Modern Applications of Linear Algebra

Games


CREDITS
2
8
SHARE
MUSIC BY
DU TONC
HelloRun™
AN HTML5 GAME BY HELLOENJOY
SETTINGS
PRESS GAMEPAD BUTTON TO START
FULL SCREEN

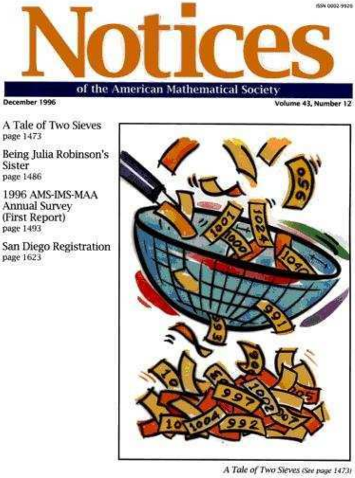
Games

Moving around in a world described in a computer game requires rotations and translations to be implemented efficiently. Hardware acceleration can help to handle this.

Rotations are represented by matrices having orthogonal properties. For example, if an object located at (0,0,0) is rotated around the y-axis by an angle φ, then every point in the object gets transformed by the matrix

$$\begin{bmatrix} \cos(\varphi) & 0 & \sin(\varphi) \\ 0 & 1 & 0 \\ -\sin(\varphi) & 0 & \cos(\varphi) \end{bmatrix}.$$

Cryptology


ISSN 0002-9920
Notices
of the American Mathematical Society
December 1996
Volume 43, Number 12
A Tale of Two Sieves
page 1473
Being Julia Robinson's Sister
page 1486
1996 AMS-IMS-MAA Annual Survey (First Report)
page 1493
San Diego Registration
page 1623
A Tale of Two Sieves (See page 1473)

Cryptology

Much of current cryptological security is based on the difficulty of factoring large integers n. One of the basic factorization ideas going back to Fermat is to find integers x such that $x^2 \pmod{n}$ is a small square y^2. Linear algebra (in particular, Gaussian elimination) can be used effectively to find such integers.

The factorization of the 193 digit RSA-640 challenge number

$$\begin{array}{l}
3107418240490043721350750035888 56\\
7930037346022842727545720161948 82\\
3206440518081504556346829671723 28\\
6782437916272838033415471073108 50\\
1919548529007337724822783525742 38\\
6454014691736602477652346609
\end{array}$$

carried a cash prize of \$20,000.

Networks

Networks

Linear algebra can be used to understand networks. A network is a collection of nodes connected by edges and are also called graphs. The adjacency matrix of a graph is defined by an array of numbers. One defines the matrix entry $A_{ij} = 1$ if there is an edge from node i to node j in the graph. Otherwise the entry is zero.

How does the array of numbers help to understand the network? An application is that one can read off the number of n-step walks in the graph which start at the vertex i and end at the vertex j. It is given by A^n_{ij}, where A^n is the n-th power of the matrix A. You will learn to compute with matrices as with numbers.

Markov Chains

Markov Chains

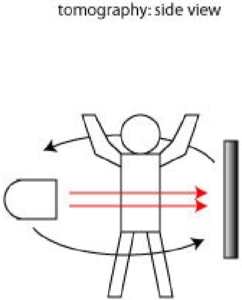
Suppose we have three bags with 10 balls each. Every time we throw a die and a 5 shows up, we move a ball from bag 1 to bag 2. If the die shows 1 or 2, we move a ball from bag 2 to bag 3. If 3 or 4 turns up, we move a ball from bag 3 to bag 1 and a ball from bag 3 to bag 2. What distribution of balls will we see on average?

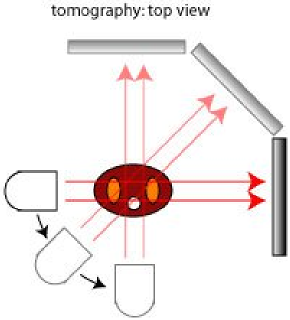
The problem defines a Markov Chain described by a matrix

$$\begin{bmatrix} 5/6 & 1/6 & 0 \\ 0 & 2/3 & 1/3 \\ 1/6 & 1/6 & 2/3 \end{bmatrix}$$

From this matrix, the equilibrium distribution can be read off as an eigenvector of a matrix. Eigenvectors will play an important role throughout the course.

Tomography

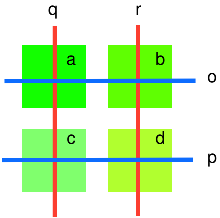




Tomography

Reconstruction of a density function from projections along lines (also called tomography) is a basic tool in applications like medical diagnosis and tokamak monitoring in plasma physics. Mathematical tools developed for the solution of this problem lead to the construction of sophisticated scanners. It is important that the inversion be fast, accurate, and robust, requiring as little data as possible.

Toy Reconstruction Problem



We have 4 containers with densities a, b, c, d arranged in a square. We measure light absorption by sending light through the containers. Like this, we get $o = a + b$, $p = c + d$, $q = a + c$ and $r = b + d$. The problem is to recover a, b, c, d. The system of equations is equivalent to $A\vec{x} = \vec{b}$ with $\vec{x} = (a, b, c, d)$, $\vec{b} = (o, p, q, r)$, and

$$A = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}.$$

Data Compression

Data Compression

Image, sound, and video compression standards like PNG, MP3, and MP4 make use of the linear Fourier transform and the fact that in the Fourier space, some parts of the information can be cut away without disturbing the important parts of the information.

Typically a picture, a sound, or a movie is cut into smaller chunks. These parts are represented by vectors. If U denotes the Fourier transform and P is a cutoff function, then $\vec{y} = PU\vec{x}$ is stored on some recording medium.

The receiver reproduces the recorded information by computing $\hat{x} = T\vec{y}$ with an appropriate transformation T. The vector $\hat{x}$ is close to $\vec{x}$ in the sense that the human eye or ear does not notice a big difference.

Acknowledgement

Application descriptions are modified from those found in
http://www.math.harvard.edu/~knill/teaching/math21b2010/21b_text.pdf .