

1023-15-1667

Gregory V Bard* (gregory.bard@ieee.org), PO Box 4878, Silver Spring, MD 20914.

Algorithms for Inverting or LUP-Factoring Matrices over $GF(2)$ in time $O(n^3/\log n)$.

In 1970, Arlazarov, Dinic, Kronrod, and Faradzev created an algorithm to calculate the transitive closure of a graph, which was later adapted to be a $GF(2)$ matrix multiplication algorithm, now known as the Method of Four Russians. A folklore variant (apparently never published) of the algorithm for matrix inversion evolved. We present a detailed analysis of the “Method of Four Russians for Inversion”, which runs in time $O(n^3/\log_q n)$, where q is the size of the field. Furthermore, we experimentally compare this method to Strassen’s Algorithm and Gaussian Elimination, and find it is faster in practice for moderately sized matrices. Finally, we show how to choose the parameter of the algorithm so that the probability of failure is approximately $1/(n \log n)$. (Received September 26, 2006)