Code Equivalence and Graph Isomorphism

Magali Bardet Ayoub Otmani Mohamed Saeed *

Introduction

Two linear codes are said to be linearly equivalent if there exists a linear isomorphism between them that preserves the Hamming weight. Equivalent codes have the same properties such as length, dimension, minimum distance, weight distribution and correction capabilities. In coding theory the goal is to have an efficient and reliable data transmission methods. Thus classification of codes by equivalence enables to identify the codes that have the same capabilities.

In cryptography, more specifically in code-based cryptosystems, code equivalence problem is extensively used in hiding the structure of secret codes such as in the McEliece-like cryptosystems. Thus proving the difficulty of this problem enables to design secure cryptosystems. On the other hand introducing an efficient algorithm to solve the problem enables to do efficient cryptanalysis.

The link between code equivalence problem and graph isomorphism problem was established by E. Petrank and R. Roth in 1997. Graph isomorphism problem is a long standing problem in graph and complexity theory. They provide a polynomial-time reduction of graph isomorphism to permutation equivalence. This shows that graph isomorphism is easier than code equivalence problem.

Recently the National Institute of Standards and Technology (NIST) has made a call to standardize Post Quantum Cryptography. In response to this call many cryptographic schemes that rely on Code Equivalence Problem were proposed.

*M. Bardet, A. Otmani and M. Saeed are with Normandie Univ, France; UR, LITIS, F-76821 Mont-Saint-Aignan, France.

Our Contribution

We focus on the permutation version of code equivalence problem. We develop algebraic model that describes the problem where we prove that the problem is well-described by this model.

We show that given access to a subroutine that decides if two weighted undirected graphs are isomorphic, one may deterministically decide the permutation code equivalence provided that the underlying vector spaces intersect trivially with their orthogonal complement with respect to an arbitrary inner product. Such a class of vector spaces is usually called linear codes with trivial hulls. The reduction is efficient because it essentially boils down to computing the inverse of a square matrix of order the length of the involved codes. Experimental results obtained with randomly drawn binary codes having trivial hulls show that permutation code equivalence can be decided in a few minutes for lengths up to $50,000$.

References

[Bab15] László Babai. Graph isomorphism in quasipolynomial time. *CoRR*, abs/1512.03547, 2015.

[Leo82] Jeffrey Leon. Computing automorphism groups of error-correcting codes. *IEEE Trans. Inform. Theory*, 28(3):496–511, 1982.

[MP14] Brendan D. McKay and Adolfo Piperno. Practical graph isomorphism II. *Journal of Symbolic Computation*, 60(0):94–112, 2014.

[PR97] Erez Petrank and Ron. Roth. Is code equivalence easy to decide? *IEEE Trans. Inform. Theory*, 43(5):1602–1604, 1997.

[Sae17] Mohamed Ahmed Saeed. *Algebraic Approach for Code Equivalence*. PhD thesis, Normandy University, France, 2017.

[SS13] Nicolas Sendrier and Dimitris E. Simos. The hardness of code equivalence over and its application to code-based cryptography. In *Post-Quantum Cryptography 2013*, volume 7932 of *LNCS*, pages 203–216. Springer, 2013.