$\{K, -1\}$-potent matrices and applications in image encryption

Leila Lebtahi* Óscar Romero† Néstor Thome*

Abstract

Involutory matrices have been widely studied. In cryptography, for example, they were first used in 1920's by Hill [1]. The Hill's idea was to use the same matrix for encrypting and decrypting avoiding the computation of an inverse matrix.

The Hill cipher's keyspace consists of all matrices of a given size that are invertible over the ring $\mathbb{Z}_m$ of the integers modulo m. The number of such matrices was computed in [2]. The authors also compared this number with the total number of matrices and the number of involutory matrices (for a given size and modulus).

Let J be the square matrix with ones on the cross diagonal and zeros elsewhere; note that J is often called the centro-symmetric permutation matrix. This matrix J allows to introduce the centro-invertible matrices as those matrices X such that its inverse coincides with the rotation of all the elements of the matrix through 180 degrees about the mid-point of the matrix, that is JXJ [3]. The author studied these matrices computing the total number of them by means of a bijection with the involutory matrices of the same size.

In this paper we introduce a more general class, namely the $\{K, -1\}$-potent matrices, as an extension of the centro-invertible matrices. For this purpose, an involutory matrix K is used instead of the centro-symmetric permutation matrix J. Our main goal is the construction of members of this class in an effective form. In order to compute them we will design an algorithm. Further, an application in image encryption will be developed and its advantages with respect to the centro-invertible matrices will be indicated. In addition, some numerical examples are presented to show the performance of our algorithms and to demonstrate their applicability.

This work was partially supported by Ministry of Education (DGI Grant MTM2010-18228) and by Universidad Nacional de La Pampa, Argentina (Grant Resol. N. 049/11).

References

[1] L.S. Hill, Cryptography in an algebraic alphabet, *Amer. Math. Monthly*, 36 3006–312, 1929.

[2] J. Overbey, W. Traves, J. Wojdylo. On the keyspace of the Hill Cipher. *Cryptologia*, 29 (1), 59–72, 2005.

[3] R.S. Wikramaratna, The centro-invertible matrix: A new type of matrix arising in pseudo-randon number generation, *Linear Algebra and its Applicatios*, 434, 1, 144–151, 2011.

*Instituto Universitario de Matemática Multidisciplinar. Universitat Politècnica de València. E–46022 Valencia, Spain. E–mail addresses: {leilebep,njthome}@mat.upv.es.

†Departamento de Comunicaciones. Universitat Politècnica de València. E–46022 Valencia, Spain. E–mail address: oromero@dcom.upv.es.