北京航空航天大學

基于矩阵的密码问题与简单应用

2011-4-1

北京航空航天大學

“冯如杯”参赛论文

基于矩阵的密码问题与简单应用

中文摘要

矩阵运算具有特殊性，尤其是矩阵乘法的线性相关性。我们现实生活中有很多模型，可以抽象成矩阵，来寻其规律，最后求解。我们可以利用旋转矩阵的良好性质，以及矩阵初等变换，产生随机矩阵，进而将普通密码改进为矩阵密码，以增强密码的随机性和安全性。本文中，笔者利用旋转矩阵设计了一种应用于电子锁具的密码，以及一种基于随机初等变换而产生并应用于智能操作系统的密码。

关键词： 矩阵 密码 初等变换 旋转

Abstract

The operation of matrix is different from the normal operation of numbers, especially the multiply of matrixes, which shows the linear independence. When faced with problems in life, we can use the model of matrix to look for the solutions. Just abstract the problem, convert it to a problem of matrix, then try to find the answer. The rotate matrix has the excellent character of rotating. We can use rotate matrix and the elementary transform of matrix to generate the random matrix and then promote the normal password to the password in matrix form. This kind of promotion may strengthen the safety and improve the random of password. In the following words, we design a lock which uses the password of rotating matrix. We also design an operating system which uses the elementary transform of matrix.

Key words: matrix, password, elementary transform, rotating

目录

第一章 引言

随着社会不断发展，人们越来越注重对特殊事务的保密工作，密码成为了必不可少的工具。

密码起源于古希腊雅典与斯巴达的一场战争。一对杂乱无章的字母被刻在腰带上。腰带呈螺旋形缠绕在手中的剑鞘上时，奇迹出现了。原来腰带上那些杂乱无章的字母，竟组成了一段文字。这边是最原始的密码。随着人类社会的发展，又不断衍生出了许多种类的密码，比如“RSA 算法”，“ECC 加密法”，四方密码等等一系列的密码。而这些密码有着一个共同的特点，就是按特定法则编成，用以对通信双方的信息进行秘密变换的符号。换而言之，密码是隐蔽了真实内容的符号序列。就是把用公开的、标准的信息编码表示的信息通过一种变换手段，将其变为除通信双方以外其他人所不能读懂的信息编码。

本文中，笔者以一种基于矩阵的运算法则来定义一种新的密码。

第二章 创意来源及公式推广

1.1 二维空间内的旋转矩阵

我们知道旋转矩阵在平面内，会有正交矩阵$\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}$满足

$$N^n=\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}^n=\begin{pmatrix}\cos n\theta & -\sin n\theta\\ \sin n\theta & \cos n\theta\end{pmatrix}$$

可以看出，矩阵 N 就是二维平面上的一个旋转算子。

这代表我们可以使向量 P 通过左乘矩阵 N 的幂指数来控制旋转的角度。

这样的结果使人想到：基于 N 矩阵具有这样好的性质，我们可以利用该矩阵来控制电路，从而控制某机械的转动角度。这样就免去了用手直接操作的转动。而且，利用 N 矩阵还有一个好处就是，比如我们要同时控制 t 个机械元件的旋转角度，我们可以利用对角阵的性质以及矩阵的分块运算，来实现用 t 个数控制一个机器中 t 维的旋转。

即：

令$N_i = \begin{pmatrix} \cos\theta_i & -\sin\theta_i \\ \sin\theta_i & \cos\theta_i \end{pmatrix}$ 对角阵 M=diag($N_1^{k_1}, N_2^{k_2} \cdots, N_t^{k_t}$) 其中$N_i^{k_i}$对应控制第 i 台机器的旋转情况。

我们再将其简化一些，就可以利用一个数组（$k_1, k_2, \cdots, k_t$）来控制 t 个旋转操作。也就是一个数组成为一个参数 K。这样，就免去了许多麻烦，而且，运用矩阵同时执行命令，机器的执行速度更快，效率会更高，运用到生产中会提高工效，进而提高产量。

比如我们设定的密码是（1,2,3,4,5）。那么，当我们输入密码时，旋转操作便被设定为了第一个机械元件逆时针方向旋转 1 倍的单位角θ_1，第二个元件逆时针 2 倍的θ_2，以此类推。当这个五维的旋转操作完成的时候，密码的效力也就结束了。

1.2 三维空间内的旋转矩阵

上面叙述的是利用二维空间上的旋转矩阵来完成旋转操作。那么我们自然可以想到，是不是也可以通过矩阵设计一个三维空间上的旋转操作呢？

那么下面我们来引入这样三个矩阵A_x, A_y, A_z

考虑空间中绕 z 轴的旋转操作：

如图 1，将向量$\vec{p} = (x, y, z)$绕 z 轴旋转 α 角得到$\overrightarrow{p'} = (x', y', z')$.

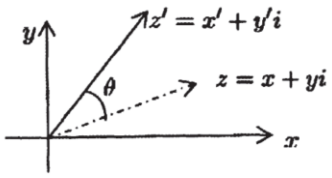

图 1 向量$\vec{p} = (x, y, z)$绕 z 轴旋转图

利用矩阵的分块运算，

即关系式$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}=\begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix}$

得到在三维空间中的坐标系下绕 z 轴旋转的矩阵为

$$A_z=\begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

同理，不难验证，绕 x y 轴旋转的矩阵分别为

$$A_x=\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix} \qquad A_y=\begin{pmatrix} \cos\theta & 0 & \sin\theta \\ 0 & 1 & 0 \\ -\sin\theta & 0 & \cos\theta \end{pmatrix}$$

由此可以很自然地和上面的想法进行类比：我们可以接着利用对角阵的良好性质

$\mathrm{diag}(A_x \quad A_y \quad A_z)$来控制一次在三维空间上的旋转操作。

比如通过数字信号发送给智能控制器，控制一个机械元件的三维旋转。

无论是二维的矩阵所控制的旋转操作，还是三维的矩阵所控制的三维旋转操作，都有一个共同的特点：就是当初始设定的旋转单位角旋转单位角 θ 越小，那么旋转一周就需要越多的单位角。这样增加了同一周期角度的密集程度，也就使得基于矩阵的旋转随机性更大，矩阵密码的安全系数越高。

1.3 矩阵的初等变换

现在讨论这样一个矩阵$\begin{pmatrix} 0 & 0 & \mathrm{a} \\ b & 0 & 0 \\ 0 & c & 0 \end{pmatrix}$

要是这个矩阵变成一个具有相同元的对角阵，我们可以这样运算：

$$\begin{pmatrix} 0 & 0 & \mathrm{a} \\ b & 0 & 0 \\ 0 & c & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}=\begin{pmatrix} \mathrm{a} & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}$$

通过矩阵的初等变换，我们可以使其变成具有相同元的对角阵。

在这里，我们设想将二维矩阵的旋转应用于一种密码锁芯。其中锁芯是多维旋转的机械元件，而刚才介绍的数组 K，正是我们所掌控的密码。这样做不仅可以通过简单的数组控制锁芯进而产生密码锁的效果，同时，由于矩阵的随机性，旋转元件的灵活性，我们可以设计智能程序来产生随机数组 T，利用函数 f(T)产生的随机值并输入。而函数 f 中的已知参数是我们所掌握的密码。也就是说，函数 f 就是人与机器默认的一种密码规则。通过这个函数来产生密码。

第三章　旋转电子密码锁的工作原理及结构设想

2.1 具体设计构想

下面我们结合图来介绍一下该旋转密码锁的原理：

创意模型：简单的**四维旋转密码锁**

简单的密码原理：设

$$N_i = \begin{pmatrix} \cos\theta_i & -\sin\theta_i \\ \sin\theta_i & \cos\theta_i \end{pmatrix}$$

令控制矩阵为

$$\begin{pmatrix} N_1^{k_1} & 0 & 0 & 0 \\ 0 & N_2^{k_2} & 0 & 0 \\ 0 & 0 & N_3^{k_3} & 0 \\ 0 & 0 & 0 & N_4^{k_4} \end{pmatrix}$$

则根据每个转子的结构。利用传感器测量出每个转子的突起与每个突起顺时针方向的定子凹槽之间的角度差 α。设这个转子所对应的旋转单位角为 θ，则满足下面的等式

$$k\theta = 120 - \alpha$$

得到

$$k = \frac{120-\alpha}{\theta}$$

这就可以作为我们产生密码的信息变换方式。

写到这里，可能读者会误以为这种变换方式有些过于简单。但是，不要忘了，我们之前曾经说过，我们机械元件的旋转单位角 θ 度虽然随着机械元件的出厂，自然而然的就定了下来，但是，我们可以通过设定控制元件旋转的控制器，来调整对应机械元件进行旋转操作时的旋转单位角，比如可以是 2θ，3θ 等等。而当机械元件出厂设置的单位旋转角 θ 越小的话，我们进行人为调整时可设定的旋转角就会越多。（这取决于元件的制造精度）。这样的话，四个转子的信息变换方式都可以不同，密码就更具有随机性了。

2.2 原理简图：

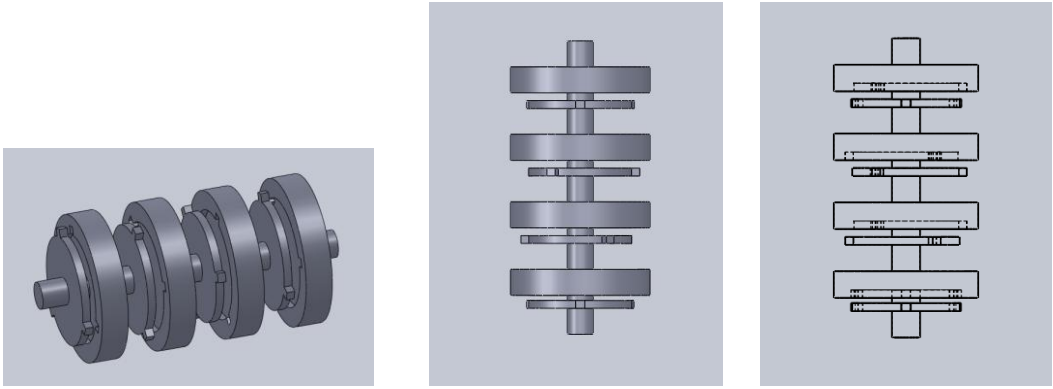

图 2 四个转子的锁芯构想图

（如图 2）四个转子套在一个主轴上。每个转子（如图 3）可以在轴上自由转动。且每个转子可以在轴上沿轴方向小范围移动。这种小范围内的移动需要每个转子所对应的控制器来实现。也就是说，在锁闭状态下，转子和它所对应的定子不是在同一个法平面（相对与主轴）内。当用户输入的密码 k 正确，即转子转动使得转子的突起和定子的凹槽在同一位置时，控制器会控制一个套在主轴上的联动装置，使转子沿主轴方向有小范围内移动，最终是定子和转子处于同一个法平面内，即完全咬合。这样，当四个转子都实现此操作的时候，锁就解开了。

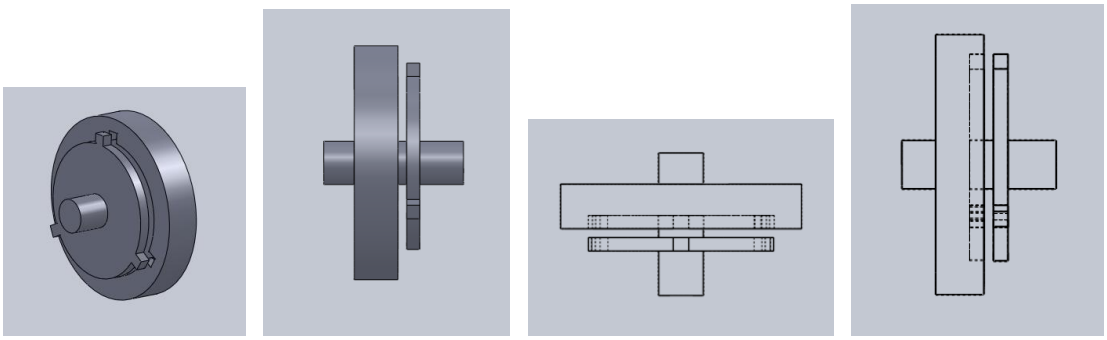

图 3 单个转子的结构

此例中转子的旋转是二维的。我们可以借助三维空间内的旋转矩阵，将这种由矩阵控制的旋转操作推广到三维空间中的机械中。当然，这只是一个设想。但是如果可以做到矩阵控制三维空间内的机械旋转，将此机械应用于锁芯，那么，这种锁的安全性应该会很高。

第三章 随机密码输入装置

3.1 设想起源

这样看来，上一章叙述的锁具结构算是成型了，但是我们回到原问题，我们的密码仍然是一个简单的数组 K=（$k_1,k_2,\cdots,k_t$）。这样的话，看起来与普通的密码没有区别。当然，我们可不可以通过矩阵的初等变换，让这个密码变成“动态密码”呢？下面我们试试通过矩阵的初等变换来实现这一目的。

3.2 四维矩阵下的随机密码输入装置

我们假定我们已知的密码为数组 K=（k_1,k_2,k_3,k_4）

定义：现在我们将数组 K 化为对角矩阵 K=$\begin{pmatrix} k_1 & 0 & 0 & 0 \\ 0 & k_2 & 0 & 0 \\ 0 & 0 & k_3 & 0 \\ 0 & 0 & 0 & k_4 \end{pmatrix}$，我们称之为目标矩阵。

定义：我们将形如$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$这样所有元均为 1，且行列式的值是 1 的矩阵称为 C 阵。

这样的话，每一个 C 阵都是可逆的。

我们分别用四种颜色对应这四个密码

红：k_1　黄：k_2　蓝：k_3　绿：k_4

这种颜色和密码之间的对应关系只有用户知道。

假设系统通过随机生成的 C 阵作用于目标矩阵，将目标矩阵转换为 $\begin{pmatrix} 0 & 0 & k_1 & 0 \\ k_2 & 0 & 0 & 0 \\ 0 & 0 & 0 & k_3 \\ 0 & k_4 & 0 & 0 \end{pmatrix}$。那么，我们通过用户端屏幕弹出的空矩阵框 $\begin{pmatrix} 0 & 0 & \text{位 } 1 & 0 \\ \text{位 } 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & \text{位 } 3 \\ 0 & \text{位 } 4 & 0 & 0 \end{pmatrix}$，在 1,2 ,3,4 位分别输入$k_1,k_2,k_3,k_4$,即可。这样，我们只需要系统每次随机生成一个 C 阵，然后进行运算

$$B = C\begin{pmatrix} k_1 & 0 & 0 & 0 \\ 0 & k_2 & 0 & 0 \\ 0 & 0 & k_3 & 0 \\ 0 & 0 & 0 & k_4 \end{pmatrix}$$

这样，系统就得到了一个用户所需要输入的矩阵 B。系统会将 B 中的非零元换成用户与及其约定好的颜色，并输出。这样，我们利用刚才的假设，那么用户所要面对的是一个这样的空阵：

$$\begin{pmatrix} 0 & 0 & \text{位 } 1 & 0 \\ \text{位 } 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & \text{位 } 3 \\ 0 & \text{位 } 4 & 0 & 0 \end{pmatrix}$$

这样，用户只需要在对应颜色中输入密码，即可。

优点：这种密码需要用户与系统之间来设定具体密码以及对应视图（例子中的对应视图是四种颜色），看似比正常密码繁琐，但是，这种密码每次输入的位置都不一样。这样就避免了传统密码在单一位置输入造成的密码外泄，遭人窥视

等弊病。例子中我们只是举了一个 4×4 矩阵的例子。如果矩阵维数进一步增加，那么，我认为安全性会进一步增强。

第四章　结束语

已经学习了半年多的线性代数课，我们真切的感觉到，矩阵运算的奇妙是任何自然数，整式和函数所不能代替的。矩阵不仅可以进行分块运算，而且特殊矩阵的乘法具有意想不到的现实意义，比如旋转矩阵，初等变换矩阵。

基于矩阵运算的良好兴致，我们设计了电子密码锁芯和智能系统下的随机密码输入装置。这只是一种初步的构想，想法比较简单，或许有些地方的设计还比较冗杂。用旋转矩阵控制锁芯转子旋转的传感器还需要电子工程上的进一步实现；智能操作系统的构建也需要去重新构建操作系统。在这里我们只是提供一个初步想法，而真正的实现可能不会那样简单。但是，我觉得在社会发展十分迅速的当今社会，密码会变得越来越重要，而矩阵密码也一定会占有一席之地。

参考文献

[1] 李尚志 《线性代数》（数学专业用）2006 年 5 月第一版

[2] 赵冬梅，张家雷. 复数乘法与旋转矩阵. 赤峰学院学报（自然科学版）（第 27 卷第 6 期 2011 年 6 月）

[3] 郁滨,徐晓辉,房礼国. 基于累积矩阵的可防欺骗视觉密码方案. 电子与信息学报 （第 31 卷第 4 期 2009 年 4 月）

[4] 王春艳，王志坚. 基于旋转矩阵理论的火炮定向精度分析. 光学 精密工程（第 12 卷第 4 期 2004 年 8 月）