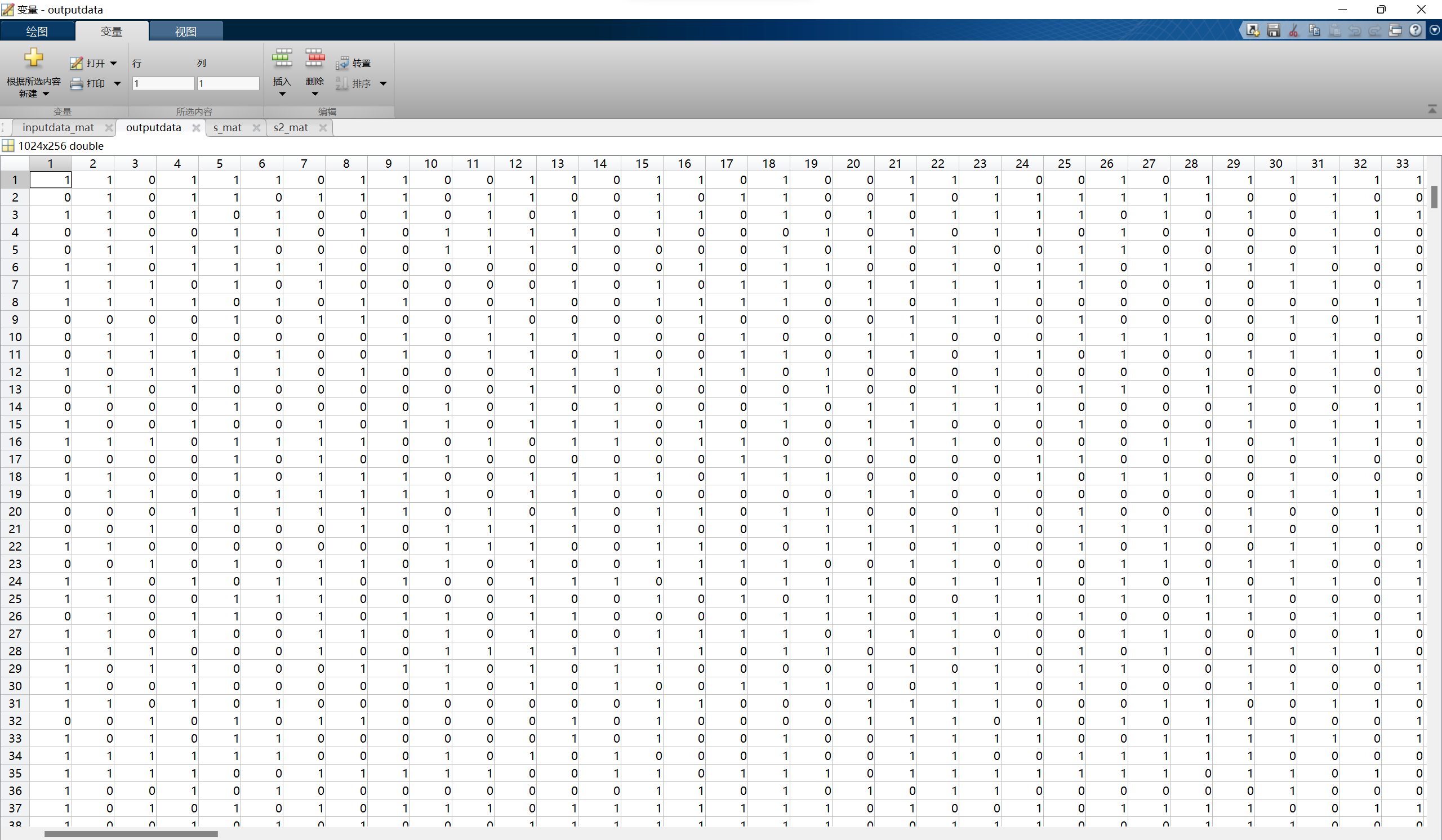


图 2 给的NTT输出数据

软件运行的NTT结果(变量名为s\_mat)和INTT(变量名为s2\_mat)结果Matlab部分截图如下图 3图 4所示。

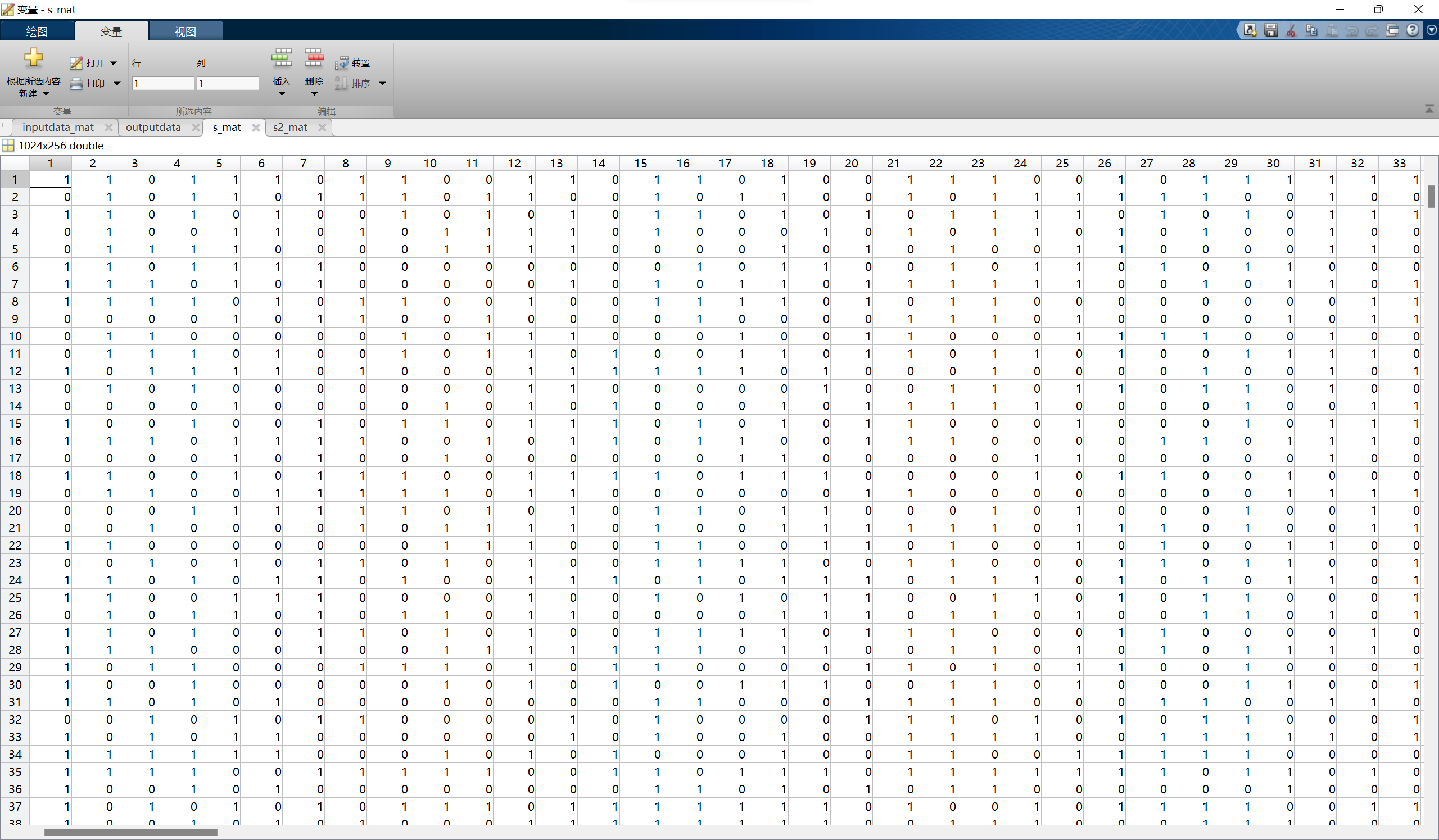


图 3 软件运行的NTT输出数据

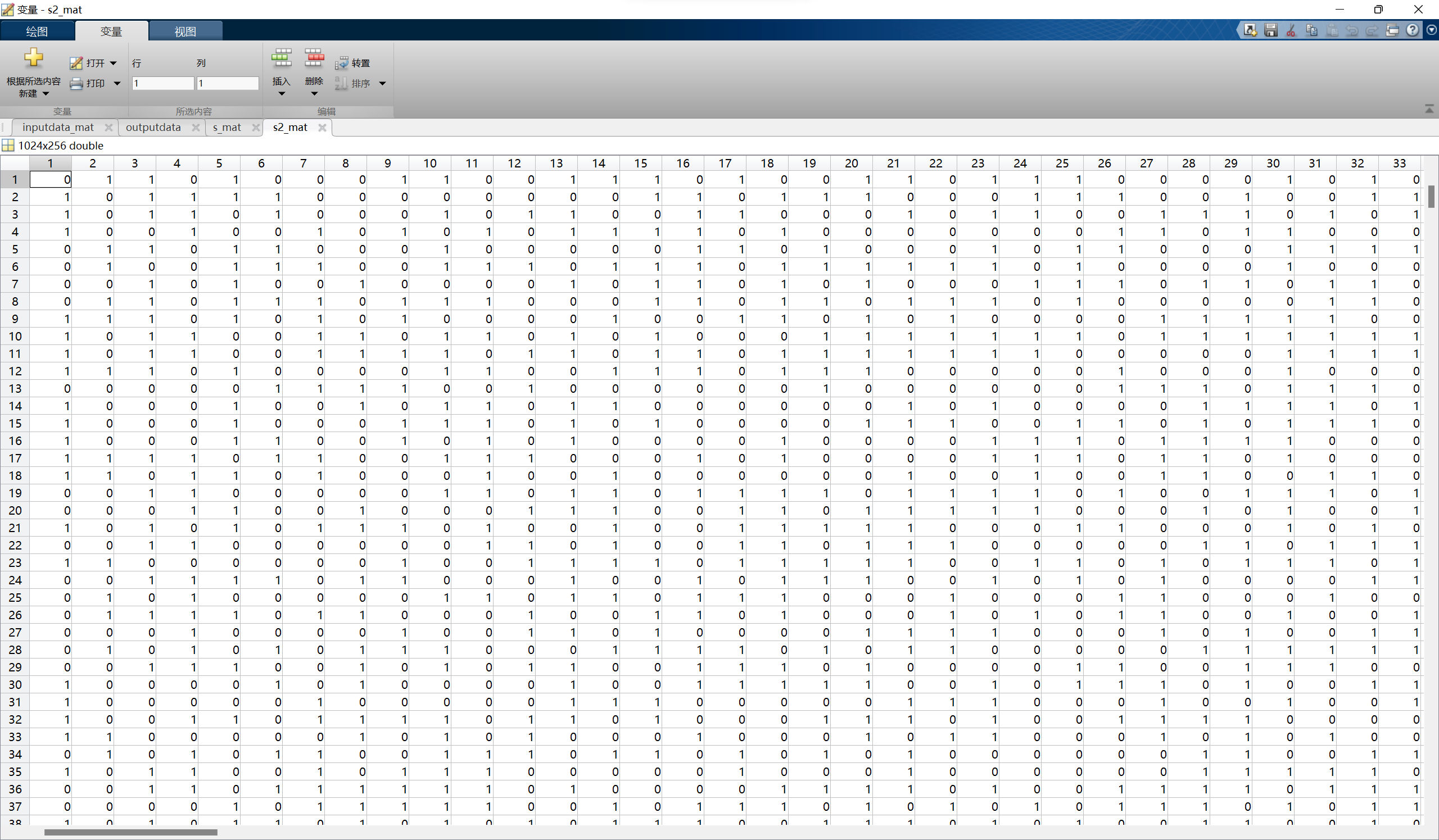


图 4 软件运行的INTT输出数据

由上四幅图，图 3结果对应图 2，图 4结果对应图 1。可以看到，测试结果完全正确。

1. MSM算法软件测试

6.1 测试函数说明

主要测试的函数为BN\_Pippenger（Pippenger算法实现椭圆曲线并行计算），BN\_Pippenger函数中调用了BN\_PADD（点加）、BN\_PMULT（倍乘）函数，涉及的算法主要是蒙哥马利和费马小定理。测试m文件为testMSM1024.m。

1. [x y] = BN\_Pippenger( n,R,s,x\_p,y\_p,k,N,a,b,N\_inverse,R2modN)

输入参数：

n：素数的计算位数。

R:默认为2，表示二进制，暂时不用。

s：选定的窗口大小，二进制计算位数，应为定值 论文中取4。

x\_p,y\_p：EC点P (x\_p,y\_p)-二进制，低位在前,x\_p和y\_p是矩阵，每一行为一个坐标。

k：标量乘法因子，低位在前，二进制矩阵，行数与x\_p相同。

N：有限域椭圆曲线的素数p。

a，b：椭圆曲线参数。

N\_inverse：N对于R的逆元。其中R=2^384（区别于第二个参数R）。

R2modN：R^2对N的模。其中R=2^384（区别于第二个参数R）。

输出参数：

[x y]：倍乘结果，二进制，低位在前。

6.2 测试的m文件

testMSM1024.m为测试m文件。读入的数据包括BN\_Pippenger函数的参数。测试数据N位384位。即R=2^384。

1. MSM算法软件测试结果

测试数据由甲方提供个。测试结果均正确。给的MSM输入（变量名为inputdat和inputdat\_k分别表示椭圆曲线坐标和标量因子）和输出数据(变量名为outputdata)Matlab部分截图如下图 5图 6图 7所示。

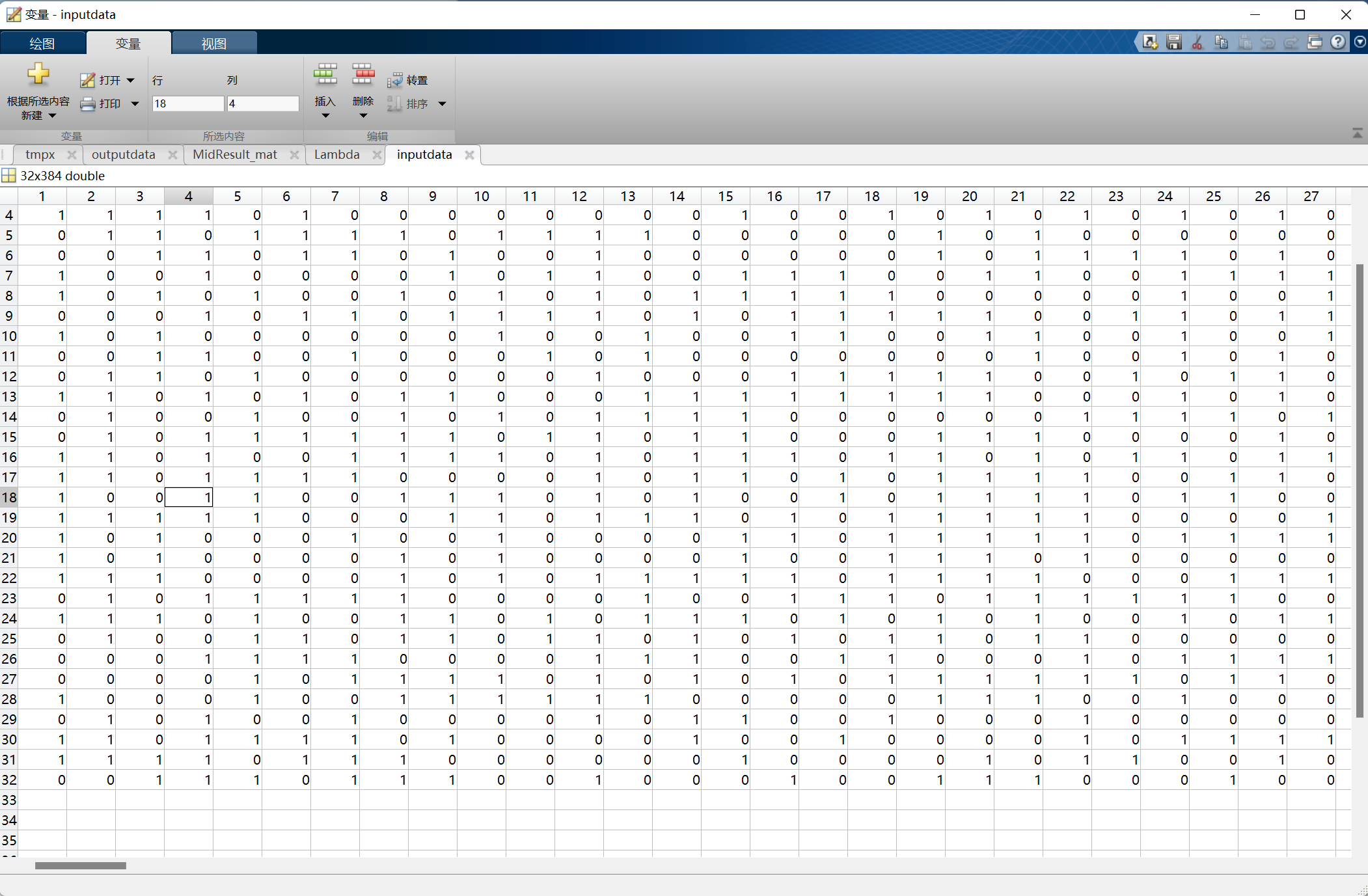


图 5 给的MSM输入椭圆曲线坐标数据

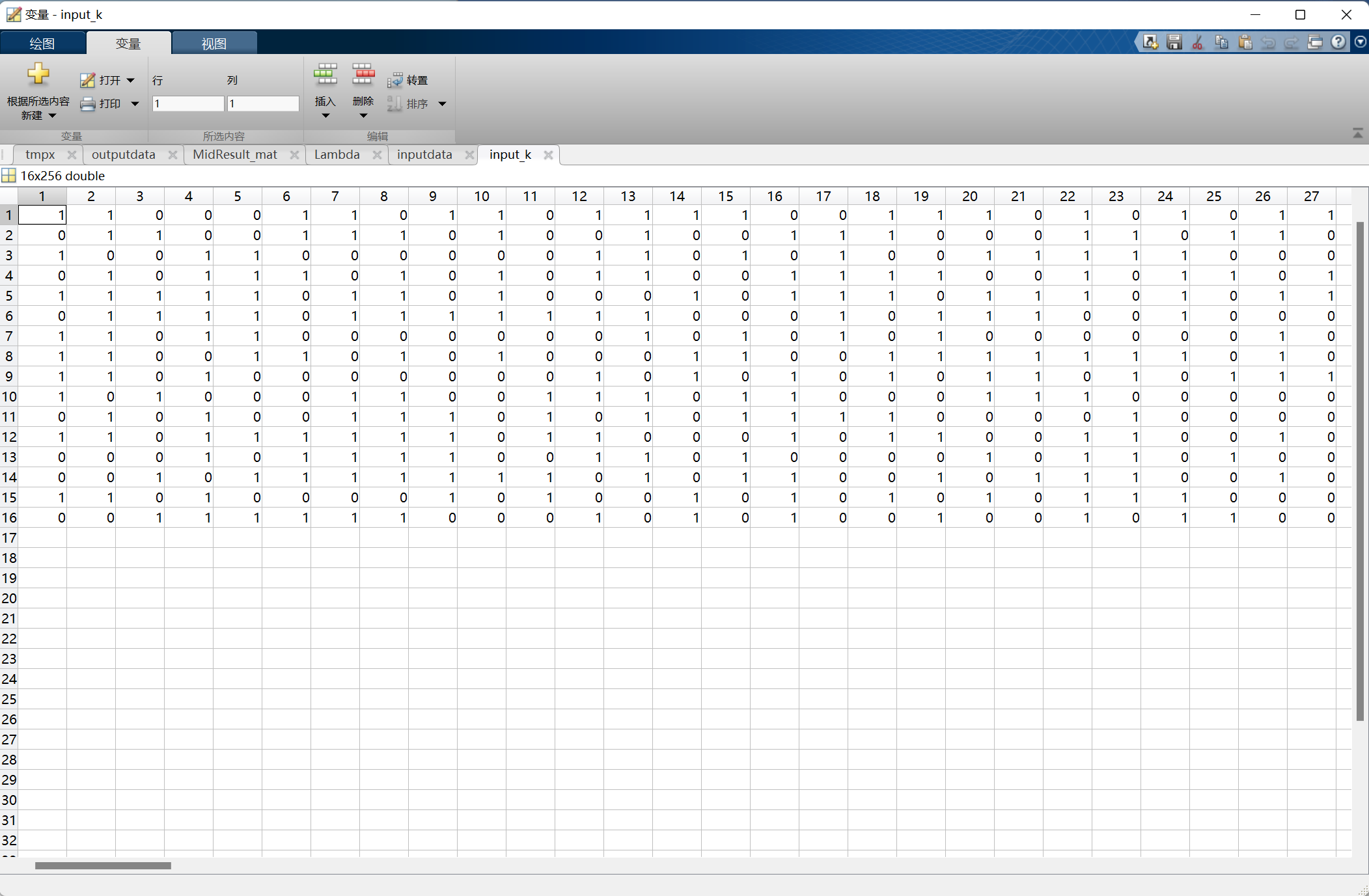


图 6 给的MSM输入标量因子

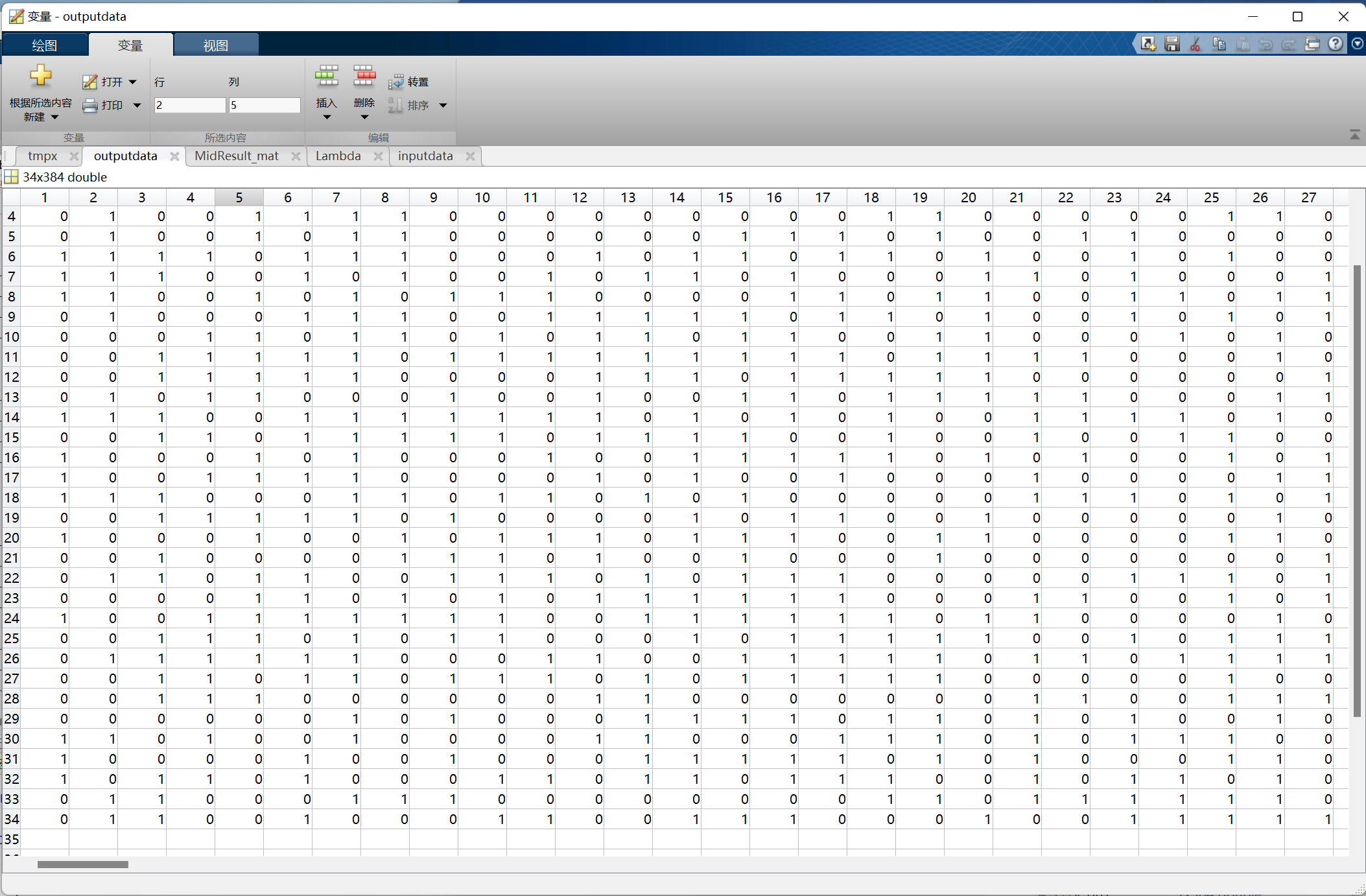


图 7 给的MSM输出数据

软件运行的MSM结果(变量名为MidResult\_mat) Matlab部分截图如下图 8所示。

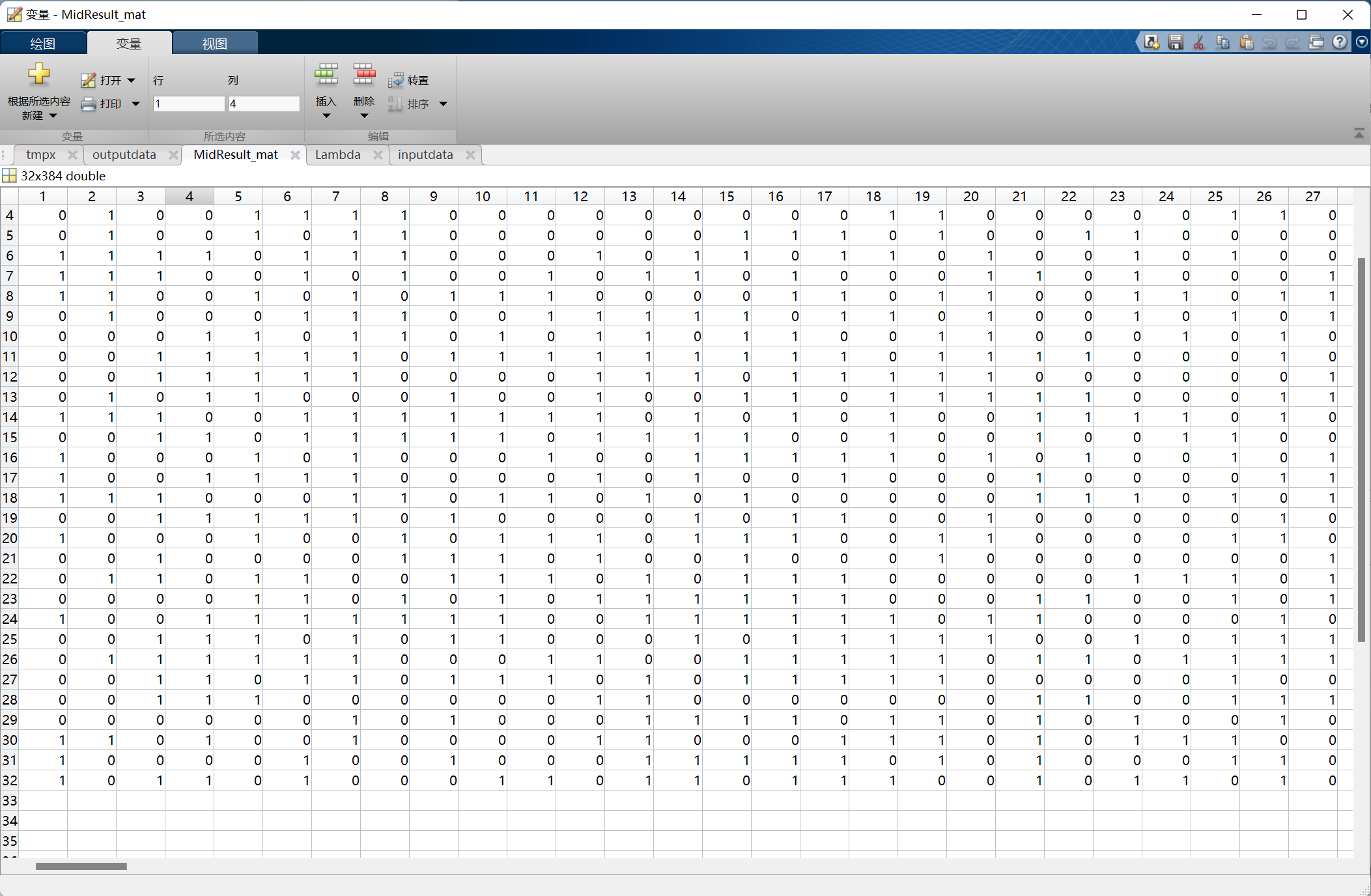


图 8 软件运行MSM结果

对比图 7和图 8，可以看到输出结果一致，测试结果完全正确。

1. 结论

本报告给出了NTT、INTT、MSM算法的Matlab仿真测试结果，代码运行结果与甲方给的输出结果完全一致，验证了仿真算法的正确性。标志本项目已完成第二阶段成果。