How Easy is Code Equivalence over $GF(q)$?

Nicolas Sendrier
INRIA Paris-Rocquencourt
Project-Team SECRET
78153 Le Chesnay Cedex, France
email: nicolas.sendrier@inria.fr

Dimitris E. Simos*
INRIA Paris-Rocquencourt
Project-Team SECRET
78153 Le Chesnay Cedex, France
email: dimitrios.simos@inria.fr

A linear $[n, k]$ code of length n and dimension k over $\mathbb{F}_q = GF(q)$ is a k-dimensional vector subspace of $\mathbb{F}_q^n$, where $GF(q)$ is the Galois field with q elements. We call such a code a q-ary code. In this work, we are interested in a decisional problem regarding linear codes over $\mathbb{F}_q$. In particular, we aim towards an efficient algorithm for deciding the code equivalance over $\mathbb{F}_q$. For q-ary codes there are three different notions of equivalence: permutation, monomial (or linear) and semi-linear, see [2].

Two q-ary codes $\mathcal{C}$ and $\mathcal{C}'$ of length n are *permutation-equivalent*, if the codewords of $\mathcal{C}'$ can be obtained from the codewords of $\mathcal{C}$ by applying a permutation σ on $I_n = \{1, \ldots, n\}$, that is $\mathcal{C}' = \sigma(\mathcal{C})$. When considering codes over $\mathbb{F}_q$ there are other maps also that preserve the weight of the codewords. These maps include those which rescale coordinates and those which are induced from field automorphisms. In particular, $\mathcal{C}$ and $\mathcal{C}'$ are *monomially-equivalent*, if there exists a linear isometry $\phi : \mathbb{F}_q^n \mapsto \mathbb{F}_q^n$ mapping $\mathcal{C}$ to $\mathcal{C}'$ (with respect to the Hamming metric). This isometry ϕ can be expressed as an element of the group of monomial permutations. When $q = p^r$ is not a prime, then the Frobenius automorphism $\tau : \mathbb{F}_q \mapsto \mathbb{F}_q,\ x \mapsto x^p$ applied on each coordinate of $\mathbb{F}_q^n$ preserves the Hamming distance, too. Therefore, the group of field automorphisms is included to a more general notion of equivalence of linear codes. We call two codes $\mathcal{C}$ and $\mathcal{C}'$ to be *semi-linearly equivalent* if there is a field automorphism $\alpha \in \mathrm{Aut}(\mathbb{F}_q)$ and a linear isometry $\iota : \mathbb{F}_q^n \mapsto \mathbb{F}_q^n$ such that $\mathcal{C}' = \iota(\alpha(\mathcal{C}))$. It is well-known that for $n \geq 3$ the set of all isometries of $\mathbb{F}_q^n$ mapping subspaces to subspaces is the group of semi-linear isometries, see [2]. Therefore, the notion of semi-linear isometry of linear codes is the most general which can be expressed as a group action on the set of linear subspaces. In the binary case, all three notions of equivalence are the same. If $\mathbb{F}_q$ is a prime field, monomial and semi-linear equivalence coincide, since there are no non-trivial automorphisms, and when q is a prime power they are all different.

The computational difficulty of the code equivalence problem is of crucial importance in the area of code-based cryptography. As an application, we mention the McEliece public-key cryptosystem [3], where the public key is an instance of a permutation-equivalent code of a binary Goppa code. The problem of permutation-equivalence is not NP-complete, however in the worst case is reduced to the graph isomorphism [4] which is conjectured to be in NP\P. The support-splitting algorithm [6] solves the code-equivalence problem exactly when the monomial transformation is a permutation. The algorithm employs the concept of invariants and signatures. Invariants are mappings such that for any pair of equivalent codes they take the same value. In that sense, invariants are global properties of the code. On the other hand, signatures depends on the code and one of its positions therefore are local properties. A good signature must be easy

*This work was carried out during the tenure of an ERCIM "Alain Bensoussan" Fellowship Programme. This Programme is supported by the Marie Curie Co-funding of Regional, National and International Programmes (COFUND) of the European Commission.

to compute and moreover be discriminant, that is the number of different values the signature can take. Such a signature can be built from the weight enumerator of the *hull* of a code, $\mathcal{H}(\mathcal{C}) = \mathcal{C} \cap \mathcal{C}^{\perp}$, for the binary and the ternary field because any invariant which is applied to the hull still remains an invariant. The complexity of the support-splitting algorithm for these cases depends exponentially on the dimension of the hull, which on average is a small constant [5], therefore the algorithm is efficient in practice.

Estimating the hardness of the code equivalence problem of q-ary codes, or even better developing an algorithm for deciding the latter problem, is of current interest. For example, recently there have been proposed code-based cryptosystems which employ "wild" Goppa codes over $\mathbb{F}_q$, see [1]. We attempt a *generalization* of the support-splitting algorithm for $\mathbb{F}_q$. In order for this generalization to be successful we set the following goals:

- Reducing the monomial or semi-linear equivalence to permutation equivalence
- Identifying an invariant for linear codes over $GF(q)$ with good properties

For the first task we introduce the *closure* of the code and the *extension* of its dual. For our second goal it is natural to ask if the hulls of q-ary linear codes can be used as a mean to provide invariants for the general case of code equivalence. Unfortunately, it turns out that the hulls of equivalent codes do not remain equivalent over $GF(q)$, $q > 4$. We provide a generalization of the hull that remains invariant in the general case, however is far from being suitable for practical applications at the monent. Finally, we provide some arguments that the code equivalence problem over $GF(q)$ is not too easy to be attacked with a polynomial-time algorithm.

References

[1] D. J. Bernstein, T. Lange and C. Peters, Wild McEliece, In *Selected Areas in Cryptography (SAC 2010), Lecture Notes in Computer Science*, vol. **6544**, pp. 143-158, Springer-Verlag, 2011.

[2] A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert and A. Wassermann, *Error-Correcting Linear Codes. Classication by Isometry and Applications*, Springer, Berlin, 2006.

[3] J. McEliece, A public-key cryptosystem based on algebraic coding theory, DSN Progress Rep. 42-44, JPL, Caltech, Pasadena, CA, pp. 114-116, Jan-Feb 1978.

[4] E. Petrank and R. M. Roth, Is code equivalence easy to decide?, *IEEE Trans. on Inform. Theory*, **43** (1997), 1602-1604.

[5] N. Sendrier, On the dimension of the hull, *SIAM J. Discete Math.*, **10** (1997), 282-293.

[6] N. Sendrier, Finding the permutation between equivalent linear codes: the support splitting algorithm, *IEEE Trans. Inform. Theory*, **46** (2000), 1193-1203.