

How close are we to Solving Code Equivalence

Other Conference Item

Author(s):

Weger, Violetta

Publication date:

2026-02-25

Permanent link:

<https://doi.org/https://doi.org/10.3929/ethz-c-000796635>

Rights / license:

[In Copyright - Non-Commercial Use Permitted](#)

How close are we to Solving Code Equivalence

Violetta Weger

Technical University of Munich
School of Computation, Information and Technology
email: violetta.weger@tum.de

Abstract—"Code Equivalence" describes the problem of finding a linear isometry between two codes. An isometry is a map which preserves the weight, in our case: the Hamming weight. We can easily identify the linear isometries in the Hamming metric to be all monomial transformations. Thus the problem reads as follows:

Given $\mathcal{C}, \mathcal{C}' \subseteq \mathbb{F}_q^n$ find $\varphi \in (\mathbb{F}_q^*)^n \rtimes S_n$, such that $\varphi(\mathcal{C}) = \mathcal{C}'$.

While the problem is interesting from a pure coding-theoretic perspective, its recent use in the signature scheme LESS has put the problem in the center of attention of the cryptographic community as well. In fact, LESS is one of the few surviving signature schemes in the second round of the additional standardization call by NIST.

The bothersome part about this problem, is that we *know* it is *not* NP-hard, without having an efficient solver.

The whole research area is only now emerging and thus still under-explored. Thus, as of today, any outcome is within the range of possibilities.

I. EXTENDED ABSTRACT

By 2035, national agencies worldwide, led by National Institute of Standards and Technology (NIST) and their European counterparts, plan to phase out today's public-key cryptosystems, requiring a rapid transition to quantum-resistant alternatives. Among the proposed post-quantum primitives, code-based cryptography stands out for its long history and conservative security foundations, relying on hardness assumptions from algebraic coding theory. Several code-based schemes were submitted to the NIST post-quantum standardization process, with HQC and Classic McEliece selected for standardization by the United States and Germany, respectively.

At the same time, the ongoing standardization efforts for post-quantum signature schemes increasingly rely on novel hardness assumptions. While adoption is accelerating, many of these assumptions remain under-explored, making it difficult to assess and compare their security. In this context, understanding the hardness of problems in code-based cryptography is essential.

One such problem is the code equivalence problem: given two linear codes, find a hidden isometry between them. This problem lies at the heart of the security of several code-based constructions, such as LESS and PERK.

An $[n, k]_q$ linear code \mathcal{C} is a k -dimensional linear subspace of \mathbb{F}_q^n . We call $G \in \mathbb{F}_q^{k \times n}$ a generator matrix of \mathcal{C} if its rows form a basis of \mathcal{C} . Two codes $\mathcal{C}, \mathcal{C}'$ are linearly equivalent, if there exists a monomial $\varphi = (d, \sigma) \in (\mathbb{F}_q^*)^n \rtimes S_n$, such that $\varphi(\mathcal{C}) = \mathcal{C}'$. To find a linear equivalence between two

given codes, is the the Linear Equivalence Problem (LEP), that is: Given two generator matrices, $G, G' \in \mathbb{F}_q^{k \times n}$ find $S \in \text{GL}_k(\mathbb{F}_q)$, a $n \times n$ permutation matrix P and a diagonal matrix $D = \text{diag}(d)$, for $d \in (\mathbb{F}_q^*)^n$, such that $SGDP = G'$.

While all combinatorial solvers for LEP have an exponential cost [1], [3], [7], related problems have been shown to be easy, e.g. the Graph Isomorphism Problem (GIP) has been proven to be quasi-polynomial [8]. It remains an open question, whether we can employ this result to efficiently solve LEP as well.

The special case of permutations, called Permutation Equivalence Problem (PEP) has a reduction to GIP [5], for codes with trivial hull, i.e., $\mathcal{H}(\mathcal{C}) = \mathcal{C} \cap \mathcal{C}^\perp = \{0\}$. In fact, in this reduction, the authors define an *adjacency matrix* corresponding to a code \mathcal{C} with generator matrix G as $G^\top (GG^\top)^{-1} G$. Clearly, such a matrix only exists, if GG^\top is invertible, i.e., $\mathcal{H}(\mathcal{C}) = \{0\}$.

As this expected of random codes with high probability, this reduction proves to be very strong and bars the use of PEP for random codes within cryptosystems. Additionally, we know how to reduce LEP to PEP, through the closure of a code [6]. For this, we let $\alpha \in \mathbb{F}_q$ be a primitive element, and denote $a = (1, \alpha, \dots, \alpha^{q-2}) \in \mathbb{F}_q^{q-1}$. The *closure* $a \otimes \mathcal{C}$ of \mathcal{C} is defined as the code with generator matrix $a \otimes G$, where \otimes denotes the Kronecker product. However, this reduction comes with intrinsic limitations as the closure is a self-orthogonal code for $q \geq 4$, that is $\mathcal{C} \subseteq \mathcal{C}^\perp$. As a result, known reductions cannot simply be combined to obtain a general, efficient solution to code equivalence.

However, recent developments show how little we have tried and know: in a recent paper [4] the square code has been used to attack the system proposed in [2] for $q = 5$. Clearly, one can generalize this result to larger powers and find many more weak keys, which should not be used. The ℓ -th *power code* of \mathcal{C} is defined as

$$\mathcal{C}^{(\ell)} = \langle \{c_1 * \dots * c_\ell \mid c_i \in \mathcal{C}\} \rangle.$$

When $\ell = 2$ we call $\mathcal{C}^{(2)}$ the *square code*.

This talk surveys the current state of the art on code equivalence, focusing on what these classical reductions tell us about the problem's hardness and which directions have been left unexplored.

This is joint work with Michele Battagliola, Anna-Lena Horlemann, Abhinaba Mazumder, Rocco Mora, Paolo Santini, Michael Schaller.

REFERENCES

- [1] Jeffrey Leon. *Computing automorphism groups of error-correcting codes*. IEEE Transactions on Information Theory, 28(3):496–511, 1982.
- [2] Martin R. Albrecht, Benjamin Bencina, and Russell W. F. Lai. *Hollow LWE: A New Spin*. In Serge Fehr and Pierre-Alain Fouque, editors, *Advances in Cryptology – EUROCRYPT 2025*, pages 363–392, Cham, 2025. Springer Nature Switzerland.
- [3] Alessandro Barengi, Jean-François Biasse, Edoardo Persichetti, and Paolo Santini. *On the computational hardness of the code equivalence problem in cryptography*. *Advances in Mathematics of Communications*, 17(1):23–55, 2023.
- [4] Michele Battagliola, Rocco Mora, and Paolo Santini. *Using the schur product to solve the code equivalence problem*. *Cryptology ePrint Archive*, Paper 2025/1017, 2025.
- [5] Magali Bardet, Ayoub Otmani, and Mohamed Saeed-Taha. *Permutation code equivalence is not harder than graph isomorphism when hulls are trivial*. In 2019 IEEE International Symposium on Information Theory (ISIT), pages 2464–2468. IEEE, 2019.
- [6] Nicolas Sendrier and Dimitrios E Simos. *How easy is code equivalence over \mathbb{F}_q ?* In *International Workshop on Coding and Cryptography-WCC 2013*, 2013.
- [7] Nicolas Sendrier. *Finding the permutation between equivalent linear codes: The support splitting algorithm*. IEEE Transactions on Information Theory, 46(4):1193–1203, 2000.
- [8] L. Babai. *Graph isomorphism in quasipolynomial time*, in *Proceedings of the forty-eighth annual ACM symposium on Theory of Computing*, 2016, pp. 684–697.