

Left ideal LRPC codes and a ROLLO-type cryptosystem based on group algebras

Martino Borello*, Paolo Santonastaso and Ferdinando Zullo†

Abstract

In this paper we introduce left ideal low-rank parity-check codes by using group algebras and we finally use them to extend ROLLO-I KEM.

Keywords: Group algebra, low-rank parity-check code, ideal matrix, ROLLO

1 Introduction

Low-rank parity-check (LRPC) codes are rank-metric codes introduced by Gaborit et al. in [1, 5] as the rank-metric analogs of low-density parity-check codes in the Hamming metric. These codes turned out to be very interesting for their efficient probabilistic decoding algorithm and their applications in several contexts, such as powerline communications [12], network coding [4] and cryptography [9]. Regarding the last one, in ROLLO cryptosystem special types of LRPC codes are used, known as ideal LRPC codes, which can be efficiently stored: they can be simply represented by a vector instead of the entire generator matrix (as in the case with circulant matrices).

Motivated by the application in cryptography, in this paper we introduce left ideal LRPC codes arising from group algebras, deriving some interesting properties, such as a systematic parity-check matrix. Thank to this latter property, we are able to describe a new variant of the Key-Encapsulation scheme ROLLO-I with the use of group algebras. A similar approach has been recently used in [3] in the Hamming-metric context (MDPC codes), to generalize the BIKE cryptosystems.

Throughout the paper, q is a prime power, m is a positive integer, \mathbb{F}_{q^m} is the field with q^m elements and G is a finite group of size n .

*Université Paris 8, Laboratoire de Géométrie, Analyse et Applications, LAGA, Université Sorbonne Paris Nord, CNRS, UMR 7539, France
martino.borello@univ-paris8.fr

†Università degli Studi della Campania “Luigi Vanvitelli”, Caserta, Italy
{paolo.santonastaso,ferdinando.zullo}@unicampania.it

2 Group algebras and left ideal matrices

The group algebra $\mathbb{F}_{q^m}G$ is the set $\left\{ \sum_{g \in G} a_g g : a_g \in \mathbb{F}_{q^m} \right\}$, which is an \mathbb{F}_{q^m} -vector space of dimension n in a natural way and it is also an \mathbb{F}_{q^m} -algebra via the multiplication

$$ab := \sum_{g \in G} \left(\sum_{h \in G} a_h b_{h^{-1}g} \right) g,$$

for $a = \sum_{g \in G} a_g g$ and $b = \sum_{g \in G} b_g g$. From now, we fix an ordering $1_G = g_1, \dots, g_n$ of the elements of G . The \mathbb{F}_{q^m} -vector spaces $\mathbb{F}_{q^m}^n$ and $\mathbb{F}_{q^m}G$ may be identified by the following \mathbb{F}_{q^m} -isomorphism:

$$\begin{aligned} \Psi: \quad \mathbb{F}_{q^m}^n &\longrightarrow \mathbb{F}_{q^m}G \\ (u_1, \dots, u_n) &\longmapsto \sum_{i=1}^n u_i g_i, \end{aligned}$$

Via the isomorphism Ψ , we may endow the \mathbb{F}_{q^m} -vector space $\mathbb{F}_{q^m}^n$ with an algebra structure, by defining the product of two elements $u, v \in \mathbb{F}_{q^m}^n$ in the following way:

$$uv := \Psi^{-1}(\Psi(u)\Psi(v)).$$

Definition 2.1. Let $a \in \mathbb{F}_{q^m}G$. The *left ideal matrix* generated by a is the matrix

$$\mathcal{LIM}(a) := \begin{pmatrix} \Psi^{-1}(g_1 a) \\ \Psi^{-1}(g_2 a) \\ \vdots \\ \Psi^{-1}(g_n a) \end{pmatrix} \in \mathbb{F}_{q^m}^{n \times n}$$

Remark 2.2. The image via Ψ of the vector space generated by the lines of $\mathcal{LIM}(a)$ is the left ideal generated by a in $\mathbb{F}_{q^m}G$.

Note that the product of two vectors of $\mathbb{F}_{q^m}^n$ can be expressed as the usual product vector-matrix: for $u = (u_1, \dots, u_n), v = (v_1, \dots, v_n) \in \mathbb{F}_{q^m}^n$,

$$\begin{aligned} uv &= \Psi^{-1}(\Psi(u)\Psi(v)) = \Psi^{-1} \left(\sum_{i=1}^n u_i g_i \Psi(v) \right) = \sum_{i=1}^n u_i \Psi^{-1}(g_i \Psi(v)) \\ &= (u_1, \dots, u_n) \begin{pmatrix} \Psi^{-1}(g_1 \Psi(v)) \\ \Psi^{-1}(g_2 \Psi(v)) \\ \vdots \\ \Psi^{-1}(g_n \Psi(v)) \end{pmatrix} = u \mathcal{LIM}(\Psi(v)). \end{aligned}$$

Moreover, $\mathcal{LIM}(1)$ is clearly the identity. We are now interested in invertible left ideal matrices. In this regard, since the group algebra is finite, if an element is left invertible, it is also right invertible and conversely. Moreover, the left inverse and the right inverses coincide.

Proposition 2.3 (Proposition 9 of [3]). *An element $a \in \mathbb{F}_{q^m}G$ is invertible if and only if the left ideal matrix $\mathcal{LIM}(a)$ is invertible.*

The investigations of units in finite group algebra is a subject of intense research (see for example [8, 10, 11] and references therein).

3 Low-rank parity-check codes from group algebras

The LRPC codes have been introduced in [6]. This family of codes can be seen as the equivalent of classical LDPC codes for the rank metric. There is a natural analogy between low density matrices and matrices with low rank.

Definition 3.1. *Let λ, K, N be positive integers with $0 < K < N$. A **low-rank parity-check code** (LRPC) with parameter (λ, K, N) is a code with a parity-check matrix H such that $H = (h_{ij}) \in \mathbb{F}_{q^m}^{(N-K) \times N}$ is a full-rank matrix such that its coefficients generate an \mathbb{F}_q -subspace \mathcal{F} of dimension λ , i.e. $\dim_{\mathbb{F}_q}(\langle h_{ij} : i \in \{1, \dots, N-K\}, j \in \{1, \dots, N\} \rangle_{\mathbb{F}_q}) = \lambda$.*

For “small” values of λ , LRPC codes admit efficient probabilistic decoding algorithm (RSR) to recover the support of the error vector. More precisely, given as input an \mathbb{F}_q -basis of \mathcal{F} , $s = (s_1, \dots, s_\lambda) = eH^\top \in \mathbb{F}_{q^m}^N$ a syndrome of an error $e \in \mathbb{F}_{q^m}^N$ whose components belong to an \mathbb{F}_q -subspace \mathcal{E} of \mathbb{F}_{q^m} , then the RSR algorithm outputs \mathcal{E} . For more details see [6].

We may describe a low-rank parity-check code via its parity-check matrix. In order to reduce the size of a representation of this code, we can introduce left ideal low-rank parity-check codes via left ideal matrices.

Definition 3.2. *Let \mathcal{F} be an \mathbb{F}_q -subspace of dimension λ of \mathbb{F}_{q^m} and let $h_1, h_2 \in \mathbb{F}_{q^m}G$. Suppose that $\langle h_{i,j} : 1 \leq i \leq n, 1 \leq j \leq 2 \rangle_{\mathbb{F}_q} = \mathcal{F}$ where $\Psi^{-1}(h_1) = (h_{1,1}, \dots, h_{n,1})$, $\Psi^{-1}(h_2) = (h_{1,2}, \dots, h_{n,2})$ and either h_1 or h_2 is an invertible element of $\mathbb{F}_{q^m}G$. A LRPC code is called **left ideal** if it has a parity-check matrix*

$$H_{h_1, h_2} := (\mathcal{LIM}(h_1)^\top \mathcal{LIM}(h_2)^\top) \in \mathbb{F}_{q^m}^{n \times 2n}.$$

Since either h_1 or h_2 is invertible, by Proposition 2.3 either $\mathcal{LIM}(h_1)$ or $\mathcal{LIM}(h_2)$ is invertible, so that H_{h_1, h_2} is a full-rank matrix.

Theorem 3.3. *If \mathcal{C} is a left ideal LRPC code with parity-matrix H_{h_1, h_2} , with $h_1, h_2 \in \mathbb{F}_{q^m}G$ and either h_1 or h_2 is invertible, then the parameters of \mathcal{C} are $(\lambda, n, 2n)$, where*

$$\lambda = \dim_{\mathbb{F}_q}(\langle h_{i,j} : i \in \{1, \dots, n\}, j \in \{1, 2\} \rangle_{\mathbb{F}_q}),$$

where $\Psi^{-1}(h_1) = (h_{1,1}, \dots, h_{n,1})$ and $\Psi^{-1}(h_2) = (h_{1,2}, \dots, h_{n,2})$. If h_1 is invertible, then the systematic parity-check matrix of \mathcal{C} is $H_{1, h_2 h_1^{-1}} = (I_n \mathcal{LIM}(h_2 h_1^{-1})^\top)$.

Proof. Note that the entries of the vectors $\Psi^{-1}(g_i h_j)$ are the same of those of h_j , for any i and j , since the map $x \in G \mapsto x g_i \in G$ is a permutation of G . This implies that the \mathbb{F}_q -span of the entries of h_1 and h_2 corresponds to \mathcal{F} (that is the \mathbb{F}_q -span of the entries of H). Straightforward computations show the second part, which we omit for brevity. \square

A way to hide the structure of a left ideal LRPC code is to reveal only its systematic parity-check matrix.

4 ROLLO-I using group algebra left ideal LRPC codes

A Key-Encapsulation scheme $\text{KEM} = (\text{KeyGen}; \text{Encap}; \text{Decap})$ is a triple of probabilistic algorithms together with a key space \mathcal{K} . The key generation algorithm KeyGen generates a pair of public and secret key $(pk; sk)$. The encapsulation algorithm Encap uses the public key pk to produce an encapsulation c and a key $K \in \mathcal{K}$. Finally Decap , using the secret key sk and an encapsulation c , recovers the key K or fails and return error.

We adapt the Key-encapsulation scheme ROLLO I by using this left ideal LRPC codes constructed using group algebras.

KeyGen: • Pick randomly an \mathbb{F}_q -subspace \mathcal{F} of \mathbb{F}_{q^m} with dimension λ and pick $(x, y) \in \mathcal{F}^n \times \mathcal{F}^n$ such that the \mathbb{F}_q -span of the components of x and y is \mathcal{F} and $\Psi(x)$ is invertible (such a choice of x depends on the group algebra, but it is important to remark that a “general” element in a group algebra is invertible and that it is easy to check if an element is invertible or not).

- Compute $\Psi(h) = \Psi(y)\Psi(x)^{-1}$.
- Define $pk = (h, G)$ and $sk = (x, y)$.

Encap(pk): • Pick randomly an \mathbb{F}_q -subspace \mathcal{E} of \mathbb{F}_{q^m} with dimension r and pick $(e_1, e_2) \in \mathcal{E}^n \times \mathcal{E}^n$ such that the \mathbb{F}_q -span of the components of e_i is \mathcal{E} , for $i \in \{1, 2\}$

- Compute $\Psi(c) = \Psi(e_1) + \Psi(e_2)\Psi(h)$.
- Compute $K = \text{Hash}(\mathcal{E})$ and give as output c .

Dec(sk): • Compute $\Psi(c)\Psi(x) = \Psi(e_1)\Psi(x) + \Psi(e_2)\Psi(y)$, since $\Psi(h) = \Psi(y)\Psi(x)^{-1}$ and recover \mathcal{E} with the algorithm RSR.

- $K = \text{Hash}(\mathcal{E})$.

The above KEM scheme relies on the supposed hardness of following problem.

Problem 4.1. *Given an element $h \in \mathbb{F}_{q^m}G$, it is “hard” to distinguish whether the code \mathcal{C} with the parity-check matrix $H = (I_n \ \mathcal{LIM}(h)^\top)$ is a random left ideal code or if it is an left ideal LRPC code with parameter $(\lambda, n, 2n)$.*

In other words, it is “hard” to distinguish if h was sampled uniformly at random or as $h_2 h_1^{-1}$ where the \mathbb{F}_q -span of the components of the vectors h_1 and h_2 has dimension λ .

The large number of invertible elements in general group algebras and the fact that in general no canonical generators of ideals are known seems to suggest that the problem is likely to be hard. Note that if G is a cyclic group our construction of left ideal codes coincide with the the notion of quasi-cyclic code of index 2. In this case, there is a structural attack against this construction (see [7]). This implies that we have to suppose that G is not cyclic and suggests also to avoid the abelian case. If G is not cyclic, left ideal codes are similar to quasi- G codes of index 2 (see [2]), even if the transposition prevents them from being properly. It would be interesting to analyse if a similar attack exists also in this case.

It is possible also to readapt the Cryptosystems ROLLO II and ROLLO III, using this approach.

Acknowledgments

The last two authors were supported by the project “VALERE: VANviteLli pEr la RicErca” of the University of Campania “Luigi Vanvitelli” and by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM).

References

- [1] N. Aragon, P. Gaborit, A. Hauteville, O. Ruatta, and G. Zémor. Low rank parity check codes: New decoding algorithms and applications to cryptography. *IEEE Transactions on Information Theory*, 65(12):7697–7717, 2019.
- [2] M. Borello and W. Willems. On the algebraic structure of quasi group codes. *Journal of Algebra and its Applications*, 2022.
- [3] H. Chimal-Dzul, N. Gassner, J. Rosenthal, and R. Schnyder. Efficient description of some classes of codes using group algebras. In *25th International Symposium on Mathematical Theory of Networks and Systems (MTNS 2022)*, 2022.
- [4] I. El Qachchach, O. Habachi, J.-P. Cances, and V. Meghdadi. Efficient multi-source network coding using low rank parity check code. In *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–6. IEEE, 2018.
- [5] P. Gaborit, G. Murat, O. Ruatta, and G. Zémor. Low rank parity check codes and their application to cryptography. In *Proceedings of the Workshop on Coding and Cryptography WCC*, volume 2013, 2013.
- [6] P. Gaborit, G. Murat, O. Ruatta, and G. Zemor. Low Rank Parity Check codes and their application to cryptography. In L. Budaghyan, T. Helleseth, and M. G. Parker, editors, *The International Workshop on Coding and Cryptography (WCC 13)*, page 13 p., Bergen, Norway, Apr. 2013.
- [7] A. Hauteville and J.-P. Tillich. New algorithms for decoding in the rank metric and an attack on the lrpc cryptosystem. In *2015 IEEE International Symposium on Information Theory (ISIT)*, pages 2747–2751. IEEE, 2015.
- [8] N. Makhijani, R. Sharma, and J. Srivastava. The unit group of finite group algebra of a generalized dihedral group. *Asian-European Journal of Mathematics*, 7(02):1450034, 2014.
- [9] C. Melchor, N. Aragon, M. Bardet, S. Bettaieb, L. Bidoux, O. Blazy, J. Deneuville, P. Gaborit, A. Hauteville, A. Otmani, et al. ROLLO (merger of Rank-Ouroboros, LAKE and LOCKER). *Second round submission to the NIST post-quantum cryptography call*, 2020.
- [10] M. Sahai and S. F. Ansari. Unit groups of group algebras of certain dihedral groups-ii. *Asian-European Journal of Mathematics*, 12(04):1950066, 2019.
- [11] R. Sandling. Units in the modular group algebra of a finite abelian p-group. *Journal of Pure and Applied Algebra*, 33(3):337–346, 1984.

- [12] A. K. Yazbek, I. El Qachchach, J.-P. Cances, and V. Meghdadi. Low rank parity check codes and their application in power line communications smart grid networks. *International Journal of Communication Systems*, 30(12):e3256, 2017.