Decoding up to 4 errors in Hyperbolic-like Abelian Codes by the Sakata Algorithm*

José Joaquín Bernal** and Juan Jacobo Simón**

**Departamento de Matemáticas, Universidad de Murcia, Spain.

The Sakata algorithm (or Berlekamp-Massey-Sakata algorithm, BMSa, for short) is one of the best known procedures to find Groebner basis for the so called ideal of linear recurrence relations on a doubly periodic array [4]. As it is known, on each step a given polynomial set (called minimal set of polynomials) is updated until get the mentioned basis. It is a common method for decoding algebraic geometric codes, specially those constructed from one-point algebraic curves [1, 2] and, within them, the family of Hyperbolic Cascade Reed-Solomon Codes (see [3]). By contrast, the original application of the BMSa: decoding Abelian Codes through locator decoding [5], has been less developed and improved.

In this paper, we deal with two interesting open problems about this algorithm. First, how to find a minimal set of steps in the sense that there are not redundant ones; that is, steps that do not contribute to go further with the minimal set of polynomials. In this respect, the main goal of our paper is to prove that, in the context of locator decoding up to 4 errors, the set of indexes of the syndrome table defined in Blahut’s work [1] (except for two elements) verifies that, no others syndromes contribute to construct the Groebner basis and, moreover, none of them may be ignored a priori. Secondly, how to know if we have obtained a Groebner basis at the final step. In this direction, Theorem 4 gives us a termination criterion.

On the other hand, we give a different approach to the locator decoding algorithm. Unlike the original BMSa, where one must begin the iterations at the index (0, 0), we define another framework that makes possible to work with a suitable set of indexes depending on the specific structure of the defining set of the codes. When codes are defined over splitting fields starting in (0, 0) is not a problem; however, in other contexts, it may happen (specially in the case of binary abelian codes) that it is impossible to implement the BMSa starting in this place.

References

[1] R.E. Blahut, Decoding of cyclic codes and codes on curves. In W.C. Huffman and V. Pless (Eds.), Handbook of Coding Theory. Vol. II, 1569-1633, 1998.

[2] D. A. Cox, J. Little, D. O’shea. Using algebraic geometry (2nd Edition). Vol. 185. Springer Science & Business Media, 2006.

[3] K. Saints, C. Heegard, Algebraic-Geometric Codes and Multidimesional Cyclic Codes: A Unified Theory and Algorithms for Decoding Using Gröbner basis, IEEE Transactions on Information Theory 41 (6) (1995) 1733-1751.

[4] S. Sakata, Finding a minimal set of linear recurring relations capable of generating a given finite two-dimensional array, J. Symbolic Computation, 5 (1988), pp. 321–337.

[5] S. Sakata, Decoding binary cyclic 2-D codes by the 2-D Berlekamp-Massey algorithm. IEEE Transactions on Information Theory 37 (4) (1991) 1200-1203.

*This work was partially supported by MINECO, project MTM2016-77445-P, and Fundación Séneca of Murcia, project 19880/GERM/15.