J Algebr Comb (2014) 40:83–136
DOI 10.1007/s10801-013-0480-7

Partial isomorphisms over finite fields

Pierre-Loïc Méliot

Received: 20 March 2013 / Accepted: 21 September 2013 / Published online: 16 October 2013

Abstract In this paper, we construct a combinatorial algebra of partial isomorphisms that gives rise to a "projective limit" of the centers of the group algebras $\mathbb{C}\mathrm{GL}(n, \mathbb{F}_q)$. It allows us to prove a $\mathrm{GL}(n, \mathbb{F}_q)$-analogue of a theorem of Farahat and Higman regarding products of conjugacy classes of permutations.

Keywords Combinatorics over finite fields · Linear groups · Ivanov–Kerov algebra

1 Introduction

In this paper, n is a positive integer; q is a prime power; $\mathbb{F}_q$ is a finite field with q elements; and $\mathrm{GL}(n, \mathbb{F}_q)$ is the group of invertible $n \times n$ matrices with coefficients in $\mathbb{F}_q$, or, equivalently, the group of linear isomorphisms of the $\mathbb{F}_q$-vector space $(\mathbb{F}_q)^n$. It will be convenient to write gh for the composition of isomorphisms $h \circ g$ (beware of the order of composition). The matrix of an isomorphism $u : V \to W$ between two $(\mathbb{F}_q)$-vector spaces and with respect to two bases $\mathcal{E} = (e_1, \dots, e_n)$ of V and $\mathcal{F} = (f_1, \dots, f_n)$ of W is

$$\mathrm{mat}_{\mathcal{E},\mathcal{F}}(u) = \mathrm{mat}_{\mathcal{F}}\big(u(e_1), \dots, u(e_n)\big),$$

the vectors being written in columns; then $\mathrm{mat}_{\mathcal{E},\mathcal{G}}(uv) = \mathrm{mat}_{\mathcal{F},\mathcal{G}}(v)\mathrm{mat}_{\mathcal{E},\mathcal{F}}(u)$.

1.1 Generic products in group algebras and the approach of Ivanov and Kerov

If $G = \mathrm{GL}(n, \mathbb{F}_q)$, we shall be interested in the group algebra $\mathbb{C}G$, and more precisely in its center $Z(\mathbb{C}G)$. A linear basis of $Z(\mathbb{C}G)$ is the set of conjugacy classes of G,

P.-L. Méliot (✉)
Laboratoire de Mathématiques, Bâtiment 425, Faculté des Sciences d'Orsay, Université Paris-Sud, 91405, Orsay, France
e-mail: pierre-loic.meliot@math.u-psud.fr

viewed as the formal sums of their elements. We want to address the following kind of problem:

Problem 1.1 Let $a \neq b \neq 1$ be two elements of $(\mathbb{F}_q)^\times$, and $C_{a,n}$ and $C_{b,n}$ the conjugacy classes of the diagonal matrices of size n

$$D_a = \begin{pmatrix} a & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \quad \textit{and} \quad D_b = \begin{pmatrix} b & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}.$$

What is the expansion $\sum_{\lambda \in \Lambda(a,b)} c^{\lambda}_{a,b,n} C_\lambda$ in conjugacy classes of the product $C_{a,n} * C_{b,n}$ computed in the center of the group algebra $Z(\mathbb{C}\mathrm{GL}(n, \mathbb{F}_q))$?

At first sight, this problem might seem to be not so difficult: since D_a and D_b each leave invariant a subspace of dimension $n-1$, the product $P = AB$ of two matrices conjugated to D_a and D_b has to leave invariant a subspace of dimension at least $n-2$, and as we shall see in a moment, this only leaves a few possibilities for the conjugacy class λ of P. Moreover, by looking at how many ways the eigenspaces of the matrices can intersect, one can guess that the coefficients $c^{\lambda}_{a,b,n}$ count configurations of subspaces in $(\mathbb{F}_q)^n$, and are therefore rational functions in q and in its powers q^k, up to $k = n$.

However, it is in practice quite hard to determine the set of possible conjugacy classes $\Lambda(a,b)$; and also quite hard to compute the structure coefficients. The reader can already have a look at Theorem 4.1, to realize that the result depends in particular on:

- whether q is even or odd;
- in the odd case, whether ab is a square in $(\mathbb{F}_q)^\times$ or not.

Also, it is *a priori* unclear that the coefficients $c^{\lambda}_{a,b,n}$ are in fact all polynomials in q^n, with rational coefficients independent of n. One might understand intuitively why this is true from the previous informal discussion: every number of subspaces of fixed dimension k in $(\mathbb{F}_q)^n$ is a polynomial in q^n (of degree k), and the same holds when counting "finite-dimensional configurations". However, a formal and rigorous proof demands a lot of combinatorial preparations, especially if one wants to *compute* the actual polynomials. The author conjectured this polynomiality a few years ago, and this will be one of the major result of the paper. We shall prove it in the general setting where D_a and D_b are replaced by arbitrary matrices A and B that are completed by 1's on the diagonal to obtain matrices of size n. We shall also provide a general framework which reduces all the computations to the case when $n = k + l$, k and l being the sizes of A and B ($k = l = 1$ for $A = D_a$ and $B = D_b$). In other words, knowing the structure coefficients $c^{\lambda}_{A,B,k+l}$, we shall have at the end of the paper an easy rule to compute all the coefficients $c^{\lambda}_{A,B,n}$.

A similar and simpler problem has been solved for permutations by Farahat and Higman in [7], and 40 years later, it was given a beautiful explanation by Ivanov and Kerov, see [12]. Fix two permutations σ and ρ of size k and l; we also assume σ and

ρ without fixed points in $[\![1,k]\!]$ and in $[\![1,l]\!]$. For any $n \geq \max(k,l)$, one can view σ and ρ as elements of the symmetric group of order n, denoted $\mathfrak{S}(n)$; σ fixes the integers after k and ρ fixes the integer after l. Denote $C_{\sigma,n}$ and $C_{\rho,n}$ the conjugacy classes of σ and ρ in $\mathbb{C}\mathfrak{S}(n)$. Then, there exist a unique finite set of permutations $S(\sigma,\rho) \subset \mathfrak{S}(k+l)$ and polynomials $p^{\nu}_{\sigma,\rho}(n)$ with rational coefficients and integer values at integers, such that

$$C_{\sigma,n} * C_{\rho,n} = \sum_{\nu \in S(\sigma,\rho)} p^{\nu}_{\sigma,\rho}(n) C_{\nu,n}.$$

Using the well-known labeling of conjugacy classes of $\mathfrak{S}(n)$ by integer partitions of size n, one can of course restate this result with two partitions λ and μ of size k and l and without parts of size 1, and a finite set of partitions of size smaller than $k+l$ and again without parts of size 1:

$$C_{\lambda \sqcup 1^{n-k}} * C_{\mu \sqcup 1^{n-l}} = \sum_{|\rho| \leq k+l} p^{\rho}_{\lambda,\mu}(n) C_{\rho \sqcup 1^{n-|\rho|}}.$$

The proof of Ivanov and Kerov uses the following idea: by manipulating *partial permutations* that are permutations with a distinguished support $A \subset [\![1,n]\!]$, one can construct an inverse system of graded algebras

$$\cdots \longrightarrow \mathscr{Z}(n+2) \longrightarrow \mathscr{Z}(n+1) \longrightarrow \mathscr{Z}(n) \longrightarrow \cdots,$$

such that:

1. each algebra $\mathscr{Z}(n)$ projects onto $Z(\mathbb{C}\mathfrak{S}(n))$ via a morphism π_n;
2. each algebra has a basis $(A_{\lambda,n})_\lambda$ labeled by partitions λ of size smaller than n, with $\pi_n(A_{\lambda,n}) = p_\lambda(n) C_{\lambda,n}$; $p_\lambda(n)$ is an explicit polynomial in n;
3. the bases $A_{\lambda,n}$ are compatible, *i.e.*, if $|\lambda| \leq n$, then the map $\mathscr{Z}(n+1) \to \mathscr{Z}(n)$ sends $A_{\lambda,n+1}$ to $A_{\lambda,n}$.

From this construction, the identity

$$A_\lambda * A_\mu = \sum_{|\nu| \leq |\lambda|+|\mu|} c^{\nu}_{\lambda,\mu} A_\nu$$

in the projective limit $\mathscr{Z}(\infty) = \varprojlim_{n\to\infty} \mathscr{Z}(n)$ gives immediately the identity

$$C_{\lambda,n} * C_{\mu,n} = \sum_{|\nu| \leq |\lambda|+|\mu|} c^{\nu}_{\lambda,\mu} \frac{p_\nu(n)}{p_\lambda(n) p_\mu(n)} C_{\nu,n}$$

in all the centers of the group algebras $Z(\mathbb{C}\mathfrak{S}(n))$; this provides an easy proof of the theorem of Farahat and Higman. The same techniques and kind of results have been studied more recently by the author for product of Geck–Rouquier elements in the centers of the Hecke algebras $\mathscr{H}_q(\mathfrak{S}_n)$ of the symmetric groups (*cf.* [16]); and by O. Tout in [24] for product of classes in the algebras $\mathbb{C}[\mathfrak{H}(n) \backslash \mathfrak{S}(2n) / \mathfrak{H}(n)]$ associated to the Gelfand pairs $(\mathfrak{S}(2n), \mathfrak{H}(n))$.

The objective of this paper is to follow the same program for general linear groups over finite fields; unfortunately, in this setting, there are a lot of complications in comparison to the framework previously described. The naive idea is of course to replace partial permutations by *partial isomorphisms*; but there are two major obstacles to this idea.

1. For permutations, if $\sigma \in \mathfrak{S}(A)$ with $A \subset [\![1,n]\!]$ of size k, then there is a unique canonical way to see σ as an element of $\mathfrak{S}(n)$; as explained before, one leaves the integers outside A fixed by σ. The same cannot be done in a canonical way for isomorphisms: if g is an $\mathbb{F}_q$-isomorphism of a subspace $V \subset (\mathbb{F}_q)^n$ of dimension k, then g admits a lot of extensions to isomorphisms of $(\mathbb{F}_q)^n$, related to the choice of complement subspaces of V inside $(\mathbb{F}_q)^n$. And there is no reason or possibility to distinguish a particular extension among those.
2. Knowing that, a natural thing to do is to take the *mean of all possible extensions*; it seems then possible to define correctly the product of partial isomorphisms. But this still does not work: as we shall explain later (see Remark 2.22), the algebra that one obtains by this construction is not associative.

The solution to these problems, and the main idea of this paper, is to define partial isomorphisms as *pairs* of isomorphisms between two subspaces.

Remark 1.2 An alternative construction of partial bijections and partial isomorphisms has been proposed by G. Olshanski in [21, 22]. Let $G = \varinjlim_{n\to\infty} G(n)$ an inductive limit of finite groups, and $G \supset K(0) \supset K(1) \supset \cdots \supset K(n) \supset \cdots$ a chain of subgroups of G, such that $K(n)$ commutes with $G(n)$ for all n. For instance one can take

$$\begin{aligned} & G(n) = \mathfrak{S}(n); && K(n) = \bigl\{\sigma \in \mathfrak{S}(\infty) \mid \sigma_{[\![1,n]\!]} = \mathrm{id}_{[\![1,n]\!]}\bigr\}; \\ \text{or}\quad & G(n) = \mathrm{GL}(n, \mathbb{F}_q); && K(n) = \bigl\{g \in \mathrm{GL}(\infty, \mathbb{F}_q) \mid g_{|(\mathbb{F}_q)^n} = \mathrm{id}_{(\mathbb{F}_q)^n}\bigr\}. \end{aligned}$$

In these situations, there is a structure of semigroup on the set of double cosets $\Gamma(n) = K(n)\backslash G/K(n)$. For instance, when $G = \mathfrak{S}(\infty)$, $\Gamma(n)$ can be identified with the set of bijections $\sigma : A \to B$ between two parts A and B of $[\![1,n]\!]$, and the product is

$$(\sigma : A \to B) * (\tau : C \to D) = \bigl(\sigma\tau : \sigma^{-1}(B \cap C) \to \tau(B \cap C)\bigr).$$

Notice that the product $*$ written above is quite different from the product of partial permutations defined in [12], or from the product of partial bijections defined in [24]. A similar construction of semigroup can be performed when $G = \mathrm{GL}(\infty, \mathbb{F}_q)$. However, these semigroups (or the sets of double cosets $K(n)\backslash G \times G/K(n)$, studied in Okounkov's thesis [19]), do not really help for the specific problem that we are looking at, namely, the understanding of the structure coefficients of the group algebra centers $\mathbb{C}G(n)$: indeed, there is no natural morphism of semigroups $\Gamma(n) \to G(n)$.

Unfortunately, we do not see how to use *semigroup algebras* $\mathcal{Z}(n, \mathbb{F}_q)$ in order to construct a projective limit of the centers $\mathbb{C}\mathrm{GL}(n, \mathbb{F}_q)$; we shall, however, be satisfied with *combinatorial algebras* labeled by partial isomorphisms, without an underlying structure of semigroup on the partial isomorphisms.

1.2 Conjugacy classes of matrices and polypartitions

For finite general linear groups, the conjugacy classes are given by Jordan's reduction of matrices. If $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ is a monic polynomial, its Jordan matrix is the $n \times n$ matrix

$$J(P) = \begin{pmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & -a_{n-2} \\ & & & 1 & -a_{n-1} \end{pmatrix}.$$

Call partition of size k a non-increasing sequence of positive integers $(\mu_1, \ldots, \mu_\ell)$ with $|\mu| = \sum_{i=1}^{\ell} \mu_i = k$.

Definition 1.3 A polypartition of size n over the finite field $\mathbb{F}_q$ is a family of partitions

$$\mathbb{\mu} = \{\mu(P_1), \ldots, \mu(P_r)\}$$

labeled by monic irreducible polynomials over $\mathbb{F}_q$, all different from X, and such that

$$|\mathbb{\mu}| = \sum_{i=1}^{r} (\deg P_i) \bigl|\mu(P_i)\bigr| = n.$$

To such a polypartition, we associate the block-diagonal matrix $J(\mathbb{\mu})$ whose blocks are the Jordan matrices $J((P_i)^{(\mu(P_i))_j})$ with $i \in [\![1, r]\!]$ and $j \in [\![1, \ell(\mu(P_i))]\!]$. For instance, if $\mathbb{\mu} = ((2,1)_{P_1}, (1,1)_{P_2})$, then

$$J(\mathbb{\mu}) = \begin{pmatrix} J((P_1)^2) & & & \\ & J(P_1) & & \\ & & J(P_2) & \\ & & & J(P_2) \end{pmatrix}.$$

Jordan's reduction ensures that each conjugacy class of $\mathrm{GL}(n, \mathbb{F}_q)$ contains a unique matrix $J(\mathbb{\mu})$ with $\mathbb{\mu}$ polypartition of size n over $\mathbb{F}_q$; this result is a classical consequence of the classification of finitely generated modules over principal rings (here, $\mathbb{F}_q[X]$). Thus, a linear basis of $Z(\mathbb{C}\mathrm{GL}(n, \mathbb{F}_q))$ consists in the classes $C_{\mathbb{\mu}}$ labeled by the set $\mathfrak{P}(n, \mathbb{F}_q)$ of these polypartitions. All the elements in $C_{\mathbb{\mu}}$ have for characteristic and minimal polynomials

$$\chi_{\mathbb{\mu}}(X) = \prod_{i=1}^{r} \bigl(P_i(X)\bigr)^{|\mu(P_i)|}; \qquad m_{\mathbb{\mu}}(X) = \prod_{i=1}^{r} \bigl(P_i(X)\bigr)^{(\mu(P_i))_1}.$$

On the other hand, it can be shown that

$$\operatorname{card} C_{\mathbb{\mu}} = \frac{(q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})}{q^{|\mathbb{\mu}| + 2b(\mathbb{\mu})} \prod_{i=1}^{r} \prod_{k \geq 1} (q^{-\deg P_i})_{m_k(\mu(P_i))}}$$

where $b(\mathbb{\mu}) = \sum_{i=1}^{r} (\deg P_i) b(\mu(P_i)) = \sum_{i=1}^{r} \sum_{j=1}^{\ell(\mu(P_i))} (\deg P_i)(j-1)(\mu(P_i))_j$; $(x)_m = (x;x)_m$ is the Pochhammer symbol $(1-x)(1-x^2)\cdots(1-x^m)$; and $m_k(\mu)$ is the number of parts k in a partition μ. This formula is proven by using Hall's theory of modules over discrete valuation rings, see [15, Chaps. 2, 4].

Example 1.4 Consider the $\mathbb{F}_5$-polypartition $\mathbb{\mu} = \{x^2+x+1 : (2), x+3 : (1,1)\}$. A representative of this conjugacy class in $\mathrm{GL}(6,\mathbb{F}_5)$ is the Jordan matrix

$$\begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 1 & 0 & 0 & 3 \\ 0 & 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 0 & 1 & 3 \end{pmatrix},$$

and the cardinality of the class is

$$\frac{(5^6-1)(5^6-5)(5^6-5^2)(5^6-5^3)(5^6-5^4)(5^6-5^5)}{5^{6+2}(1-5^{-2})(1-5^{-1})(1-5^{-2})} = 38418317437500000000.$$

For a polypartition $\mathbb{\mu}$ of size $k \leq n$, denote $\mathbb{\mu}\uparrow^n$ the polypartition of size n obtained by adding parts 1 to the partition $\mu(X-1)$. This amounts to complete matrices with 1's on the diagonal in the bottom right corner. Therefore, our initial problem can be reformulated and generalized as follows:

Problem 1.5 Fix two polypartitions $\mathbb{\lambda}$ and $\mathbb{\mu}$ of size k and l. What is the expansion of $C_{\mathbb{\lambda}\uparrow^n} * C_{\mathbb{\mu}\uparrow^n}$ in completed conjugacy classes

$$\sum_{\mathbb{\nu}} c_{\mathbb{\lambda}\mathbb{\mu}}^{\mathbb{\nu}}(n) C_{\mathbb{\nu}\uparrow^n}?$$

In particular, what is the dependence in n of the structure coefficients $c_{\mathbb{\lambda}\mathbb{\mu}}^{\mathbb{\nu}}(n)$?

1.3 Centers as Hecke algebras and outline of the paper

Denote G^{opp} the set G endowed with the opposite of the product of the group G; $g \mapsto g^{-1}$ is then an isomorphism of groups between G and G^{opp}. It will be extremely important in our discussion to see $\mathscr{Z}(\mathbb{C}G)$ as the Hecke algebra $\mathbb{C}[G\backslash(G \times G^{\mathrm{opp}})/G^{\mathrm{opp}}]$—this fact is true for every finite group G. Consider indeed the double action of G and G^{opp} on $G \times G^{\mathrm{opp}}$ given by $g \cdot (g_1, g_2) \cdot h = ((g g_1 h^{-1}), (h g_2 g^{-1}))$. These actions correspond to the injective maps

$$\begin{aligned} G &\hookrightarrow G \times G^{\mathrm{opp}}; & G^{\mathrm{opp}} &\hookrightarrow G \times G^{\mathrm{opp}} \\ g &\mapsto (g, g^{-1}) & h &\mapsto (h^{-1}, h). \end{aligned}$$

Let us determine the orbit of an element (g_1, g_2) under the action on the left by G and on the right by G^{opp}. Since one can multiply on the right by (g_2, g_2^{-1}) to obtain

(g_1g_2, e_G), the orbit depends only on g_1g_2. Then, if (g_1g_2, e_G) and (h_1h_2, e_G) are in the same orbit, there exist $k, l \in G$ such that

$$g_1g_2 = k(h_1h_2)l^{-1}; \qquad lk^{-1} = e_G.$$

Thus, $g_1g_2 = k(h_1h_2)k^{-1}$, and we have proved that the orbit of (g_1, g_2) consists in pairs (h_1, h_2) such that g_1g_2 and h_1h_2 are conjugated. For a conjugacy class C_λ of G, denote

$$C'_\lambda = \frac{1}{\operatorname{card} G} \sum_{g_1g_2 \in C_\lambda} (g_1, g_2) \in \mathbb{C}\bigl[G\backslash\bigl(G \times G^{\mathrm{opp}}\bigr)/G^{\mathrm{opp}}\bigr].$$

Suppose that $C_\lambda C_\mu = \sum_\nu a^\nu_{\lambda\mu} C_\nu$. Then, a simple computation allows one to check that $C'_\lambda C'_\mu = \sum_\nu a^\nu_{\lambda\mu} C'_\nu$. Therefore, the map

$$\begin{aligned} \mathbb{C}\bigl[G\backslash\bigl(G \times G^{\mathrm{opp}}\bigr)/G^{\mathrm{opp}}\bigr] &\to \mathbb{Z}(\mathbb{C}G) \\ C'_\lambda &\mapsto C_\lambda \end{aligned}$$

realizes an isomorphism of commutative complex algebras.

We are looking for a family of algebras $\mathcal{Z}(n, \mathbb{F}_q)$ with the following properties. We want them to form an inverse system of graded algebras

$$\cdots \longrightarrow \mathcal{Z}(n+2, \mathbb{F}_q) \longrightarrow \mathcal{Z}(n+1, \mathbb{F}_q) \longrightarrow \mathcal{Z}(n, \mathbb{F}_q) \longrightarrow \cdots,$$

so that in the end we will be able to look at the projective limit $\mathcal{Z}(\infty, \mathbb{F}_q)$, which will allow us to make generic computations. Then, we want these algebras to project onto the centers $Z(\mathbb{C}\mathrm{GL}(n, \mathbb{F}_q))$ of the group algebras of the general linear groups over $\mathbb{F}_q$, so that these generic computations will turn into generic identities between conjugacy classes of isomorphisms. Finally, we wish to construct the $\mathcal{Z}(n, \mathbb{F}_q)$'s in a fashion similar to [12, 24], which is very combinatorial and natural. This means that we want to define the elements of $\mathcal{Z}(n, \mathbb{F}_q)$ as linear combinations of partial isomorphisms of $(\mathbb{F}_q)^n$, this notion staying for the moment vague and undefined.

Since $Z(n, \mathbb{F}_q) = Z(\mathbb{C}\mathrm{GL}(n, \mathbb{F}_q))$ can be seen as a Hecke subalgebra of the algebra $\mathbb{C}[\mathrm{GL}(n, \mathbb{F}_q) \times (\mathrm{GL}(n, \mathbb{F}_q))^{\mathrm{opp}}]$, the way to do it will be to do the same construction with algebras $\mathcal{A}(n, \mathbb{F}_q)$ that project onto the group algebras $\mathbb{C}[\mathrm{GL}(n, \mathbb{F}_q) \times (\mathrm{GL}(n, \mathbb{F}_q))^{\mathrm{opp}}]$. Then, to obtain the $\mathcal{Z}(n, \mathbb{F}_q)$'s, we shall just look at invariant subalgebras of these $\mathcal{A}(n, \mathbb{F}_q)$'s. Our paper is therefore organized as follows:

- In Sect. 2, we define partial isomorphisms of $(\mathbb{F}_q)^n$ and their product, and we prove that we obtain indeed an algebra $\mathcal{A}(n, \mathbb{F}_q)$ (Theorem 2.8). The main difficulty is to see that the product is associative; this is related to the properties of certain linear operators on the algebra, and the associativity in $\mathcal{A}(n, \mathbb{F}_q)$ is essentially equivalent to the commutativity of the algebra formed by these operators.
- In Sect. 3, we look at some invariant subalgebras $\mathcal{Z}(n, \mathbb{F}_q) \subset \mathcal{A}(n, \mathbb{F}_q)$, and we prove that they form an inverse system of graded commutative algebras that project onto the centers $Z(n, \mathbb{F}_q)$. We deduce from it the result of polynomiality of the structure coefficients that we have evoked in this introduction; see our main Theorem 3.7.

– Finally, in Sect. 4, we give the table of multiplication of all elements of degree 1 in the projective limit $\mathscr{Z}(\infty, \mathbb{F}_q)$. This gives in particular a concrete answer to the first problem stated in this paper.

We conclude this introduction by two important remarks.

Remark 1.6 In essence, this paper relies only on linear algebra and combinatorics over finite fields. However, some of the results and proofs will be written using the language of probability: so, we shall speak freely of probability laws, conditional laws, Markov chains, *etc*., and we refer to [3] for any detail on these notions. The reason is that the product of the algebra $\mathscr{A}(n, \mathbb{F}_q)$ of partial isomorphisms that we shall study will be defined by taking averages of certain extensions of the partial isomorphisms. Thus, discrete probability will provide in many situations a convenient way to describe and prove identities in $\mathscr{A}(n, \mathbb{F}_q)$. Since we are only dealing with finite sets, for pure algebraists, every "probabilistic" statement can be replaced by a statement with a function on a finite set taking non-negative values that sum to 1. So probability is rather a commodity of language and a way of thinking than an absolute necessity in our reasonings.

Remark 1.7 The reader may naturally ask what could be the uses of the theory of partial isomorphisms developed in this paper. We think of it as a first step in a much larger program, namely, the asymptotic representation theory of the finite general linear groups $\mathrm{GL}(n, \mathbb{F}_q)$—other important approaches appear in the papers [10, 11, 14]. For symmetric groups $\mathfrak{S}(n)$, an important problem is to understand the asymptotic behavior of the random character value $\chi^\lambda(\sigma)$, where σ is a fixed permutation and χ^λ is a random irreducible character of $\mathfrak{S}(n)$ taken under some spectral measure, for instance the Plancherel measure of the group. These random character values are important examples of random variables "with a non-commutative flavor", and their asymptotic behavior is related to random matrix theory, exclusion processes of particles, free probability, and many other topics; see for instance [1, 4, 5, 20]. The Ivanov–Kerov algebra of partial permutations has proven extremely useful in order to compute the moments of these random character values $\chi^\lambda(\sigma)$; thus, they allowed to determine their asymptotic distribution. Indeed, the computation of the moments $\mathbb{E}[(\chi^\lambda(\sigma))^k]$ is directly related to the computation of products and powers of conjugacy classes in symmetric group algebras. We refer in particular to [2, 8, 13, 17, 18, 23], where such techniques and results are detailed.

We hope to be able to follow the same program for finite linear groups $\mathrm{GL}(n, \mathbb{F}_q)$. In particular, among the problems that we wish to solve after this paper, let us ask the following question. Take the normalized trace $\mathbb{1}_{I_n}$ of $\mathbb{C}\mathrm{GL}(n, \mathbb{F}_q)$, which expands as linear combination of all irreducible normalized characters of the group:

$$\mathbb{1}_{(g=I_n)} = \sum_{\mathbb{\lambda} \in \mathfrak{P}(n, \mathbb{F}_q)} \frac{(\dim V^{\mathbb{\lambda}})^2}{\operatorname{card} \mathrm{GL}(n, \mathbb{F}_q)} \chi^{\mathbb{\lambda}}(g).$$

For g fixed (say, g is a diagonal matrix D_a) and completed by 1's on the diagonal, we consider $X_g = \chi^{\mathbb{\lambda}}(g)$ as a random variable under the probability measure

$$\mathbb{P}_{n,q}[\mathbb{\lambda}] = \frac{(\dim V^{\mathbb{\lambda}})^2}{\operatorname{card} \mathrm{GL}(n, \mathbb{F}_q)},$$

which is the Plancherel measure of the group. What are the asymptotics of the law of X_g? To compute the moments of X_g amounts to compute the powers of $C_{\mathbb{\mu}}$ in the group algebras $\mathbb{C}\mathrm{GL}(n, \mathbb{F}_q)$, where $\mathbb{\mu}$ is the conjugacy class of g; whence the interest of our results for the asymptotic analysis of the random character values X_g. The idea would then be to use these observables X_g to get a better understanding of the properties of asymptotic concentration of the measures $\mathbb{P}_{n,q}$; in particular, one should be able to recover this way the results of [6, 9].

1.4 List of common notations

To help the reader keep track of the notations, and of the various characters appearing as exponents or indices throughout the paper, we have listed hereafter the conventions that we shall use, see Table 1. On the other hand, we recall the Pochhammer symbol $(q^{-1})_n = (1 - q^{-1})(1 - q^{-2}) \cdots (1 - q^{-n})$. In the following we shall try to write every enumeration as a polynomial in q and in these Pochhammer symbols in q^{-1}.

2 Partial isomorphisms and their algebra

Fix $n \geq 1$ and a finite field $\mathbb{F}_q$.

2.1 Partial isomorphisms and trivial extensions

Definition 2.1 A partial isomorphism of $(\mathbb{F}_q)^n$ is a pair $(g_1 : V \to W, g_2 : W \to V)$, where V and W are two vector subspaces of same dimension k in $(\mathbb{F}_q)^n$, and g_1 and g_2 are isomorphisms between these spaces.

We shall use the notation $(V \;{}^{g_1}\!\rightleftarrows_{g_2}\; W)$ for a partial isomorphism, and the set of all partial isomorphisms of $(\mathbb{F}_q)^n$ will be denoted $\mathscr{I}(n, \mathbb{F}_q)$. Recall that the number of isomorphisms of a $\mathbb{F}_q$-vector space of dimension k is

$$\left(q^k - 1\right)\left(q^k - q\right) \cdots \left(q^k - q^{k-1}\right) = q^{k^2} \left(q^{-1}\right)_k,$$

and the number of vector subspaces of dimension k inside $(\mathbb{F}_q)^n$ is

$$\frac{(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1})}{(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})} = q^{(n-k)k} \frac{(q^{-1})_n}{(q^{-1})_{n-k} (q^{-1})_k}.$$

Therefore, the cardinality of $\mathscr{I}(n, \mathbb{F}_q)$ is

$$\sum_{k=0}^{n} q^{2nk} \left(\frac{(q^{-1})_n}{(q^{-1})_{n-k}} \right)^2.$$

Table 1 List of common notations

q	cardinality of the base field $\mathbb{F}_q$
n	dimension of the ambient vector space $(\mathbb{F}_q)^n$
$\mathrm{M}(k \times l, \mathbb{F}_q)$	space of matrices with k rows and l columns, and coefficients in $\mathbb{F}_q$
$\mathrm{GL}(n, \mathbb{F}_q)$	group of linear isomorphisms of $(\mathbb{F}_q)^n$
$\mathscr{I}(n, \mathbb{F}_q)$	set of partial isomorphisms of $(\mathbb{F}_q)^n$
$\mathscr{A}(n, \mathbb{F}_q)$	algebra of partial isomorphisms over $(\mathbb{F}_q)^n$
$\mathscr{Z}(n, \mathbb{F}_q)$	subalgebra of invariants for the double action of $\mathrm{GL}(n, \mathbb{F}_q)$
$U, V, W, \ldots$	vector subspaces of the ambient vector space
$U^+, V^+, \ldots$	larger vector subspaces containing $U, V, \ldots$
$k, l, m, \ldots$	dimensions of vector subspaces of $(\mathbb{F}_q)^n$
$\mathcal{E} = (e_1, \ldots, e_k)$	basis of a vector subspace of dimension k
$\mathcal{E}^+ = (e_1, \ldots, e_{k^+})$	completion of the basis $\mathcal{E}$ in a basis of a larger subspace of dimension k^+
$\mathrm{Span}(e_1, \ldots, e_k)$	vector space spanned by the independent vectors $e_1, \ldots, e_k$
$\boldsymbol{\mu}$	polypartition (family of partitions labeled by polynomials)
$t(g)$	type of an automorphism $g : V \to V$, given by a polypartition
$\mu(P)$	partition in a polypartition $\boldsymbol{\mu}$ corresponding to the polynomial P
g_1, g_2	isomorphisms between vector subspaces of $(\mathbb{F}_q)^n$
g^+	extension of an isomorphism $g : V \to W$ to larger subspaces V^+ and W^+
$\mathrm{mat}_{\mathcal{E},\mathcal{F}}(g)$	matrix of $g : V \to W$ written with respect to two bases $\mathcal{E}$ of V and $\mathcal{F}$ of W
$(V\ {}^{g_1}\!\rightleftarrows_{g_2} W)$	partial isomorphism given by the two arrows $g_1 : V \to W$ and $g_2 : W \to V$
k_1	dimension of $\mathrm{Fix}(g_1 g_2)$, which is also $\ell(\mu(X-1))$ if $t(g_1 g_2) = \boldsymbol{\mu}$
k_{11}	$m_1(\mu(X-1))$ if $t(g_1 g_2) = \boldsymbol{\mu}$
$\mathscr{E}(V\ {}^{g_1}\!\rightleftarrows_{g_2} W \uparrow W^+)$	set of trivial extensions of $(V\ {}^{g_1}\!\rightleftarrows_{g_2} W)$ with fixed right subspace W^+
$\mathscr{E}(V^+ \uparrow V\ {}^{g_1}\!\rightleftarrows_{g_2} W)$	set of trivial extensions of $(V\ {}^{g_1}\!\rightleftarrows_{g_2} W)$ with fixed left subspace V^+
$E_q(n, k^+, k, k_1)$	cardinality of the previous sets if $k^+ = \dim V^+$, $k = \dim V$ and $k_1 = \dim \mathrm{Fix}(g_1 g_2)$
$\mathscr{E}(V^+ \uparrow V\ {}^{g_1}\!\rightleftarrows_{g_2} W \uparrow W^+)$	set of trivial extensions of $(V\ {}^{g_1}\!\rightleftarrows_{g_2} W)$ with fixed left and right subspaces V^+ and W^+
$F_q(k^+, k, k_1)$	cardinality of the previous sets if $k^+ = \dim V^+$, $k = \dim V$ and $k_1 = \dim \mathrm{Fix}(g_1 g_2)$
$\mathrm{L}_V^{V^+}, \mathrm{R}_W^{W^+}, \mathrm{LR}_{(V,W)}^{(V^+,W^+)}$	extension operators with fixed subspaces
$\mathrm{L}^V, \mathrm{R}^W$	extension operators
X_n	$\mathrm{rank}(v_1, \ldots, v_n)$, with the v_i's independent uniform random vectors
$\mathbb{P}_{d,q}$	probabilities related to $(X_n)_{n \in \mathbb{N}}$ in a $\mathbb{F}_q$-vector space of dimension d
$\mathbb{UF}_m, \mathbb{UF}_V$	uniform law on free families of size m in $(\mathbb{F}_q)^n$, or on bases of V
$\mathbb{U}_m, \mathbb{U}_{m,V}$	uniform law on vector subspaces of dimension m, or on vector subspaces of dimension m and containing V
$\mathbb{C}_{l,U,W,Y}$	uniform law on vector subspaces of dimension l, containing U, and whose sum with W is Y

Table 1 (*Continued*)

π_n	projection from $\mathcal{A}(n, \mathbb{F}_q)$ to $\mathbb{C}[\mathrm{GL}(n, \mathbb{F}_q) \times (\mathrm{GL}(n, \mathbb{F}_q))^{\mathrm{opp}}]$
$\phi_n^{n'}$	projection from $\mathcal{Z}(n', \mathbb{F}_q)$ to $\mathcal{Z}(n, \mathbb{F}_q)$
Π_n	projection from $\mathcal{Z}(\infty, \mathbb{F}_q)$ to $Z(\mathbb{C}\mathrm{GL}(n, \mathbb{F}_q))$
$A_{\pmb{\mu},n}, \widehat{A}_{\pmb{\mu},n}, \widetilde{A}_{\pmb{\mu},n}$	various renormalizations of the class of label $\pmb{\mu}$ in $\mathcal{Z}(n, \mathbb{F}_q)$
$\widehat{A}_{\pmb{\mu}}$	generic conjugacy class of label $\pmb{\mu}$ in $\mathcal{Z}(\infty, \mathbb{F}_q)$
$C_{\pmb{\mu}\uparrow^n}$	completed conjugacy class of label $\pmb{\mu}$ in $Z(\mathbb{C}\mathrm{GL}(n, \mathbb{F}_q))$
$\widetilde{C}_{\pmb{\mu}\uparrow^n}$	normalized class $C_{\pmb{\mu}\uparrow^n}/(\mathrm{card}\, C_{\pmb{\mu}\uparrow^n})$

There is a natural action of $\mathrm{GL}(n, \mathbb{F}_q)$ (respectively, of $(\mathrm{GL}(n, \mathbb{F}_q))^{\mathrm{opp}}$) on the left (resp., on the right) of $\mathcal{I}(n, \mathbb{F}_q)$, namely,

$$k \cdot \left(V\ {}^{g_1}\!\rightleftarrows_{g_2}\ W\right) \cdot l = \left(k^{-1}(V)\ {}^{kg_1l^{-1}}\!\rightleftarrows_{lg_2k^{-1}}\ l^{-1}(W)\right).$$

The orbits of this double action are labeled by polypartitions of size $k \in [\![0, n]\!]$. Indeed, it is easy to see that the orbit of a partial isomorphism $(V\ {}^{g_1}\!\rightleftarrows_{g_2}\ W)$ is entirely determined by the type (polypartition) of the composed isomorphism $g_1g_2 : V \to V$ (or, of the composed isomorphism $g_2g_1 : W \to W$, since they have same type). Thus, if we are able to construct an algebra $\mathcal{A}(n, \mathbb{F}_q)$ out of $\mathcal{I}(n, \mathbb{F}_q)$, we will readily obtain a candidate for $\mathcal{Z}(n, \mathbb{F}_q)$ by looking at these orbits. Therefore, the main problem that we shall address in this section is the definition of the product of two partial isomorphisms.

Example 2.2 Over the finite field $\mathbb{F}_5$, consider the subspaces $V = \mathrm{Span}((1, 0, 0), (0, 1, 0))$ and $W = \mathrm{Span}((0, 1, 0), (0, 0, 1))$ inside $(\mathbb{F}_5)^3$. With respect to the previously given bases, the matrices $\left(\begin{smallmatrix}1&2\\0&1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}3&3\\1&2\end{smallmatrix}\right)$ define two isomorphisms $g_1 : V \to W$ and $g_2 : W \to V$. The type of the partial isomorphism $(V\ {}^{g_1}\!\rightleftarrows_{g_2}\ W)$ is the polypartition associated to the conjugacy class of the matrix

$$\begin{pmatrix}1 & 2\\0 & 1\end{pmatrix}\begin{pmatrix}3 & 3\\1 & 2\end{pmatrix} = \begin{pmatrix}0 & 2\\1 & 2\end{pmatrix}.$$

This is the Jordan matrix of the irreducible polynomial X^2+3X+3, so $t(V\ {}^{g_1}\!\rightleftarrows_{g_2}\ W) = \{X^2 + 3X + 3 : (1)\}$.

A preliminary step for our program is to define properly what is an extension of a partial isomorphism.

Definition 2.3 An extension of a partial isomorphism $(V\ {}^{g_1}\!\rightleftarrows_{g_2}\ W)$ is a partial isomorphism $(V^+\ {}^{g_1^+}\!\rightleftarrows_{g_2^+}\ W^+)$ with $V \subset V^+$, $W \subset W^+$, $(g_1^+)_{|V} = g_1$ and $(g_2^+)_{|W} = g_2$.

Denote $k = \dim V = \dim W$ and $k^+ = \dim V^+ = \dim W^+$. The extension is called trivial if one of the following equivalent assertions is satisfied:

1. Its type is obtained from the type $\mu\!\!\mu = (\mu(P_1), \ldots, \mu(P_r))$ of the partial isomorphism $(V\ {}^{g_1}\!\rightleftarrows_{g_2} W)$ by adding parts 1 to the partition $\mu(X-1)$ (which might have been empty).
2. There are decompositions $V^+ = V \oplus A$ and $W^+ = W \oplus B$, such that
$$g_1^+ = g_1 \oplus \psi; \qquad g_2^+ = g_2 \oplus \psi^{-1}$$
with ψ isomorphism between A and B.
3. The induced quotient isomorphisms
$$\widetilde{g_1} : V^+/V \to W^+/W \quad \text{and} \quad \widetilde{g_2} : W^+/W \to V^+/V$$
are inverse of one another: $\widetilde{g_1}\widetilde{g_2} = \mathrm{id}_{V^+/V}$.
4. Fix any basis $\mathcal{E}^+ = (e_1, \ldots, e_k^+)$ of V^+ such that $\mathcal{E} = (e_1, \ldots, e_k)$ is a basis of V. Denote then $\mathcal{F}^+ = (f_1, \ldots, f_k^+)$ the basis of W^+ given by $f_i = g_1^+(e_i)$; the matrix of g_1^+ with respect to these two bases is then I_{k^+}. One has
$$\mathrm{mat}_{\mathcal{F}^+,\mathcal{E}^+}\bigl(g_2^+\bigr) = \begin{pmatrix} G & P \\ 0 & I_{k^+-k} \end{pmatrix},$$
where $G = \mathrm{mat}_{\mathcal{E}}(g_1g_2)$, and $P = (G - I_k)R$ with R arbitrary rectangular matrix of size $k \times (k^+ - k)$.

Proof We denote $(V^+\ {}^{g_1^+}\!\rightleftarrows_{g_2^+} W^+)$ an extension of $(V\ {}^{g_1}\!\rightleftarrows_{g_2} W)$.

(1) ⇒ (2) Suppose that $t(g_1^+g_2^+) = \mu\!\!\mu \sqcup (X-1 : 1^{k^+-k})$. There is a basis $\mathcal{E}^+ = (e_1, \ldots, e_{k^+})$ of V^+ such that $\mathcal{E} = (e_1, \ldots, e_k)$ is a basis of V, and
$$\mathrm{mat}_{\mathcal{E}^+}\bigl(g_1^+g_2^+\bigr) = \begin{pmatrix} \mathrm{mat}_{\mathcal{E}}(g_1g_2) & 0 \\ 0 & I_{k^+-k} \end{pmatrix}. \tag{1}$$

We take for basis $\mathcal{F}^+$ of W^+ the images $f_1, \ldots, f_{k^+}$ of the vectors $e_1, \ldots, e_{k^+}$ by g_1^+. Since $(g_1^+)_{|V} = g_1$, the k first vectors $f_1, \ldots, f_k$ form a basis $\mathcal{F}$ of W. Set then $A = \mathrm{Span}(e_{k+1}, \ldots, e_{k^+})$ and $B = \mathrm{Span}(f_{k+1}, \ldots, f_{k^+})$. By choice of $\mathcal{F}^+$, one has
$$\mathrm{mat}_{\mathcal{E}^+,\mathcal{F}^+}\bigl(g_1^+\bigr) = \begin{pmatrix} I_k & 0 \\ 0 & I_{k^+-k} \end{pmatrix}, \tag{2}$$
whereas
$$\mathrm{mat}_{\mathcal{F}^+,\mathcal{E}^+}\bigl(g_2^+\bigr) = \begin{pmatrix} \mathrm{mat}_{\mathcal{F},\mathcal{E}}(g_2) & P \\ 0 & M \end{pmatrix}, \tag{3}$$
where M is invertible and P is *a priori* an arbitrary matrix. However, the matrix in Eq. (1) is the product of the matrices in (2) and (3), so, by identification, $\mathrm{mat}_{\mathcal{F},\mathcal{E}}(g_2) = \mathrm{mat}_{\mathcal{E}}(g_1g_2)$, $M = I_{k^+-k}$ and $P = 0$. The isomorphism ψ is then the one sending e_j to f_j for $j \in [\![k+1, k^+]\!]$, and the proof of the implication is done.

(2) ⇒ (1) Conversely, with respect to the decomposition $V^+ = V \oplus A$, one has
$$g_1^+g_2^+ = (g_1 \oplus \psi)\bigl(g_2 \oplus \psi^{-1}\bigr) = g_1g_2 \oplus \mathrm{id}_A,$$

so $t(g_1^+ g_2^+) = t(g_1 g_2) \sqcup (X-1 : 1^{k^+-k})$.

(2) $\Leftrightarrow$ (3) Obvious since there are natural isomorphisms $A \simeq V^+/V$ and $B \simeq W^+/W$.

(2) $\Rightarrow$ (4) For any basis $\mathcal{D}^+$ adapted to the decomposition $V^+ = V \oplus A$,

$$\mathrm{mat}_{\mathcal{D}^+}\bigl(g_1^+ g_2^+\bigr) = \begin{pmatrix} G & 0 \\ 0 & I_{k^+-k} \end{pmatrix}.$$

Fix a basis $\mathcal{E}^+ = (e_1, \dots, e_k, e_{k+1}, \dots, e_{k^+})$ of V^+, and another basis $\mathcal{C}^+ = (e_1, \dots, e_k, c_{k+1}, \dots, c_{k^+})$ adapted to the decomposition $V^+ = V \oplus A$. One has

$$\mathrm{mat}_{\mathcal{C}^+}\bigl(\mathcal{E}^+\bigr) = \begin{pmatrix} I_k & R \\ 0 & Q \end{pmatrix},$$

and since this is an invertible matrix, Q has to be invertible. Consider now the basis $\mathcal{D}^+$ with

$$\mathrm{mat}_{\mathcal{D}^+}\bigl(\mathcal{C}^+\bigr) = \begin{pmatrix} I_k & 0 \\ 0 & Q^{-1} \end{pmatrix};$$

it is again adapted to the decomposition $V^+ = V \oplus A$. If $R' = Q^{-1}R$, then one has

$$\mathrm{mat}_{\mathcal{D}^+}\bigl(\mathcal{E}^+\bigr) = \mathrm{mat}_{\mathcal{D}^+}\bigl(\mathcal{C}^+\bigr)\mathrm{mat}_{\mathcal{C}^+}\bigl(\mathcal{E}^+\bigr) = \begin{pmatrix} I_k & R' \\ 0 & I_{k^+-k} \end{pmatrix},$$

and, therefore,

$$\begin{aligned} \mathrm{mat}_{\mathcal{E}^+}\bigl(g_1^+ g_2^+\bigr) &= \mathrm{mat}_{\mathcal{E}^+}\bigl(\mathcal{D}^+\bigr)\mathrm{mat}_{\mathcal{D}^+}\bigl(g_1^+ g_2^+\bigr)\mathrm{mat}_{\mathcal{D}^+}\bigl(\mathcal{E}^+\bigr) \\ &= \begin{pmatrix} I_k & -R' \\ 0 & I_{k^+-k} \end{pmatrix} \begin{pmatrix} G & 0 \\ 0 & I_{k^+-k} \end{pmatrix} \begin{pmatrix} I_k & R' \\ 0 & I_{k^+-k} \end{pmatrix} \\ &= \begin{pmatrix} G & (G-I_k)R' \\ 0 & I_{k^+-k} \end{pmatrix}, \end{aligned}$$

where $G = \mathrm{mat}_{\mathcal{E}}(g_1 g_2)$. With $f_i = g_1^+(e_i)$, this matrix is also $\mathrm{mat}_{\mathcal{F}^+,\mathcal{E}^+}(g_2^+)$, so (2) $\Rightarrow$ (4) is proven.

(4) $\Rightarrow$ (2) From a writing $\mathrm{mat}_{\mathcal{F}^+,\mathcal{E}^+}(g_2^+) = \bigl(\begin{smallmatrix} G & (G-I_k)R \\ 0 & I_{k^+-k} \end{smallmatrix}\bigr)$, one can go backwards and look at the basis $\mathcal{D}^+$ of V^+ given by

$$\mathrm{mat}_{\mathcal{D}^+}\bigl(\mathcal{E}^+\bigr) = \begin{pmatrix} I_k & R \\ 0 & I_{k^+-k} \end{pmatrix};$$

the matrix of $g_1^+ g_2^+$ in this new basis is $\bigl(\begin{smallmatrix} G & 0 \\ 0 & I_{k^+-k} \end{smallmatrix}\bigr)$. Taking $A = \mathrm{Span}(d_{k+1}, \dots, d_{k^+})$ and $B = g_1^+(A)$, one gets back the hypothesis (2). □

In the following, we shall need to know the number of trivial extensions of a given partial isomorphism $(V \;{}^{g_1}\!\rightleftarrows_{g_2}\; W)$ of degree k (the dimension of V and W) to spaces V^+ and W^+ of dimension k^+, with W^+ fixed among the subspaces of $(\mathbb{F}_q)^n$

containing W, but V^+ free. The fourth characterization of trivial extensions will ease this enumeration a lot.

Lemma 2.4 *There is a bijection between trivial extensions* $(V^+ \; {}^{g_1^+}\!\rightleftarrows_{g_2^+} \; W^+)$ *of a partial isomorphism* $(V \; {}^{g_1}\!\rightleftarrows_{g_2} \; W)$ *with* W^+ *fixed, and pairs* $((e_{k+1}, \dots, e_{k^+}), P)$, *where*:

1. $(e_1, \dots, e_{k^+})$ *is a completion of a basis* $(e_1, \dots, e_k)$ *of* V *into a family of* k^+ *linearly independent vectors*;
2. $P = (G - I_k)R$ *is a rectangular matrix of size* $k \times (k^+ - k)$, *where* R *is arbitrary and* $G = \mathrm{mat}_{(e_1,\dots,e_k)}(g_1 g_2)$.

Proof In the following, we fix a basis $\mathcal{F}^+ = (f_1, \dots, f_k^+)$ of W^+ such that $\mathcal{F} = (f_1, \dots, f_k)$ is a basis of W. We then denote $e_i = (g_1^+)^{-1}(f_i)$ for $i \in [\![1, k]\!]$; this basis $\mathcal{E}$ of V is also fixed.

Fix a pair $((e_{k+1}, \dots, e_{k^+}), P)$ such as in the statement of the lemma. One defines a trivial extension of the partial isomorphism by setting

$$\begin{aligned}
\mathrm{Span}(e_1, \dots, e_{k^+}) &= V^+\\
\mathrm{mat}_{\mathcal{E}^+, \mathcal{F}^+}\bigl(g_1^+\bigr) &= I_{k^+}\\
\mathrm{mat}_{\mathcal{F}^+, \mathcal{E}^+}\bigl(g_2^+\bigr) &= \begin{pmatrix} G & P \\ 0 & I_{k^+-k} \end{pmatrix}.
\end{aligned}$$

The fourth characterization of trivial extensions ensures that this extension is indeed trivial. Conversely, given a trivial extension $(V^+ \; {}^{g_1^+}\!\rightleftarrows_{g_2^+} \; W^+)$, one gets back e_i for $i \in [\![k+1, k^+]\!]$ by setting $e_i = (g_1^+)^{-1}(f_i)$; and then P by looking at the upper-right block of the matrix $\mathrm{mat}_{\mathcal{F}^+, \mathcal{E}^+}(g_2^+)$. □

Corollary 2.5 *Let* $(V \; {}^{g_1}\!\rightleftarrows_{g_2} \; W)$ *be a partial isomorphism of* $(\mathbb{F}_q)^n$. *Denote* $k = \dim V = \dim W$, *and* k_1 *the dimension of the set of fixed points of* $g_1 g_2$—*this is also the length of* $\mu(X-1)$ *if* $t(g_1 g_2) = \boldsymbol{\mu}$. *If* $W^+ \supset W$ *is a fixed vector subspace of dimension* $k^+ \geq k$, *then the number of trivial extensions of* $(V \; {}^{g_1}\!\rightleftarrows_{g_2} \; W)$ *with right vector subspace* W^+ *and free left vector subspace* V^+ *is*

$$\begin{aligned}
E_q\bigl(n, k^+, k, k_1\bigr) &= q^{(k-k_1)(k^+-k)}\bigl(q^n - q^k\bigr) \cdots \bigl(q^n - q^{k^+-1}\bigr)\\
&= q^{(n+k-k_1)(k^+-k)} \frac{(q^{-1})_{n-k}}{(q^{-1})_{n-k^+}}.
\end{aligned}$$

By symmetry, one obtains of course the same number if V^+ *is fixed but* W^+ *is left free.*

Proof The first factor $q^{(k-k_1)(k^+-k)}$ is the cardinality of the image of the map

$$\begin{aligned}
\mathrm{M}\bigl(k \times \bigl(k^+ - k\bigr), \mathbb{F}_q\bigr) &\to \mathrm{M}\bigl(k \times \bigl(k^+ - k\bigr), \mathbb{F}_q\bigr)\\
R &\mapsto (G - I_k)R,
\end{aligned}$$

and the second factor is the number of possible completions of the basis $\mathcal{E} = (e_1, \dots, e_k)$ into a family of linearly independent vectors of size k^+. □

To be complete, let us state the equivalent of Corollary 2.5 with fixed left and right subspaces.

Corollary 2.6 *The number of trivial extensions of a partial isomorphism* $(V \,{}^{g_1}\!\!\rightleftarrows_{g_2} W)$ *with fixed left and right subspaces* V^+ *and* W^+ *is*

$$\begin{aligned} F_q\big(k^+, k, k_1\big) &= q^{(k-k_1)(k^+-k)}\big(q^{k^+} - q^k\big)\big(q^{k^+} - q^{k+1}\big)\cdots\big(q^{k^+} - q^{k^+-1}\big) \\ &= q^{(k^++k-k_1)(k^+-k)}\big(q^{-1}\big)_{k^+-k}. \end{aligned}$$

Proof In the set of all trivial extensions of $(V \,{}^{g_1}\!\!\rightleftarrows_{g_2} W)$ with fixed right subspace W^+, each left subspace V^+ is obtained the same number of times, because if V_1^+ and V_2^+ are two such subspaces, then one can use an isomorphism between them that fixes V to get a bijection between trivial extensions. Therefore,

$$F_q\big(k^+, k, k_1\big) = \frac{E_q(n, k^+, k, k_1)}{\text{number of subspaces of } (\mathbb{F}_q)^n \text{ containing } V \text{ and of dimension } k^+}.$$

The denominator of this fraction is equal to

$$\frac{(q^n - q^k)(q^n - q^{k+1})\cdots(q^n - q^{k^+-1})}{(q^{k^+} - q^k)(q^{k^+} - q^{k+1})\cdots(q^{k^+} - q^{k^+-1})},$$

as can by seen by first enumerating families $(e_1, \dots, e_{k^+})$ of linearly independent vectors completing a basis $(e_1, \dots, e_k)$ of V, and then counting how many families give the same subspace $V^+ = \mathrm{Span}(e_1, \dots, e_{k^+})$. □

2.2 Combinatorics of the extension operators

The notion of extension of a partial isomorphism being clarified, one can define correctly the product of two partial isomorphisms. Let $\mathscr{A}(n, \mathbb{F}_q)$ be the $\mathbb{C}$-vector space with basis the set $\mathscr{I}(n, \mathbb{F}_q)$ of partial isomorphisms over $(\mathbb{F}_q)^n$. Given a partial isomorphism $(V \,{}^{g_1}\!\!\rightleftarrows_{g_2} W)$, we denote $\mathscr{E}(V^+ \uparrow V \,{}^{g_1}\!\!\rightleftarrows_{g_2} W)$ the set of trivial extensions with fixed left vector subspace V^+, and $\mathscr{E}(V \,{}^{g_1}\!\!\rightleftarrows_{g_2} W \uparrow W^+)$ the set of trivial extensions with fixed right vector subspace W^+.

Definition 2.7 The product of two elements of $\mathscr{A}(n, \mathbb{F}_q)$ is defined by linear extension of the rule

$$\begin{aligned} &(U \,{}^{g_1}\!\!\rightleftarrows_{g_2} V) * (W \,{}^{h_1}\!\!\rightleftarrows_{h_2} X) \\ &\quad = \frac{1}{E_q(n, m, k, k_1)E_q(n, m, l, l_1)} \sum \big(U^+ \,{}^{g_1^+h_1^+}\!\!\rightleftarrows_{h_2^+g_2^+} X^+\big), \end{aligned}$$

where the sum runs over trivial extensions

$$\big(U^+ \;{}^{g_1^+}{\rightleftarrows}_{g_2^+}\; V+W\big) \in \mathscr{E}\big(U \;{}^{g_1}{\rightleftarrows}_{g_2}\; V \uparrow (V+W)\big)$$

$$\text{and} \quad \big(V+W \;{}^{h_1^+}{\rightleftarrows}_{h_2^+}\; X^+\big) \in \mathscr{E}\big((V+W) \uparrow W \;{}^{h_1}{\rightleftarrows}_{h_2}\; X\big).$$

The parameters m, k, l are the dimensions of $V+W$, V and W, and k_1 and l_1 are the dimensions of the spaces of fixed points of $g_1 g_2$ and $h_1 h_2$.

Theorem 2.8 *Endowed with the product* $*$, $\mathscr{A}(n, \mathbb{F}_q)$ *is an associative complex algebra.*

The unity of the algebra is trivially the “empty” partial isomorphism $(\{0\} \;{}^{\mathrm{id}}{\rightleftarrows}_{\mathrm{id}}\; \{0\})$, so the only thing to check in Theorem 2.8 is the associativity of the product, and this is surprisingly difficult. Let us introduce a few more notations. If $V \subset V^+$ and $W \subset W^+$, denote

$$\mathrm{L}_V^{V^+}(V \;{}^{g_1}{\rightleftarrows}_{g_2}\; W) = \frac{1}{E_q(n, k^+, k, k_1)} \sum_{\mathscr{E}(V^+ \uparrow V \;{}^{g_1}{\rightleftarrows}_{g_2}\; W)} \big(V^+ \;{}^{g_1^+}{\rightleftarrows}_{g_2^+}\; W^+\big)$$

$$\mathrm{R}_W^{W^+}(V \;{}^{g_1}{\rightleftarrows}_{g_2}\; W) = \frac{1}{E_q(n, k^+, k, k_1)} \sum_{\mathscr{E}(V \;{}^{g_1}{\rightleftarrows}_{g_2}\; W \uparrow W^+)} \big(V^+ \;{}^{g_1^+}{\rightleftarrows}_{g_2^+}\; W^+\big)$$

the means of the trivial extensions of a given partial isomorphism, with fixed left or right vector subspace. The multiplication rule is then

$$(U \;{}^{g_1}{\rightleftarrows}_{g_2}\; V) * (W \;{}^{h_1}{\rightleftarrows}_{h_2}\; X) = \mathrm{R}_V^{V+W}(U \;{}^{g_1}{\rightleftarrows}_{g_2}\; V) \cdot \mathrm{L}_W^{V+W}(W \;{}^{h_1}{\rightleftarrows}_{h_2}\; X),$$

where on the right-hand side the product is the usual composition of arrows $U^+ \to V+W$ and $V+W \to X^+$, or of arrows in the reverse directions. Notice that the operators L and R are particular cases of multiplications:

$$\mathrm{L}_V^{V^+}(V \;{}^{g_1}{\rightleftarrows}_{g_2}\; W) = \big(V^+ \;{}^{\mathrm{id}}{\rightleftarrows}_{\mathrm{id}}\; V^+\big) * (V \;{}^{g_1}{\rightleftarrows}_{g_2}\; W);$$

$$\mathrm{R}_W^{W^+}(V \;{}^{g_1}{\rightleftarrows}_{g_2}\; W) = (V \;{}^{g_1}{\rightleftarrows}_{g_2}\; W) * \big(W^+ \;{}^{\mathrm{id}}{\rightleftarrows}_{\mathrm{id}}\; W^+\big).$$

Proposition 2.9 *Consider nested subspaces* $W \subset W^+ \subset W^{++}$. *One has*

$$\mathrm{R}_{W^+}^{W^{++}} \circ \mathrm{R}_W^{W^+} = \mathrm{R}_W^{W^{++}},$$

and similarly for the operators L.

Proof Even if one already knew the associativity of the product $*$, this would not be obvious, since the product $(W^+ \;{}^{\mathrm{id}}{\rightleftarrows}_{\mathrm{id}}\; W^+) * (W^{++} \;{}^{\mathrm{id}}{\rightleftarrows}_{\mathrm{id}}\; W^{++})$ is an average of partial isomorphisms between spaces $(W^+)^+$ containing W^+, and W^{++}. Hence, it is different from $(W^{++} \;{}^{\mathrm{id}}{\rightleftarrows}_{\mathrm{id}}\; W^{++})$. However, these intermediary spaces $(W^+)^+$ will disappear when one multiplies on the left by a partial isomorphism $(V \;{}^{g_1}{\rightleftarrows}_{g_2}\; W)$. A similar idea will be used in the proof of Lemma 2.21.

Fix a basis $(f_1, \dots, f_{k^{++}})$ of W^{++}, such that $(f_1, \dots, f_k)$ is a basis of W and $(f_1, \dots, f_{k^+})$ is a basis of W^+. We then denote $e_1, \dots, e_k$ the reciprocal images of the vectors $f_1, \dots, f_k$ by g_1; and $G = \mathrm{mat}_{\mathcal{F},\mathcal{E}}(g_1 g_2)$. A convenient way to write $\mathrm{R}_W^{W^{++}}(V \,{}^{g_1}\!\rightleftarrows_{g_2} W)$ is as follows:

$$\begin{aligned}
&\mathrm{R}_W^{W^{++}}(V \,{}^{g_1}\!\rightleftarrows_{g_2} W)\\
&\quad= \frac{1}{q^{(k-k_1)(k^{++}-k)}(q^n - q^k)(q^n - q^{k+1}) \cdots (q^n - q^{k^{++}-1})}\\
&\quad\quad\times \sum_{\substack{\mathcal{E}^{++}\setminus\mathcal{E}=(e_{k+1},\dots,e_{k^{++}})\\ P=(G-I_k)R}} \left(\mathrm{Span}\bigl(\mathcal{E}^{++}\bigr) \,\middle|\, I_{k^{++}} \rightleftarrows \begin{pmatrix} G & P \\ 0 & I_{k^{++}-k} \end{pmatrix} \,\middle|\, W^{++}\right).
\end{aligned} \tag{4}$$

This equation corresponds to the content of Lemma 2.4. Using the same notations, we get

$$\begin{aligned}
\mathrm{R}_W^{W^{+}}(V \,{}^{g_1}\!\rightleftarrows_{g_2} W) &= \frac{1}{q^{(k-k_1)(k^{+}-k)}(q^n - q^k)(q^n - q^{k+1}) \cdots (q^n - q^{k^{+}-1})}\\
&\quad\times \sum_{\substack{(e_{k+1},\dots,e_{k^{+}})\\ M=(G-I_k)S}} \left(\mathrm{Span}\bigl(\mathcal{E}^{+}\bigr) \,\middle|\, I_{k^{+}} \rightleftarrows \begin{pmatrix} G & M \\ 0 & I_{k^{+}-k} \end{pmatrix} \,\middle|\, W^{+}\right);\\
\mathrm{R}_W^{W^{+}}(V \,{}^{g_1}\!\rightleftarrows_{g_2} W) &= \frac{1}{q^{(k-k_1)(k^{+}-k)}(q^n - q^k)(q^n - q^{k+1}) \cdots (q^n - q^{k^{+}-1})}\\
&\quad\times \frac{1}{q^{(k-k_1)(k^{++}-k^{+})}(q^n - q^{k^+})(q^n - q^{k^{+}+1}) \cdots (q^n - q^{k^{++}-1})}\\
&\quad\times \sum_{\substack{(e_{k+1},\dots,e_{k^{++}})\\ M=(G-I_k)S\\ N=(G'-I_{k^+})T}} \left(\mathrm{Span}\bigl(\mathcal{E}^{++}\bigr) \,\middle|\, I_{k^{+}}\right.\\
&\quad\left. \rightleftarrows \begin{pmatrix} \left(\begin{smallmatrix} G & M \\ 0 & I_{k^{+}-k} \end{smallmatrix}\right) & N \\ 0 & I_{k^{++}-k^{+}} \end{pmatrix} \,\middle|\, W^{++}\right);
\end{aligned} \tag{5}$$

where in the last term G' denotes the intermediary matrix. Notice that the number of terms in Eqs. (4) and (5) is the same. Therefore, it suffices to show that each term of (5) appears in (4). This is immediate from the following computation:

$$\begin{aligned}
&\begin{pmatrix} \left(\begin{smallmatrix} G & M \\ 0 & I_{k^{+}-k} \end{smallmatrix}\right) & N \\ 0 & I_{k^{++}-k^{+}} \end{pmatrix}\\
&\quad= \begin{pmatrix} \left(\begin{smallmatrix} G & (G-I_k)S \\ 0 & I_{k^{+}-k} \end{smallmatrix}\right) & \left(\left(\begin{smallmatrix} G & (G-I_k)S \\ 0 & I_{k^{+}-k} \end{smallmatrix}\right) - I_{k^+}\right)\left(\begin{smallmatrix} T_1 \\ T_2 \end{smallmatrix}\right) \\ 0 & I_{k^{++}-k^{+}} \end{pmatrix}
\end{aligned}$$

$$= \begin{pmatrix} \begin{pmatrix} G & (G-I_k)S \\ 0 & I_{k^+-k} \end{pmatrix} & \begin{pmatrix} G-I_k & (G-I_k)S \\ 0 & 0 \end{pmatrix}\begin{pmatrix} T_1 \\ T_2 \end{pmatrix} \\ 0 & I_{k^{++}-k^+} \end{pmatrix}$$

$$= \begin{pmatrix} G & (G-I_k)S & (G-I_k)T_3 \\ 0 & I_{k^+-k} & 0 \\ 0 & 0 & I_{k^{++}-k^+} \end{pmatrix}$$

with $T_3 = T_1 + ST_2$, which is again an arbitrary rectangular matrix. □

In the following, we shall work with slightly more general operators L and R.

Definition 2.10 For W arbitrary subspace of $(\mathbb{F}_q)^n$ and $(U\ {}^{g_1}\!\rightleftarrows_{g_2} V)$ arbitrary element of $\mathcal{I}(n, \mathbb{F}_q)$, we set

$$\mathrm{R}^W(U\ {}^{g_1}\!\rightleftarrows_{g_2} V) = \mathrm{R}_V^{V+W}(U\ {}^{g_1}\!\rightleftarrows_{g_2} V),$$

and similarly for the operators L^W. We call these generalized operators L^W and R^W the extension operators; they give rise to well-defined linear endomorphisms of $\mathcal{A}(n, \mathbb{F}_q)$.

Proposition 2.11 *Consider two arbitrary subspaces W and X of $(\mathbb{F}_q)^n$. One has*

$$\mathrm{R}^X \circ \mathrm{R}^W = \mathrm{R}^{W+X},$$

and similarly for the operators L.

Proof For any partial isomorphism $(U\ {}^{g_1}\!\rightleftarrows_{g_2} V)$, if $W \subset V$, then

$$\mathrm{R}^W(U\ {}^{g_1}\!\rightleftarrows_{g_2} V) = \mathrm{R}_V^{V+W}(U\ {}^{g_1}\!\rightleftarrows_{g_2} V) = \mathrm{R}_V^{V}(U\ {}^{g_1}\!\rightleftarrows_{g_2} V) = (U\ {}^{g_1}\!\rightleftarrows_{g_2} V).$$

Consider a partial isomorphism appearing in $\mathrm{R}^X \circ \mathrm{R}^W(U\ {}^{g_1}\!\rightleftarrows_{g_2} V)$. Its right subspace contains both W and X (and V), so it must contain $W+X$. Therefore, one can apply again R^{W+X} without changing the result, and

$$\mathrm{R}^X \circ \mathrm{R}^W = \mathrm{R}^{W+X} \circ \mathrm{R}^X \circ \mathrm{R}^W.$$

As a consequence, the proposition will be shown if one proves that for nested subspaces $W \subset W'$, $\mathrm{R}^{W'} \circ \mathrm{R}^W = \mathrm{R}^{W'}$. Indeed, assuming this is true, one has then

$$\begin{aligned} \mathrm{R}^X \circ \mathrm{R}^W &= \mathrm{R}^{W+X} \circ \big(\mathrm{R}^X \circ \mathrm{R}^W\big) \\ &= \big(\mathrm{R}^{W+X} \circ \mathrm{R}^X\big) \circ \mathrm{R}^W \\ &= \mathrm{R}^{W+X} \circ \mathrm{R}^W \quad \text{since } X \subset W+X, \\ &= \mathrm{R}^{W+X} \quad \text{since } W \subset W+X. \end{aligned}$$

Fix two nested subspaces $W \subset W'$, and a partial isomorphism $(U\ {}^{g_1}\!\rightleftarrows_{g_2} V)$. One has

$$\mathrm{R}^{W'}\big(\mathrm{R}^W(U\ {}^{g_1}\!\rightleftarrows_{g_2} V)\big) = \mathrm{R}^{W'}\big(\mathrm{R}_U^{U+W}(U\ {}^{g_1}\!\rightleftarrows_{g_2} V)\big)$$

$$
\begin{aligned}
&= \mathrm{R}_{U+W}^{U+W'}\big(\mathrm{R}_{U}^{U+W}(U\ {}^{g_1}\!\!\rightleftarrows_{g_2}\ V)\big)\\
&= \mathrm{R}_{U}^{U+W'}(U\ {}^{g_1}\!\!\rightleftarrows_{g_2}\ V)\\
&= \mathrm{R}^{W'}(U\ {}^{g_1}\!\!\rightleftarrows_{g_2}\ V)
\end{aligned}
$$

by using Proposition 2.9 on the third line. □

This leads us to the main result regarding extension operators:

Theorem 2.12 *The algebra of extension operators* $\langle \mathrm{L}^W, \mathrm{R}^W\rangle_{W \text{ subspace of } (\mathbb{F}_q)^n}$ *is a commutative subalgebra of* $\mathrm{End}(\mathscr{A}(n,\mathbb{F}_q))$.

Proposition 2.11 obviously implies that $\mathrm{R}^W \circ \mathrm{R}^X = \mathrm{R}^X \circ \mathrm{R}^W$ and $\mathrm{L}^W \circ \mathrm{L}^X = \mathrm{L}^X \circ \mathrm{L}^W$, so it remains to prove that

$$\mathrm{L}^W \circ \mathrm{R}^X = \mathrm{R}^X \circ \mathrm{L}^W. \tag{6}$$

The difficulty here is that when applied to an element $(U\ {}^{g_1}\!\!\rightleftarrows_{g_2}\ V)$, both sides of (6) yield averages of partial isomorphisms whose left and right subspaces are not fixed. Indeed, these subspaces must contain $U + W$ and $V + X$, but they can be larger. Consequently, the first thing to check will be that both sides induce the same probability measure on pairs (W', X') of subspaces of same dimension. Then, we shall prove the following decomposition:

$$\mathrm{L}^W \circ \mathrm{R}^X(U\ {}^{g_1}\!\!\rightleftarrows_{g_2}\ V) = \sum_{\substack{U+W\subset Y\\ V+X\subset Z}} \mathbb{P}\big[(Y,Z)\big]\Psi_{(U,W;V,X)}^{(Y;Z)}(U\ {}^{g_1}\!\!\rightleftarrows_{g_2}\ V),$$

where $\mathbb{P}[(Y,Z)]$ is a probability measure, and the $\Psi_{(U,W;V,X)}^{(Y;Z)}$ are operators that yield averages of certain trivial extensions with fixed left and right subspaces. It will be clear from the final formula that the same decomposition holds for the right-hand side of Eq. (6), and this will end the proof of Theorem 2.12.

2.3 Probabilities of conditioned random trivial extensions

Let us define new operators

$$\mathrm{LR}_{(V,W)}^{(V^+,W^+)}(V\ {}^{g_1}\!\!\rightleftarrows_{g_2}\ W) = \frac{1}{F_q(k^+,k,k_1)} \sum_{\mathscr{E}(V^+\uparrow V\ {}^{g_1}\!\rightleftarrows_{g_2}\ W\uparrow W^+)} \big(V^+\ {}^{g_1^+}\!\!\rightleftarrows {}_{g_2^+}\ W^+\big),$$

where the sum runs over trivial extensions of $(V\ {}^{g_1}\!\!\rightleftarrows_{g_2}\ W)$ with fixed left subspace V^+ and right subspace W^+. One has

$$
\begin{aligned}
&\mathrm{R}_W^{W^+}(V\ {}^{g_1}\!\!\rightleftarrows_{g_2}\ W)\\
&\quad= \frac{(q^{k^+}-q^k)\cdots(q^{k^+}-q^{k^+-1})}{(q^n-q^k)\cdots(q^n-q^{k^+-1})} \sum_{\substack{V\subset V^+\\ \dim V^+=\dim W^+}} \mathrm{LR}_{(V,W)}^{(V^+,W^+)}(V\ {}^{g_1}\!\!\rightleftarrows_{g_2}\ W),
\end{aligned}
$$

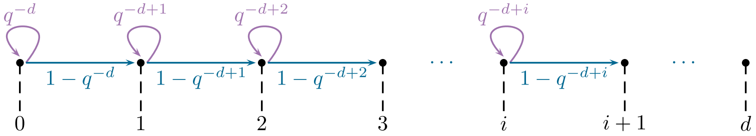

Fig. 1 The graph of the transitions of the Markov chain $(X_k)_{k\geq 0}$ in a vector space of dimension d over $\mathbb{F}_q$

and similarly for the operators L.

Lemma 2.13 *Fix two subspaces U and W of $(\mathbb{F}_q)^n$, with $j = \dim U$ and $k = \dim(U + W)$. We choose a random subspace U^+ of fixed dimension $l \geq j$, uniformly among all such subspaces containing U. The law of $m = \dim(U^+ + W)$ is*

$$\mathbb{P}[m] = q^{(k+l-j-m)(m-n)} \frac{(q^{-1})_{n-k}(q^{-1})_{n-l}(q^{-1})_{k-j}(q^{-1})_{l-j}}{(q^{-1})_{k+l-j-m}(q^{-1})_{n-m}(q^{-1})_{n-j}(q^{-1})_{m-k}(q^{-1})_{m-l}}.$$

Proof Fix a basis $\mathcal{E} = (e_1, \dots, e_n)$ of $(\mathbb{F}_q)^n$ such that $(e_1, \dots, e_j)$ is a basis of U, and $(e_1, \dots, e_k)$ is a basis of $(U + W)$. To choose a subspace U^+ of dimension l uniformly among those that contains U, it suffices to choose random vectors $(f_{j+1}, \dots, f_l)$ among the $(q^n - q^j) \cdots (q^n - q^{l-1})$ families of vectors such that $(e_1, \dots, e_j, f_{j+1}, \dots, f_l)$ is of rank l, and to take $U^+ = \mathrm{Span}(e_1, \dots, e_j, f_{j+1}, \dots, f_l)$. Denote

$$A = \mathrm{mat}_{\mathcal{E}}(f_{j+1}, \dots, f_l) = \begin{pmatrix} a_{1,1} & \cdots & a_{1,l-j} \\ \vdots & & \vdots \\ a_{j,1} & \cdots & a_{j,l-j} \\ \vdots & & \vdots \\ a_{k,1} & \cdots & a_{k,l-j} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,l-j} \end{pmatrix}.$$

The condition $\dim U^+ = l$ is equivalent to $\mathrm{rank}(A') = l - j$, where A' is the submatrix of A that consists in the $(n - j)$ last rows. Then, $m = k + p$, where $p = \mathrm{rank}(A'')$ and A'' is the submatrix of A that consists in the $(n - k)$ last rows. So, the law of $(m - k)$ is the law of the rank of the $(n - k)$ last rows of a random matrix of size $(l - j) \times (n - j)$, uniformly chosen among those that are of rank $(l - j)$.

Thus, our problem can be reformulated as follows. Fix a dimension d, and consider the random process $X_k = \mathrm{rank}(v_1, \dots, v_k)$, where the v_i's are uniform random vectors of $(\mathbb{F}_q)^d$ chosen independently. The process $(X_k)_{k\geq 0}$ is a Markov chain with transition matrix

$$p(i, i) = \frac{1}{q^{d-i}}; \qquad p(i, i + 1) = 1 - \frac{1}{q^{d-i}}.$$

See Fig. 1.

We are looking at the probabilities $\mathbb{P}_{d,q}[X_a = c | X_b = d]$, with $a \leq b$ and $c \leq d$. Let us first compute $\mathbb{P}_{d,q}[X_a = c]$. To go from rank 0 to rank c in a steps, one has to go through the c transitions $0 \to 1$, $1 \to 2$, *etc.*, $(c-1) \to c$, which gives a factor

$$\left(1 - \frac{1}{q^d}\right)\left(1 - \frac{1}{q^{d-1}}\right) \cdots \left(1 - \frac{1}{q^{d-c+1}}\right) = \frac{(q^{-1})_d}{(q^{-1})_{d-c}};$$

and during the other $(a-c)$ transitions, one stays with the same rank. Therefore,

$$\begin{aligned}\mathbb{P}_{d,q}[X_a = c] &= \frac{(q^{-1})_d}{(q^{-1})_{d-c}} \sum_{\substack{A\ (a-c)\text{-multiset} \\ \text{with elements in } [\![0,c]\!]}} \prod_{x \in A} \frac{1}{q^{d-x}} \\ &= q^{d(c-a)} \frac{(q^{-1})_d}{(q^{-1})_{d-c}} h_{a-c}\big(1, q, \ldots, q^c\big),\end{aligned}$$

where the h_k's are the homogeneous symmetric polynomials. We refer to [15, §1.2], where the evaluations of these polynomials on geometric progressions are also computed. One obtains

$$\mathbb{P}_{d,q}[X_a = c] = q^{(d-c)(c-a)} \frac{(q^{-1})_a (q^{-1})_d}{(q^{-1})_c (q^{-1})_{a-c} (q^{-1})_{d-c}}.$$

In particular, $\mathbb{P}_{d,q}[X_a = d] = \frac{(q^{-1})_a}{(q^{-1})_{a-d}}$. Now,

$$\begin{aligned}\mathbb{P}_{d,q}[X_a = c | X_b = d] &= \frac{\mathbb{P}_{d,q}[X_b = d | X_a = c]\mathbb{P}_{d,q}[X_a = c]}{\mathbb{P}_{d,q}[X_b = d]} \\ &= \frac{\mathbb{P}_{d-c,q}[X_{b-a} = d-c]\mathbb{P}_{d,q}[X_a = c]}{\mathbb{P}_{d,q}[X_b = d]} \\ &= q^{(d-c)(c-a)} \frac{(q^{-1})_a (q^{-1})_d (q^{-1})_{b-a} (q^{-1})_{b-d}}{(q^{-1})_b (q^{-1})_c (q^{-1})_{a-c} (q^{-1})_{d-c} (q^{-1})_{b-a-d+c}}\end{aligned}$$

by taking on the second line the quotient of $(\mathbb{F}_q)^d$ by the vector subspace generated by $(v_1, \ldots, v_a)$ in order to transform the conditional probability. Finally, we set $a = n-k$, $b = n-j$, $c = p = m-k$, and $d = l-j$:

$$\mathbb{P}[m] = q^{(k+l-j-m)(m-n)} \frac{(q^{-1})_{n-k} (q^{-1})_{n-l} (q^{-1})_{k-j} (q^{-1})_{l-j}}{(q^{-1})_{k+l-j-m} (q^{-1})_{n-m} (q^{-1})_{n-j} (q^{-1})_{m-k} (q^{-1})_{m-l}}.$$

This expression is non-zero if and only if $\sup(k,l) \leq m \leq \inf(n, k+l-j)$; moreover, it is symmetric in k and l. □

Corollary 2.14 *Fix subspaces U, V, W, X with $j = \dim U = \dim V$, $k = \dim(U + W)$ and $l = \dim(V + X)$. One chooses a subspace U^+ randomly among those containing U and of dimension l, and then set $Y = U^+ + W$ and $Z = (V + X)^+$, where*

Z is again chosen randomly among the subspaces containing $V+X$ and of dimension $m=\dim Y$. The law of m is given by Lemma 2.13, and conditionally on m, the law of (Y,Z) is the uniform law on pairs of spaces of same dimension m and with $U+W\subset Y$ and $V+X\subset Z$.

Proof One only needs to verify that conditionally on m, the law of (Y,Z) is the uniform law on pairs of spaces containing $U+W$ and $V+X$ (in particular, Y and Z are independent conditionally on their dimension). By construction, $Z=(V+X)^+$ is independent of Y conditionally on m, and uniformly distributed. Consider then $Y=U^+ + W$, conditioned by its dimension m. We construct Y in the same way as in Lemma 2.13:

$$U=\mathrm{Span}(e_1,\dots,e_j);\qquad U+W=\mathrm{Span}(e_1,\dots,e_k)$$
$$U^+=\mathrm{Span}(e_1,\dots,e_j,f_{j+1},\dots,f_l)$$

with $(f_{j+1},\dots,f_l)$ uniformly chosen among completions of $(e_1,\dots,e_j)$ into a free family of length l. Denote $f^U_{j+1},\dots,f^U_l$ the images of the random vectors $f_{j+1},\dots,f_l$ by the quotient map $\pi^U:(\mathbb{F}_q)^n\to(\mathbb{F}_q)^n/U$, and similarly with $f^{U+W}_{j+1},\dots,f^{U+W}_l$.

The family $f^U_{j+1},\dots,f^U_l$ is a uniform family of $(l-j)$ linearly independent vectors in $(\mathbb{F}_q)^n/U$: indeed, each such family has $q^{(l-j)j}$ preimages by π^U, and all with the same weight. Denote then π^{U+W}_U the quotient map $(\mathbb{F}_q)^n/U\to(\mathbb{F}_q)^n/(U+W)$: one has $f^{U+W}_i=\pi^{U+W}_U(f_i)$, and on the other hand, to say that $Y|m$ is the uniform random subspace containing $U+W$ and with dimension m is the same as saying that $(f^{U+W}_{j+1},\dots,f^{U+W}_l)|m$ is a uniform family of random vectors in $(\mathbb{F}_q)^n/(U+W)$ among those of rank $p=m-k$. Therefore, it suffices to prove the following general statement: if $(e_1,\dots,e_d)$ is a uniform random family of d linearly independent vectors in a $\mathbb{F}_q$-vector space K, then knowing the rank p of $(\pi(e_1),\dots,\pi(e_d))$ in a quotient $K/H=\pi(K)$, the family $(f_1,\dots,f_d)=(\pi(e_1),\dots,\pi(e_d))$ is uniformly distributed among those of rank p. Again, this is because each family $(f_1,\dots,f_d)$ with given rank p in K/H has the same number of preimages and all with same weight, namely,

$$q^{nm}\mathbb{P}_{n,q}[X_n=d|X_{n-m}=p],$$

where $n=\dim K$, $m=\dim H$, and $(X_k)_{k\geq 0}$ is the same Markov chain as before. □

An important consequence of the previous discussion is that the law of (Y,Z) is the same law on pairs of subspaces of same dimension m containing $U+W$ and $V+X$

1. if one first chooses U^+ random extension of U of dimension l, and then set $Y=U^+ + W$ and $Z=(V+X)^+$
2. or if one first chooses V^+ random extension of V of dimension k, and then set $Z=V^+ + X$ and $Y=(U+W)^+$.

Indeed, this law is $\mathbb{P}[(Y,Z)]=\mathbb{P}[m]\mathbb{U}_{m,U+W}[Y]\mathbb{U}_{m,V+X}[Z]$, where $\mathbb{P}[m]$ is given by Lemma 2.13 (remember the symmetry of the roles played by k and l), and the $\mathbb{U}_m$'s are the uniform laws on subspaces described by Corollary 2.14.

This symmetry plays an essential role in the proof of Theorem 2.12. Fix a partial isomorphism $I=(U\ {}^{g_1}\!\rightleftarrows_{g_2}\ V)$. One has

$$\mathrm{R}^X(I)=\sum_{U\subset U^+,\dim U^+=l}\mathbb{U}_{l,U}\big[U^+\big]\mathrm{LR}_{(U,V)}^{(U^+,V+X)}(I)$$

$$\mathrm{L}^W\circ\mathrm{R}^X(I)=\sum_{\substack{U\subset U^+,\dim U^+=l\\ V+X\subset Z,\dim Z=m}}\mathbb{U}_{l,U}\big[U^+\big]\mathbb{U}_{m,V+X}[Z]\mathrm{LR}_{(U^+,V+X)}^{(Y,Z)}\mathrm{LR}_{(U,V)}^{(U^+,V+X)}(I)$$

with $Y=U^++W$ and $m=\dim Y$ on the second line. According to the previous discussion, this is also:

$$\mathrm{L}^W\circ\mathrm{R}^X(I)=\sum_{\substack{\sup(k,l)\le m\le\inf(n,k+l-j)\\ \dim Y=\dim Z=m,U+W\subset Y,V+X\subset Z\\ \dim U^+=l,U\subset U^+,Y=U^++W}}\mathbb{P}\big[(Y,Z)\big]\mathbb{P}\big[U^+|(Y,Z)\big]$$
$$\times\,\mathrm{LR}_{(U^+,V+X)}^{(Y,Z)}\mathrm{LR}_{(U,V)}^{(U^+,V+X)}(I),$$

where $\mathbb{P}[(Y,Z)]$ is the law on pair on subspaces described by Corollary 2.14. It remains then to understand what

$$\varPsi_{(U,W;V,X)}^{(Y;Z)}(I)=\sum_{\dim U^+=l,U\subset U^+,Y=U^++W}\mathbb{P}\big[U^+|(Y,Z)\big]\mathrm{LR}_{(U^+,V+X)}^{(Y,Z)}\mathrm{LR}_{(U,V)}^{(U^+,V+X)}(I)\tag{7}$$

is when Y and Z are fixed.

Remark 2.15 Notice that $\varPsi_{(U,W;V,X)}^{(Y;Z)}(I)$ cannot be the same as $\mathrm{LR}_{(U,V)}^{(Y,Z)}(I)$. A partial isomorphism appearing in (7) satisfies

$$g_2^{++}(V+X)+W=g_2^{+}(V+X)+W=U^++W=Y,$$

and in general this is not the case of a trivial extension of $(U\ {}^{g_1}\!\rightleftarrows_{g_2}\ V)$ to Y and Z. Similarly,

$$\begin{aligned}g_1^{++}(U+W)+X&=g_1(U)+g_1^{++}(W)+X=(V+X)+g_1^{++}(W)\\&=g_1^{+}\big(U^+\big)+g_1^{++}(W)=g_1^{++}(Y)=Z,\end{aligned}$$

which is not in general the case of an extension in $\mathscr{E}(Y\uparrow U\ {}^{g_1}\!\rightleftarrows_{g_2}\ V\uparrow Z)$. We are actually going to prove that the expression (7) is the mean of all trivial extensions of I to spaces Y and Z such that $g_1^{++}(U+W)+X=Z$ and $g_2^{++}(V+X)+W=Y$; see Theorem 2.19.

First, we need to understand the distribution of U^+ knowing Y and Z. Obviously, U^+ is in fact independent from Z, so we only need to condition by Y.

Lemma 2.16 *In the previous probabilistic scheme, the law of U^+ knowing Y is the uniform law on vector subspaces U^+ satisfying the three conditions*

$$\dim U^+ = l; \qquad U \subset U^+ \subset Y; \qquad U^+ + W = Y. \tag{8}$$

The number of such spaces (hence, the inverse of the probability $\mathbb{P}[U^+|Y]$) is

$$q^{(m-l)(l-j)} \frac{(q^{-1})_{k-j}}{(q^{-1})_{m-l}(q^{-1})_{k+l-j-m}}.$$

Proof We start by counting subspaces U^+ satisfying the three conditions. It is useful to introduce the quotient map $\pi^U : Y \to Y/U$; then, the three conditions (8) rewrite as

$$\dim \pi^U\big(U^+\big) = l - j; \qquad \pi^U\big(U^+\big) + \pi^U(W) = Y/U. \tag{9}$$

So, given two nested spaces $H \subset K$ of respective dimensions a and b, the problem is now to count subspaces $G \subset K$ with fixed dimension c and with $G + H = K$. One will then take

$$a = k - j; \qquad b = m - j; \qquad c = l - j; \qquad G = \pi^U\big(U^+\big);$$
$$H = \pi^U(W); \qquad K = Y/U.$$

This problem falls again in the setting of the Markov chain $(X_k)_{k \geq 0}$. Consider vectors $e_1, \dots, e_c$, and write their matrix in a basis of K whose first vectors form a basis of H. Then, setting $G = \mathrm{Span}(e_1, \dots, e_c)$, one has $G + H = K$ if and only if the $(b-a)$ last rows of the matrix are of rank $(b-a)$, so G satisfies the previous assumptions in

$$\begin{aligned} & q^{bc}\mathbb{P}_{c,q}[X_{b-a} = b - a \wedge X_b = c] \\ & \quad = q^{bc}\mathbb{P}_{c,q}[X_{b-a} = b - a]\mathbb{P}_{a+c-b,q}[X_a = a + c - b] \\ & \quad = q^{bc} \frac{(q^{-1})_a (q^{-1})_c}{(q^{-1})_{b-c}(q^{-1})_{a+c-b}} \end{aligned}$$

cases. Dividing this expression by the number $q^{c^2}(q^{-1})_c$ of bases of G, and replacing a, b, c, one obtains the number

$$q^{(m-l)(l-j)} \frac{(q^{-1})_{k-j}}{(q^{-1})_{m-l}(q^{-1})_{k+l-j-m}}$$

of subspaces satisfying the two "quotient" conditions (9). Finally, π^U establishes a bijection between subspaces of Y containing U and subspaces of Y/U, whence the formula in the statement of the lemma.

Now, we check that $\mathbb{P}[U^+|Y]$ is indeed the inverse of the previous quantity. Write $\mathrm{Comp}(U^+, Y)$ for the characteristic function of the three compatibility conditions (8). One has

$$\mathbb{P}\big[U^+|Y\big] = \frac{\mathbb{P}[(U^+, Y)]}{\mathbb{P}[Y]} = \frac{\mathbb{U}_{l,U}[U^+]\mathrm{Comp}(U^+, Y)}{\mathbb{P}[m]\mathbb{U}_{m,U+W}[Y]}$$

$$= q^{(l-m)(l-j)} \frac{(q^{-1})_{m-l}(q^{-1})_{k+l-j-m}}{(q^{-1})_{k-j}} \operatorname{Comp}\bigl(U^+, Y\bigr)$$

by using Lemma 2.13 for $\mathbb{P}[m]$, and twice the formula $\mathbb{U}_{a,b,c} = \frac{(q^{-1})_{c-b}(q^{-1})_{b-a}}{q^{(c-b)(b-a)}(q^{-1})_{c-a}}$ for the uniform probability of a random space of dimension b contained in one of dimension c, and containing a fixed subspace of dimension a. □

To reintroduce some symmetry in Eq. (7), let us fix U^+, Y and Z, and for $(Y \underset{g_2^{++}}{\overset{g_1^{++}}{\rightleftarrows}} Z)$ appearing in $\mathrm{LR}^{(Y,Z)}_{(U^+,V+X)}\mathrm{LR}^{(U^+,V+X)}_{(U,V)}(I)$, consider the space

$$V^+ = g_1^{++}(U + W).$$

Since $\mathrm{LR}^{(Y,Z)}_{(U^+,V+X)}\mathrm{LR}^{(U^+,V+X)}_{(U,V)}(I)$ is an average of partial isomorphisms, one can then consider V^+ as a random subspace of Z, with probability conditioned by U^+, Y and Z.

Lemma 2.17 *The law of V^+ knowing U^+, Y and Z is the uniform law on subspaces of Z satisfying the three conditions*

$$\dim V^+ = k; \qquad V \subset V^+ \subset Z; \qquad V^+ + X = Z.$$

Proof As in the previous Lemma, we have to show that $\mathbb{P}[V^+|(U^+, Y, Z)]$ is equal to the inverse of

$$q^{(m-k)(k-j)} \frac{(q^{-1})_{l-j}}{(q^{-1})_{m-k}(q^{-1})_{k+l-j-m}},$$

and on the other hand,

$$\begin{aligned}
\mathbb{P}\bigl[V^+|\bigl(U^+, Y, Z\bigr)\bigr] &= \frac{\mathbb{P}[(U^+, V^+, Y, Z)]}{\mathbb{P}[(U^+, Y, Z)]} \\
&= \frac{\mathbb{P}[(U^+, V^+)]\operatorname{Comp}(U^+, Y)\operatorname{Comp}(V^+, Z)}{\mathbb{P}[m]\mathbb{U}_{m,U+W}[Y]\mathbb{U}_{m,V+X}[Z]\mathbb{P}[U^+|Y]}
\end{aligned}$$

since Y and Z are entirely determined by U^+ and V^+ and by the compatibility conditions. The denominator can be calculated by using the previous results:

$$\mathbb{P}\bigl[\bigl(U^+, Y, Z\bigr)\bigr] = q^{(m-n)(m-j)+(l-m)(l-j)} \frac{(q^{-1})_{n-m}(q^{-1})_{m-l}(q^{-1})_{l-j}}{(q^{-1})_{n-j}}.$$

Therefore, the claim of the lemma is equivalent to

$$\begin{aligned}
\mathbb{P}\bigl[\bigl(U^+, V^+\bigr)\bigr] &= q^{(m-n)(m-j)+(l-m)(l-j)+(k-m)(k-j)} \\
&\quad \times \frac{(q^{-1})_{n-m}(q^{-1})_{m-l}(q^{-1})_{m-k}(q^{-1})_{k+l-j-m}}{(q^{-1})_{n-j}},
\end{aligned} \tag{10}$$

where the probability refers to the random choices of spaces and trivial extensions that are done during the computation of $\mathrm{L}^W \circ \mathrm{R}^X(I)$.

We decompose this succession of random choices as follows, keeping track at each step of the probability to obtain a trivial extension $(Y\ {}^{g_1^{++}}\!\rightleftarrows_{g_2^{++}} Z)$ with given subspaces U^+ and V^+.

1. When applying R^X, there is a probability

$$\frac{(q^{-1})_{n-l}(q^{-1})_{l-j}}{q^{(n-l)(l-j)}(q^{-1})_{n-j}}$$

to obtain a given space U^+. Denote then W' a subspace of W such that $U + W = U \oplus W'$; it is of dimension $(k - j)$, and

$$\dim\bigl(U^+ \cap W'\bigr) = \dim U^+ + \dim W' - \dim\bigl(U^+ + W\bigr) = k + l - j - m.$$

Fix a basis $(e_1, \dots, e_l)$ of U^+, such that

$$(e_1, \dots, e_j) \text{ is a basis of } U;$$

$$(e_{j+1}, \dots, e_{k+l-m}) \text{ is a basis of } U^+ \cap W'.$$

The (random) trivial extension $(U^+\ {}^{g_1^+}\!\rightleftarrows_{g_2^+} V + X)$ of $(U\ {}^{g_1}\!\rightleftarrows_{g_2} V)$ is obtained by first choosing a completion $(f_{j+1}, \dots, f_l) = (g_1^+(e_{j+1}), \dots, g_1^+(e_l))$ of the basis $(f_1, \dots, f_j) = (g_1(e_1), \dots, g_1(e_l))$ of V into a basis of $V + X$, and then by choosing the matrix of g_2^+. For the computation of V^+, one only needs to know what is $g_1^+(U^+ \cap W')$. This is a subspace of $V + X$ of dimension $(k + l - j - m)$, linearly independent from $g_1(U) = V$, and arbitrary among those such subspaces, because its basis $(f_{j+1}, \dots, f_{k+l-m})$ is itself arbitrary and uniformly distributed. There are

$$\frac{(q^l - q^j)\cdots(q^l - q^{k+l-m-1})}{(q^{k+l-j-m} - 1)\cdots(q^{k+l-j-m} - q^{k+l-j-m-1})} = \frac{q^{(m+j-k)(k+l-m-j)}(q^{-1})_{l-j}}{(q^{-1})_{m-k}(q^{-1})_{k+l-j-m}}$$

such subspaces, each with the same probability. So, the extension operator R^X yields the subspace U^+ and an arbitrary subspace $g_1^+(U^+ \cap W')$ of $V + X$ of dimension $(k + l - j - m)$ and linearly independent from V, with probability

$$\frac{(q^{-1})_{n-l}(q^{-1})_{m-k}(q^{-1})_{k+l-j-m}}{q^{(n-l)(l-j)+(m+j-k)(k+l-j-m)}(q^{-1})_{n-j}}. \tag{11}$$

2. Let us now apply L^W. Fix $W'' \subset W'$ a complement of $U^+ \cap W'$ inside W', so that $\dim W'' = m - l$ and

$$\begin{aligned} V^+ &= g_1^{++}(U + W) = g_1^{++}\bigl(U \oplus W'\bigr) = V \oplus g_1^{++}\bigl(W'\bigr) \\ &= V \oplus g_1^+\bigl(U^+ \cap W'\bigr) \oplus g_1^{++}\bigl(W''\bigr). \end{aligned}$$

By similar arguments as before, $g_1^{++}(W'')$ is an arbitrary subspace of $(\mathbb{F}_q)^n$ that is supplementary to $V+X$ and of dimension $(m-l)$, so it has probability

$$q^{(n+l-m)(l-m)}\frac{(q^{-1})_{n-m}(q^{-1})_{m-l}}{(q^{-1})_{n-l}}.$$

From this and Eq. (11), we see that a given choice of U^+, $g_1^+(U^+\cap W')$ and $g_1^{++}(W'')$ has probability

$$q^{(n+l-m)(l-m)+(l-n)(l-j)+(m+j-k)(m+j-k-l)} \times \frac{(q^{-1})_{n-m}(q^{-1})_{m-l}(q^{-1})_{m-k}(q^{-1})_{k+l-j-m}}{(q^{-1})_{n-j}}. \tag{12}$$

It remains to see how many choices of $g_1^+(U^+\cap W')$ and $g_1^{++}(W'')$ yield the same V^+. The first part

$$V\oplus g_1^+\bigl(U^+\cap W'\bigr)=g_1^+\bigl(U^+\cap(U+W)\bigr)$$

is a subspace of $V+X$ of dimension $(k+l-m)$, and it does not change if one takes for $g_1^+(U^+\cap W')$ another complement subspace of V inside $g_1^+(U^+\cap(U+W))$. So, one will have to multiply Eq. (12) by the factor $q^{j(k+l-m-j)}$. One will also have to multiply this probability by the factor $q^{(m-l)(k+l-m)}$, which is the number of complement subspaces $g_1^{++}(W')$ of $g_1^+(U^+\cap(U+W))$ inside V^+. So in the end,

$$\mathbb{P}\bigl[\bigl(U^+,V^+\bigr)\bigr] = q^{(n+l-m)(l-m)+(l-n)(l-j)+(m+j-k)(m+j-k-l)+j(k+l-m-j)+(m-l)(k+l-m)}R_q,$$

where R_q is the quotient of symbols $(q^{-1})_a$ appearing in Eq. (12)—notice that it is also the expected quotient from Formula (10). It is now easy to see that the power of q simplifies as $(m-n)(m-j)+(l-m)(l-j)+(k-m)(k-j)$. □

Denote $\mathbb{C}_{l,U,W,Y}$ the uniform probability on subspaces U^+ satisfying the three conditions of compatibility (8). Lemmas 2.16 and 2.17 show that $\Psi^{(Y;Z)}_{(U,W;V,X)}(I)$ is equal to

$$\sum_{\substack{U^+,V^+\\ g_1^{++},g_2^{++}}}\mathbb{C}_{l,U,W,Y}\bigl[U^+\bigr]\mathbb{C}_{k,V,X,Z}\bigl[V^+\bigr] \times\mathbb{P}\bigl[\bigl(g_1^{++},g_2^{++}\bigr)|\bigl(Y,Z,U^+,V^+\bigr)\bigr](Y\ {}^{g_1^{++}}\!\rightleftarrows_{g_2^{++}} Z).$$

It remains to see that the last conditional expectation is in fact the uniform probability on trivial extensions with fixed left and right subspaces Y and Z, and sending $U+W$ to V^+ and $V+X$ to U^+—we shall say that these extensions are compatible with Y, Z, U^+ and V^+.

We shall use the following counting argument. In Eq. (7), each partial isomorphism that appears has a subspace U^+ which is entirely determined, because it is equal to $g_2^{++}(V+X)$. Therefore, $\Psi^{(Y,Z)}_{(U,W;V,X)}(I)$ is a linear combination of

$$\begin{aligned}&\frac{q^{(m-l)(l-j)}(q^{-1})_{k-j}}{(q^{-1})_{m-l}(q^{-1})_{k+l-j-m}}F_q(m,l,l-j+j_1)F_q(l,j,j_1)\\&\quad=q^{(m+j-j_1)(m-j)}\frac{(q^{-1})_{k-j}(q^{-1})_{l-j}}{(q^{-1})_{k+l-j-m}}\end{aligned}$$

distinct partial isomorphisms, each with the same weight (the inverse of this number of terms). So, $\mathbb{P}[(g_1^{++},g_2^{++})|(Y,Z,U^+,V^+)]$, which is a probability on trivial extensions compatible with Y, Z, U^+ and V^+, is equal either to 0 or to the constant

$$P=\frac{q^{(m-k)(k-j)+(m-l)(l-j)-(m+j-j_1)(m-j)}}{(q^{-1})_{m-k}(q^{-1})_{m-l}(q^{-1})_{k+l-j-m}}.$$

As a consequence, it suffices to show:

Lemma 2.18 *The number of trivial extensions compatible with Y, Z, U^+ and V^+ is*

$$\frac{1}{P}=q^{(m+j-j_1)(m-j)-(m-k)(k-j)-(m-l)(l-j)}\big(q^{-1}\big)_{m-k}\big(q^{-1}\big)_{m-l}\big(q^{-1}\big)_{k+l-j-m}.$$

So, $\mathbb{P}[(g_1^{++},g_2^{++})|(Y,Z,U^+,V^+)]$ is never equal to 0 for a compatible extension, and it is the uniform probability on these compatible trivial extensions.

Proof With the same notations as in Lemma 2.16, one chooses a basis $(e_1,\dots,e_m)$ of Y such that:

$$\begin{aligned}&(e_1,\dots,e_j)\text{ is a basis of }U;\\&(e_1,\dots,e_l)\text{ is a basis of }U^+;\\&(e_{l+1},\dots,e_m)\text{ is a basis of }W'';\\&(e_{m+j-k+1},\dots,e_l)\text{ is a basis of }U^+\cap W';\\&(e_{m+j-k+1},\dots,e_m)\text{ is a basis of }W'.\end{aligned}$$

Fix a compatible trivial extension, and denote $f_i=g_1^{++}(e_i)$.

1. The first j vectors $(f_1,\dots,f_j)$ are fixed since $(g_1^{++})_{|U}=g_1$, so there is no choice there.
2. The $(k+l-j-m)$ vectors $(f_{m+j-k+1},\dots,f_l)$ form a basis of a supplementary of V in $V^+\cap(V+X)$; here one has

$$\big(q^{k+l-m}-q^j\big)\cdots\big(q^{k+l-m}-q^{k+l-m-1}\big)=q^{(k+l-m)(k+l-j-m)}\big(q^{-1}\big)_{k+l-j-m}$$

possibilities.

3. The $(m-k)$ vectors $(f_{j+1},\dots,f_{m+j-k})$ form a basis of a complement subspace of $V^+\cap(V+X)$ inside $V+X$; this gives $q^{l(m-k)}(q^{-1})_{m-k}$ possibilities.
4. Finally, the $(m-l)$ vectors $(f_{l+1},\dots,f_m)$ form a basis of a complement subspace of $V^+\cap(V+X)$ inside V^+; this gives $q^{k(m-l)}(q^{-1})_{m-l}$ possibilities.

So, there are

$$q^{k(m-l)+l(m-k)+(k+l-m)(k+l-j-m)}\left(q^{-1}\right)_{m-k}\left(q^{-1}\right)_{m-l}\left(q^{-1}\right)_{k+l-j-m}$$

possibilities for g_1^{++}. Then, with respect to the two bases $\mathcal{E}$ and $\mathcal{F}$ previously chosen, Condition (4) in Definition 2.3 ensures that a trivial extension of $(U\ {}^{g_1}\!\rightleftarrows_{g_2} V)$ to spaces Y and Z is given by a matrix

$$\operatorname{mat}_{\mathcal{F},\mathcal{E}}\left(g_2^{++}\right)=\begin{pmatrix}G & (G-I_{m-j})R\\ 0 & I_{m-j}\end{pmatrix},$$

with R rectangular matrix. This rectangular matrix R can really be chosen arbitrarily, because the conditions of compatibility have all been ensured by the choice of g_1^{++}. So, there are $q^{(m-j)(j-j_1)}$ possibilities for $(G-I_{m-j})R$. This last factor multiplied by the previous quantity gives indeed

$$q^{(m+j-j_1)(m-j)-(m-k)(k-j)-(m-l)(l-j)}\left(q^{-1}\right)_{m-k}\left(q^{-1}\right)_{m-l}\left(q^{-1}\right)_{k+l-j-m}$$

distinct trivial extensions that are compatible with Y, Z, U^+ and V^+. □

Thus, we have proved the following decomposition theorem for $\mathrm{L}^W\circ\mathrm{R}^X$:

Theorem 2.19 *If $I=(U\ {}^{g_1}\!\rightleftarrows_{g_2} V)$, then*

$$\mathrm{L}^W\circ\mathrm{R}^X(I)=\sum\mathbb{P}[m]\mathbb{U}_{m,U+W}[Y]\mathbb{U}_{m,V+X}[Z]\Psi^{(Y,Z)}_{(U,W;V,X)}(I)$$

$$\Psi^{(Y,Z)}_{(U,W;V,X)}(I)=\sum\mathbb{C}_{l,U,W,Y}\left[U^+\right]\mathbb{C}_{k,V,X,Z}\left[V^+\right]\times\mathbb{D}_{\substack{U,U^+,W\\ V,V^+,X}}\left(g_1^{++},g_2^{++}\right)\left(Y\ {}^{g_1^{++}}\!\rightleftarrows_{g_2^{++}} Z\right),$$

where:

- *m runs over $[\![\sup(k,l),\inf(n,k+l-j)]\!]$, and it has probability $\mathbb{P}[m]$ given by Lemma 2.13*;
- *(Y,Z) runs over pair of subspaces of dimension m containing, respectively, $U+W$ and $V+X$, and it has uniform probability $\mathbb{U}_{m,U+W}[Y]\mathbb{U}_{m,V+X}[Z]$ among these pairs of subspaces*;
- *U^+ (respectively, V^+) runs over subspaces satisfying the three conditions of Lemma 2.16 (respectively, Lemma 2.17), and it has uniform probability $\mathbb{C}_{l,U,W,Y}[U^+]$ (resp., $\mathbb{C}_{k,V,X,Z}[V^+]$) among them*;
- *and (g_1^{++},g_2^{++}) runs over trivial extensions of (g_1,g_2) to Y and Z with the additional constraints*

$$g_1^{++}(U+W)=V^+;\qquad g_2^{++}(V+X)=U^+;$$

and it has uniform probability $\mathbb{D}_{\substack{U,U^+,W\\ V,V^+,X}}(g_1^{++},g_2^{++})$ *among these trivial extensions.*

Since this description is symmetric in the entries of I on the left and on the right, one obtains the same expansion for $\mathrm{R}^X\circ\mathrm{L}^W(I)$, so Theorem 2.12 is true.

2.4 Proof of the associativity

Fix three partial isomorphisms $G=(S\ {}^{g_1}{\rightleftarrows}_{g_2}\ T)$, $H=(U\ {}^{h_1}{\rightleftarrows}_{h_2}\ V)$ and $I=(W\ {}^{i_1}{\rightleftarrows}_{i_2}\ X)$, of respective dimensions j_G, j_H and j_L. The last step before the proof of Theorem 2.8 is a more concrete description of $\mathrm{R}^W(\mathrm{R}^U(G)\cdot\mathrm{L}^T(H))$, where $\cdot$ indicates that one takes the product of two partial isomorphisms such that the right subspace of the left-hand side corresponds to the left subspace of the right-hand side (this restriction $\cdot$ of the product $*$ is clearly associative). Recall the description

$$\mathrm{R}^W\mathrm{L}^T(H)=\sum\mathbb{P}[m]\mathbb{U}_{m,T+U}[Y]\mathbb{U}_{m,V+W}[Z]\varPsi^{(Y;Z)}_{(U,T;V,W)}(H),$$

where $\mathbb{P}[m]$ is an explicit probability on integers between $\max(\dim(T+U),\dim(V+W))$ and $\min(n,\dim(T+U)+\dim(V+W)-j_H)$, see Lemma 2.13.

Proposition 2.20 *With the same notations,*

$$\mathrm{R}^W\big(\mathrm{R}^U(G)\cdot\mathrm{L}^T(H)\big)=\sum\mathbb{P}[m]\mathbb{U}_{m,T+U}[Y]\mathbb{U}_{m,V+W}[Z]\big(\mathrm{R}^Y_T(G)\cdot\varPsi^{(Y;Z)}_{(U,T;V,W)}(H)\big).$$

Lemma 2.21 *Consider two partial isomorphisms G defined over spaces A and B, and H defined over spaces D and E. If $A\subset A^+\subset A^{++}$, $E\subset E^+\subset E^{++}$, and $B+D\subset C^+$, then*

$$\begin{aligned}&\mathrm{LR}^{(A^{++},E^{++})}_{(A^+,E^+)}\big(\mathrm{LR}^{(A^+,C^+)}_{(A,B)}(G)\cdot\mathrm{LR}^{(C^+,E^+)}_{(D,E)}(H)\big)\\&\quad=\sum\mathbb{U}_{m,C^+}\big[C^{++}\big]\big(\varPhi^{(A^{++};C^{++})}_{(A,A^+;B,C^+)}(G)\cdot\varPhi^{(C^{++};E^{++})}_{(D,C^+;E,E^+)}(H)\big),\end{aligned}$$

where $m=\dim A^{++}=\dim E^{++}$; and

$$\varPhi^{(A^{++};C^{++})}_{(A,A^+;B,C^+)}(G)=\mathrm{LR}^{(A^{++},C^{++})}_{(A^+,C^+)}\mathrm{LR}^{(A^+,C^+)}_{(A,B)}(G)$$

is the mean of all trivial extensions of G to spaces A^{++} and C^{++} that send A^+ to C^+ (and similarly for $\varPhi^{(C^{++};E^{++})}_{(D,C^+;E,E^+)}(H)$).

Proof Let $G=(U\ {}^{g_1}{\rightleftarrows}_{g_2}\ V)$ and $H=(V\ {}^{h_1}{\rightleftarrows}_{h_2}\ W)$ be two partial isomorphisms of same dimension k, and $m=\dim U^+=\dim W^+$ with $U\subset U^+$ and $W\subset W^+$. We claim that

$$\mathrm{LR}^{(U^+,W^+)}_{(U,W)}(G\cdot H)=\sum\mathbb{U}_{m,V}\big[V^+\big]\big(\mathrm{LR}^{(U^+,V^+)}_{(U,V)}(G)\cdot\mathrm{LR}^{(V^+,W^+)}_{(V,W)}(H)\big).\qquad(13)$$

To begin with, notice that both sides of (13) are averages of partial isomorphisms contained in the set $\mathscr{E}(U^+ \uparrow U \,{}^{g_1h_1}\!\rightleftarrows_{h_2g_2}\, W \uparrow W^+)$. This is obvious for the left-hand side, and for the right-hand side, if $(U^+ \,{}^{g_1^+}\!\rightleftarrows_{g_2^+}\, V^+)$ and $(V^+ \,{}^{h_1^+}\!\rightleftarrows_{h_2^+}\, W^+)$ are two trivial extensions of G and H, then with the notations of Definition 2.3, $\widetilde{g_1}\widetilde{g_2} = \mathrm{id}_{U^+/U}$ and $\widetilde{h_1}\widetilde{h_2} = \mathrm{id}_{V^+/V}$, so

$$\widetilde{g_1h_1}\widetilde{h_2g_2} = \widetilde{g_1}(\widetilde{h_1}\widetilde{h_2})\widetilde{g_2} = \widetilde{g_1}\widetilde{g_2} = \mathrm{id}_{U^+/U},$$

which means that the product of trivial extensions is a trivial extension. Therefore, it suffices to show that every element of $\mathscr{E}(U^+ \uparrow U \,{}^{g_1h_1}\!\rightleftarrows_{h_2g_2}\, W \uparrow W^+)$ appears in the right-hand side of (13), and with the same weight. Fix two bases $\mathcal{E}^+$ and $\mathcal{G}^+$ of U^+ and W^+ such that

$$\mathrm{mat}_{\mathcal{E},\mathcal{G}}(g_1h_1) = I_k; \qquad \mathrm{mat}_{\mathcal{G},\mathcal{E}}(h_2g_2) = GH.$$

By Lemma 2.4, a trivial extension of $(G \cdot H)$ is given by two matrices

$$\mathrm{mat}_{\mathcal{E}^+,\mathcal{G}^+}\big((g_1h_1)^+\big) = \begin{pmatrix} I_k & R_1 \\ 0 & K \end{pmatrix}$$

with K invertible and R_1 rectangular;

$$\mathrm{mat}_{\mathcal{G}^+,\mathcal{E}^+}\big((h_2g_2)^+\big) = \begin{pmatrix} GH & (GH - I_k)R_2 \\ 0 & I_{m-k} \end{pmatrix} \begin{pmatrix} I & -R_1K^{-1} \\ 0 & K^{-1} \end{pmatrix}$$

with R_2 rectangular.

Thus, introducing the two subgroups of $\mathrm{GL}(m, \mathbb{F}_q)$

$$\mathrm{P}(m,k) = \left\{ \begin{pmatrix} I_k & R \\ 0 & K \end{pmatrix}, \text{ with } K \text{ invertible and } R \text{ rectangular} \right\};$$

$$\mathrm{N}(m, GH) = \left\{ \begin{pmatrix} I_k & (GH - I_k)R \\ 0 & I_{m-k} \end{pmatrix}, \text{ with } R \text{ rectangular} \right\},$$

the group $\mathrm{P}(m,k) \times \mathrm{N}(m, GH)$ acts on $\mathcal{E}(U^+ \uparrow U \,{}^{g_1h_1}\!\rightleftarrows_{h_2g_2}\, W \uparrow W^+)$ in a free transitive way. Consequently, it suffices to verify that the right-hand side of Eq. (13) is invariant under this action. In the following we denote RHS this right-hand side.

Set $f_i = g_1(e_i)$ for $i \in [\![1, k]\!]$, and

$$\mathrm{mat}_{\mathcal{E},\mathcal{F}}(g_1) = I_k; \qquad \mathrm{mat}_{\mathcal{F},\mathcal{E}}(g_2) = G$$

$$\mathrm{mat}_{\mathcal{F},\mathcal{G}}(h_1) = I_k; \qquad \mathrm{mat}_{\mathcal{G},\mathcal{F}}(h_2) = H.$$

To choose randomly V^+ in RHS, one can choose a random completion $(f_{k+1}, \dots, f_m)$ of $(f_1, \dots, f_k)$ into a family of m independent vectors of $(\mathbb{F}_q)^n$, and then set $V^+ = \mathrm{Span}(f_1, \dots, f_m)$. This allows to choose simultaneously the extension g_1^+ by requiring that $\mathrm{mat}_{\mathcal{E}^+,\mathcal{F}^+}(g_1^+) = I_m$. Then, in RHS, conditionally on the previous choice of $\mathcal{F}^+$,

$$\mathrm{mat}_{\mathcal{F}^+,\mathcal{G}^+}\big(h_1^+\big) = \begin{pmatrix} I_k & R_1 \\ 0 & K \end{pmatrix};$$

$$\mathrm{mat}_{\mathcal{G}^+,\mathcal{F}^+}\big(h_2^+\big) = \begin{pmatrix} H & (H-I_k)R_2 \\ 0 & I_{m-k} \end{pmatrix} \begin{pmatrix} I_k & -R_1K^{-1} \\ 0 & K^{-1} \end{pmatrix};$$

$$\mathrm{mat}_{\mathcal{F}^+,\mathcal{E}^+}\big(g_2^+\big) = \begin{pmatrix} G & (G-I_k)R_3 \\ 0 & I_{m-k} \end{pmatrix}$$

where K has uniform law on $\mathrm{GL}(m-k,\mathbb{F}_q)$, and R_1, R_2 and R_3 are independent and uniformly distributed rectangular matrices in $\mathrm{M}(k\times(m-k),\mathbb{F}_q)$. So,

$$\begin{aligned}\mathrm{RHS} &= \sum \mathbb{U}\big[\mathcal{F}^+,K,R_1,R_2,R_3\big]\left(\begin{pmatrix} I_k & R_1 \\ 0 & K \end{pmatrix}\right. \\ &\qquad \left.\rightleftarrows \begin{pmatrix} G & (G-I_k)R_3 \\ 0 & I_{m-k} \end{pmatrix}\begin{pmatrix} H & (H-I_k)R_2 \\ 0 & I_{m-k} \end{pmatrix}\begin{pmatrix} I_k & -R_1K^{-1} \\ 0 & K^{-1} \end{pmatrix}\right) \\ &= \sum \mathbb{U}\big[\mathcal{F}^+,K,R_1,R_2,R_3\big]\left(\begin{pmatrix} I_k & R_1 \\ 0 & K \end{pmatrix}\right. \\ &\qquad \left.\rightleftarrows \begin{pmatrix} GH & (GH-G)R_2+(G-I_k)R_3 \\ 0 & I_{m-k} \end{pmatrix}\begin{pmatrix} I_k & -R_1K^{-1} \\ 0 & K^{-1} \end{pmatrix}\right)\end{aligned}$$

where the $\mathbb{U}$'s denote the previously described uniform laws. Now, note that the random free family $\mathcal{F}^+$ does not appear anymore in the description of the partial isomorphisms from U^+ to W^+. Thus,

$$\begin{aligned}\mathrm{RHS} &= \sum \mathbb{U}[K,R_1,R_2,R_3]\left(\begin{pmatrix} I_k & R_1 \\ 0 & K \end{pmatrix}\right. \\ &\qquad \left.\rightleftarrows \begin{pmatrix} GH & (GH-G)R_2+(G-I_k)R_3 \\ 0 & I_{m-k} \end{pmatrix}\begin{pmatrix} I_k & -R_1K^{-1} \\ 0 & K^{-1} \end{pmatrix}\right),\end{aligned}$$

with the matrices written w.r.t. the two bases $\mathcal{E}^+$ and $\mathcal{G}^+$. In this representation of RHS, the invariance by action of $\mathrm{P}(m,k)$ is obvious. On the other hand, if one makes act an element $\left(\begin{smallmatrix} I_k & (GH-I_k)R \\ 0 & I_{m-k} \end{smallmatrix}\right)$ of $\mathrm{N}(m,GH)$, then the random matrix

$$\begin{pmatrix} GH & (GH-G)R_2+(G-I_k)R_3 \\ 0 & I_{m-k} \end{pmatrix} \quad \text{becomes}$$

$$\begin{pmatrix} GH & (GH-G)(R_2+R)+(G-I_k)(R_3+R) \\ 0 & I_{m-k} \end{pmatrix}.$$

Since R_2 and R_3 are independent uniformly distributed rectangular matrices, the law of (R_2+R, R_3+R) is the same as the law of (R_2,R_3), so the invariance by action of $\mathrm{N}(m,GH)$ is also shown. Finally, Lemma 2.21 follows from the simpler and more general identity (13) by expanding linearly $\mathrm{LR}_{(A,B)}^{(A^+,C^+)}(G)$ and $\mathrm{LR}_{(D,E)}^{(C^+,E^+)}(H)$. □

Proof of Proposition 2.20 Set $k=\dim(T+U)$ and $l=\dim(V+W)$. One has by definition of the extension operators:

$$\mathrm{R}^U(G)\cdot\mathrm{L}^T(H) = \sum \mathbb{U}_{k,S}\big[S^+\big]\mathbb{U}_{k,V}\big[V^+\big]\big(\mathrm{LR}_{(S,T)}^{(S^+,T+U)}(G)\cdot\mathrm{LR}_{(U,V)}^{(T+U,V^+)}(H)\big).$$

By Lemma 2.13, the law of $m=\dim(V^{+}+W)$ is given by $\mathbb{P}[m]$, and then by Corollary 2.14 and Lemma 2.16, one obtains for $\mathrm{R}^{W}(\mathrm{R}^{U}(G)\cdot\mathrm{L}^{T}(H))$

$$\sum\mathbb{P}[m]\mathbb{U}_{k,S}\big[S^{+}\big]\mathbb{U}_{m,S^{+}}\big[S^{++}\big]\mathbb{U}_{m,V+W}[Z]\mathbb{C}_{k,V,W,Z}[V^{+}]\Theta_{(m,S^{+},S^{++},Z,V^{+})}(G,H)$$

with

$$\begin{aligned}\Theta_{(m,S^{+},S^{++},Z,V^{+})}(G,H)&=\mathrm{LR}^{(S^{++},Z)}_{(S^{+},V^{+})}\big(\mathrm{LR}^{(S^{+},T+U)}_{(S,T)}(G)\cdot\mathrm{LR}^{(T+U,V^{+})}_{(U,V)}(H)\big)\\&=\sum\mathbb{U}_{m,T+U}[Y]\big(\Phi^{(S^{++},Y)}_{(S,S^{+};T,T+U)}(G)\\&\quad\cdot\Phi^{(Y;Z)}_{(U,T+U;V,V^{+})}(H)\big)\end{aligned}$$

by Lemma 2.21. Therefore, by changing the order of summation,

$$\begin{aligned}&\mathrm{R}^{W}\big(\mathrm{R}^{U}(G)\cdot\mathrm{L}^{T}(H)\big)\\&\quad=\sum\mathbb{P}[m]\mathbb{U}_{m,T+U}[Y]\mathbb{U}_{m,V+W}[Z]\mathbb{C}_{k,V,W,Z}\big[V^{+}\big]\Xi_{(m,Y,Z,V^{+})}(G,H),\end{aligned}$$

where

$$\begin{aligned}&\Xi_{(m,Y,Z,V^{+})}(G,H)\\&\quad=\sum\mathbb{U}_{k,S}\big[S^{+}\big]\mathbb{U}_{m,S^{+}}\big[S^{++}\big]\big(\Phi^{(S^{++};Y)}_{(S,S^{+};T,T+U)}(G)\cdot\Phi^{(Y;Z)}_{(U,T+U;V,V^{+})}(H)\big)\\&\quad=\sum\mathbb{U}_{m,S}\big[S^{++}\big]\big(\mathrm{LR}^{(S^{++},Y)}_{(S,T)}(G)\cdot\Phi^{(Y;Z)}_{(U,T+U;V,V^{+})}(H)\big)\\&\quad=\mathrm{R}^{Y}_{T}(G)\cdot\Phi^{(Y;Z)}_{(U,T+U;V,V^{+})}(H).\end{aligned}$$

Finally, by using the remark at the beginning of the proof of Lemma 2.21, the definition of the operators Ψ, and Lemma 2.16,

$$\sum\mathbb{C}_{k,V,W,Z}\big[V^{+}\big]\Phi^{(Y;Z)}_{(U,T+U;V,V^{+})}(H)=\Psi^{(Y;Z)}_{(U,T;V,W)}(H),$$

which leads to the expansion stated in the proposition. □

Proof of Theorem 2.8 Proposition 2.20 shows that

$$\begin{aligned}(G*H)*I&=\big(\mathrm{R}^{W}\big(\mathrm{R}^{U}(G)\cdot\mathrm{L}^{T}(H)\big)\big)*I\\&=\sum\mathbb{P}[m]\mathbb{U}_{m,T+U}[Y]\mathbb{U}_{m,V+W}[Z]\big(\big(\mathrm{R}^{Y}_{T}(G)\cdot\Psi^{(Y;Z)}_{(U,T;V,W)}(H)\big)*I\big)\\&=\sum\mathbb{P}[m]\mathbb{U}_{m,T+U}[Y]\mathbb{U}_{m,V+W}[Z]\big(\mathrm{R}^{Y}_{T}(G)\cdot\Psi^{(Y;Z)}_{(U,T;V,W)}(H)\cdot\mathrm{L}^{Z}_{W}(I)\big).\end{aligned}$$

The symmetry of this form ensures that one obtains the same with $G*(H*I)$. Thus, we have finally shown that $\mathscr{A}(n,\mathbb{F}_q)$ is an algebra. □

Remark 2.22 The whole proof of the associativity of the product $*$ justifies Definition 2.1 of partial isomorphisms as pairs of isomorphisms between two arbitrary subspaces of same dimension. One could have tried the following simpler construction of partial isomorphisms: a partial isomorphism is one linear automorphism g of a subspace $V \subset (\mathbb{F}_q)^n$, and the product of these simpler partial isomorphisms is defined by taking means of trivial extensions, a trivial extension of (g, V) to a space V^+ containing V being an automorphism g^+ of V^+ such $(g^+)_{|V} = g$ and $t(g^+) = t(g) \sqcup (X - 1 : 1^{k^+ - k})$. This seems easier and more natural, but it does not work: the underlying "algebra" is not associative as soon as $n \geq 2$. Indeed, given two "naive" partial isomorphisms G, H defined on the same space L of dimension 1, and I the partial isomorphism which is the identity on a 2-dimensional space P containing L, it is easy to see that for G and H non-trivial, $G * (H * I)$ is not the same as $(G * H) * I$: the last product contains only diagonalizable partial isomorphisms of P, and it is not the case of the first product.

3 Constructions around $\mathcal{A}(n, \mathbb{F}_q)$ and $\mathcal{Z}(n, \mathbb{F}_q)$

In this section, we analyze the relations between $\mathbb{C}[\mathrm{GL}(n, \mathbb{F}_q) \times (\mathrm{GL}(n, \mathbb{F}_q))^{\mathrm{opp}}]$ and $\mathcal{A}(n, \mathbb{F}_q)$; between $Z(n, \mathbb{F}_q)$ and a subalgebra of invariants $\mathcal{Z}(n, \mathbb{F}_q) \subset \mathcal{A}(n, \mathbb{F}_q)$; and between the algebras $\mathcal{Z}(n, \mathbb{F}_q)$ for various values of n. Our main goal is to prove Theorem 3.7, which generalizes an old result of Farahat and Higman for products of conjugacy classes in the symmetric group algebras ([7, Theorem 2.2]), see also [12, Proposition 7.3], [16, Theorem 1] and [24, Theorem 2.1].

3.1 The map from $\mathcal{A}(n, \mathbb{F}_q)$ to $\mathbb{C}[\mathrm{GL}(n, \mathbb{F}_q) \times (\mathrm{GL}(n, \mathbb{F}_q))^{\mathrm{opp}}]$

Consider the extension operator

$$\pi_n = \mathrm{L}^{(\mathbb{F}_q)^n} = \mathrm{R}^{(\mathbb{F}_q)^n};$$

it is idempotent, and it sends $\mathcal{A}(n, \mathbb{F}_q)$ to a subalgebra of it which is isomorphic to $\mathbb{C}[\mathrm{GL}(n, \mathbb{F}_q) \times \mathrm{GL}(n, \mathbb{F}_q)^{\mathrm{opp}}]$. Indeed, a partial isomorphism with underlying spaces $(\mathbb{F}_q)^n$ and $(\mathbb{F}_q)^n$ is just a pair of isomorphisms (g_1, g_2), the product being

$$(g_1, g_2)(h_1, h_2) = (g_1 h_1, h_2 g_2),$$

that is to say the product of $\mathrm{GL}(n, \mathbb{F}_q) \times (\mathrm{GL}(n, \mathbb{F}_q))^{\mathrm{opp}}$.

Proposition 3.1 *The map $\pi_n : \mathcal{A}(n, \mathbb{F}_q) \to \mathbb{C}[\mathrm{GL}(n, \mathbb{F}_q) \times (\mathrm{GL}(n, \mathbb{F}_q))^{\mathrm{opp}}]$ is a morphism of algebras. Moreover, it is compatible with the action of* $\mathrm{GL}(n, \mathbb{F}_q)$ *on the left and on the right.*

Proof Take two partial isomorphisms $G = (S\ {}^{g_1}\!\rightleftarrows_{g_2}\ T)$ and $H = (U\ {}^{h_1}\!\rightleftarrows_{h_2}\ V)$. By Proposition 2.20, one has

$$\begin{aligned}\pi_n(G * H) &= \mathrm{R}^{(\mathbb{F}_q)^n}\big(\mathrm{R}^U(G) \cdot \mathrm{L}^T(H)\big)\\ &= \sum \mathbb{P}[m]\mathbb{U}_{m,T+U}[Y]\mathbb{U}_{m,V+(\mathbb{F}_q)^n}[Z]\big(\mathrm{R}^Y_T(G) \cdot \Psi^{(Y;Z)}_{(U,T;V,(\mathbb{F}_q)^n)}(H)\big)\end{aligned}$$

$$= \mathrm{R}_T^{(\mathbb{F}_q)^n}(G) \cdot \Psi^{((\mathbb{F}_q)^n;(\mathbb{F}_q)^n)}_{(U,T;V,(\mathbb{F}_q)^n)}(H) = \pi_n(G) \cdot \pi_n(H).$$

Consider the inclusion

$$\begin{aligned} \mathrm{GL}(n,\mathbb{F}_q) &\hookrightarrow \mathrm{GL}(n,\mathbb{F}_q) \times \big(\mathrm{GL}(n,\mathbb{F}_q)\big)^{\mathrm{opp}} \\ g &\mapsto \big(g, g^{-1}\big). \end{aligned}$$

The compatibility of $\pi_n = \mathrm{R}^{(\mathbb{F}_q)^n}$ with the action of $\mathrm{GL}(n,\mathbb{F}_q)$ on the left follows from the general relations

$$g \cdot \big(\mathrm{R}_V^{V^+}(U\ {}^{g_1}\!\rightleftarrows_{g_2} V)\big) = \mathrm{R}_V^{V^+}\big(g \cdot (U\ {}^{g_1}\!\rightleftarrows_{g_2} V)\big); \tag{14}$$

$$\big(\mathrm{L}_U^{U^+}(U\ {}^{g_1}\!\rightleftarrows_{g_2} V)\big) \cdot k = \mathrm{L}_U^{U^+}\big((U\ {}^{g_1}\!\rightleftarrows_{g_2} V) \cdot k\big). \tag{15}$$

They are themselves easily seen for instance from characterization (2) of trivial extensions in Definition 2.3. Since $\pi_n = \mathrm{L}^{(\mathbb{F}_q)^n}$, one obtains for the same reasons the compatibility of π_n with the action of $(\mathrm{GL}(n,\mathbb{F}_q))^{\mathrm{opp}}$ on the right. □

At this point one might want to construct an algebra $\mathscr{A}(\infty,\mathbb{F}_q)$ which would be a projective limit of the $\mathscr{A}(n,\mathbb{F}_q)$'s, in order to do generic computations directly for all the algebras $\mathbb{C}[\mathrm{GL}(n,\mathbb{F}_q) \times (\mathrm{GL}(n,\mathbb{F}_q))^{\mathrm{opp}}]$. However, the product of two partial isomorphisms $G = (S\ {}^{g_1}\!\rightleftarrows_{g_2} T)$ and $H = (U\ {}^{h_1}\!\rightleftarrows_{h_2} V)$ in an algebra $\mathscr{A}(n',\mathbb{F}_q)$ involves arbitrary subspaces $S^+ \supset S$ and $V^+ \supset V$ inside $(\mathbb{F}_q)^{n'}$. So, even if U, V, S, T are included into $(\mathbb{F}_q)^n$ with $n < n'$, there is no natural way to view the terms of $G * H$ as elements of $\mathscr{A}(n,\mathbb{F}_q)$, even after applying a morphism to "bring back" S^+ and V^+ into $(\mathbb{F}_q)^n$. In other terms,

$$\begin{aligned} p_{n' \to n} : \mathscr{A}\big(n',\mathbb{F}_q\big) &\to \mathscr{A}(n,\mathbb{F}_q) \\ (U\ {}^{g_1}\!\rightleftarrows_{g_2} V) &\mapsto \begin{cases} (U\ {}^{g_1}\!\rightleftarrows_{g_2} V) & \text{if } U, V \subset (\mathbb{F}_q)^n, \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

is not a morphism of algebras, in opposition to what happens for partial permutations (*cf.* [12]). This difficulty seems to be a common feature for products defined by taking means, see [24, Proposition 3.11]. It disappears by looking at subalgebras of invariants: indeed, one knows then the proportion of configurations that stay in $(\mathbb{F}_q)^n$, and this will enable us to construct projections $\mathscr{Z}(n',\mathbb{F}_q) \to \mathscr{Z}(n,\mathbb{F}_q)$ that are now morphisms of (commutative) algebras.

3.2 The graded algebras of invariants $\mathscr{Z}(n,\mathbb{F}_q)$

We define $\mathscr{Z}(n,\mathbb{F}_q)$ as the subspace of $\mathscr{A}(n,\mathbb{F}_q)$ that consists in elements invariants under the actions of $\mathrm{GL}(n,\mathbb{F}_q)$ on the left and of $(\mathrm{GL}(n,\mathbb{F}_q))^{\mathrm{opp}}$ on the right. Equations (14) and (15) show that for general elements of $\mathscr{I}(n,\mathbb{F}_q)$,

$$g \cdot (x * y) = (g \cdot x) * y,$$

$$(x * y) \cdot h = x * (y \cdot h);$$

therefore, $\mathscr{Z}(n, \mathbb{F}_q)$ is a subalgebra of $\mathscr{A}(n, \mathbb{F}_q)$. Then, Proposition 3.1 ensures that $\pi_n(\mathscr{Z}(n, \mathbb{F}_q))$ is included into the center of the group algebra $Z(n, \mathbb{F}_q)$, and it is in fact equal to this center. Indeed, the injective map

$$\begin{aligned} i_n : \mathbb{C}\bigl[\mathrm{GL}(n, \mathbb{F}_q) \times \bigl(\mathrm{GL}(n, \mathbb{F}_q)\bigr)^{\mathrm{opp}}\bigr] &\to \mathscr{A}(n, \mathbb{F}_q) \\ (g, h) &\mapsto ((\mathbb{F}_q)^n \ {}^{g}\rightleftarrows_{h} \ \bigl(\mathbb{F}_q\bigr)^n) \end{aligned}$$

satisfies $\pi_n \circ i_n = \mathrm{id}_{\mathbb{C}[G \times G^{\mathrm{opp}}]}$, and it sends $Z(n, \mathbb{F}_q)$ into $\mathscr{Z}(n, \mathbb{F}_q)$. So, for every n, we obtain an algebra that sends onto $Z(n, \mathbb{F}_q)$ in a natural way. In this paragraph, we detail the properties of $\mathscr{Z}(n, \mathbb{F}_q)$.

To start with, we endow $\mathscr{A}(n, \mathbb{F}_q)$ with the grading $\deg(V \ {}^{g_1}\rightleftarrows_{g_2} \ W) = \dim V = \dim W$. This is a grading of algebras: indeed, for two partial isomorphisms $(U \ {}^{g_1}\rightleftarrows_{g_2} \ V)$ and $(W \ {}^{h_1}\rightleftarrows_{h_2} \ X)$,

$$\begin{aligned} \deg\bigl(\bigl(U \ {}^{g_1}\rightleftarrows_{g_2} \ V\bigr) * \bigl(W \ {}^{h_1}\rightleftarrows_{h_2} \ X\bigr)\bigr) &= \deg\bigl(\bigl(\mathrm{R}_V^{V+W}(U \ {}^{g_1}\rightleftarrows_{g_2} \ V)\bigr) \\ &\quad \cdot \bigl(\mathrm{L}_W^{V+W}(W \ {}^{h_1}\rightleftarrows_{h_2} \ X)\bigr)\bigr) \\ &= \dim(V + W) \\ &\leq \dim V + \dim W \\ &\leq \deg(U \ {}^{g_1}\rightleftarrows_{g_2} \ V) + \deg(W \ {}^{h_1}\rightleftarrows_{h_2} \ X). \end{aligned}$$

For a polypartition $\mathbb{\mu}$ of size $k \leq n$, recall that $\mathbb{\mu} \uparrow^n$ is the polypartition of size n obtained by adding parts 1 to the partition $\mu(X-1)$. We also set $k = |\mathbb{\mu}|$, $k_1 = \ell(\mu(X-1))$ and $k_{11} = m_1(\mu(X-1))$. These quantities, and Pochhammer symbols of them, appear in the quotients of cardinalities

$$\frac{\operatorname{card} C_{\mathbb{\mu}\uparrow^n}}{\operatorname{card} C_{\mathbb{\mu}}},$$

as follows from the formula given after Definition 1.3.

Proposition 3.2 *The space of invariants $\mathscr{Z}(n, \mathbb{F}_q)$ is a graded algebra, with homogeneous basis given by*

$$A_{\mathbb{\mu},n} = \sum_{\substack{\mathcal{E}=(e_1,\ldots,e_k) \\ \mathcal{F}=(f_1,\ldots,f_k)}} \bigl(\mathrm{Span}(\mathcal{E}) \ {}^{I_k}\rightleftarrows_{J(\mathbb{\mu})} \ \mathrm{Span}(\mathcal{F})\bigr),$$

where $\mathbb{\mu}$ runs over the set $\bigsqcup_{k=0}^{n} \mathfrak{P}(k, \mathbb{F}_q)$ of polypartitions of size $k \in [\![0, n]\!]$; the sum is over free families $\mathcal{E}$ and $\mathcal{F}$ of size $k = |\mathbb{\mu}|$; and the matrices I_k and $J(\mathbb{\mu})$ determine isomorphisms with respect to the chosen bases $\mathcal{E}$ and $\mathcal{F}$. One has then $\deg A_{\mathbb{\mu},n} = |\mathbb{\mu}| = k$, *and*

$$\pi_n(A_{\mathbb{\mu},n}) = q^{2(n-k)k_1} \frac{q^{2k^2} (q^{-1})_k (q^{-1})_{n-k+k_{11}} (q^{-1})_n}{(q^{-1})_{k_{11}} ((q^{-1})_{n-k})^2 (\operatorname{card} C_{\mathbb{\mu}})} C'_{\mathbb{\mu}\uparrow^n},$$

where as in the introduction $C'_{\mathbb{\nu}} = \frac{1}{\mathrm{card}\,\mathrm{GL}(n,\mathbb{F}_q)} \sum_{t(g_1 g_2)=\mathbb{\nu}} (g_1, g_2)$ *for a polypartition* $\mathbb{\nu}$ *of size* n.

Proof The grading on $\mathscr{A}(n, \mathbb{F}_q)$ restricts to $\mathscr{Z}(n, \mathbb{F}_q)$, with obviously $\deg A_{\mathbb{\mu},n} = |\mathbb{\mu}| = k$. Let us check that $(A_{\mathbb{\mu},n})_{|\mathbb{\mu}|\leq n}$ is indeed a basis of $\mathscr{Z}(n, \mathbb{F}_q)$. By a previous remark, the orbit of a partial isomorphism $(V\ {}^{g_1}\!\rightleftarrows_{g_2} W)$ is uniquely determined by the conjugacy type of $g_1 g_2 \in \mathrm{GL}(V)$, and an invariant element of $\mathscr{Z}(n, \mathbb{F}_q)$ writes uniquely as a linear combination of such orbits. Since $A_{\mathbb{\mu},n}$ consists obviously in elements of type $\mathbb{\mu}$, it suffices to verify that it is an invariant element; it will then be a multiple of the orbit of type $\mathbb{\mu}$. Let $g \in \mathrm{GL}(n, \mathbb{F}_q)$; one has

$$\begin{aligned} g \cdot A_{\mathbb{\mu},n} &= \sum_{\substack{\mathcal{E}=(e_1,\ldots,e_k)\\ \mathcal{F}=(f_1,\ldots,f_k)}} g \cdot \bigl(\mathrm{Span}(\mathcal{E})\ {}^{I_k}\!\rightleftarrows_{J(\mathbb{\mu})} \mathrm{Span}(\mathcal{F})\bigr) \\ &= \sum_{\substack{\mathcal{E}'=(g^{-1}(e_1),\ldots,g^{-1}(e_k))\\ \mathcal{F}=(f_1,\ldots,f_k)}} \bigl(\mathrm{Span}\bigl(\mathcal{E}'\bigr)\ {}^{I_k}\!\rightleftarrows_{J(\mathbb{\mu})} \mathrm{Span}(\mathcal{F})\bigr) = A_{\mathbb{\mu},n} \end{aligned}$$

since g^{-1} yields a permutation of all free families of size k in $(\mathbb{F}_q)^n$. This shows the invariance on the left, and the invariance on the right is proven similarly.

Thus, $(A_{\mathbb{\mu},n})_{|\mathbb{\mu}|\leq n}$ is a basis of $\mathscr{Z}(n, \mathbb{F}_q)$, and $\pi_n(A_{\mathbb{\mu},n})$ is an element of $Z(n, \mathbb{F}_q)$ that consists in elements all of type $\mathbb{\mu} \uparrow^n$ (they are trivial extensions of elements of type $\mathbb{\mu}$). So, $\pi_n(A_{\mathbb{\mu},n}) = \alpha_{\mathbb{\mu}} C'_{\mathbb{\mu}\uparrow^n}$, and the coefficient $\alpha_{\mathbb{\mu}}$ is given by the quotient of the cardinalities of $A_{\mathbb{\mu},n}$ and of $C_{\mathbb{\mu}\uparrow^n}$, the conjugacy class of elements of type $\mathbb{\mu} \uparrow^n$ in $\mathrm{GL}(n, \mathbb{F}_q)$. Denote $k_1 = \ell(\mu(X-1))$, and $k_{11} = m_1(\mu(X-1))$. We have

$$\begin{aligned} \mathrm{card}\, A_{\mathbb{\mu},n} &= \left(q^{nk} \frac{(q^{-1})_n}{(q^{-1})_{n-k}}\right)^2 \\ \mathrm{card}\, C_{\mathbb{\mu}\uparrow^n} &= \left(\frac{q^{2(n-k)(k-k_1)}(q^{-1})_n (q^{-1})_{k_{11}}}{(q^{-1})_k (q^{-1})_{n-k+k_{11}}}\right) \mathrm{card}\, C_{\mathbb{\mu}} \\ \alpha_{\mathbb{\mu}} &= q^{2(n-k)k_1} \frac{q^{2k^2}(q^{-1})_k (q^{-1})_{n-k+k_{11}} (q^{-1})_n}{(q^{-1})_{k_{11}} ((q^{-1})_{n-k})^2 (\mathrm{card}\, C_{\mathbb{\mu}})}. \end{aligned}$$

□

In the following, we shall deal with various scalar multiples of the (completed) conjugacy classes $C_{\mathbb{\mu}\uparrow^n}$ and of the classes of partial isomorphisms $A_{\mathbb{\mu},n}$. A list of notations for these objects is given in Table 2. By number of elements, we mean the image by the linear map $g \in \mathbb{C}\mathrm{GL}(n, \mathbb{F}_q) \mapsto 1 \in \mathbb{C}$, or by the linear map $(V\ {}^{g_1}\!\rightleftarrows_{g_2} W) \in \mathscr{A}(n, \mathbb{F}_q) \mapsto 1 \in \mathbb{C}$. Most manipulations are eased by dealing with the normalized versions of classes (those with a $\sim$).

Proposition 3.3 *The algebra* $\mathscr{Z}(n, \mathbb{F}_q)$ *is commutative.*

Proof Ultimately the result comes from the commutativity of all the algebras $Z(\mathbb{C}\mathrm{GL}(V))$ with V subspace of $(\mathbb{F}_q)^n$, but the verifications are not obvious at all. On

Table 2 Normalizations of conjugacy classes

classes	number of elements
$C_{\mathbb{\mu}\uparrow n} = \sum_{\substack{g \in \mathrm{GL}(n,\mathbb{F}_q) \\ t(g) = \mathbb{\mu}\uparrow n}} g$	$\big(\frac{q^{2(n-k)(k-k_1)}(q^{-1})_n (q^{-1})_{k_{11}}}{(q^{-1})_k (q^{-1})_{n-k+k_{11}}}\big) \operatorname{card} C_{\mathbb{\mu}}$
$\widetilde{C}_{\mathbb{\mu}\uparrow n} = \frac{C_{\mathbb{\mu}\uparrow n}}{\operatorname{card} C_{\mathbb{\mu}\uparrow n}}$	1
$A_{\mathbb{\mu},n} = \sum_{\substack{\mathcal{E}=(e_1,\dots,e_k) \\ \mathcal{F}=(f_1,\dots,f_k)}} (\mathrm{Span}(\mathcal{E}) \;{}^{I_k}\!\rightleftarrows_{J(\mathbb{\mu})} \mathrm{Span}(\mathcal{F}))$	$(q^{nk} \frac{(q^{-1})_n}{(q^{-1})_{n-k}})^2$
$\widehat{A}_{\mathbb{\mu},n} = \frac{A_{\mathbb{\mu},n}}{\sqrt{\operatorname{card} A_{\mathbb{\mu},n}}}$	$q^{nk} \frac{(q^{-1})_n}{(q^{-1})_{n-k}}$
$\widetilde{A}_{\mathbb{\mu}\uparrow n} = \frac{A_{\mathbb{\mu},n}}{\operatorname{card} A_{\mathbb{\mu},n}}$	1

the other hand, we really need to do them in order to obtain a formula for the product of two classes $A_{\mathbb{\mu},n}$ and $A_{\mathbb{\nu},n}$; so we cannot skip this proof of commutativity. Take two random independent subspaces V and W of dimension k and l inside $(\mathbb{F}_q)^n$. The law of $m = \dim(V+W)$ is the case $j=0$ of Lemma 2.13:

$$\begin{aligned}
&\mathbb{P}\big[\dim(V+W) = m\big] \\
&\quad = q^{(k+l-m)(m-n)} \frac{(q^{-1})_{n-k}(q^{-1})_{n-l}(q^{-1})_k (q^{-1})_l}{(q^{-1})_{k+l-m}(q^{-1})_{n-m}(q^{-1})_n (q^{-1})_{m-k}(q^{-1})_{m-l}}.
\end{aligned}$$

Then, since the law of the pair (V, W) is invariant under action by $\mathrm{GL}(n, \mathbb{F}_q)$, $Z = V + W$ is a random subspace with a law invariant under $\mathrm{GL}(n, \mathbb{F}_q)$, so its law is a mixture of the uniform laws on random subspaces of fixed dimension m. Hence,

$$\mathbb{P}[Z] = \mathbb{P}[m]\mathbb{U}_m[Z] \quad \text{with } m = \dim Z.$$

Corollary 2.14 then tells us that knowing Z, V is uniformly distributed among spaces of dimension k included into Z; and knowing Z, W is uniformly distributed among spaces of dimension l included into Z. Notice, however, that the joint law of (V, W) is not the product of these uniform laws; in other words, V and W are not independent conditionally on Z. One can rewrite $A_{\mathbb{\mu},n}$ as a multiple of the normalized sum

$$\widetilde{A}_{\mathbb{\mu},n} = \sum_{\mathcal{E},\mathcal{F} \text{ free families}} \mathbb{UF}_k[\mathcal{E}]\mathbb{UF}_k[\mathcal{F}]\big(\mathrm{Span}(\mathcal{E}) \;{}^{I_k}\!\rightleftarrows_{J(\mathbb{\mu})} \mathrm{Span}(\mathcal{F})\big),$$

where $\mathbb{UF}_k[\mathcal{E}]$ and $\mathbb{UF}_k[\mathcal{F}]$ are the uniform probabilities on free families of size $k = |\mathbb{\mu}|$. Notice then that

$$\begin{aligned}
&\mathrm{R}_V^{V^+}\Bigg(\sum_{\substack{\mathcal{E},\mathcal{F} \text{ free families} \\ \mathrm{Span}(\mathcal{F})=V}} \mathbb{UF}_k[\mathcal{E}]\mathbb{UF}_V[\mathcal{F}]\big(\mathrm{Span}(\mathcal{E}) \;{}^{I_k}\!\rightleftarrows_{J(\mathbb{\mu})} \mathrm{Span}(\mathcal{F})\big)\Bigg) \\
&\quad = \sum_{\substack{\mathcal{E}^+,\mathcal{F}^+ \text{ free families} \\ \mathrm{Span}(\mathcal{F}^+)=V^+, \mathrm{Span}(\mathcal{F})=V}} \mathbb{UF}_{k^+}\big[\mathcal{E}^+\big]\mathbb{UF}_{V^+,V}\big[\mathcal{F}^+\big] \\
&\qquad \times \big(\mathrm{Span}\big(\mathcal{E}^+\big) \;{}^{I_{k^+}}\!\rightleftarrows_{J(\mathbb{\mu}\uparrow k^+)} \mathrm{Span}\big(\mathcal{F}^+\big)\big)
\end{aligned}$$

if $V \subset V^+$ have dimension k and k^+; here $\mathbb{UF}_V[\mathcal{F}]$ (resp., $\mathbb{UF}_{V^+,V}[\mathcal{F}^+]$) is the uniform law on free families of $(\mathbb{F}_q)^n$ such that $\mathrm{Span}(\mathcal{F}) = V$ (resp., such that $\mathrm{Span}(\mathcal{F}^+) = V^+$ and $\mathrm{Span}(\mathcal{F}) = V$, with $\mathcal{F}$ the family of the k first vectors of $\mathcal{F}^+$).

A product of two normalized sums $\widetilde{A}_{\mu,n}$ and $\widetilde{A}_{\nu,n}$ writes now as

$$\sum_{\mathcal{E},\mathcal{F},\mathcal{G},\mathcal{H}} \mathbb{UF}[\mathcal{E},\mathcal{F},\mathcal{G},\mathcal{H}]\big(\mathrm{Span}(\mathcal{E})\ {}^{I_k}\!\rightleftarrows_{J(\mu)} \mathrm{Span}(\mathcal{F})\big) * \big(\mathrm{Span}(\mathcal{G})\ {}^{I_l}\!\rightleftarrows_{J(\nu)} \mathrm{Span}(\mathcal{H})\big)$$

$$= \sum_{\substack{\dim V=k\\ \dim W=l\\ \mathcal{E},\mathcal{F},\mathcal{G},\mathcal{H}\\ \mathrm{Span}(\mathcal{F})=V\\ \mathrm{Span}(\mathcal{G})=W}} \begin{pmatrix} \mathbb{U}_k[V]\mathbb{U}_l[W]\mathbb{UF}[\mathcal{E},\mathcal{H}]\mathbb{UF}_V[\mathcal{F}]\mathbb{UF}_W[\mathcal{G}]\times \\ (\mathrm{Span}(\mathcal{E})\ {}^{I_k}\!\rightleftarrows_{J(\mu)} \mathrm{Span}(\mathcal{F})) * (\mathrm{Span}(\mathcal{G})\ {}^{I_l}\!\rightleftarrows_{J(\nu)}|\mathrm{Span}(\mathcal{H})) \end{pmatrix}$$

$$= \sum_{\substack{Z,V,W\\ \mathcal{E},\mathcal{F},\mathcal{G},\mathcal{H}\\ \mathrm{Span}(\mathcal{F})=V\\ \mathrm{Span}(\mathcal{G})=W}} \begin{pmatrix} \mathbb{P}[m]\mathbb{U}_m[Z]\mathbb{P}[(V,W)|Z]\mathbb{UF}[\mathcal{E},\mathcal{H}]\mathbb{UF}_V[\mathcal{F}]\mathbb{UF}_W[\mathcal{G}]\times \\ \mathrm{R}_V^{V+W}(\mathrm{Span}(\mathcal{E})\ {}^{I_k}\!\rightleftarrows_{J(\mu)} \mathrm{Span}(\mathcal{F}))\cdot \\ \mathrm{L}_W^{V+W}(\mathrm{Span}(\mathcal{G})\ {}^{I_l}\!\rightleftarrows_{J(\nu)} \mathrm{Span}(\mathcal{H})) \end{pmatrix}$$

$$= \sum_{\substack{Z,V,W\\ \mathcal{E}^+,\mathcal{F}^+,\mathcal{G}^+,\mathcal{H}^+\\ \mathrm{Span}(\mathcal{F}^+)=Z,\mathrm{Span}(\mathcal{F})=V\\ \mathrm{Span}(\mathcal{G}^+)=Z,\mathrm{Span}(\mathcal{G})=W}} \begin{pmatrix} \mathbb{P}[m]\mathbb{U}_m[Z]\mathbb{UF}_m[\mathcal{E}^+,\mathcal{H}^+]\times \\ \mathbb{P}[V|Z]\mathbb{UF}_{Z,V}[\mathcal{F}^+]\mathbb{P}[W|(Z,V)]\mathbb{UF}_{Z,W}[\mathcal{G}^+]\times \\ (\mathrm{Span}(\mathcal{E}^+)\ {}^{I_m}\!\rightleftarrows_{J(\mu\uparrow^m)} \mathrm{Span}(\mathcal{F}^+))\cdot \\ (\mathrm{Span}(\mathcal{G}^+)\ {}^{I_m}\!\rightleftarrows_{J(\nu\uparrow^m)} \mathrm{Span}(\mathcal{H}^+)) \end{pmatrix}$$

$$= \sum_{\substack{Z,V,W\\ \mathcal{E}^+,\mathcal{F}^+,\mathcal{G}^+,\mathcal{H}^+\\ \mathrm{Span}(\mathcal{F}^+)=Z,\mathrm{Span}(\mathcal{F})=V\\ \mathrm{Span}(\mathcal{G}^+)=Z,\mathrm{Span}(\mathcal{G})=W}} \begin{pmatrix} \mathbb{P}[m]\mathbb{U}_m[Z]\mathbb{UF}_m[\mathcal{E}^+,\mathcal{H}^+]\mathbb{UF}_Z[\mathcal{F}^+]\times \\ \mathbb{P}[W|(Z,V)]\mathbb{UF}_{Z,W}[\mathcal{G}^+]\times \\ (\mathrm{Span}(\mathcal{E}^+)\ {}^{P^{-1}}\!\rightleftarrows_{J(\nu\uparrow^m)PJ(\mu\uparrow^m)} \mathrm{Span}(\mathcal{H}^+)) \end{pmatrix}$$

$$= \sum_{\substack{Z,V,W\\ \mathcal{E}^+,\mathcal{F}^+,\mathcal{G}^+,\mathcal{H}^+\\ \mathrm{Span}(\mathcal{F}^+)=Z,\mathrm{Span}(\mathcal{F})=V\\ \mathrm{Span}(\mathcal{G}^+)=Z,\mathrm{Span}(\mathcal{G})=W}} \begin{pmatrix} \mathbb{P}[m]\mathbb{UF}_m[Z]\mathbb{UF}_m[\mathcal{E}^+,\mathcal{H}^+]\mathbb{UF}_Z[\mathcal{F}^+]\times \\ \mathbb{P}[W|(Z,V)]\mathbb{UF}_{Z,W}[\mathcal{G}^+]\times \\ (\mathrm{Span}(\mathcal{E}^+)\ {}^{I_m}\!\rightleftarrows_{P^{-1}J(\nu\uparrow^m)PJ(\mu\uparrow^m)} \mathrm{Span}(\mathcal{H}^+)) \end{pmatrix}$$

where P stands for the matrix $\mathrm{mat}_{\mathcal{F}^+}(\mathcal{G}^+)$. Notice that this matrix P is the only part depending on $V, W, \mathcal{F}^+$ and $\mathcal{G}^+$ in the last average of partial isomorphisms. Therefore, the sum will be simplified if we are able to identify the law of P under the probability $\mathbb{UF}_Z[\mathcal{F}^+]\mathbb{P}[W|(Z,V)]\mathbb{UF}_{Z,W}[\mathcal{G}^+]$, which is a conditional probability depending on the random variable Z. We claim that this law is just the uniform law on matrices in $\mathrm{GL}(m,\mathbb{F}_q)$. Remember that $\mathcal{F}^+$ is chosen uniformly, that the law of W knowing Z and V is the uniform law on spaces with dimension l and with $V + W = Z$, and that $\mathcal{G}^+$ is then the uniform law on bases of Z with $\mathrm{Span}(\mathcal{G}) = W$. This implies that:

1. The probability of a given matrix P is invariant under conjugation by elements of $\mathrm{GL}(m, \mathbb{F}_q)$:
$$\mathbb{P}\big[\mathrm{mat}_{\mathcal{F}^+}\big(\mathcal{G}^+\big) = P\big] = \mathbb{P}\big[\mathrm{mat}_{g\left(\mathcal{F}^+\right)}\big(g(\mathcal{G}^+)\big) = P\big] = \mathbb{P}\big[\mathrm{mat}_{\mathcal{F}^+}\big(\mathcal{G}^+\big) = gPg^{-1}\big].$$
2. For V fixed, the probability conditionally on Z and V of $\mathcal{G}^+$ is invariant under action of the parabolic subgroup $\mathrm{T}(k, m-k, \mathbb{F}_q)$ of block-triangular matrices
$$\begin{pmatrix} K_1 & R \\ 0 & K_2 \end{pmatrix} \quad \text{with } K_1 \in \mathrm{GL}(k, \mathbb{F}_q), K_2 \in \mathrm{GL}(m-k, \mathbb{F}_q),$$
$$R \in \mathrm{M}\big(k \times (m-k), \mathbb{F}_q\big),$$
since this is the stabilizer of V inside $\mathrm{GL}(m, \mathbb{F}_q)$.

If $k = 0$ or m the second point proves the claim. Otherwise, the group that leaves invariant the probability $\mathbb{P}[P]$ is a subgroup of $\mathrm{GL}(m, \mathbb{F}_q)$ that contains the maximal parabolic subgroup $\mathrm{T}(k, m-k, \mathbb{F}_q)$, but also all its conjugates. Therefore it contains strictly $\mathrm{T}(k, m-k, \mathbb{F}_q)$, so it can only be $\mathrm{GL}(m, \mathbb{F}_q)$ itself, and the claim is shown in full generality.

We can finally write

$$\begin{aligned}
\widetilde{A}_{\mathbb{\mu},n} * \widetilde{A}_{\mathbb{\nu},n} &= \sum_{\substack{\mathcal{E}^+,\mathcal{H}^+ \\ P\in\mathrm{GL}(m,\mathbb{F}_q)}} \frac{\mathbb{P}[m]\mathbb{UF}_m[\mathcal{E}^+, \mathcal{H}^+]}{\mathrm{card}\,\mathrm{GL}(m, \mathbb{F}_q)} \\
&\quad \times \big(\mathrm{Span}\big(\mathcal{E}^+\big) \ {}^{I_m}\!\rightleftarrows_{P^{-1}J(\mathbb{\nu}\uparrow^m)PJ(\mathbb{\mu}\uparrow^m)} \mathrm{Span}\big(\mathcal{H}^+\big)\big) \\
&= \sum_{\substack{\mathcal{E}^+,\mathcal{H}^+ \\ P\in\mathrm{GL}(m,\mathbb{F}_q)}} \frac{\mathbb{P}[m]\mathbb{UF}_m[\mathcal{E}^+, \mathcal{H}^+]}{\mathrm{card}\,\mathrm{GL}(m, \mathbb{F}_q)} \\
&\quad \times \big(\mathrm{Span}\big(\mathcal{E}^+\big) \ {}^{I_m}\!\rightleftarrows_{J(\mathbb{\mu}\uparrow^m P^{-1}J(\mathbb{\nu}\uparrow^m)P)} \mathrm{Span}\big(\mathcal{H}^+\big)\big) \\
&= \sum_{\substack{\mathcal{F}^+,\mathcal{H}^+ \\ P\in\mathrm{GL}(m,\mathbb{F}_q)}} \frac{\mathbb{P}[m]\mathbb{UF}_m[\mathcal{F}^+, \mathcal{H}^+]}{\mathrm{card}\,\mathrm{GL}(m, \mathbb{F}_q)} \\
&\quad \times \big(\mathrm{Span}\big(\mathcal{F}^+\big) \ {}^{P}\!\rightleftarrows_{J(\mathbb{\mu}\uparrow^m)P^{-1}J(\mathbb{\nu}\uparrow^m)} \mathrm{Span}\big(\mathcal{H}^+\big)\big) \\
&= \sum_{\substack{\mathcal{F}^+,\mathcal{G}^+ \\ P\in\mathrm{GL}(m,\mathbb{F}_q)}} \frac{\mathbb{P}[m]\mathbb{UF}_m[\mathcal{F}^+, \mathcal{G}^+]}{\mathrm{card}\,\mathrm{GL}(m, \mathbb{F}_q)} \\
&\quad \times \big(\mathrm{Span}\big(\mathcal{F}^+\big) \ {}^{I_m}\!\rightleftarrows_{PJ(\mathbb{\mu}\uparrow^m)P^{-1}J(\mathbb{\nu}\uparrow^m)} \mathrm{Span}\big(\mathcal{G}^+\big)\big) \\
&= \sum_{\substack{\mathcal{F}^+,\mathcal{G}^+ \\ P\in\mathrm{GL}(m,\mathbb{F}_q)}} \frac{\mathbb{P}[m]\mathbb{UF}_m[\mathcal{F}^+, \mathcal{G}^+]}{\mathrm{card}\,\mathrm{GL}(m, \mathbb{F}_q)}
\end{aligned}$$

$$\times \big(\mathrm{Span}\big(\mathcal{F}^+\big)\ {}^{I_m}\!\rightleftarrows_{P^{-1}J(\mu\uparrow^m)PJ(\nu\uparrow^m)}\ \mathrm{Span}\big(\mathcal{G}^+\big)\big)$$
$$= \widetilde{A}_{\nu,n} * \widetilde{A}_{\mu,n}$$

by using on the second line the fact that $\sum_P P^{-1}J(\nu\uparrow^m)P$ commutes with everyone in $\mathbb{C}\mathrm{GL}(m,\mathbb{F}_q)$, because it is a multiple of a conjugacy class. □

Remark 3.4 Starting from the last computation in the proof of commutativity, one can give a useful expression for the product of two normalized classes $\widetilde{A}_{\mu,n}$ and $\widetilde{A}_{\nu,n}$: this is

$$\widetilde{A}_{\mu,n} * \widetilde{A}_{\nu,n} = \sum_{\substack{\mathcal{E}^+,\mathcal{H}^+\\ t(G)=\mu\uparrow^m,\, t(H)=\nu\uparrow^m}} \frac{\mathbb{P}[m]\mathbb{UF}_m[\mathcal{E}^+,\mathcal{H}^+]}{(\mathrm{card}\, C_{\mu\uparrow^m})(\mathrm{card}\, C_{\nu\uparrow^m})}$$
$$\times \big(\mathrm{Span}(\mathcal{E}^+)\ {}^{I_m}\!\rightleftarrows_{HG}\ \mathrm{Span}(\mathcal{H}^+)\big).$$

With this expansion, it becomes obvious that $\widetilde{A}_{\mu,n} * \widetilde{A}_{\nu,n} = \widetilde{A}_{\nu,n} * \widetilde{A}_{\mu,n}$, because in any group algebra $\mathbb{C}\mathrm{GL}(m,\mathbb{F}_q)$, $\widetilde{C}_{\mu\uparrow^m} * \widetilde{C}_{\nu\uparrow^m} = \widetilde{C}_{\nu\uparrow^m} * \widetilde{C}_{\mu\uparrow^m}$.

3.3 The projective limit $\mathcal{Z}(\infty,\mathbb{F}_q)$

We focus now on the construction of a projective limit of the subalgebras of invariants (in the category of graded algebras). The main tool is the following:

Proposition 3.5 *Consider the linear maps*

$$\phi_n^{n+p} : \mathcal{A}(n+p,\mathbb{F}_q) \to \mathcal{A}(n,\mathbb{F}_q)$$
$$(V\ {}^{g_1}\!\rightleftarrows_{g_2}\ W) \mapsto \begin{cases} q^{pk\frac{(q^{-1})_{n+p}(q^{-1})_{n-k}}{(q^{-1})_{n+p-k}(q^{-1})_n}}(V\ {}^{g_1}\!\rightleftarrows_{g_2}\ W) & \textit{if } V+W\subset(\mathbb{F}_q)^n, \\ 0 & \textit{otherwise}, \end{cases}$$

k denoting the degree of the partial isomorphism. Their restrictions $\phi_n^{n+p} : \mathcal{Z}(n+p,\mathbb{F}_q) \to \mathcal{Z}(n,\mathbb{F}_q)$ are morphisms of commutative algebras and they satisfy the relations

$$\phi_n^{n+p}(\widehat{A}_{\mu,n+p}) = \widehat{A}_{\mu,n}, \tag{16}$$

where

$$\widehat{A}_{\mu,n} = \frac{A_{\mu,n}}{\sqrt{\mathrm{card}\, A_{\mu,n}}} = \frac{(q^{-1})_{n-k}}{q^{nk}(q^{-1})_n} A_{\mu,n}.$$

Proof To avoid any ambiguity, we shall precise by indices the notations of the proof of Proposition 3.3. Thus, we shall denote $\mathbb{P}_{k,l,n}[m]$ the probability of m in the previous probabilistic scheme and in $(\mathbb{F}_q)^n$, and $\mathbb{UF}_{k,n}[\mathcal{E}]$ the uniform probability over free family of size k in $(\mathbb{F}_q)^n$. Fix two polypartitions μ and ν of sizes k and l. If k or l is strictly bigger than n, then $\phi_n^{n+p}(\widehat{A}_{\mu,n+p})$ or $\phi_n^{n+p}(\widehat{A}_{\nu,n+p})$ is equal to zero, and on the other hand, every partial isomorphism appearing in $\widehat{A}_{\mu,n+p} * \widehat{A}_{\nu,n+p}$ will have degree bigger than $\max(k,l) > n$, so one has

$$\phi_n^{n+p}(\widehat{A}_{\mu,n+p} * \widehat{A}_{\nu,n+p}) = 0 = \phi_n^{n+p}(\widehat{A}_{\mu,n+p}) * \phi_n^{n+p}(\widehat{A}_{\nu,n+p}).$$

Suppose now $k \leq n$ and $l \leq n$. We compute $\phi_n^{n+p}(\widehat{A}_{\mu,n+p} * \widehat{A}_{\nu,n+p})$ as follows:

$$\phi_n^{n+p}(\widehat{A}_{\mu,n+p} * \widehat{A}_{\nu,n+p}) = \frac{q^{(n+p)(k+l)}((q^{-1})_{n+p})^2}{(q^{-1})_{n+p-k}(q^{-1})_{n+p-l}} \phi_n^{n+p}(\widetilde{A}_{\mu,n+p} * \widetilde{A}_{\nu,n+p})$$

and

$$\begin{aligned}
&\phi_n^{n+p}(\widetilde{A}_{\mu,n+p} * \widetilde{A}_{\nu,n+p}) \\
&\quad = \sum_{\substack{\mathcal{E}^+,\mathcal{H}^+ \\ t(G)=\mu\uparrow^m \\ t(H)=\nu\uparrow^m}} \frac{\mathbb{P}_{k,l,n+p}[m]\mathbb{UF}_{m,n+p}[\mathcal{E}^+,\mathcal{H}^+]}{\operatorname{card}(C_{\mu\uparrow^m} \times C_{\nu\uparrow^m})} \phi_n^{n+p}\bigl(\operatorname{Span}(\mathcal{E}^+)\ {}^{I_m}\!\rightleftarrows_{HG} \operatorname{Span}(\mathcal{H}^+)\bigr),
\end{aligned}$$

where the families $\mathcal{E}^+$ and $\mathcal{H}^+$ run *a priori* over free families of size m in $(\mathbb{F}_q)^{n+p}$, but in fact over free families of size m in $(\mathbb{F}_q)^n$, since otherwise $\phi_n^{n+p}(\operatorname{Span}(\mathcal{E}^+)\ {}^{I_m}\!\rightleftarrows_{HG} \operatorname{Span}(\mathcal{H}^+))$ vanishes. The quantity $\mathbb{P}_{k,l,n+p}[m]\mathbb{UF}_{m,n+p}[\mathcal{E}^+,\mathcal{H}^+]$ is equal to

$$\begin{aligned}
&\frac{q^{(k+l-m)(m-n-p)}(q^{-1})_{n+p-k}(q^{-1})_{n+p-l}(q^{-1})_k(q^{-1})_l}{(q^{-1})_{k+l-m}(q^{-1})_{n+p-m}(q^{-1})_{n+p}(q^{-1})_{m-k}(q^{-1})_{m-l}} \left(\frac{(q^{-1})_{n+p-m}}{q^{m(n+p)}(q^{-1})_{n+p}}\right)^2 \\
&\quad = \frac{q^{(k+l-m)(m-n-p)}(q^{-1})_{n+p-k}(q^{-1})_{n+p-l}(q^{-1})_{n+p-m}(q^{-1})_k(q^{-1})_l}{((q^{-1})_{n+p})^3(q^{-1})_{k+l-m}(q^{-1})_{m-k}(q^{-1})_{m-l}} \\
&\quad\quad \times \left(\frac{1}{q^{m(n+p)}}\right)^2,
\end{aligned}$$

which multiplied by $\sqrt{(\operatorname{card} A_{\mu,n+p}) \times (\operatorname{card} A_{\nu,n+p})}$ gives

$$\frac{q^{(k+l-m-n-p)m}(q^{-1})_{n+p-m}(q^{-1})_k(q^{-1})_l}{(q^{-1})_{n+p}(q^{-1})_{k+l-m}(q^{-1})_{m-k}(q^{-1})_{m-l}}.$$

Multiplying again by the coefficient in the statement of the proposition, we get

$$\begin{aligned}
&\phi_n^{n+p}(\widehat{A}_{\mu,n+p} * \widehat{A}_{\nu,n+p}) \\
&\quad = \sum_{\substack{\mathcal{E}^+,\mathcal{H}^+ \\ t(G)=\mu\uparrow^m \\ t(H)=\nu\uparrow^m}} \frac{q^{(k+l-m-n)m}(q^{-1})_k(q^{-1})_l(q^{-1})_{n-m}}{(q^{-1})_{k+l-m}(q^{-1})_{m-k}(q^{-1})_{m-l}(q^{-1})_n} \\
&\quad\quad \times \frac{(\operatorname{Span}(\mathcal{E}^+)\ {}^{I_m}\!\rightleftarrows_{HG} \operatorname{Span}(\mathcal{H}^+))}{\operatorname{card}(C_{\mu\uparrow^m} \times C_{\nu\uparrow^m})}.
\end{aligned} \tag{17}$$

On the other hand,

$$\begin{aligned}
\phi_n^{n+p}(\widehat{A}_{\mathbb{\mu},n+p}) &= \frac{q^{k(n+p)}(q^{-1})_{n+p}}{(q^{-1})_{n+p-k}}\phi_n^{n+p}(\widetilde{A}_{\mathbb{\mu},n+p}) \\
&= \frac{q^{k(n+p)}(q^{-1})_{n+p}}{(q^{-1})_{n+p-k}} \sum_{\substack{\mathcal{E},\mathcal{F}\\ t(G)=\mathbb{\mu}}} \frac{\mathbb{UF}_{k,n+p}[\mathcal{E},\mathcal{F}]}{\operatorname{card} C_{\mathbb{\mu}}}\phi_n^{n+p} \\
&\quad \times \big(\operatorname{Span}(\mathcal{E}) \;{}^{I_k}\!\rightleftarrows_G \operatorname{Span}(\mathcal{F})\big) \\
&= \sum_{\substack{\mathcal{E},\mathcal{F}\\ t(G)=\mathbb{\mu}}} \frac{q^{-nk}(q^{-1})_{n-k}}{(q^{-1})_n} \frac{(\operatorname{Span}(\mathcal{E}) \;{}^{I_k}\!\rightleftarrows_G \operatorname{Span}(\mathcal{F}))}{\operatorname{card} C_{\mathbb{\mu}}},
\end{aligned}$$

where again the families $\mathcal{E}$ and $\mathcal{F}$ run *a priori* over free families of size k in $(\mathbb{F}_q)^{n+p}$, but in fact over free families of size k in $(\mathbb{F}_q)^n$, since otherwise $\phi_n^{n+p}(\operatorname{Span}(\mathcal{E}) \;{}^{I_k}\!\rightleftarrows_G \operatorname{Span}(\mathcal{F}))$ vanishes. Therefore, one can rewrite this as

$$\begin{aligned}
\phi_n^{n+p}(\widehat{A}_{\mathbb{\mu},n+p}) &= \frac{q^{nk}(q^{-1})_n}{(q^{-1})_{n-k}} \sum_{\substack{\mathcal{E},\mathcal{F}\\ t(G)=\mathbb{\mu}}} \frac{\mathbb{UF}_{k,n}[\mathcal{E},\mathcal{F}]}{\operatorname{card} C_{\mathbb{\mu}}}\big(\operatorname{Span}(\mathcal{E}) \;{}^{I_k}\!\rightleftarrows_G \operatorname{Span}(\mathcal{F})\big) \\
&= \frac{q^{nk}(q^{-1})_n}{(q^{-1})_{n-k}}\widetilde{A}_{\mathbb{\mu},n} = \widehat{A}_{\mathbb{\mu},n}.
\end{aligned}$$

This proves in particular that $\phi_n^{n+p}(\mathcal{Z}(n+p,\mathbb{F}_q)) = \mathcal{Z}(n,\mathbb{F}_q)$. Finally,

$$\widetilde{A}_{\mathbb{\mu},n} * \widetilde{A}_{\mathbb{\nu},n} = \sum_{\substack{\mathcal{E}^+,\mathcal{H}^+\\ t(G)=\mathbb{\mu}\uparrow^m\\ t(H)=\mathbb{\nu}\uparrow^m}} \frac{\mathbb{P}_{k,l,n}[m]\mathbb{UF}_{m,n}[\mathcal{E}^+,\mathcal{H}^+]}{(\operatorname{card} C_{\mathbb{\mu}\uparrow^m})(\operatorname{card} C_{\mathbb{\nu}\uparrow^m})}\big(\operatorname{Span}(\mathcal{E}^+) \;{}^{I_m}\!\rightleftarrows_{HG} \operatorname{Span}\big(\mathcal{H}^+\big)\big);$$

the quantity $\mathbb{P}_{k,l,n}[m]\mathbb{UF}_{m,n}[\mathcal{E}^+,\mathcal{H}^+]$ is equal to

$$\frac{q^{(k+l-m)(m-n)}(q^{-1})_{n-k}(q^{-1})_{n-l}(q^{-1})_{n-m}(q^{-1})_k(q^{-1})_l}{((q^{-1})_n)^3(q^{-1})_{k+l-m}(q^{-1})_{m-k}(q^{-1})_{m-l}}\left(\frac{1}{q^{mn}}\right)^2,$$

which multiplied by $\sqrt{(\operatorname{card} A_{\mathbb{\mu},n}) \times (\operatorname{card} A_{\mathbb{\nu},n})}$ gives

$$\frac{q^{(k+l-m-n)m}(q^{-1})_{n-m}(q^{-1})_k(q^{-1})_l}{(q^{-1})_n(q^{-1})_{k+l-m}(q^{-1})_{m-k}(q^{-1})_{m-l}}.$$

This is exactly the coefficient of Eq. (17), so the morphism property is shown—notice that if

$$\mathbb{1}_n = \big(\{0\} \;{}^{\mathrm{id}}\!\rightleftarrows_{\mathrm{id}} \{0\}\big) = A_\emptyset = \widehat{A}_\emptyset$$

is the unity of $\mathcal{A}(n,\mathbb{F}_q)$, then one has indeed also $\phi_n^{n+p}(\mathbb{1}_{n+p})=\mathbb{1}_n$. The compatibility between the maps ϕ_n^{n+p} is obvious from the relations (16), so one gets as announced an inverse system of graded commutative algebras

$$\cdots \longrightarrow \mathcal{Z}(n+2,\mathbb{F}_q) \longrightarrow \mathcal{Z}(n+1,\mathbb{F}_q) \longrightarrow \mathcal{Z}(n,\mathbb{F}_q) \longrightarrow \cdots.$$

□

From now on everything gets easy. With $|\mathbb{\lambda}|=k$ and $|\mathbb{\mu}|=l$, denote $S_{\mathbb{\lambda}\mathbb{\mu}}^{\mathbb{\nu}}$ the structure coefficients given by the product

$$\widehat{A}_{\mathbb{\lambda},k+l} * \widehat{A}_{\mathbb{\mu},k+l} = \sum_{|\mathbb{\nu}|\leq k+l} S_{\mathbb{\lambda}\mathbb{\mu}}^{\mathbb{\nu}} \widehat{A}_{\mathbb{\nu},k+l}$$

in $\mathcal{Z}(k+l,\mathbb{F}_q)$. If $|\mathbb{\nu}|>n$, we convene that $\widehat{A}_{\mathbb{\nu},n}=0$. Since the maps ϕ_n^{k+l} are morphisms of algebras, for every $n\leq k+l$, one also has

$$\widehat{A}_{\mathbb{\lambda},n} * \widehat{A}_{\mathbb{\mu},n} = \sum_{|\mathbb{\nu}|\leq k+l} S_{\mathbb{\lambda}\mathbb{\mu}}^{\mathbb{\nu}} \widehat{A}_{\mathbb{\nu},n}.$$

We claim that this identity still holds for $n>k+l$. Indeed, denote $S_{\mathbb{\mu}\mathbb{\nu}}^{\mathbb{\lambda}}(n)$ the structure coefficients in $\mathcal{Z}(n,\mathbb{F}_q)$, such that

$$\widehat{A}_{\mathbb{\lambda},n} * \widehat{A}_{\mathbb{\mu},n} = \sum_{|\mathbb{\nu}|\leq n} S_{\mathbb{\lambda}\mathbb{\mu}}^{\mathbb{\nu}}(n) \widehat{A}_{\mathbb{\nu},n}.$$

The grading ensures that the sum is indeed over polypartitions of size less than $k+l$. By applying the map ϕ_{k+l}^{n} to the previous identity, we get

$$\widehat{A}_{\mathbb{\lambda},k+l} * \widehat{A}_{\mathbb{\mu},k+l} = \sum_{|\mathbb{\nu}|\leq k+l} S_{\mathbb{\lambda}\mathbb{\mu}}^{\mathbb{\nu}}(n) \widehat{A}_{\mathbb{\nu},k+l}.$$

Since $(A_{\mathbb{\nu}})_{|\mathbb{\nu}|\leq k+l}$ is a basis of $\mathcal{Z}(k+l,\mathbb{F}_q)$, this shows that $S_{\mathbb{\lambda}\mathbb{\mu}}^{\mathbb{\nu}}(n)=S_{\mathbb{\lambda}\mathbb{\mu}}^{\mathbb{\nu}}(k+l)=S_{\mathbb{\lambda}\mathbb{\mu}}^{\mathbb{\nu}}$. As a consequence:

Theorem 3.6 *The graded commutative algebra $\mathcal{Z}(\infty,\mathbb{F}_q)$ with linear basis $\widehat{A}_{\mathbb{\mu}}$, $\mathbb{\mu}\in\bigsqcup_{n=0}^{\infty}\mathfrak{P}(n,\mathbb{F}_q)$ and with product*

$$\widehat{A}_{\mathbb{\lambda}} * \widehat{A}_{\mathbb{\mu}} = \sum_{|\mathbb{\nu}|\leq|\mathbb{\lambda}|+|\mathbb{\mu}|} S_{\mathbb{\lambda}\mathbb{\mu}}^{\mathbb{\nu}} \widehat{A}_{\mathbb{\nu}}$$

is well-defined and forms a projective limit of the $\mathcal{Z}(n,\mathbb{F}_q)$'s in the category of graded algebras.

The structure coefficients $S_{\mathbb{\lambda}\mathbb{\mu}}^{\mathbb{\nu}}$ are rational numbers: they are obviously in $\mathbb{Q}(q)$ since every product in $\mathcal{A}(k+l,\mathbb{F}_q)$ involves averages with coefficients in $\mathbb{Q}(q)$, and assuming q fixed, $\mathbb{Q}(q)$ is identified with $\mathbb{Q}$. Denote $\Pi_n=\pi_n\circ\phi_n^{\infty}$, where $\phi_n^{\infty}:\mathcal{Z}(\infty,\mathbb{F}_q)\to\mathcal{Z}(n,\mathbb{F}_q)$ is the canonical projection, and π_n is the map from

Proposition 3.1. This is a morphism of algebras from $\mathscr{Z}(\infty, \mathbb{F}_q)$ to $Z(\mathbb{C}\mathrm{GL}(n, \mathbb{F}_q))$, with

$$\Pi_n(\widehat{A}_{\boldsymbol{\mu}}) = \begin{cases} q^{n(2k_1-k)} \dfrac{q^{2k(k-k_1)}(q^{-1})_k(q^{-1})_{n-k+k_{11}}}{(q^{-1})_{k_{11}}(q^{-1})_{n-k}} \dfrac{C_{\boldsymbol{\mu}\uparrow^n}}{\mathrm{card}\, C_{\boldsymbol{\mu}}} & \text{if } |\boldsymbol{\mu}| = k \leq n \\ 0 & \text{otherwise.} \end{cases}$$

Fix two polypartitions $\boldsymbol{\lambda}$ and $\boldsymbol{\mu}$ of sizes k and l, and with $k_{11} = m_1(\lambda(X-1)) = 0$ and $l_{11} = m_1(\mu(X-1)) = 0$; hence, they correspond to classes of partial isomorphisms that are not trivial extensions of smaller partial isomorphisms. This is the analogue of the restriction "without fixed points" for permutations in our statement of Farahat–Higman's theorem in the introduction. Notice, however, that one does not require $k_1 = \ell(\lambda(X-1))$ or $l_1 = \ell(\mu(X-1))$ to vanish; so, the isomorphisms considered may have non-zero fixed vectors, but no non-zero fixed vector with a stable complement subspace. Under the previous assumption, most of the previous formula simplifies and we get

$$\begin{aligned} &q^{n(2k_1+2l_1-k-l)} q^{2k(k-k_1)+2l(l-l_1)} \big(q^{-1}\big)_k \big(q^{-1}\big)_l \frac{C_{\boldsymbol{\lambda}\uparrow^n} \times C_{\boldsymbol{\mu}\uparrow^n}}{\mathrm{card}(C_{\boldsymbol{\lambda}} \times C_{\boldsymbol{\mu}})} \\ &\quad = \sum_{|\boldsymbol{\nu}|=m\leq k+l} S_{\boldsymbol{\lambda}\boldsymbol{\mu}}^{\boldsymbol{\nu}} q^{n(2m_1-m)} \frac{q^{2m(m-m_1)}(q^{-1})_m(q^{-1})_{n-m+m_{11}}}{(q^{-1})_{m_{11}}(q^{-1})_{n-m}} \frac{C_{\boldsymbol{\nu}\uparrow^n}}{\mathrm{card}\, C_{\boldsymbol{\nu}}}. \end{aligned}$$

By putting everything independent from n in modified structure coefficients

$$s_{\boldsymbol{\lambda}\boldsymbol{\mu}}^{\boldsymbol{\nu}} = S_{\boldsymbol{\lambda}\boldsymbol{\mu}}^{\boldsymbol{\nu}} \frac{\mathrm{card}(C_{\boldsymbol{\lambda}} \times C_{\boldsymbol{\mu}})}{\mathrm{card}\, C_{\boldsymbol{\nu}}} \frac{q^{2m(m-m_1)-2k(k-k_1)-2l(l-l_1)}(q^{-1})_m}{(q^{-1})_k(q^{-1})_l(q^{-1})_{m_{11}}},$$

we obtain finally

$$C_{\boldsymbol{\lambda}\uparrow^n} \times C_{\boldsymbol{\mu}\uparrow^n} = \sum_{|\boldsymbol{\nu}|=m\leq k+l} s_{\boldsymbol{\lambda}\boldsymbol{\mu}}^{\boldsymbol{\nu}} q^{n((k-2k_1)+(l-2l_1)-(m-2m_1))} \frac{(q^{-1})_{n-m+m_{11}}}{(q^{-1})_{n-m}} C_{\boldsymbol{\nu}\uparrow^n}.$$

This leads to a $\mathrm{GL}(n, \mathbb{F}_q)$ version of a theorem of Farahat and Higman, which to our knowledge was not known before.

Theorem 3.7 *Fix two polypartitions $\boldsymbol{\lambda}$ and $\boldsymbol{\mu}$ of sizes k and l, with $k_{11} = m_1(\lambda(X-1)) = 0$ and $l_{11} = m_1(\mu(X-1)) = 0$. There exist polynomials $p_{\boldsymbol{\lambda}\boldsymbol{\mu}}^{\boldsymbol{\nu}}(X)$ with rational coefficients such that for every $n \geq k+l$, in the center of the group algebra $\mathbb{C}\mathrm{GL}(n, \mathbb{F}_q)$,*

$$C_{\boldsymbol{\lambda}\uparrow^n} \times C_{\boldsymbol{\mu}\uparrow^n} = \sum p_{\boldsymbol{\lambda}\boldsymbol{\mu}}^{\boldsymbol{\nu}}\big(q^n\big) C_{\boldsymbol{\nu}\uparrow^n},$$

where the sum runs over polypartitions $\boldsymbol{\nu}$ of size $m \leq k+l$, and again with $m_{11} = m_1(\nu(X-1)) = 0$.

Proof The n-dependent part of the coefficient of $C_{\mathbb{\nu}\uparrow^n}$ in the previous expansion writes as

$$\begin{aligned} &q^{n((k-2k_1)+(l-2l_1)-(m-2m_1))}\,\frac{(q^{-1})_{n-m+m_{11}}}{(q^{-1})_{n-m}} \\ &\quad= q^{n((k-2k_1)+(l-2l_1)-(m-2m_1))}\big(1-q^{-(n-m+1)}\big) \\ &\qquad\times\big(1-q^{-(n-m+2)}\big)\cdots\big(1-q^{-(n-m+m_{11})}\big). \end{aligned}$$

This is *a priori* a Laurent polynomial in q^n with rational coefficients. Gathering together the polypartitions $\mathbb{\nu}$ which give the same completed polypartition $\mathbb{\nu}\uparrow^n$ (they differ by the number of parts 1 in $\nu(X-1)$), we conclude from the previous discussion that

$$C_{\mathbb{\lambda}\uparrow^n}\times C_{\mathbb{\mu}\uparrow^n}=\sum p^{\mathbb{\nu}}_{\mathbb{\lambda}\mathbb{\mu}}(q^n)C_{\mathbb{\nu}\uparrow^n},$$

where the sum is over the finite set of polypartitions $\mathbb{\nu}$ with $|\mathbb{\nu}|\leq|\mathbb{\lambda}|+|\mathbb{\mu}|$ and $\nu(X-1)$ without parts of size 1; and the coefficients $p^{\mathbb{\nu}}_{\mathbb{\lambda}\mathbb{\mu}}(q^n)$ are rational Laurent polynomials in $\mathbb{Q}[X,X^{-1}]$. However, the group algebra of a finite group is defined over $\mathbb{Z}$, so for every integer n, $p^{\mathbb{\nu}}_{\mathbb{\lambda}\mathbb{\mu}}(q^n)$ is an integer. With $q=p^e$, by looking at the p-valuation in $\mathbb{Q}$, one sees that $p^{\mathbb{\nu}}_{\mathbb{\lambda}\mathbb{\mu}}$ cannot have negative powers, so it is in fact a polynomial in $\mathbb{Q}[X]$. □

4 Explicit computations with degree 1 terms

In this section we make the previous discussion concrete by computing the polynomials $p^{\mathbb{\nu}}_{\mathbb{\lambda}\mathbb{\mu}}(q^n)$ when $\mathbb{\lambda}$ and $\mathbb{\mu}$ have degree 1, hence correspond to irreducible polynomials $X-a$ and $X-b$ with $a,b\in(\mathbb{F}_q)^\times$. The generic invariant $\widehat{A}_{\{X-a:1\}}$, which we shall abbreviate as $\widehat{A}_{X-a}$, has for projections in the algebras $\mathscr{Z}(n,\mathbb{F}_q)$:

$$\widehat{A}_{X-a,n}=\frac{1}{q^n-1}\sum_{u,v\in(\mathbb{F}_q)^n\setminus\{0\}}\big(u\ {}^1\!\rightleftarrows_a\ v\big).$$

Here $(u\ {}^1\!\rightleftarrows_a\ v)$ means that one sends the vector u to v by the first arrow, and v to au by the second arrow. To compute the generic product $\widehat{A}_{X-a}*\widehat{A}_{X-b}$ in $\mathscr{Z}(\infty,\mathbb{F}_q)$, it suffices to do so in $\mathscr{Z}(2,\mathbb{F}_q)$ by the discussion of the previous section. Take two partial isomorphisms $(u\ {}^1\!\rightleftarrows_a\ v)$ and $(w\ {}^1\!\rightleftarrows_b\ x)$ in $\mathscr{I}(2,\mathbb{F}_q)$. Among the $(q^2-1)^4$ possibilities for u,v,w,x, the vectors v and w are collinear in $(q^2-1)^3(q-1)$ cases, the factor $(q-1)$ corresponding to the possibilities for the factor of proportionality α such that $w=\alpha v$. In all these cases,

$$(u\ {}^1\!\rightleftarrows_a\ v)*(w\ {}^1\!\rightleftarrows_b\ x)=(u\ {}^1\!\rightleftarrows_{ab}\ \alpha^{-1}x)$$

has type $\{X-ab:1\}$. So, this situation contributes to a term

$$\big(q^2-1\big)(q-1)\widetilde{A}_{X-ab}=(q-1)\widehat{A}_{X-ab} \tag{18}$$

in $\widehat{A}_{X-a} * \widehat{A}_{X-b}$. In every other situation, $(\mathbb{F}_q)^2 = \mathrm{Span}(v,w)$ and we have to compute trivial extensions. It should be noticed here that the form of $\pi_2((u\ {}^1\!\rightleftarrows_a v))$ is different when $a=1$ and when $a \neq 1$. Therefore, we have several cases to treat separately, the most interesting cases being when $a \neq 1$ and $b \neq 1$. Suppose then v and w not collinear. One has

$$\begin{aligned}
&\mathrm{R}^{\mathrm{Span}(v,w)}_{\mathrm{Span}(v)}(u\ {}^1\!\rightleftarrows_a v) \\
&\quad = \frac{1}{q^2(q-1)} \sum_{\substack{t \neq \alpha u \\ r \in \mathbb{F}_q}} \left(\mathrm{Span}(u,t) \,\middle|\, I_2 \rightleftarrows \begin{pmatrix} a & (a-1)r \\ 0 & 1 \end{pmatrix} \,\middle|\, \mathrm{Span}(v,w) \right) \\
&\quad = \frac{1}{q^2(q-1)} \sum_{\substack{t \neq \alpha u \\ r \in \mathbb{F}_q}} \left(\mathrm{Span}(u,t) \,\middle|\, I_2 \rightleftarrows \begin{pmatrix} a & r \\ 0 & 1 \end{pmatrix} \,\middle|\, \mathrm{Span}(v,w) \right);
\end{aligned}$$

$$\mathrm{L}^{\mathrm{Span}(v,w)}_{\mathrm{Span}(w)}(w\ {}^1\!\rightleftarrows_b x) = \frac{1}{q^2(q-1)} \sum_{\substack{y \neq \alpha x \\ s \in \mathbb{F}_q}} \left(\mathrm{Span}(v,w) \,\middle|\, I_2 \rightleftarrows \begin{pmatrix} 1 & 0 \\ s & b \end{pmatrix} \,\middle|\, \mathrm{Span}(y,x) \right).$$

So, outside the terms of (18), the remaining part of the product $\widehat{A}_{X-a} * \widehat{A}_{X-b}$ is equal to

$$\frac{1}{q^3(q-1)(q^2-1)} \sum_{\substack{u,t,x,y \\ r,s}} \left(\mathrm{Span}(u,t) \,\middle|\, I_2 \rightleftarrows \begin{pmatrix} a+rs & rb \\ s & b \end{pmatrix} \,\middle|\, \mathrm{Span}(y,x) \right). \tag{19}$$

4.1 Irreducible polynomials of degree 2 over $\mathbb{F}_q$

We then need to recognize irreducible polynomials of degree 2 over $\mathbb{F}_q$. The theory is a bit different when q is even and when q is odd. Suppose to begin with that q is odd. Then,

$$X^2 + aX + b = \left(X + \frac{a}{2} \right)^2 + \frac{4b - a^2}{4}$$

is irreducible if and only if $a^2 - 4b$ is not a square in $\mathbb{F}_q$. In $\mathbb{F}_q^\times$, there are $\frac{q-1}{2}$ squares identified by the Jacobi symbol $(\frac{a}{q}) = 1$, and $\frac{q-1}{2}$ non-squares identified by the Jacobi symbol $(\frac{a}{q}) = -1$, $(\frac{\cdot}{q})$ being a morphism from $(\mathbb{F}_q)^\times$ to $\{\pm 1\}$. So:

- $X^2 + aX + b$ is irreducible if $(\frac{a^2-4b}{q}) = -1$;
- otherwise, it is equal to $(X - \frac{-a+\delta}{2})(X - \frac{-a-\delta}{2})$, where $\delta^2 = a^2 - 4b$.

This criterion has the following consequence. Suppose $b \neq 0$ fixed and consider the family of polynomials $P_b = \{X^2 + aX + b, a \in \mathbb{F}_q\}$. Notice that

$$\mathrm{card}\big\{ a \in \mathbb{F}_q \,\big|\, X^2 + aX + b \text{ is irreducible} \big\} = \mathrm{card}\left\{ a \in \mathbb{F}_q \,\middle|\, \left(\frac{a^2 - 4b}{q} \right) = -1 \right\}$$

$$\begin{aligned}&= q - \{a \in \mathbb{F}_q \mid a^2 - 4b \text{ is a square}\}\\&= q - \mathbb{1}_{(\frac{b}{q})=1} - \{a \in \mathbb{F}_q \mid a^2 - 4b \text{ is a non-zero square}\}\\&= q - \mathbb{1}_{(\frac{b}{q})=1} - \frac{q-1}{2}.\end{aligned}$$

Therefore, $I_b = \{a \in \mathbb{F}_q \mid X^2 + aX + b \text{ is irreducible}\}$ is of cardinality $\frac{q+1}{2} - \mathbb{1}_{(\frac{b}{q})=1}$ for $b \neq 0$.

Suppose now q even; the solution to the quadratic equation is then a particular case of the Artin–Schreier theory. Recall that on a field of characteristic 2, $x \mapsto x^2$ is a linear map. The trace of an element of $\mathbb{F}_{2^n}$ is the linear map

$$\mathrm{Tr}(x) = x + x^2 + \cdots + x^{2^{n-1}} \in \mathbb{F}_2 = \{0, 1\}.$$

The image of the Artin–Schreier map $x \mapsto x^2 + x$ is the $\mathbb{F}_2$-subspace of $\mathbb{F}_{2^n}$ of elements with trace zero. Then, given an arbitrary monic polynomial $X^2 + aX + b$ of degree 2:

- if $a = 0$, then $X^2 + b = (X + b)^2$ is not irreducible.
- if $a \neq 0$ and $\mathrm{Tr}(ba^{-2}) = 0$, then $X^2 + aX + b = (X + a(u + 1))(X + au)$, where u and $u + 1$ are the two elements of $\mathbb{F}_{2^n}$ such that $u^2 + u = ba^{-2}$.
- otherwise, if $a \neq 0$ and $\mathrm{Tr}(ba^{-2}) = 1$, then $X^2 + aX + b$ is irreducible.

This implies that for every $b \neq 0$, $I_b = \{a \in \mathbb{F}_q \mid X^2 + aX + b \text{ is irreducible}\}$ is of cardinality $\frac{q}{2}$.

4.2 The case $a, b \neq 1$, q odd

Suppose q odd and $a \neq 1$, $b \neq 1$. Going back to Eq. (19), the characteristic polynomial of the matrix $\left(\begin{smallmatrix} a+rs & rb \\ s & b \end{smallmatrix}\right)$ is $X^2 - (a + rs + b)X + ab$. Notice that the multiplication map $m : (r, s) \in \mathbb{F}_q \times \mathbb{F}_q \mapsto rs \in \mathbb{F}_q$ satisfies $\mathrm{card}\, m^{-1}(\{0\}) = 2q - 1$ and $\mathrm{card}\, m^{-1}(\{c\}) = q - 1$ for $c \neq 0$. Therefore, with u, t, x, y fixed:

1. One obtains q times the polynomial $X^2 - (a + b)X + ab$, corresponding for instance to the case $r = 0$ and $s \in \mathbb{F}_q$ arbitrary. If $a \neq b$ this gives a contribution

$$q\widetilde{A}_{\{X-a:1,X-b:1\}} = \frac{1}{(q-1)(q^2-1)}\widehat{A}_{\{X-a:1,X-b:1\}}; \tag{20}$$

otherwise if $a = b$ one gets

$$\begin{aligned}&\widetilde{A}_{\{X-a:1^2\}} + (q-1)\widetilde{A}_{\{X-a:2\}}\\&\quad= \frac{1}{q(q-1)(q^2-1)}\widehat{A}_{\{X-a:1^2\}} + \frac{1}{q(q^2-1)}\widehat{A}_{\{X-a:2\}}\\&\quad= \frac{\mathbb{1}_{a=b}}{q(q^2-1)}(\widehat{A}_{\{X-a:2\}} - \widehat{A}_{\{X-a:1^2\}}) + \frac{1}{(q-1)(q^2-1)}\widehat{A}_{\{X-a:1,X-b:1\}}.\end{aligned} \tag{21}$$

One can also replace (20) by (21) thanks to the symbol $\mathbb{1}_{a=b}$.

2. Then, for every $c \in \mathbb{F}_q$, including 0, one obtains $(q-1)$ times the polynomial $X^2+cX+ab$. By the discussion of Sect. 4.1, $\frac{q+1}{2} - \mathbb{1}_{(\frac{ab}{q})=1}$ values of c give an irreducible polynomial, whence a contribution

$$(q-1)\sum_{c\in I_{ab}} \widetilde{A}_{\{X^2+cX+ab:1\}} = \frac{1}{q(q^2-1)}\sum_{c\in I_{ab}} \widehat{A}_{\{X^2+cX+ab:1\}}. \tag{22}$$

The other values of c correspond to decompositions $X^2+cX+ab=(X-\alpha)(X-\beta)$. If ab is not a square, then $\alpha \neq \beta$ and one obtains a contribution

$$\begin{aligned}(q-1)\sum_{c\notin I_{ab}} \widetilde{A}_{\{X-\alpha:1,X-\beta:1\}} &= \frac{q-1}{2}\sum_{d\in(\mathbb{F}_q)^\times} \widetilde{A}_{\{X-ad^{-1}:1,X-bd:1\}}\\ &= \frac{1}{2q(q^2-1)}\sum_{d\in(\mathbb{F}_q)^\times} \widehat{A}_{\{X-ad^{-1}:1,X-bd:1\}}. \end{aligned}\tag{23}$$

If ab is a square then one can have $\alpha=\beta$; in this case the type of the matrix $M = \left(\begin{smallmatrix} a+rs & rb \\ s & b\end{smallmatrix}\right)$ can be either $\{X-\alpha:1^2\}$ or $\{X-\alpha:2\}$. The first case is excluded since $rb \neq 0$, and therefore $M-\alpha I \neq 0$. So, if $ab=\delta^2$ is a square, then one obtains a contribution

$$\begin{aligned}&(q-1)\widetilde{A}_{\{X-\delta:2\}} + (q-1)\widetilde{A}_{\{X+\delta:2\}}\\ &\quad + \frac{q-1}{2}\sum_{d\in(\mathbb{F}_q)^\times\setminus\{-b^{-1}\delta,b^{-1}\delta\}} \widetilde{A}_{\{X-ad^{-1}:1,X-bd:1\}}\\ &= \frac{1}{q(q^2-1)}(\widehat{A}_{\{X-\delta:2\}} + \widehat{A}_{\{X+\delta:2\}})\\ &\quad + \frac{1}{2q(q^2-1)}\sum_{d\in(\mathbb{F}_q)^\times\setminus\{-b^{-1}\delta,b^{-1}\delta\}} \widehat{A}_{\{X-ad^{-1}:1,X-bd:1\}}\\ &= \frac{\mathbb{1}_{ab=\delta^2}}{2q(q^2-1)}(2\widehat{A}_{\{X-\delta:2\}} - \widehat{A}_{\{X-\delta:1^2\}} + 2\widehat{A}_{\{X+\delta:2\}} - \widehat{A}_{\{X+\delta:1^2\}})\\ &\quad + \frac{1}{2q(q^2-1)}\sum_{d\in(\mathbb{F}_q)^\times} \widehat{A}_{\{X-ad^{-1}:1,X-bd:1\}}. \end{aligned}\tag{24}$$

Again, one can replace (23) by (24) thanks to the symbol $\mathbb{1}_{ab=\delta^2}$.

So, the remaining part (19) of the product $\widehat{A}_{X-a} * \widehat{A}_{X-b}$ is equal to $\frac{(q-1)(q^2-1)}{q}$ times the sum of (21), (22) and (24), that is to say,

$$\frac{1}{q}\widehat{A}_{\{X-a:1,X-b:1\}} + \frac{q-1}{q^2}\Bigg(\sum_{c\in I_{ab}} \widehat{A}_{\{X^2+cX+ab:1\}} + \frac{1}{2}\sum_{d\in(\mathbb{F}_q)^\times} \widehat{A}_{\{X-ad^{-1}:1,X-bd:1\}}$$

$$+\frac{\mathbb{1}_{ab=\delta^2}}{2}(2\widehat{A}_{\{X-\delta:2\}}-\widehat{A}_{\{X-\delta:1^2\}}+2\widehat{A}_{\{X+\delta:2\}}-\widehat{A}_{\{X+\delta:1^2\}})$$
$$+\mathbb{1}_{a=b}(\widehat{A}_{\{X-a:2\}}-\widehat{A}_{\{X-a:1^2\}})\Bigg). \tag{25}$$

Hence, the product $\widehat{A}_{X-a}*\widehat{A}_{X-b}$ is the sum of the quantities (18) and (25) when $a,b\neq 1$ and q is odd.

4.3 Other cases and the general product formula

Exactly the same discussion applies to the case $a\neq 1$, $b\neq 1$ and q even. Formula (21) can be kept, and it remains to add for every $c\in\mathbb{F}_q$ the $(q-1)$ terms with characteristic polynomial equal to $X^2+cX+ab$. Half of the cases yield the contribution (22), the only difference with the odd case being that the sum is over a fixed number of values of c (independent of ab), namely, $\frac{q}{2}$. For the other values of c, remark that ab is always a square in $\mathbb{F}_q$, namely, the square of $\delta=(ab)^{\frac{q}{2}}$. Therefore, these over values of $c\notin I_{ab}$ give a contribution

$$\frac{1}{2q(q^2-1)}(2\widehat{A}_{\{X-\delta:2\}}-\widehat{A}_{\{X-\delta:1^2\}})+\frac{1}{2q(q^2-1)}\sum_{d\in(\mathbb{F}_q)^\times}\widehat{A}_{\{X-ad^{-1}:1,X-bd:1\}},$$

which replaces (24). Thus, in the even case, the remaining part of $\widehat{A}_{X-a}*\widehat{A}_{X-b}$ is equal to

$$\frac{1}{q}\widehat{A}_{\{X-a:1,X-b:1\}}+\frac{q-1}{q^2}\Bigg(\sum_{c\in I_{ab}}\widehat{A}_{\{X^2+cX+ab:1\}}+\frac{1}{2}\sum_{d\in(\mathbb{F}_q)^\times}\widehat{A}_{\{X-ad^{-1}:1,X-bd:1\}}$$
$$+\frac{1}{2}(2\widehat{A}_{\{X-\delta:2\}}-\widehat{A}_{\{X-\delta:1^2\}})+\mathbb{1}_{a=b}(\widehat{A}_{\{X-a:2\}}-\widehat{A}_{\{X-a:1^2\}})\Bigg). \tag{26}$$

The sum of (18) and (26) gives $\widehat{A}_{X-a}*\widehat{A}_{X-b}$ when $a,b\neq 1$ and q is even.

Finally, when one of the coefficient a or b is equal to 1, the unique corresponding trivial extension on $(\mathbb{F}_q)^2$ is the identity (partial) isomorphism $((\mathbb{F}_q)^2\ {}^{\mathrm{id}}\!\rightleftarrows_{\mathrm{id}}\ (\mathbb{F}_q)^2)$. The computation is then trivial and one obtains for instance for $\widehat{A}_{X-a}*\widehat{A}_{X-1}$ with $a\neq 1$ the result

$$(q-1)\widehat{A}_{X-a}+\widehat{A}_{\{X-a:1;X-1:1\}}.$$

The first term corresponds to collinear vectors u and v, and the second term to noncollinear vectors. When a is also equal to 1, the same reasoning gives

$$(q-1)\widehat{A}_{X-1}+\widehat{A}_{\{X-1:1^2\}}.$$

Thus, we have proven the following:

Theorem 4.1 *The product of two generic degree* 1 *classes* $\widehat{A}_{X-a}$ *and* $\widehat{A}_{X-b}$ *is given by the following formulas. Each time, the writing is decreasing in degree and without* *terms appearing more than once, but in the sums preceded by a* $\frac{1}{2}$, *where each term appears twice.*

- $a \neq b \neq 1$, *q odd*, $(\frac{ab}{q}) = 1$, $ab = \delta^2$:

$$\begin{aligned}&\frac{q-1}{q^2}\biggl(\widehat{A}_{\{X-\delta:2\}} + \widehat{A}_{\{X+\delta:2\}} + \sum_{c \in I_{ab}} \widehat{A}_{\{X^2+cX+ab:1\}} \\ &\quad + \frac{1}{2} \sum_{d \in (\mathbb{F}_q)^\times \setminus \{1, b^{-1}a, \pm b^{-1}\delta\}} \widehat{A}_{\{X-ad^{-1}:1, X-bd:1\}}\biggr) \\ &\quad + \frac{2q-1}{q^2}\widehat{A}_{\{X-a:1, X-b:1\}} + (q-1)\widehat{A}_{X-ab}.\end{aligned}$$

- $a \neq b \neq 1$, *q odd*, $(\frac{ab}{q}) = -1$:

$$\begin{aligned}&\frac{q-1}{q^2}\biggl(\sum_{c \in I_{ab}} \widehat{A}_{\{X^2+cX+ab:1\}} \\ &\quad + \frac{1}{2} \sum_{d \in (\mathbb{F}_q)^\times \setminus \{1, b^{-1}a\}} \widehat{A}_{\{X-ad^{-1}:1, X-bd:1\}}\biggr) \\ &\quad + \frac{2q-1}{q^2}\widehat{A}_{\{X-a:1, X-b:1\}} + (q-1)\widehat{A}_{X-ab}.\end{aligned}$$

- $a \neq b \neq 1$, *q even*, $\delta = (ab)^{\frac{q}{2}}$:

$$\begin{aligned}&\frac{q-1}{q^2}\biggl(\widehat{A}_{\{X-\delta:2\}} + \sum_{c \in I_{ab}} \widehat{A}_{\{X^2+cX+ab:1\}} \\ &\quad + \frac{1}{2} \sum_{d \in (\mathbb{F}_q)^\times \setminus \{1, b^{-1}a, b^{-1}\delta\}} \widehat{A}_{\{X-ad^{-1}:1, X-bd:1\}}\biggr) \\ &\quad + \frac{2q-1}{q^2}\widehat{A}_{\{X-a:1, X-b:1\}} + (q-1)\widehat{A}_{X-ab}.\end{aligned}$$

- $a = b \neq 1$, *q odd*:

$$\begin{aligned}&\frac{q-1}{q^2}\biggl(2\widehat{A}_{\{X-a:2\}} + \widehat{A}_{\{X+a:2\}} + \sum_{c \in I_{a^2}} \widehat{A}_{\{X^2+cX+a^2:1\}} \\ &\quad + \frac{1}{2} \sum_{d \in (\mathbb{F}_q)^\times \setminus \{\pm 1\}} \widehat{A}_{\{X-ad^{-1}:1, X-ad:1\}}\biggr) \\ &\quad + \frac{1}{q^2}\widehat{A}_{\{X-a:1^2\}} + (q-1)\widehat{A}_{X-a^2}.\end{aligned}$$

- $a = b \neq 1$, q *even*:

$$\frac{q-1}{q^2}\left(2\widehat{A}_{\{X-a:2\}} + \sum_{c\in I_{a^2}} \widehat{A}_{\{X^2+cX+a^2:1\}} + \frac{1}{2}\sum_{d\in(\mathbb{F}_q)^\times\setminus\{1\}} \widehat{A}_{\{X-ad^{-1}:1,X-ad:1\}}\right)$$
$$+\frac{1}{q^2}\widehat{A}_{\{X-a:1^2\}} + (q-1)\widehat{A}_{X-a^2}.$$

- $a \neq 1$, $b = 1$: $\widehat{A}_{\{X-a:1;X-1:1\}} + (q-1)\widehat{A}_{X-a}$.
- $a = b = 1$: $\widehat{A}_{\{X-1:1^2\}} + (q-1)\widehat{A}_{X-1}$.

The theorem yields readily the product of two completed conjugacy classes of degree 1 for any $n \in \mathbb{N}$, since

$$\Pi_n(\widehat{A}_{\mathbb{\mu}}) = q^{n(2k_1-k)}\frac{q^{2k(k-k_1)}(q^{-1})_k(q^{-1})_{n-k+k_{11}}}{(q^{-1})_{k_{11}}(q^{-1})_{n-k}}\frac{C_{\mathbb{\mu}\uparrow^n}}{\operatorname{card} C_{\mathbb{\mu}}}$$

for any polypartition $\mathbb{\mu}$. More specifically,

$$\begin{aligned}
\Pi_n(\widehat{A}_{\{X-1:1\}}) &= \big(q^n-1\big)C_{\emptyset\uparrow^n}\\
\Pi_n(\widehat{A}_{\{X-1:1^2\}}) &= \big(q^n-1\big)\big(q^n-q\big)C_{\emptyset\uparrow^n}\\
\Pi_n(\widehat{A}_{\{X-a:1\}}) &= q^{1-n}(q-1)C_{\{X-a:1\}\uparrow^n}\\
\Pi_n(\widehat{A}_{\{X-a:2\}}) &= q^{5-2n}(q-1)C_{\{X-a:2\}\uparrow^n}\\
\Pi_n(\widehat{A}_{\{X-a:1^2\}}) &= q^{5-2n}(q-1)\big(q^2-1\big)C_{\{X-a:1^2\}\uparrow^n}\\
\Pi_n(\widehat{A}_{\{X-a:1;X-1:1\}}) &= q^{2-n}(q-1)\big(q^{n-1}-1\big)C_{\{X-a:1\}\uparrow^n}\\
\Pi_n(\widehat{A}_{\{X-a:1;X-b:1\}}) &= q^{4-2n}(q-1)^2C_{\{X-a:1;X-b:1\}\uparrow^n}\\
\Pi_n(\widehat{A}_{\{X^2+aX+b:1\}}) &= q^{4-2n}\big(q^2-1\big)C_{\{X^2+aX+b:1\}\uparrow^n}.
\end{aligned} \tag{27}$$

Applying these formulas to the seven cases of Theorem 4.1, one obtains the expansion in completed conjugacy classes of

$$\Pi_n(\widehat{A}_{X-a} * \widehat{A}_{X-b}) = \big(q^n-1\big)^2\frac{C_{\{X-a\}\uparrow^n} * C_{\{X-b\}\uparrow^n}}{\operatorname{card} C_{\{X-a\}\uparrow^n} \times \operatorname{card} C_{\{X-b\}\uparrow^n}}. \tag{28}$$

So for instance, if q is odd and $a \neq b \neq 1$, $(\frac{ab}{q}) = 1$, $ab = \delta^2$, then by projection by Π_n of the first case of Theorem 4.1, the product of completed conjugacy classes $C_{\{X-a\}\uparrow^n} * C_{\{X-b\}\uparrow^n}$ in $\mathbb{C}\mathrm{GL}(n,\mathbb{F}_q)$ is given by

$$\begin{aligned}
C_{\{X-a\}\uparrow^n} * C_{\{X-b\}\uparrow^n} = {} & qC_{\{X-\delta:2\}\uparrow^n} + qC_{\{X+\delta:2\}\uparrow^n} + (2q-1)C_{\{X-a:1,X-b:1\}}\\
& + q^{n-1}C_{\{X-ab:1\}\uparrow^n} + \sum_{c\in I_{ab}}(q+1)C_{\{X^2+cX+ab:1\}\uparrow^n}\\
& + \frac{1}{2}\sum_{d\in(\mathbb{F}_q)^\times\setminus\{1,b^{-1}a,\pm b^{-1}\delta\}}(q-1)C_{\{X-ad^{-1}:1,X-bd:1\}\uparrow^n}.
\end{aligned}$$

Each structure coefficient is indeed a polynomial in q^n, here of degree 0 or 1. Notice that this formula *cannot* be specialized to the case $a = 1$ or $b = 1$ (in this case, the sixth and seventh cases of Theorem 4.1 give indeed the much simpler expansion $C_{\{X-a:1\}\uparrow^n} * C_{\{X-1:1\}\uparrow^n} = C_{\{X-a:1\}\uparrow^n}$, as can be expected). The other cases are similar and easy computations after Theorem 4.1 and Formulas (27) and (28).

From these computations, it becomes clear that the determination of the whole multiplication table of $\mathscr{Z}(\infty, \mathbb{F}_q)$ is not possible. However, there might exist simple rules to determine certain structure polynomials $p^{\lambda}_{\mu\nu}(q^n)$, especially those with $|\lambda| = |\mu| + |\nu|$. If it exists, a general rule for these coefficients "of maximal degree" probably involves deep arithmetics and Galois theory of polynomials over $\mathbb{F}_q[X]$.

Acknowledgements The author would like to thank Valentin Féray for several discussions of the construction of "generic" center group algebras; and the anonymous referee for his valuable comments, which allowed to improve the quality of the paper.

References

1. Baik, J., Deift, P., Johansson, K.: On the distribution of the length of the longest increasing subsequence of random permutations. J. Am. Math. Soc. **12**, 1119–1178 (1999)
2. Biane, P.: Approximate factorization and concentration for characters of symmetric groups. Int. Math. Res. Not. **4**, 179–192 (2001)
3. Billingsley, P.: Probability and Measure, 3rd edn. Wiley Series in Probability and Statistics. Wiley, New York (1995)
4. Borodin, A.: Determinantal point processes (2009). arXiv:0911.1153v1 [math.PR]
5. Borodin, A., Okounkov, A., Olshanski, G.: Asymptotics of Plancherel measures for symmetric groups. J. Am. Math. Soc. **13**, 491–515 (2000)
6. Dudko, A.: Asymptotics of Plancherel measures for $GL(n,q)$ (2008). arXiv:0806.1345v2 [math.RT]
7. Farahat, H.K., Higman, G.: The centres of symmetric group rings. Proc. R. Soc. Lond. Ser. A, Math. Phys. Sci. **250**(1261), 212–221 (1959)
8. Féray, V., Méliot, P.-L.: Asymptotics of q-Plancherel measures. Probab. Theory Relat. Fields **152**(3–4), 589–624 (2012)
9. Fulman, J.: Convergence rates of random walk on irreducible representations of finite groups. J. Theor. Probab. **21**, 193–211 (2008)
10. Gnedin, A., Olshanski, G.: q-exchangeability via quasi-invariance. Ann. Probab. **38**(6), 2103–2135 (2010)
11. Gorin, V., Kerov, S., Vershik, A.: Finite traces and representations of the group of infinite matrices over a finite field (2012). arXiv:1209.4945v2 [math.RT]
12. Ivanov, V., Kerov, S.: The algebra of conjugacy classes in symmetric groups, and partial permutations. Zap. Nauč. Semin. POMI **256**(3), 95–120 (1999)
13. Ivanov, V., Olshanski, G.: Kerov's central limit theorem for the Plancherel measure on Young diagrams. In: Symmetric Functions 2001. NATO Science Series II. Mathematics, Physics and Chemistry, vol. 74, pp. 93–151 (2002)
14. Kerov, S., Vershik, A.: Four drafts on the representation theory of the group of infinite matrices over a finite field. J. Math. Sci. (N.Y.) **147**(6), 7129–7144 (2007)
15. Macdonald, I.G.: Symmetric Functions and Hall Polynomials. Oxford Mathematical Monographs. Clarendon Press, Oxford (1995)
16. Méliot, P.-L.: Products of Geck–Rouquier conjugacy classes and the Hecke algebra of composed permutations. In: Proceedings of the 22nd International Conference on Formal Power Series and Algebraic Combinatorics, San Francisco, USA, pp. 790–801 (2010)
17. Méliot, P.-L.: Kerov's central limit theorem for Schur-Weyl and Gelfand measures. In: Proceedings of the 23th International Conference on Formal Power Series and Algebraic Combinatorics, Reykjavík, Iceland, pp. 669–680 (2011)
18. Méliot, P.-L.: Fluctuations of central measures on partitions. In: Proceedings of the 24th International Conference on Formal Power Series and Algebraic Combinatorics, Nagoya, Japan, pp. 387–398 (2012)

19. Okounkov, A.: On the representations of the infinite symmetric group. Ph.D. thesis, Moscow State University (1995)
20. Okounkov, A.: Random matrices and random permutations. Int. Math. Res. Not. **20**, 1043–1095 (2000)
21. Olshanski, G.: Unitary representations of (G, K)-pairs that are connected with the infinite symmetric group $S(\infty)$. Leningr. Math. J. **1**(4) (1990)
22. Olshanski, G.: On semigroups related to infinite-dimensional groups. In: Kirillov, A.A. (ed.) Topics in Representation Theory. Advances in Soviet Mathematics, vol. 2, pp. 67–101. AMS, Providence (1991)
23. Śniady, P.: Gaussian fluctuations of characters of symmetric groups and of Young diagrams. Probab. Theory Relat. Fields **136**(2), 263–297 (2006)
24. Tout, O.: Structure coefficients of the Hecke algebra of $(\mathcal{S}_{2n}, \mathcal{B}_n)$ (2012). arXiv:1212.5375 [math.CO]