Square integer matrix with a single non-integer entry in its inverse

ABSTRACT

Matrix inversion is one of the most significant operations on a matrix. For any non-singular matrix $A \in Zn\times n$, the inverse of this matrix may contain countless numbers of non-integer entries. These entries could be endless floating-point numbers. Storing, transmitting, or operating such an inverse could be cumbersome, especially when the size n is large. The only square integer matrix that is guaranteed to have an integer matrix as its inverse is a unimodular matrix $U \in Zn\times n$. With the property that $\det(U)=\pm 1$, then $U-1 \in Zn\times n$ is guaranteed such that $UU-1=I$, where $I \in Zn\times n$ is an identity matrix. In this paper, we propose a new integer matrix $\tilde{G} \in Zn\times n$, which is referred to as an almost-unimodular matrix. With $\det(\tilde{G}) \neq \pm 1$, the inverse of this matrix, $\tilde{G}-1 \in Rn\times n$, is proven to consist of only a single non-integer entry. The almost-unimodular matrix could be useful in various areas, such as lattice-based cryptography, computer graphics, lattice-based computational problems, or any area where the inversion of a large integer matrix is necessary, especially when the determinant of the matrix is required not to equal ± 1. Therefore, the almost-unimodular matrix could be an alternative to the unimodular matrix.

Keyword: Square integer matrix; Inversion of integer matrix; Unimodular matrix; Algebraic number theory; Lattice-based cryptography