Mini-Bibliography... Codes

by Joseph Malkevitch

This mini-bibliography addresses the major applications of codes. In the future, some of the specific ways codes are used in each of these areas below will be explored in more detail.

1. CODES FOR SECRECY

*Chaum, D., **Achieving Electronic Privacy,** Scientific American, Aug. 1992, p. 96-100.* This article documents dramatic new uses for ideas related to public-key cryptography.

*Kahn, D., **The Code-Breakers,** Macmillan, New York, 1967.* Kahn treats in detail the history of the use of secret codes and writes in such an exciting manner that this long book reads like a novel.

*Kahn, D., **Kahn On Codes,** Macmillan, New York, 1983.* This is a series of short essays which details the saga of secret codes during the cold war era.

*Sinkov, A., **Elementary Cryptanalysis,** Mathematical Association of America, Washington, 1968.* This book serves as a primer concerning the design of substitution ciphers (both monoalphabetic and polyalphabetic) and how to break such ciphers.

*Hellman, M., **The Mathematics of Public-key Cryptography,** Scientific American, Aug. 1979, p. 146-157.* Hellman gives an account of the pioneering concept he helped to develop, now called public-key cryptography. Public-key systems are now being used in the commercial sector of the economy and offer great promise for exciting new possibilities such as ''smart'' credit cards.

2. ERROR DETECTING AND CORRECTING CODES

*Malkevitch, J., and G. Froelich, **Codes Galore,** COMAP, Lexington, 1991.* An account of some of the ways error detecting and correcting codes are designed and are being used. Also, historical background on secret codes.

*Gallian, J. and S. Winters, **Modular Arithmetic In The Market Place,** Amer. Math. Monthly, 91 (1988) 548-551.* An account of a great variety of error-detection schemes.

*Hill, R., **A First Course In Coding Theory,** Oxford U. Press, New York, 1988.* A lucid but technical account of the theory of error correcting codes.

*Truxel, J., **The Age of Electronic Messages,** Mc Graw Hill, 1990.* An expository account of the revolution wrought by information theory, the branch of mathematics pioneered by Claude Shannon.

3. DATA COMPRESSION CODES

*Malkevitch, J., and G. Froelich, **Loads of Codes,** COMAP, Lexington, 1993.* This volume (which complements ***Codes Galore***) provides brief descriptions of the use of substitution and transposition ciphers. It includes material on the use of matrices to design codes. Finally, a discussion of the need for and construction of codes to compress data is given.

*Meyer, W., **Huffman Codes and Data Compression,** UMAP Journal, 5 (1984) 277-297.* A clear and detailed account of various points of view about the data compression codes developed by David Huffman.

References:

(Continued from page 8)

6. *Powell, R., **Digitizing TV Into Obsolescence,** NY Times, Oct. 20, 1991, v. 141 p. F11(N).* An account of how data compression technology is causing rethinking about how television technology can be advanced.
7. *Shapiro, E., **Self-Serve At The Checkout Lane; Bar Code Scanning In Its Ultimate Test,** NY Times, Jan. 6, 1991, v. 140 p. C1(N).* This article describes experiments to show the feasibility of using bar codes to allow self-service in stores.
8. *Stix, G., **Encoding The ''Neatness'' Of Ones and Zeroes,** Scientific American, Sept. 1991, v. 265 p. 54.* A biographical account of David Huffman, a mathematical engineer, who developed codes for data compression.
9. *Weber, J., **New Electronics To Pack More In Less Space,** LA Times, Jan. 15, 1991 p. D6.* An account of new products that are being developed based on data compression techniques.

TEACHING BRIEFS...The NBA Draft Lottery

(Continued from page 7)

Here are examples of questions which might be asked concerning this lottery; for ''Solutions...'' see page 11.

a. What is the probability that Dallas gets the first pick?
b. What is the probability that Minnesota does not get the first pick?
c. What is the probability that at least one of the first two ping-pong balls drawn had Minnesota's logo on it? (Note: The first two balls drawn could both have Minnesota's logo on them but by rule 3 the second ball would not be counted towards the lottery.)
d. Give an example of a draft lottery sequence where Washington gets the seventh pick.
e. Explain why it is not possible for Minnesota to get a draft pick worse than fourth.
f. What is the probability that Washington gets the fourth pick?