Contemporary algebraic and geometric techniques in coding theory and cryptography
Summer school — July 18-22, 2022
Università degli Studi della Campania "Luigi Vanvitelli"

The Matrix Code Equivalence Problem and Applications

Monika Trimoska

Affiliation: Radboud University
The Netherlands

Abstract

A *matrix code* is a subspace $\mathcal{C}$ of $m \times n$ matrices over $\mathbb{F}_q$ endowed with the rank metric defined as $d(\mathbf{A}, \mathbf{B}) = \text{Rank}(\mathbf{A} - \mathbf{B})$. We denote by k the dimension of $\mathcal{C}$ as a subspace of $\mathbb{F}_q^{m \times n}$ and its basis by $\langle \mathbf{C_1}, \ldots, \mathbf{C_k} \rangle$, where $\mathbf{C_i} \in \mathbb{F}_q^{m \times n}$ are linearly independent. Since their introduction in 1951 by Loo-Keng Hu, rank metric error-correcting codes have found applications in various domains such as network coding, space-time coding and public key cryptography. The growing interest in the latter domain is due to the urgent necessity in the cryptographic community to find and explore problems that are hard to solve, even for an attacker that has access to a quantum computer. The security of *classical* (in contrast to *post-quantum*) public key cryptography is based on the hardness of factorisation and the discrete log problem, both of which can be solved in polynomial time using Shor's quantum algorithm [13]. Thus, for building post-quantum cryptographic schemes we need *one-way* functions that are easy to compute on a classical computer, but hard to invert both in the classical and the quantum setting. The problem we are exploring in this work, called the Matrix code equivalence (MCE), gives rise to such a one-way function. Formally, the MCE problem can be defined as follows.

$\mathsf{MCE}(k, n, m, \mathcal{C}, \mathcal{D})$:
Input: Two k-dimensional matrix codes $\mathcal{C}, \mathcal{D} \subset \mathcal{M}_{m,n}(q)$
Question: Find – if any – $\mathbf{A} \in \text{GL}_m(q), \mathbf{B} \in \text{GL}_n(q)$ such that for all $\mathbf{C} \in \mathcal{C}$, it holds that $\mathbf{ACB} \in \mathcal{D}$.

The map $\varphi : \mathbf{C} \mapsto \mathbf{ACB}$ is called an *isometry* between $\mathcal{C}$ and $\mathcal{D}$. An isometry preserves the rank i.e. $\text{Rank}\,\mathbf{C} = \text{Rank}\,\varphi(\mathbf{C})$.

Our motivation for studying the MCE problem comes from the fact that it can be considered as a *cryptographic group action.* A group action is considered *cryptographic* when it has some hardness properties that are useful for cryptographic applications (see, for instance [1]). In the case of MCE, the isometries $\varphi \in \mathrm{GL}_m(q) \times \mathrm{GL}_n(q)$ form a group that acts on the set of k-dimensional matrix codes of size $m \times n$ over a base field $\mathbb{F}_q$. The group action is simply applying the map $\varphi : \mathbf{C} \mapsto \mathbf{ACB}$, and it constitutes a cryptographic group action, only if the MCE problem is hard. This makes MCE a good candidate for constructing post-quantum cryptographic schemes. More specifically, as with every "graph isomorphism"-like problem, we can construct a sigma protocol to be used as an identification scheme or to be transformed to a digital signature scheme via the Fiat-Shamir transform. In related work, the Hamming variation of the Code Equivalence problem has been used to build the LESS-FM [2] signature scheme.

Before we use MCE as an underlying hard problem in different cryptographic applications, we need to do a thorough analysis on its complexity. The Hamming metric version of the problem, simply known as Code Equivalence, was first studied by Leon [9] and it was recently improved by Beullens [4]. Sendrier [12] proposed the Support Splitting Algorithm (SSA), which takes a different approach and is exponential in the dimension of the hull. The rank metric version has been introduced by Berger in [3], but it was only recently that Couvreur et al. [7] showed the first concrete statements about its hardness. Namely, they showed that MCE is at least as hard as the Code Equivalence problem in the Hamming metric, while for only right equivalence, or when the codes are $\mathbb{F}_{q^m}$-linear, the problem becomes easy. In this work, we describe the first explicit algorithms for solving MCE.

First, we show that MCE can be reduced to a well-explored problem, called Quadratic Maps Linear Equivalence (QMLE). QMLE is a variant of the Isomorphism of Polynomials (IP) problem , first defined by Patarin in [10] for the purpose of designing a "graph isomorphism"-like identification scheme and a digital signature using the Fiat-Shamir transform. The QMLE problem can be formally defined as follows.

QMLE$(N, k, \mathcal{F}, \mathcal{P})$:
Input: Two k-tuples of multivariate polynomials $\mathcal{F} = (f_1, f_2, \ldots, f_k)$, $\mathcal{P} = (p_1, p_2, \ldots, p_k) \in \mathbb{F}_q[x_1, \ldots, x_N]^k$
Question: Find – if any – $\mathbf{S} \in \mathrm{GL}_N(q), \mathbf{T} \in \mathrm{GL}_k(q)$ such that $\mathcal{P}(\mathbf{x}) = \mathcal{F}(\mathbf{xS})\mathbf{T}$.

In this work, we show how a positive instance $(N, k, \mathcal{F}, \mathcal{P})$ of the homogenous version of QMLE can be transformed to a positive instance $(k, N, N, \mathcal{C}, \mathcal{D})$ of MCE, and similarly, how a positive instance $(k, n, m, \mathcal{C}, \mathcal{D})$ of MCE can be transformed to a positive instance $(m+n, k, \mathcal{F}, \mathcal{P})$ of the homogenous version of QMLE. The latter reduction is more significant as it allows us to derive the first algorithm for solving the MCE problem. Specifically, we describe a generalization of a birthday-based approach previously developed for the QMLE problem [6]. This results in an algorithm for solving MCE with a complexity of $\mathcal{O}^*(q^{\frac{2}{3}(n+m)})$. However, our reduction shows that a QMLE instance derived from an MCE instance has a specific structure. Namely, the unknown matrix $\mathbf{S}$ is of the form $\begin{bmatrix}\mathbf{A} & \mathbf{0}\\ \mathbf{0} & \mathbf{B}^\top\end{bmatrix}$. The consequences of this structure are twofold. First, an algebraic modelization of the problem results in a bilinear system of equations. Such a system can naively be solved in the square root of the time it takes to solve a polynomial system with the same parameters but without the bilinear structure.[1] Second, the bilinear structure can be exploited in the birthday-based approach to decrease the collision-search domain and thus, significantly reduce the complexity of the overall algorithm. This optimization can be used for a certain subset of parameters, roughly when $k \leq m+n$, and it allows us to propose a refined algorithm that runs in time $\mathcal{O}^*(q^m)$ deterministically.

To confirm our theoretical findings, we implemented both algorithms and used them to solve randomly generated positive instances of the MCE problem. Our algorithms are implemented in MAGMA [5] and use the F4 [8] algorithm for parts of the computation that require solving a polynomial system of equations. Our experimental results show that the first algorithm has a success probability higher than 63%, which is consistent with birthday-based algorithms. Recall that the second algorithm is deterministic and can be applied roughly when $k \leq m+n$. The running times that we obtain reflect its superiority over the first algorithm and are aligned with our theoretical findings. In conclusion, these results provide a better understanding of the hardness of the MCE problem for different parameter sets.

This work was presented for the first time at The Twelfth International Workshop on Coding and Cryptography (WCC 2022) and an extended abstract can be found at [11]. This is a joint work with Krijn Reijnders and Simona Samardjiska.

[1] In the balanced case where $m = n$, which is also the hardest.

Keywords: matrix code equivalence, post-quantum cryptography, birthday algorithms

References

[1] N. Alamati, L. De Feo, H. Montgomery, and S. Patranabis. Cryptographic group actions and applications. In *ASIACRYPT '20*, pages 411–439. Springer, 2020.

[2] A. Barenghi, J.-F. Biasse, E. Persichetti, and P. Santini. LESS-FM: Fine-tuning Signatures from the Code Equivalence Problem. Cryptology ePrint Archive, Report 2021/396, 2021. `https://ia.cr/2021/396`.

[3] T. P. Berger. Isometries for rank distance and permutation group of Gabidulin codes. *IEEE Trans. Inf. Theory*, 49:3016–3019, 2003.

[4] W. Beullens. Not enough LESS: An improved algorithm for solving Code Equivalence Problems over $\mathbb{F}_q$. Cryptology ePrint Archive, Report 2020/801, 2020. `https://ia.cr/2020/801`.

[5] W. Bosma, J. Cannon, and C. Playoust. The Magma Algebra System. I. The User Language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[6] C. Bouillaguet, P.-A. Fouque, and A. Véber. Graph-theoretic algorithms for the "Isomorphism of Polynomials" problem. pages 211–227, 2013.

[7] A. Couvreur, T. Debris-Alazard, and P. Gaborit. On the hardness of code equivalence problems in rank metric, 2021.

[8] J.-C. Faugère. A New Efficient Algorithm for Computing Gröbner basis (F4). *Journal of Pure and Applied Algebra*, 139(1-3):61–88, 1999.

[9] J. Leon. Computing automorphism groups of error-correcting codes. *IEEE Transactions on Information Theory*, 28(3):496–511, 1982.

[10] J. Patarin. Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms. In *Advances in Cryptology – EUROCRYPT '96*, volume 1070 of *LNCS*, pages 33–48. Springer, 1996.

[11] K. Reijnders, S. Samardjiska, and M. Trimoska. Hardness estimates of the Code Equivalence Problem in the Rank Metric. *Cryptology ePrint Archive*, 2022.

[12] N. Sendrier. Finding the permutation between equivalent linear codes: The support splitting algorithm. *IEEE Trans. Inf. Theory*, 46:1193–1203, 2000.

[13] P. W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.*, 26(5):1484–1509, Oct. 1997.