Monodromy of local systems and applications to coding theory

A master's thesis presented by
Francisco García Cortés

Advised by
Antonio Rojas León

Facultad de Matemáticas
Departamento de Álgebra
Universidad de Sevilla

November 14, 2023
Sevilla

Monodromy of local systems and applications to coding theory

Francisco García Cortés

2020 *Mathematics Subject Classification.* 11T23, 11Y16, 14G50

Key words and phrases. ℓ-adic local systems, Exponential sums, Monodromy groups, Linear Binary Codes, Cryptography

Abstract. The present work concerns the study of monodromy of ℓ-adic sheaves with an strong focus on computational matters. After reviewing étale and ℓ-adic cohomology, we introduce some families of local systems and consider the problem of determining whether their monodromy is finite or not. To this end, we propose a sieve-based approach and an algorithm is described. Actual implementations are used to explore the question for the described families and to compare the outputs with recent results in the area. The algorithm is further used to obtain some numerical data showing certain phenomena that allows us to identify major obstructions to the performance of the implementations. We conclude with some motivation coming from coding theory and cryptography as well as an application of the study of monodromy to coding theory.

A mis padres, mis hermanas y Marisa,
por acompañarme en mi camino.

Contents

Introduction

This work deals with the study of exponential sums with a specially simple expression such as

$$\sum_{x\in\mathbb{F}_q} \psi \circ \mathtt{trace}_{\mathbb{F}_q/\mathbb{F}_p}(x^d + tx)$$

for $t \in \mathbb{F}_q$, where p is a prime number, q a p-power, $d > 0$ a positive integer coprime to p and $\psi : \mathbb{F}_p \to \mathbb{C}^\times$ a non-trivial additive character of a prime finite field. As explained in Chapter 3, when $p = 2$ these specific sums are well-known for coding theorists and cryptographers, since they can be used to measure the auto-correlation and cross-correlation between randomness simulating sequences. Hence, a good deal of information about them is already established by means of coding theory.

But nowadays, after the work of Deligne, we commonly think in ℓ-adic cohomology as soon as we hear about exponential sums. This is how we will study those easy-to-remember exponential sums in this master's thesis. ℓ-adic cohomology is much broad and deep than what we really need for our goals, so we should specify what we mean by reviewing étale and ℓ-adic cohomology. We have two main interests in the tools of ℓ-adic cohomology:

1. First, to understand the equivalence between lisse ℓ-adic sheaves over varieties over finite fields and representations of the étale fundamental group of the variety.
2. Second, to see how the study of ℓ-adic cohomology groups can be used to obtain estimates and information about exponential sums by using fundamental results such as Grothendieck's Lefschetz trace formula or Deligne's theorem on weights.

We explain as much ℓ-adic cohomology as needed to understand those stated goals and the involved concepts. This is the content of Chapter 1, which must be understood as an introduction to the subject for a working number theorist.

After describing the equivalence between local systems and representation of fundamental groups, we can introduce the main actors of the work: the monodromy groups. In Chapter 2 we introduce sensible concepts and review well-known results that allow us to study the question of finiteness of monodromy for lisse ℓ-adic sheaves. After this, we introduce the sort of easy-to-remember families of ℓ-adic sheaves we are interested in, showing that they are suitable for applying and specializing the described criteria. This way, we will obtain explicit, i.e. numerical, criteria for the finiteness of their monodromy.

After obtaining those explicit conditions, that are just inequalities but infinitely many of them, the main content of the present work starts (Section 2.3). This thesis is mainly concerned with the computational counterpart of the mentioned inequalities. We have two goals that complement each other:

1. On the first hand, to developed sufficiently general strategies so we can explore the problem of finiteness of monodromy for the introduced families (or more generally any family for which such a numeric criterion can be obtained).
2. On the second hand, translate the strategies into actual algorithms (preferably with implementations) so we can indeed explore the problem and obtain computational evidences that might be used, for example, to improve the existing strategies or identify some unexpected phenomena.

Our contribution to this problem is to describe a sieve-based approach taking advantage of the properties of the sum-of-digits functions involved in the inequalities appearing in the criteria. We implemented algorithms (using Julia Programming Language, see Appendix) for the families we deal here with and study the experimental complexity of our approach through them. After using our strategy on previously studied families, we compare the results with recent theorems of Katz–Tiep that determine when the monodromy groups are finite. For a specific family of local systems not studied before in the literature, namely the family denoted by $\mathcal{B}$, we show that the parameters found by the algorithm indeed give raise to a lisse ℓ-adic sheaf with finite monodromy group.

To conclude this introduction, it should be mentioned that the work can be read in at least two ways. For readers looking for an stronger applied motivation, Chapter 3 can be read first despite the truth of some facts treated in previous chapters should be assumed. The point of reading Chapter 3 first is that the last theorem proven there nicely motivates why we are concerned with the finiteness of the monodromy groups of certain local systems. If the reader prefers an expositon free of backward jumps, the suggested reading is the linear one.

Acknowledgements

The author was partially supported by US-1262169 (Consejería de Economía y Conocimiento; Junta de Andalucía) and P_2001056 (Consejería de Economía, Conocimiento, Empresas y Universidad; Junta de Andalucía). The author wishes to express his gratitude to the people who comprise the Departamento de Álgebra of Universidad de Sevilla for providing him with the aproppiate environment to learn and developd his ideas. Especially to Antonio Rojas-León, for advising him during the preparation of this work and for showing him what mathematics is really about.

CHAPTER 1

Review of ℓ-adic cohomology and ℓ-adic sheaves

In this chapter we briefly review important results from ℓ-adic cohomology on varieties. We have two major goals with this section. The first one is to explain enough ℓ-adic and étale cohomology in order to explain concretely the equivalence between the category of lisse $\overline{\mathbb{Q}}_\ell$-sheaves and finite-dimensional continuous representations of the corresponding fundamental group. The second one is to illustrate some of the ideas involved in the translation of questions about exponentials (or character, or trigonometric) sums into questions in ℓ-adic cohomology. For example, we describe Gauss sums and Kloosterman sums together with their geometric incarnation via ℓ-adic sheaves on $\mathbb{G}_m$.

Relative to references and literature, we cite original sources together with modern works scrupulously. Having said this, we should mention the usage of several texts that were extremely useful while diving through the several pages of SGA volumes, Deligne's Weil II and Laumon's article on Fourier transform. The citation of these was difficult due to their expository nature. The mentioned works are [**Ill87**], [**Kat88b**], [**Kat94**], [**Kat01**], [**Ill06**], [**Ngo17**, Chapter 1], [**Fre19**], [**KR20**] and [**FFK23**, Appendices A and D]. The influence of the aforementioned works on this thesis is reflected in the selected topics and the way in which they are presented.

1.1. Étale fundamental group

Given a locally noetherian and connected scheme X, we denote by $\mathtt{FÉt}_X$ the category of étale coverings $Y \to X$, i.e. finite étale morphisms $Y \to X$. A *geometric point of* X is a morphism $\overline{x} : \mathtt{Spec}\ \Omega \to X$ where Ω is an algebraically closed field. Giving a geometric point $\overline{x}$ is equivalent to giving a point x of X and an algebraically closed overfield of the residue field $k(x)$. In this case we say that $\overline{x}$ lies over x. Given an étale covering $f : Y \to X$ and a geometric point $\overline{y} : \mathtt{Spec}\ \Omega \to Y$, we denote the geometric point $f \circ \overline{y}$ by $f(\overline{y})$.

Given a geometric point $\overline{x} : \mathtt{Spec}\ \Omega \to X$, the functor that sends each $Y \to X$ to the underlying set of the fibre $Y_{\overline{x}} := Y \times_X \mathtt{Spec}\ \Omega$ is denoted by $\mathtt{Fib}_{\overline{x}} : \mathtt{FÉt}_X \to \mathtt{FinSets}$. Following Grothendieck [**SGA 1**, Exposé V, §4,7], we define the *étale fundamental group of* X *with basepoint* $\overline{x}$, denoted $\pi_1(X, \overline{x})$, as the automorphism group of $\mathtt{Fib}_{\overline{x}}$. This means that $\pi_1(X, \overline{x})$ is the group of natural isomorphisms of $\mathtt{Fib}_{\overline{x}}$.

The fundamental group satisfies the following theorem:

THEOREM 1.1.0.1 ([**SGA 1**, Exposé V, §4]). *Let X be a locally noetherian connected scheme and $\overline{x}$ a geometric point of X. The étale fundamental group $\pi_1(X, \overline{x})$ is a profinite group and the functor $\mathtt{Fib}_{\overline{x}}$ induces an equivalence of categories*

$$\mathtt{FÉt}_X \longleftrightarrow \{\textit{finite discrete continuous } \pi_1(X, \overline{x})\textit{-sets}\}. \qquad \square$$

REMARK 1.1.0.2. In the previous theorem *continuous* means that we assume the defining morphism of the action, say $\pi_1(X, \overline{x}) \times S \to S$, continuous where S is a discrete set and $\pi_1(X, \overline{x})$ is seen as a profinite group (in particular, a toplogical group). This condition is easily seen to be equivalent to: the stabilizer of every element $s \in S$ is an open subgroup of $\pi_1(X, \overline{x})$. ■

The following two properties are analogous to the classical properties of fundamental groups:

THEOREM 1.1.0.3 ([**SGA 1**, Exposé V, §7]).

(a) *Given two geometric points $\overline{x}_1, \overline{x}_2$ of X, the functors $\mathtt{Fib}_{\overline{x}_1}$ and $\mathtt{Fib}_{\overline{x}_2}$ are isomorphic. Choosing an isomorphism between the functors $\mathtt{Fib}_{\overline{x}_1}, \mathtt{Fib}_{\overline{x}_2}$ gives an isomorphism between the fundamental groups $\pi_1(X, \overline{x}_1), \pi_1(X, \overline{x}_2)$. Choosing another isomorphism between $\mathtt{Fib}_{\overline{x}_1}, \mathtt{Fib}_{\overline{x}_2}$ vary the isomorphism between groups by an inner automorphism.*

(b) *A morphism between locally noetherian connected schemes $f : X \to X'$ induces the "preimage" functor*

$$\begin{array}{rccc} f^\bullet : & \mathtt{F\acute{E}t}_{X'} & \to & \mathtt{F\acute{E}t}_X \\ & Y \to X' & \mapsto & Y \times_{X'} X. \end{array}$$

For each geometric point $\overline{x}$ of X, $f^\bullet$ induces a canonical continuous homomorphism between étale fundamental groups (compatible with the equivalence of 1.1.0.1)

$$f_* : \pi_1(X, \overline{x}) \to \pi_1(X', f(\overline{x})). \qquad \square$$

More generally, we will speak of the induced homomorphism $f_* : \pi_1(X, \overline{x}) \to \pi_1(X', \overline{x}')$ for arbitrary geometric points. This makes sense up to conjugation on the target and the source.

EXAMPLE 1.1.0.4. *The fundamental group of the point* $\mathtt{Spec}\ k$:

Fixed a field k, a geometric point $\overline{x}$ of $X = \mathtt{Spec}\ k$ is just an embedding of k in an algebraically closed field $k^{\mathtt{alg}}$. In this case [**Stacks**, tag 0BNE], the étale fundamental group $\pi_1(X, \overline{x})$ can be identified with the absolute Galois group $\mathtt{Gal}(k^{\mathtt{sep}}/k)$, where $k^{\mathtt{sep}}$ is the separable closure of k inside $k^{\mathtt{alg}}$.

In particular, if $k = \mathbb{F}_q$ is a finite field, the étale fundamental group is canonically isomorphic to the profinite completion $\hat{\mathbb{Z}}$ of $\mathbb{Z}$, with topological generator the Frobenius map $t \mapsto t^q$. We call *geometric Frobenius* the inverse $\mathtt{Frob}_k$ of $x \mapsto x^q$. Given a degree n extension E/k, the map induced by $\mathtt{Spec}\ E \to \mathtt{Spec}\ k$ on the fundamental groups sends $\mathtt{Frob}_E$ to $\mathtt{Frob}_k^n$. ■

THEOREM 1.1.0.5 ([**SGA 1**, Exposé IX, Théorème 6.1],[**Stacks**, tag 0BTX]). *Let k be a field, $k^{\mathtt{alg}}/k$ an algebraic closure of k, X a k-scheme, $\overline{X} = X \otimes_k k^{\mathtt{alg}}$, $\overline{x}$ a geometric point of $\overline{X}$, x its image over X and b its image over $\mathtt{Spec}\ k$. Assuming that X is quasi-compact and geometrically connected over k, the sequence of canonical homomorphisms*

$$1 \longrightarrow \pi_1(\overline{X}, \overline{x}) \longrightarrow \pi_1(X, x) \longrightarrow \pi_1(\mathtt{Spec}\ k, b) \longrightarrow 1$$

is exact and

$$\pi_1(\mathtt{Spec}\ k, b) \xleftarrow{\sim} \pi_1(\mathtt{Spec}\ k, k^{\mathtt{alg}}) = \mathtt{Gal}(k^{\mathtt{alg}}/k). \qquad \square$$

If $\mathbb{F}_q$ is a finite field (in particular a perfect field), the previous theorem and Example 1.1.0.4 give us the following exact sequence:

$$1 \longrightarrow \pi_1(X_{k^{\mathtt{sep}}}, \overline{x}) \longrightarrow \pi_1(X, x) \xrightarrow{\mathtt{deg}} \hat{\mathbb{Z}} \longrightarrow 1.$$

We call the group $\pi_1(X_{k^{\mathtt{sep}}}, \overline{x})$ the *geometric fundamental group*, and denote it by $\pi_1^{\mathtt{geom}}(X)$. Similarly, $\pi_1(X, x)$ is the *arithmetic fundamental group* and is denoted by $\pi_1^{\mathtt{arith}}(X)$. Since $\pi_1^{\mathtt{geom}}(X) = \mathtt{ker}(\mathtt{deg})$, $\pi_1^{\mathtt{geom}}(X) \lhd \pi_1^{\mathtt{arith}}(X)$.

1.2. Étale topology and étale cohomology

1.2.1. Étale topology and the étale site. Let X be a scheme and denote by $\mathtt{\acute{E}t}/X$ be the category of étale X-schemes, i.e. its objects are étale maps $U \to X$ and arrows from $U \to X$ to $V \to X$ are morphisms $U \to V$ between X schemes. Given $U \to X \in \mathtt{\acute{E}t}/X$ and a collection $\mathscr{U} = \{f_i : U_i \to U\}_{i \in I}$ of morphisms in $\mathtt{\acute{E}t}/X$, we say $\mathscr{U}$ is an étale covering of $U \to X$ if the sets $f_i(U_i) \subset U$ cover the whole of U. From standard results about étale morphisms we derive the following properties [**Mil80**, Proposition 3.3]:

(a) If $V \to U$ is an isomorphism then $\{V \to U\}$ is an étale covering of U.

(b) (stability under composition) If $\{U_i \to U\}_{i\in I}$ is an étale covering of U and for every $i \in I$ we have an étale covering $\{V_{ij} \to U_i\}_{j\in J_i}$ of U_i, then the family $\{V_{ij} \to U\}_{i\in I, j\in J_i}$ is an étale covering of U.
(c) (stability under base change) If $\{U_i \to U\}_{i\in I}$ is an étale covering of U and $V \to U$ is a morphism then $\{\pi_2 : U_i \times_U V \to V\}_{i\in I}$ is an étale covering of V.

The collection of étale coverings on the category $\acute{\mathtt{Et}}/X$ is called the étale topology [**SGA 4₂**, Exposé VII,§1]. It is an instance of a Grothendieck topology (see [**Art62**, Chapter 1, Definition 0.1] for further details). It is important to observe that $\acute{\mathtt{Et}}/X$ has a final object, namely the identity morphism $X \to X$. The category $\acute{\mathtt{Et}}/X$ together with the collection of étale coverings is called the étale site and denoted by $X_{\acute{\mathtt{et}}}$. A warning is in order, we are careless about the set theoretic issues underlying these definitions. Further foundational details can be found in [**SGA 4₁**].

1.2.2. Étale sheaves.

Definition 1.2.2.1 ([**SGA 4₁**, Exposé II, §2, §6]). Let X be a scheme.

(a) An *(abelian) étale presheaf on X* is a functor $\mathcal{F} : (\acute{\mathtt{Et}}/X)^{\mathtt{opp}} \to \mathtt{Ab}$.
(b) An étale presheaf on X is said to be an *(abelian) étale sheaf on X* (or simply a *sheaf on $X_{\acute{\mathtt{et}}}$*) if for every étale map $U \to X$ and all coverings $\{U_i \to U\}_{i\in I}$ the sequence

$$0 \to \mathcal{F}(U) \to \prod_{i\in I} \mathcal{F}(U_i) \to \prod_{i,j\in I} \mathcal{F}(U_i \times_U U_j)$$

is exact in the category $\mathtt{Ab}$, where the first arrow is $s \mapsto (s_{|U_i})_{i\in I}$ and the second one is $(s_i)_{i\in I} \mapsto (s_{i|U_i\times_U U_j} - s_{j|U_i\times_U U_j})_{i,j\in I}$.

Remark 1.2.2.2. Lets spell out what condition (b) in the above definition means. The morphism $\prod_{i\in I} \mathcal{F}(U_i) \rightrightarrows \prod_{i,j\in I} \mathcal{F}(U_i \times_U U_j)$ sends $(s_i)_{i\in I} \in \prod \mathcal{F}(U_i)$ to $(s_i|_{U_i\times_U U_j} - s_j|_{U_i\times_U U_j})_{i,j\in I} \in \prod_{i,j} \mathcal{F}(U_i \times_U U_j)$ where we denote by $t|_V$ the image of a section $t \in \mathcal{F}(U)$ under the image of the group homomorphism $\mathcal{F}(\varphi) : \mathcal{F}(U) \to \mathcal{F}(V)$ whenever $\varphi : V \to U \in \acute{\mathtt{Et}}/X$. The exactness of the sequence is the following usual gluing condition: Given $(s_i) \in \prod_{i\in I} \mathcal{F}(U_i)$ such that for every pair $i, j \in I$ the equality $s_i|_{U_i\times_U U_j} = s_j|_{U_i\times_U U_j}$ holds, then there is a unique section $s \in \mathcal{F}(U)$ such that $s|_{U_i} = s_i$ for all $i \in I$. ■

A morphism between étale presheaves is a natural transformation between functors. The category of sheaves on $X_{\acute{\mathtt{et}}}$ is considered as a full subcategory of the category of presheaves on $X_{\acute{\mathtt{et}}}$.

If $\mathcal{F}$ is a presheaf on $X_{\acute{\mathtt{et}}}$ then there exists a sheaf $\mathtt{s}\mathcal{F}$ on $X_{\acute{\mathtt{et}}}$ and a morphism $\mathcal{F} \to \mathtt{s}\mathcal{F}$ such that any morphism $\mathcal{F} \to \mathcal{G}$ with $\mathcal{G}$ a sheaf on $X_{\acute{\mathtt{et}}}$ factors uniquely through $\mathcal{F} \to \mathtt{s}\mathcal{F}$ (see [**SGA 4₁**, Exposé II, §3] or [**Art62**, Chapter II, Theorem 1.1]). Furthermore, the construction of $\mathtt{s}\mathcal{F}$ is functorial, hence we obtain a functor $\mathtt{s}$ from the category of presheaves on $X_{\acute{\mathtt{et}}}$ (denoted $\mathtt{PAb}(X_{\acute{\mathtt{et}}})$, or simply $\mathtt{PAb}(X)$) to the category of sheaves on $X_{\acute{\mathtt{et}}}$ (denoted $\mathtt{Ab}(X_{\acute{\mathtt{et}}})$ or $\mathtt{Ab}(X)$). The universal property stated above can be rephrased as follows: the inclusion $\iota : \mathtt{Ab}(X_{\acute{\mathtt{et}}}) \hookrightarrow \mathtt{PAb}(X_{\acute{\mathtt{et}}})$ has $\mathtt{s} : \mathtt{PAb}(X_{\acute{\mathtt{et}}}) \to \mathtt{Ab}(X_{\acute{\mathtt{et}}})$ as left adjoint functor, that is, for all $\mathcal{F} \in \mathtt{PAb}(X_{\acute{\mathtt{et}}}), \mathcal{G} \in \mathtt{Ab}(X_{\acute{\mathtt{et}}})$ there is a bifunctorial bijection

$$\mathtt{Hom}_{\mathtt{PAb}(X_{\acute{\mathtt{et}}})}(\mathcal{F}, \iota\mathcal{G}) \cong \mathtt{Hom}_{\mathtt{Ab}(X_{\acute{\mathtt{et}}})}(\mathtt{s}\mathcal{F}, \mathcal{G}).$$

The categories $\mathtt{PAb}(X)$ and $\mathtt{Ab}(X)$ are both abelian categories [**SGA 4₁**, Exposé II, Proposition 6.7]. Furthermore, $\mathtt{Ab}(X)$ has enough injectives (see [**SGA 4₁**, Exposé II, Remarque 6.9]). A sequence $\mathcal{F}' \xrightarrow{f} \mathcal{F} \xrightarrow{g} \mathcal{F}''$ in $\mathtt{Ab}(X)$ is exact if and only if for every $U \in \acute{\mathtt{Et}}/X$ and every $s \in \mathcal{F}(U)$ such that $g(U)(s) = 0$, there exists a covering $\{\varphi_i : U_i \to U\}$ of U and sections $t_i \in \mathcal{F}'(U_i)$ with $f(U_i)(t_i) = s|_{\varphi_i}$. We recover the classical criterion of exactnes via stalks at all the geometric points [**SGA 4₂**, Exposé VIII, Corollaire 3.8], where the notion of stalk of a sheaf at a point for the étale topology is defined as follows [**SGA 4½**, Arcata, §II.3]: Given $\overline{x} \to X$, an étale open $U \to X$ is said to be an étale neighborhood of $\overline{x}$ if the morphism $\overline{x} \to X$ factors through some morphism

$\overline{x} \to U$. Then, for an étale sheaf $\mathcal{F}$ on X, its stalk at $\overline{x}$ is $\mathcal{F}_{\overline{x}} := \varinjlim \mathcal{F}(U)$, where the limit is over étale neighborhoods of $\overline{x}$.

EXAMPLE 1.2.2.3.

(a) *Representable sheaf:* Let $G \to X$ be a group object of $\text{Ét}/X$. Consider the functor

$$\begin{array}{rccc} h_G: & (\text{Ét}/X)^{\text{opp}} & \to & \texttt{Ab} \\ & U & \mapsto & \texttt{Hom}_{\text{Ét}/X}(U, G) \\ & V \xrightarrow{f} U & \mapsto & (\cdot) \circ f : h_G(V) \to h_G(U). \end{array}$$

Initially this functor is only a presheaf but since we are working over the étale site $X_{\text{ét}}$, it is a sheaf [**Stacks**, tag 03O3, tag 03O4].

(b) *Constant sheaf:* Let C be a noetherian ring and assume X to be a noetherian scheme. We denote by $\underline{C}_X$ the sheaf defined by $U \mapsto C^{\pi_0(U)}$ where $\pi_0(U)$ denotes the finite set of connected components of X.

(c) $\mathbb{G}_{a,X}$ and $\mathbb{G}_{m,X}$: The presheaves $U \mapsto \Gamma(U, \mathcal{O}_U) = \mathcal{O}_U(U)$ and $U \mapsto \Gamma(U, \mathcal{O}_U)^\times = \mathcal{O}_U(U)^\times$ are sheaves, called respectively the *structure sheaf* and the *multiplicative group* of $X_{\text{ét}}$. Both sheaves are examples of representable sheaves via the schemes $X \otimes_{\mathbb{Z}} \mathbb{Z}[T]$ (resp. $X \otimes_{\mathbb{Z}} \mathbb{Z}[T, T^{-1}]$) [**Mil80**, pg. 51]. They are also denoted by $\mathcal{O}_X$ or $\mathbb{G}_a$ (resp. $\mathcal{O}_X^\times$ or $\mathbb{G}_m$).

(d) *Roots of unity* $\mu_{n,X}$: Let $n \in \mathbb{N}$ and define $\mu_{n,X}$ as the kernel of multiplication by n on $\mathbb{G}_{m,X}$. When n is not divisible by the characteristic of residue fields at any point $x \in X$ this sheaf is represented by the scheme $X \otimes_{\mathbb{Z}} \mathbb{Z}[T]/(T^n - 1)$. In particular, $\mu_{n,X}$ associates to any $U \to X \in \text{Ét}/X$ the group of n-th roots of unity in $\Gamma(U, \mathcal{O}_U)$. It is also denoted by μ_n. ■

For a point $\texttt{Spec}\ k$ we have the following description of étale sheaves on it:

THEOREM 1.2.2.4 ([**SGA 4$_2$**, Exposé VIII, Corollaire 2.2],[**Con**, Theorem 1.1.4.3]). *Let k be a field, $X = \texttt{Spec}\ k$ and k^{sep} a separable closure of k. The category of abelian sheaves on $X_{\text{ét}}$ is equivalent to the category of discrete continuous $\texttt{Gal}(k^{\text{sep}}/k)$-modules. Furthermore, the global sections functor $\mathcal{F} \mapsto \Gamma(X, \mathcal{F})$ and the $\texttt{Gal}(k^{\text{sep}}/k)$-invariants functor $M \mapsto M^{\texttt{Gal}(k^{\text{sep}}/k)}$ are identified under this equivalence.* □

We have the following short exact sequences:

THEOREM 1.2.2.5 ([**SGA 4$_3$**, Exposé IX, Statements 3.2 and 3.5]).

(a) KUMMER THEORY: *If $n \in \mathbb{N}$ is invertible in the scheme X (that is, $\texttt{char}(k(x)) \nmid n$ for all $x \in X$), the following sequence is exact:*

$$0 \longrightarrow \mu_{n,X} \longrightarrow \mathbb{G}_{m,X} \xrightarrow{(\cdot)^n} \mathbb{G}_{m,X} \longrightarrow 0.$$

(b) ARTIN-SCHREIER THEORY: *If X is a scheme of characteristic $p > 0$ (that is, $X \to \texttt{Spec}\ \mathbb{Z}$ factors through $\texttt{Spec}\ \mathbb{F}_p$), the following sequence is exact*

$$0 \longrightarrow \underline{\mathbb{Z}/p\mathbb{Z}}_X \longrightarrow \mathbb{G}_{a,X} \xrightarrow{(\cdot)^p - 1} \mathbb{G}_{a,X} \longrightarrow 0.$$ □

These two sequences are exact since we are working over the étale site $X_{\text{ét}}$. If we study them using classical Zariski topologies they are not exact in general.

1.2.3. Direct image, inverse image and extension by zero. Given a morphism between schemes $f : X \to Y$ and $\mathcal{F}$ a sheaf on $X_{\text{ét}}$, we define the *direct image* of $\mathcal{F}$ under f by

$$\begin{array}{rccc} f_*\mathcal{F}: & Y_{\text{ét}}{}^{\text{opp}} & \longrightarrow & \texttt{Sets} \\ & V \to Y & \longmapsto & \mathcal{F}(X \times_Y V \to X). \end{array}$$

It is a well-defined presheaf on $X_{\text{ét}}$ because étale morphisms are preserved under base change. Since $\mathcal{F}$ is a sheaf on $X_{\text{ét}}$, $f_*\mathcal{F}$ is a sheaf on $Y_{\text{ét}}$. Indeed [**Stacks**, tag 03PX], if $\{V_j \to V\}$ is a covering in $Y_{\text{ét}}$, then $\{X \times_Y V_j \to X \times_Y V\}$ is a covering in $X_{\text{ét}}$. Hence, $\mathcal{F}$ being a sheaf, the following sequence

$$\mathcal{F}(X \times_Y V) \to \prod_{i\in I} \mathcal{F}(X \times_Y V_i) \rightrightarrows \prod_{i,j\in I} \mathcal{F}(X \times_Y V_i \times_Y V_j)$$

is exact and by definition $f_*\mathcal{F}$ is a sheaf on $Y_{\text{ét}}$. This construction provides us with a left exact functor $f_* : \mathtt{Ab}(X_{\text{ét}}) \to \mathtt{Ab}(Y_{\text{ét}})$, called the *direct image functor*. The left exactness follows from the fact that if a sequence $0 \to \mathcal{F}' \to \mathcal{F} \to \mathcal{F}''$ is exact on $X_{\text{ét}}$ then for every $U \in \text{Ét}/X$ the sequence of abelian groups $0 \to \mathcal{F}'(U) \to \mathcal{F}(U) \to \mathcal{F}''(U)$ is exact. Then, for every $V \in \text{Ét}/Y$ the previous sequence is exact with $U = X \times_Y V$. Hence, the sequence $0 \to f_*\mathcal{F}'(V) \to f_*\mathcal{F}(V) \to f_*\mathcal{F}''(V)$ is exact. When f is a finite morphism we have that f_* is exact (see [**SGA 4$_2$**, Exposé VIII, Proposition 5.5]). If $g : Y \to Z$ is another scheme morphism we have immediately $(g \circ f)_* \cong g_*f_*$.

The functor $f_* : \mathtt{Ab}(X_{\text{ét}}) \to \mathtt{Ab}(Y_{\text{ét}})$ admits a left adjoint denoted by $f^* : \mathtt{Ab}(Y_{\text{ét}}) \to \mathtt{Ab}(X_{\text{ét}})$ and called the *inverse image functor*. It can be proved that for every geometric point $\overline{x}$ of X the formula $(f^*\mathcal{F})_{\overline{x}} = \mathcal{F}_{f(\overline{x})}$ holds (see [**SGA 4$_2$**, Exposé VIII, §3.4]). It shows that f^* is an exact functor. Analogously to the situation with direct images, if $g : Y \to Z$ is another scheme morphism, we have $(g \circ f)^* = f^*g^*$. Indeed this follows from the adjunction property between f_* and f^*.

For an étale morphism $j : U \to X$, the inverse image functor j^* (that now is just the *restriction functor* for the étale toplogy, i.e. $(j^*\mathcal{F})(U' \to U) = \mathcal{F}(U' \to U \xrightarrow{j} X)$) has a left adjoint $j_! : \mathtt{Ab}(U_{\text{ét}}) \to \mathtt{Ab}(X_{\text{ét}})$ called *extension by zero*. If $\overline{x}$ is a geometric point of X then $(j_!\mathcal{F})_{\overline{x}} = \bigoplus_{j(\overline{u})=\overline{x}} \mathcal{F}_{\overline{u}}$ where the direct sum runs over the geometric points of U above $\overline{x}$ (see [**SGA 4$_1$**, Exposé IV, Proposition 11.3.1] and [**Stacks**, tag 03S5]). This shows that $j_!$ is an exact functor. Again, if $g : Y \to Z$ is a scheme morphism, it holds that $(g \circ f)_! \cong g_!f_!$. In fact, this follows from the adjunction property between f^* and $f_!$.

When $j : U \to X$ is separated and étale, there is a functorial injective map $j_!\mathcal{F} \to j_*\mathcal{F}$ where $\mathcal{F} \in \mathtt{Ab}(X)$ (see [**Stacks**, tag 04FL]). Moreover, if the map $j : U \to X$ is assumed to be finite then the morphism $j_!\mathcal{F} \to j_*\mathcal{F}$ is an isomorphism for all $\mathcal{F} \in \mathtt{Ab}(X)$ (see [**Stacks**, tag 03S7]).

1.2.4. Locally constant sheaves and constructible sheaves.

Definition 1.2.4.1 ([**SGA 4$_3$**, Exposé IX, §2],[**SGA 4½**, Arcata, §IV.3]). Let X be a noetherian scheme and $\mathcal{F}$ an étale sheaf on $X_{\text{ét}}$.

(a) $\mathcal{F}$ is said to be locally constant if there is an étale covering $\{\varphi_i : U_i \to X\}_{i\in I}$ such that each $\mathcal{F}_{|U_i} := \varphi_i^*\mathcal{F}$ is a constant sheaf (see Example 1.2.2.3.(b)). We say that $\mathcal{F}$ is locally constant constructible (abreviated by l.c.c.) if it is locally constant and each value group is a finite group.

(b) $\mathcal{F}$ is said to be constructible if for every affine open $U \subset X$ there exists a decomposition of U into a finite number of constructible locally closed reduced subschemes U_i such that the induced sheaf of $\mathcal{F}$ over each U_i is locally constant constructible.

The inverse image under a morphism of schemes $f : X \to Y$ of a l.c.c. sheaf is again l.c.c. (see [**Stacks**, tag 095A]). If $f : X \to Y$ is an étale covering, the analogous result for direct images holds (see [**Stacks**, tag 095B]).

If X is a quasi-compact and quasi-separated noetherian scheme, a sheaf $\mathcal{F}$ is constructible if and only if there is a decomposition of X into constructible locally closed sets X_i such that $\mathcal{F}$ is l.c.c. on each X_i (see [**SGA 4$_3$**, Exposé IX, Proposition 2.4]).

The following lemma on representability of l.c.c. sheaves is essential for us:

LEMMA 1.2.4.2 ([**SGA 4$_3$**, Exposé IX, Lemme 2.2],[**Stacks**, tag 03RV]). *Let X be a noetherian scheme and $\mathcal{F}$ an étale sheaf on $X_{\text{ét}}$. $\mathcal{F}$ is locally constant constructible if and only if $\mathcal{F}$ is representable (Example 1.2.2.3.(a)) by an étale covering $U \to X$.* □

From this lemma it follows that the sheaf $\mu_{n,X}$ (with n invertible in X) of Example 1.2.2.3 is locally constant constructible since it is represented by the scheme $X \otimes_{\mathbb{Z}} \mathbb{Z}[T]/(T^n - 1)$.

Combining Lemma 1.2.4.2 and Theorem 1.1.0.1 we obtain the following theorem:

THEOREM 1.2.4.3 ([**Stacks**, tag 0DV5]). *Let X be a connected noetherian scheme and $\overline{x}$ a geometric point of X. The functor $\mathcal{F} \mapsto \mathcal{F}_{\overline{x}}$ defines an equivalence of categories*

$$\left\{\textit{l.c.c. abelian sheaves on } X_{\text{ét}}\right\} \longleftrightarrow \left\{\textit{finite discrete continuous } \pi_1(X,\overline{x})\textit{-modules}\right\}.$$

Furthermore, if $f : Y \to X$ is a morphism between connected schemes, $\overline{y}$ is a geometric point of Y and $\overline{x} = f(\overline{y})$, then the diagram

$$\begin{array}{ccc} \{\textit{l.c.c abelian sheaves on } Y_{\text{ét}}\} & \longleftrightarrow & \{\textit{finite discrete continuous } \pi_1(Y,\overline{y})\textit{-modules}\} \\ {\scriptstyle f^*}\uparrow & & \uparrow \\ \{\textit{l.c.c. abelian sheaves on } X_{\text{ét}}\} & \longleftrightarrow & \{\textit{finite discrete continuous } \pi_1(X,\overline{x})\textit{-modules}\} \end{array}$$

is commutative, where the vertical right arrow is precomposition of the action with the homomorphism f_* introduced in Theorem 1.1.0.3.(b). □

1.2.5. Some remarks on sheaves of modules. So far we have worked with abelian sheaves on $X_{\text{ét}}$. If the target category of our presheaves and sheaves is the category of A-modules (A a commutative unitary ring), we speak of presheaves and sheaves of A-modules respectively. We denote the corresponding categories by $\texttt{PMod}(X_{\text{ét}}, A)$ and $\texttt{Mod}(X_{\text{ét}}, A)$. All the stated properties in §1.2.2 hold for them.

Given sheaves of A-modules $\mathcal{F}$ and $\mathcal{G}$ on $X_{\text{ét}}$ we can consider the A-module $\texttt{Hom}_{\texttt{Mod}(X_{\text{ét}},A)}(\mathcal{F},\mathcal{G})$, that is, the set of all natural transformations between functors $\mathcal{F}$ and $\mathcal{G}$ endowed with its natural structure of A-module. However, it is desirable to have an internal "hom" in the category $\texttt{Mod}(X_{\text{ét}}, A)$. To this end, given $\mathcal{F}$ and $\mathcal{G}$ in $\texttt{Mod}(X_{\text{ét}}, A)$ consider the presheaf

$$U \xrightarrow{j} X \in \text{Ét}/X \mapsto \texttt{Hom}_{\texttt{Mod}(U_{\text{ét}},A)}(\mathcal{F}|_U, \mathcal{G}|_U)$$

where $\mathcal{F}|_U := j^*\mathcal{F}$ and $\mathcal{G}|_U := j^*\mathcal{G}$. It is easy (but tedious) to check that the previous presheaf is in fact a sheaf. We denote it by $\mathcal{H}om_A(\mathcal{F},\mathcal{G})$.

Analogously, we can define the presheaf $U \mapsto \mathcal{F}(U) \otimes_A \mathcal{G}(U)$. In general, this presheaf is not a sheaf and we should consider its associated sheaf. We define this way the tensor product of sheaves of A-modules denoted by $\mathcal{F} \otimes_A \mathcal{G}$. We introduce locally free sheaves of rank $r \in \mathbb{N}$:

DEFINITION 1.2.5.1. Let A be a noetherian ring, X a scheme and $\mathcal{F}$ a sheaf of A-modules on $X_{\text{ét}}$. $\mathcal{F}$ is said to be locally free if there exists an étale covering $\{X_i \to X\}_{i\in I}$ such that each restriction $\mathcal{F}|_{X_i}$ is a free sheaf of A-modules, that is $\mathcal{F}|_{X_i} \sim \bigoplus_{j\in J} A$ for some index set J. Moreover, if the rank of the free sheaves of A-modules $\mathcal{F}|_{X_i}$ is the same value $r \in \mathbb{N}$ for all $i \in I$ we say that $\mathcal{F}$ is locally free of (constant) rank r.

Despite all the notions introduced in §1.2.2 and §1.2.3 can be stated without major changes for sheaves of A-modules, the notion of locally constant constructible sheaf needs an important modification. We define them as follows:

DEFINITION 1.2.5.2. Let A be a ring, X a noetherian scheme and $\mathcal{F}$ a sheaf of A-modules on $X_{\text{ét}}$. We say that $\mathcal{F}$ is locally constant constructible (l.c.c.) if there exists an étale covering $\{U_i \to X\}_{i\in I}$ such that for all $i \in I$ the sheaf $\mathcal{F}|_{U_i}$ is constant and its associated value group is a finitely generated A-module.

Observe [**SGA 4$_3$**, Exposé IX, §2.3.1] that an abelian sheaf $\mathcal{F}$ on $X_{\text{ét}}$ is locally constant constructible as an abelian sheaf if and only if it is locally constant constructible as a sheaf of $\mathbb{Z}$-modules and its associated value groups are all finite. However the sheaf $\underline{\mathbb{Z}}_X$ is locally constant constructible as a sheaf of $\mathbb{Z}$-modules but not as an abelian sheaf.

When $A = \mathbb{Z}/n\mathbb{Z}$, we will usually refer to constructible sheaves of $\mathbb{Z}/n\mathbb{Z}$-modules simply by torsion abelian sheaves such that n is one of its torsion orders.

1.2.6. Étale cohomology. Let X be a scheme. We already know that the category of abelian sheaves on $\mathtt{Ab}(X)$ (resp. $\mathtt{Mod}(X_{\text{ét}}, A)$) is abelian and has enough injectives. Furthermore, the global sections functor $\mathcal{F} \in \mathtt{Ab}(X) \mapsto \mathcal{F}(X) = \Gamma(X, \mathcal{F})$ is left exact. Hence, we can speak about its right derived functors. Also, a morphism of schemes $f : X \to Y$ induces a left exact functor $f_* : \mathtt{Ab}(X) \to \mathtt{Ab}(Y)$ and we can consider its right derived functors. We name them in the following definition:

Definition 1.2.6.1. Let X be a scheme. We denote by $\mathtt{H}^\bullet(X, \cdot)$ the right derived functors of the global sections functor $\Gamma(X, \cdot)$ and call $\mathtt{H}^i(X, \mathcal{F})$ the i-th étale cohomology group of X with values in $\mathcal{F} \in \mathtt{Ab}(X)$. If $f : X \to Y$ is a morphism of schemes, we denote by $\mathtt{R}^\bullet f_*$ the right derived functors of f_* and call $\mathtt{R}^i f_* \mathcal{F}$ the i-th higher direct image functor of $\mathcal{F} \in \mathtt{Ab}(X)$.

Since the functor f_* is exact when f is a finite morphism, by definition $\mathtt{R}^i f_* = 0$ for all $i > 0$. In general, to "compute" higher direct images we have to introduce two objects. Following the notation of [**Mil80**, §2.1]:

(a) Given $j : U \to X$ an étale morphism, the functor $\mathcal{F} \in \mathtt{Ab}(X) \mapsto \Gamma(U, \mathcal{F})$ is left exact and we can consider its right derived functors. We denote them by $\mathtt{H}^\bullet(U, \mathcal{F})$.
(b) The functor $\iota : \mathtt{Ab}(X) \to \mathtt{PAb}(X)$ is left exact. Its right derived functors are written $\mathcal{H}^\bullet(X, \mathcal{F})$.

It is obvious that the presheaf $\mathcal{H}^i(X, \mathcal{F})$ is just the presheaf $U \mapsto \mathtt{H}^i(U, \mathcal{F})$. Observe that for $j : U \to X$ a given étale morphism the functor j^* takes injectives objects of $\mathtt{Ab}(X)$ to injectives objects of $\mathtt{Ab}(U)$. This simply follows from the adjunction property

$$\mathtt{Hom}_{\mathtt{Ab}(U)}(\mathcal{F}, j^*\mathcal{I}) \cong \mathtt{Hom}_{\mathtt{Ab}(X)}(j_!\mathcal{F}, \mathcal{I})$$

and the exactness of $j_!$ since, if we assume $\mathcal{I}$ to be injective, then the functor on the left hand side is clearly exact. Using this observation, the fact that $j_!$ is exact and working directly with injective resolutions, we see that the cohomology groups $\mathtt{H}^\bullet(U, \mathcal{F})$ introduced in (b) above and the standard cohomology groups $\mathtt{H}^\bullet(U, j^*\mathcal{F})$ are canonically isomorphic. Combining all these remarks we conclude that the presheaf $\mathcal{H}^i(X, \mathcal{F})$ is just the presheaf $U \mapsto \mathtt{H}^i(U, \mathcal{F}|_U)$. With this in mind we can state the following proposition:

Proposition 1.2.6.2 ([**SGA 4$_2$**, Exposé V, Proposition 5.1]). *Let $f : Y \to X$ be a morphism of schemes and $\mathcal{F}$ an abelian sheaf on $Y_{\text{ét}}$. Then $\mathtt{R}^i f_* \mathcal{F}$ is the sheaf associated to the presheaf*

$$U \to X \in \text{Ét}/X \longmapsto \mathtt{H}^i(U \times_X Y, \mathcal{F}|_{U \times_X Y}). \qquad \square$$

In the case of points we already know how to compute cohomology. In fact, as a direct consequence of Theorem 1.2.2.4 we have the following:

Corollary 1.2.6.3 ([**SGA 4$_2$**, Exposé II, Corollaire 2.3]). *Let k be a field, k^{sep} a separable closure of k and $X = \mathtt{Spec}\ k$. Let $\mathcal{F}$ be an abelian sheaf on $X_{\text{ét}}$ and M its associated $\mathtt{Gal}(k^{\text{sep}}/k)$-module under the equivalence of Theorem 1.2.2.4. Then we have a canonical isomorphism (functorial in $\mathcal{F}$) of δ-functors*

$$\mathtt{H}^\bullet(X, \mathcal{F}) \cong \mathtt{H}^\bullet(\mathtt{Gal}(k^{\text{sep}}/k), M)$$

where the groups on the right are Galois cohomology groups. $\square$

The following theorem is quite important for the general theory of constructible sheaves on shcemes of finite type over a separably closed field. It shows that higher direct images preserve constructibility:

THEOREM 1.2.6.4 ([**SGA 4½**, Th. Finitude, Théorèmes 1.1 and 1.9]). *Let k be a separably closed field, $f : X \to Y$ a morphism between k-schemes of finite type and $\mathcal{F}$ a constructible sheaf on X whose torsion orders are invertible on S. Then the higher direct images $\mathtt{R}^i f_*\mathcal{F}$ are constructible for every $i \in \mathbb{N}$ and they are not zero for only finitely many integers $i \in \mathbb{N}$. Furthermore, the formation of $\mathtt{R}^i f_*\mathcal{F}$ commutes with arbitrary extension to a separably closed field.* □

Setting $Y = \mathtt{Spec}\ k$ in the previous theorem we obtain the following:

COROLLARY 1.2.6.5 ([**SGA 4½**, Th. Finitude, Corollaire 1.10]). *Let k be a separably closed field, X a scheme of finite type over k and $\mathcal{F}$ a constructible abelian sheaf on X whose torsion orders are invertible on k. Then the groups $\mathtt{H}^i(X, \mathcal{F})$ are finite, vanish for every i except for finitely many integers $i \in \mathbb{N}$ and are invariant under extension from k to any separably closed overfield.* □

For a more precise statement on the vanishing part of these theorems see Corollary 1.2.7.3.

1.2.7. Proper base change theorem. We want to state one of the most important theorems in étale cohomology, namely *proper base change theorem*. To this end we introduce the base change maps [**SGA 4₃**, Exposé XII, §4]. Let

$$\begin{array}{ccc} X' & \xrightarrow{g'} & X \\ \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} \\ S' & \xrightarrow{g} & S \end{array}$$

be a cartesian square. We construct a natural transformation $g^* f_* \xrightarrow{\varphi} f'_*(g')^*$ as follows. Using that g^* is left adjoint to g_*, to give a morphism $g^* f_* \to f'_*(g')^*$ is equivalent to give a morphism

$$f_* \to g_* f'_*(g')^* \cong (gf')_*(g')^* = (fg')_*(g')^* \cong f_* g'_*(g')^*.$$

It is easy to give such a morphism just applying f_* to the adjunction morphism $\mathtt{id} \to g'_*(g')^*$. Observe that we can proceed simmetrically using that f'_* is right adjoint to $(f')^*$ and arguing as before we can apply $(g')^*$ to the adjunction morphism $f^* f_* \to \mathtt{id}$. Despite it seems we can construct two different base change maps, it was proved (in a broader context) by Deligne in [**SGA 4₃**, Exposé XVII,Proposition 2.1.3] that both procedures give us the same morphism between functors.

More generally, we can give a base change map for every $i \geq 0$

$$g^*(\mathtt{R}^i f_*) \xrightarrow{\varphi^i} (\mathtt{R}^i f'_*)(g')^*.$$

Indeed, reasoning as before but using this time the desription of $\mathtt{R}^i$ provided by Proposition 1.2.6.2, we construct

$$\mathtt{R}^i f_* \to (\mathtt{R}^i f_*) g'_*(g')^* \to \mathtt{R}^i(fg')_*(g')^* = \mathtt{R}^i(gf')_*(g')^* \to g^* \mathtt{R}^i f'_*(g')^*.$$

Using these functors we can state proper base change theorem:

THEOREM 1.2.7.1 ([**SGA 4₃**, Exposé XII, Théorème 5.1.(iii)]).
Let

$$\begin{array}{ccc} X' & \xrightarrow{g'} & X \\ \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} \\ S' & \xrightarrow{g} & S \end{array}$$

be a cartesian diagram with f a proper morphism and let $\mathcal{F}$ be a torsion abelian sheaf on $X_{\mathtt{\acute{e}t}}$. Then the base change morphism

$$\varphi^i : g^* \mathtt{R}^i f_* \mathcal{F} \to \mathtt{R}^i f'_*(g')^* \mathcal{F}$$

is an isomorphism for every $i \geq 0$. □

Proper base change theorem has some remarkable consequences. We state two of them:

COROLLARY 1.2.7.2 ([**SGA 4₃**, Exposé XII, Corollaire 5.2.(iii)]). *Let $f : X \to S$ be a proper morphism, $\overline{s} \to S$ a geometric point and $X_{\overline{s}}$ the fiber of f at $\overline{s}$. If $\mathcal{F}$ is a torsion abelian sheaf on $X_{\text{ét}}$, for every $i \geq 0$ the base change morphism*

$$(\mathtt{R}^i f_* \mathcal{F})_{\overline{s}} \to \mathtt{H}^i(X_{\overline{s}}, \mathcal{F}|_{X_{\overline{s}}})$$

is an isomorphism. □

The next corollary is a vanishing statement for higher direct images:

COROLLARY 1.2.7.3 ([**SGA 4₃**, Exposé XII, Corollaire 5.3.bis]). *Let $f : X \to S$ be a proper morphism and assume the fibers of f are of dimension $\leq n$. Then for every torsion abelian sheaf $\mathcal{F}$ on $X_{\text{ét}}$ it holds $\mathtt{R}^i f_* \mathcal{F} = 0$ for every $i > 2n$.* □

In [**SGA 4₃**, Exposé XII, §2] it is shown the torsion hypothesis on $\mathcal{F}$ is necessary for Theorem 1.2.7.1 to hold.

A last result on étale cohomology that is useful in applications is the so called *Affine Lefschetz theorem*:

PROPOSITION 1.2.7.4 ([**SGA 4₃**, Exposé XIV, Corollaire 3.2]). *Let X be an affine scheme of finite type over a separably closed field k and $\mathcal{F}$ a torsion abelian sheaf on $X_{\text{ét}}$. Then $\mathtt{H}^i(X, \mathcal{F}) = 0$ for every $i \geq \mathtt{dim}\ X$.* □

1.2.8. Étale cohomology with compact support. It is desirable to have an étale analog of cohomology with compact support so we can try to give duality theorems similar to Poincaré duality. In this section we construct such "compactly" supported cohomology groups.

Let $f : X \to S$ be a separated and finite type map of schemes and assume that S is quasi-compact and quasi-separated (succintly, S is a qcqs scheme). After Nagata's compactification theorem [**Nag62**] (see [**Con07**] for a version of this theorem without noetherian hypothesis on S) we know there is an open immersion $j : X \to \overline{X}$ into a proper S-scheme $\overline{f} : \overline{X} \to S$ such that $f = \overline{f} j$. We call the previous data a compactification of f. With this notation we define:

DEFINITION 1.2.8.1. With f, j and $\overline{f}$ as above, we define the i-th higher direct image with compact support $\mathtt{R}^i f_!$ as the composed functor $\mathtt{R}^i \overline{f}_* \circ j_!$ restricted to the category of torsion abelian sheaves. If $S = \mathtt{Spec}\ k$ with k a separably closed field then we denote the higher direct images with compact support by $\mathtt{H}^\bullet_{\mathtt{c}}(X, \mathcal{F})$, named cohomology groups with compact support.

This definition needs two observations. First of all, the definition of $\mathtt{R}^i f_!$ does not depend on the chosen compactification. Checking this fact needs the proper base change theorem (see [**SGA 4½**, Arcata IV, §5] and [**SGA 4₃**, Exposé XVII, Théorème 5.1.8]) and this explains why in the definition we have restricted our functors to the category of torsion étale sheaves (otherwise proper base change would be false). Finally observe that $\mathtt{H}^\bullet_{\mathtt{c}}(X, \mathcal{F}) = \mathtt{H}^\bullet(\overline{X}, j_! \mathcal{F})$.

Higher direct images with compact support verify theorems analogous to those of higher direct images. Specially important is the following one:

THEOREM 1.2.8.2 ([**SGA 4₃**, Exposé XVII, Proposition 5.2.8]). *Let $f : X \to S$ be a separated and finite type map of schemes and $\mathcal{F}$ a torsion abelian sheaf on X. For every geometric point $\overline{s}$ of S let $X_{\overline{s}}$ be the fiber of f at $\overline{s}$. Then the identiy*

$$(\mathtt{R}^i f_! \mathcal{F})_{\overline{s}} = \mathtt{H}^i_{\mathtt{c}}(X_{\overline{s}}, \mathcal{F}|_{X_{\overline{s}}})$$

holds canonically. □

We obtain the corresponding vanishing result:

COROLLARY 1.2.8.3 ([**SGA 4₃**, Exposé XVII, Corollaire 5.2.8.1]). *Let $f : X \to S$ be a separated and finite map with fibers of dimension $\leq n$. Then for every torsion abelian sheaf over X it holds $\mathtt{R}^i f_! \mathcal{F} = 0$ for every $i > 2n$.* □

The following important theorem on constructibility of higher direct images with compact support holds:

THEOREM 1.2.8.4 ([**SGA 4½**, Arcata IV, Théorème de finitude (6.2)],[**SGA 4$_3$**, Exposé XVII, Théorème 5.3.6]). *Let $f : X \to S$ be a separated finite-type map and $\mathcal{F}$ a torsion constructible abelian sheaf on X whose torsion orders are invertible on S. Then the sheaf $\mathtt{R}^i f_!\mathcal{F}$ is constructible for every index i.* □

From this theorem it follows the following finiteness result:

COROLLARY 1.2.8.5 ([**SGA 4$_3$**, Exposé XVII, Corollaire 5.3.8]). *Let k be a separably closed field, X a separated of finite type scheme over k and $\mathcal{F}$ a torsion constructible abelian sheaf on X whose torsion orders are invertible on k. Then the groups $\mathtt{H}^i_{\mathtt{c}}(X, \mathcal{F})$ are finite, vanish for every i except for finitely many integers $i \in \mathbb{N}$ and are invariant under extension from k to any separably closed overfield.* □

1.2.9. Poincaré duality. Before stating Poincaré duality we describe Tate twists of sheaves of A-modules. We restrict A to be either $\mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{N}$ or $\mathcal{O}_\lambda/\mathfrak{m}_\lambda^n$ where $\mathcal{O}_\lambda$ is the ring of integers of a finite extension $K/\mathbb{Q}_\ell$ (ℓ prime number), $n \in \mathbb{N}$ and $\mathfrak{m}_\lambda$ its maximal ideal. The main properties we want from these rings are: A is noetherian and injective as an A-module. This last property easily follows from Baer's criterion on injectivity [**Stacks**, tag 05NU]. Let X be an scheme where n (resp. ℓ) is invertible. We can consider the sheaf $\mu_{n,X}$ of $\mathbb{Z}/n\mathbb{Z}$-modules (resp. $\mu_{\ell^n,X}$ of $\mathbb{Z}/\ell^n\mathbb{Z}$-modules). It is a locally free sheaf of modules of rank 1. For $i \in \mathbb{Z}$ we define

$$\mathbb{Z}/n\mathbb{Z}(i) := \begin{cases} \mu_{n,X}^{\otimes i} & \text{if } i > 0, \\ \mathbb{Z}/n\mathbb{Z} & \text{if } i = 0, \\ \mathcal{H}om_{\mathbb{Z}/n\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}(-i), \mathbb{Z}/n\mathbb{Z}) & \text{if } i < 0. \end{cases}$$

More generally for every sheaf of $\mathbb{Z}/n\mathbb{Z}$-modules (resp. sheaf of $\mathcal{O}_\lambda/\mathfrak{m}_\lambda^n$-modules) $\mathcal{F}$ and $i \in \mathbb{Z}$ we define $\mathcal{F}(i) := \mathcal{F} \otimes_{\mathbb{Z}/n\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}(i)$ (resp. $\mathcal{F}(i) = \mathcal{F} \otimes_{\mathbb{Z}/\ell^n\mathbb{Z}} \mathbb{Z}/\ell^n\mathbb{Z}(i)$). Observe the use we make of the fact that $\mathcal{O}_\lambda/\mathfrak{m}_\lambda^n$ is a $\mathbb{Z}/\ell^n\mathbb{Z}$-algebra.

Poincaré duality is the following statement:

THEOREM 1.2.9.1 ([**Fu15**, Corollary 8.5.3],[**Con**, Theorem 1.3.8.1]). *Let X be a smooth, spearated of finite type and pure of dimension d scheme over a separably closed field k. Assume that n (resp. ℓ) is invertible on X and k. For any locally constant constructible sheaf of $\mathbb{Z}/n\mathbb{Z}$-modules (resp. $\mathcal{O}_\lambda/\mathfrak{m}_\lambda^n$-modules) $\mathcal{F}$ on X and any i, we have an isomorphism*

$$\mathtt{H}^{2d}_{\mathtt{c}}(X, \mathbb{Z}/n\mathbb{Z}(d)) \xrightarrow{\simeq} \mathbb{Z}/n\mathbb{Z}$$

and

$$\mathtt{H}^{2d-i}(X, \mathcal{H}om_{\mathbb{Z}/n\mathbb{Z}}(\mathcal{F}, \mathbb{Z}/n\mathbb{Z}(d))) \times \mathtt{H}^i_{\mathtt{c}}(X, \mathcal{F}) \to \mathtt{H}^{2d}_{\mathtt{c}}(X, \mathbb{Z}/n\mathbb{Z}(d)) \sim \mathbb{Z}/n\mathbb{Z}$$

is a perfect pairing (resp. we have an isomorphism

$$\mathtt{H}^{2d}_{\mathtt{c}}(X, \mathcal{O}_\lambda/\mathfrak{m}_\lambda^n(d)) \xrightarrow{\simeq} \mathcal{O}_\lambda/\mathfrak{m}_\lambda^n$$

and

$$\mathtt{H}^{2d-i}(X, \mathcal{H}om_{\mathcal{O}_\lambda/\mathfrak{m}_\lambda^n}(\mathcal{F}, \mathcal{O}_\lambda/\mathfrak{m}_\lambda^n(d))) \times \mathtt{H}^i_{\mathtt{c}}(X, \mathcal{F}) \to \mathtt{H}^{2d}_{\mathtt{c}}(X, \mathcal{O}_\lambda/\mathfrak{m}_\lambda^n(d)) \sim \mathcal{O}_\lambda/\mathfrak{m}_\lambda^n$$

is a perfect pairing). □

1.3. ℓ-adic sheaves and ℓ-adic cohomology

As we have seen, étale cohomology is a good cohomology theory satisfaying the expected properties when the values are in a torsion sheaf. The torsion hypothesis should be removed in order to obtain theorems such as *Lefschetz fixed-point formula*, otherwise we would be counting fixed points modulo torsion orders. The remedy for this is to extend our definition of étale sheaves while working in a more restricted context. For this section we mainly follow [**Con**, §1.4].

1.3.1. ℓ-adic sheaves. We fix some notation. Let $\Lambda = \mathcal{O}_\lambda$ be the ring of integers of a finite extension K of $\mathbb{Q}_\ell$. Λ is a complete local noetherian ring, denote its maximal ideal by $\mathfrak{m}_\lambda$ (or simply $\mathfrak{m}$) and its residue field by $\mathbb{F}_\lambda$ (or simply $\mathbb{F}$). We also fix an uniformizing parameter of Λ, i.e. a generator π of $\mathfrak{m}$. Define $\Lambda_n = \Lambda/\mathfrak{m}^{n+1}$ for $n \geq 0$. In the sequel we consider $0 \in \mathbb{N}$.

DEFINITION 1.3.1.1 ([**SGA 4½**, Rapport, Définition 2.1]). Let X be a noetherian scheme. A Λ-sheaf $\mathcal{F}_\bullet$ on X is a projective system of sheaves $\mathcal{F}_n$ $(n \geq 0)$, where $\mathcal{F}_n$ is a *constructible* sheaf of Λ_n-modules such that the transition morphism $\mathcal{F}_n \to \mathcal{F}_{n-1}$ factors through an isomorphism $\mathcal{F}_n \otimes_{\Lambda_n} \Lambda_{n-1} \to \mathcal{F}_{n-1}$. We say $\mathcal{F}$ is *lisse* if the sheaves $\mathcal{F}_n$ are locally constant constructible.

REMARK 1.3.1.2. The condition that $\mathcal{F}_n \to \mathcal{F}_{n-1}$ factors through an isomorphism $\mathcal{F}_n \otimes_{\Lambda_n} \Lambda_{n-1} \to \mathcal{F}_{n-1}$ means that there is an isomorphism such that the diagram

$$\begin{array}{ccc} \mathcal{F}_n & \longrightarrow & \mathcal{F}_{n-1} \\ & \searrow \quad \nearrow_{\sim} & \\ & \mathcal{F}_n \otimes_{\Lambda_n} \Lambda_{n-1} & \end{array}$$

is commutative. Equivalently, $\mathcal{F}_n \to \mathcal{F}_{n-1}$ induces an isomorphism $\mathcal{F}_n/\pi^n\mathcal{F}_n \to \mathcal{F}_{n-1}$. Lastly, it is also equivalent to the exactness of the sequence $\mathcal{F}_n \xrightarrow{\pi^n} \mathcal{F}_n \longrightarrow \mathcal{F}_{n-1} \longrightarrow 0$. ■

We can extend ordinary sheaf constructions to these Λ-sheaves just applying them termwise. For example, if $\mathcal{F}_\bullet$ and $\mathcal{G}_\bullet$ are two Λ-modules, we define $\mathtt{Hom}_\Lambda(\mathcal{F}_\bullet, \mathcal{G}_\bullet) = (\mathtt{Hom}_{\Lambda_n}(\mathcal{F}_n, \mathcal{G}_n))_{n\in\mathbb{N}}$. Similarly, we define $\mathcal{F}_\bullet \otimes_\Lambda \mathcal{G}_\bullet = (\mathcal{F}_n \otimes_{\Lambda_n} \mathcal{G}_n)_{n\in\mathbb{N}}$. To define inner "hom" we have to take $\mathcal{F}_\bullet$ such that each $\mathcal{F}_n$ is a locally free sheaf of Λ_n-modules of finite rank (see [**SGA 5**, Exposé VI, §1.3.3]). With this assumption, we define $\mathcal{H}om_\Lambda(\mathcal{F}_\bullet, \mathcal{G}_\bullet) = (\mathcal{H}om_{\Lambda_n}(\mathcal{F}_n, \mathcal{G}_n))_{n\in\mathbb{N}}$. The hypothesis we make on $\mathcal{F}_\bullet$ assures us that we have an exact sequence

$$\mathcal{H}om_{\Lambda_n}(\mathcal{F}_n, \mathcal{G}_n) \xrightarrow{\pi^n} \mathcal{H}om_{\Lambda_n}(\mathcal{F}_n, \mathcal{G}_n) \longrightarrow \mathcal{H}om_{\Lambda_n}(\mathcal{F}_n, \mathcal{G}_{n-1}) \longrightarrow 0.$$

Since $\pi^n\mathcal{G}_{n-1} = 0$, the exact sequence $\mathcal{F}_n \xrightarrow{\pi^n} \mathcal{F}_n \longrightarrow \mathcal{F}_{n-1} \longrightarrow 0$ shows that precomposing with $\mathcal{F}_n \to \mathcal{F}_{n-1}$ induces an isomorphism $\mathcal{H}om_{\Lambda_{n-1}}(\mathcal{F}_{n-1}, \mathcal{G}_{n-1}) \to \mathcal{H}om_{\Lambda_n}(\mathcal{F}_n, \mathcal{G}_{n-1})$. Combining this facts we conclude that our definition of $\mathcal{H}om_\Lambda(\mathcal{F}_\bullet, \mathcal{G}_\bullet)$ indeed defines a Λ-sheaf.

EXAMPLE 1.3.1.3 ([**SGA 5**, Exposé VI, Exemple 1.2.2]). The $\mathbb{Z}_\ell$-sheaves $\mathbb{Z}_{\ell,\bullet}(r)$:

Let ℓ be a prime number invertible on X. For every $n \in \mathbb{Z}$, we have a morphism of locally constant sheaves $(\cdot)^\ell : \mu_{l^{n+1},X} \to \mu_{l^n,X}$. They obviously define a $\mathbb{Z}_\ell$-sheaf on X denoted $\mathbb{Z}_{\ell,\bullet}(1) := (\mu_{\ell^{n+1},X})_{n\in\mathbb{N}}$. In fact, $\mathbb{Z}_{\ell,\bullet}(1)$ is a lisse $\mathbb{Z}_\ell$-sheaf. We extend the definition for $i \geq 1$ as $\mathbb{Z}_{\ell,\bullet}(i) := \mathbb{Z}_{\ell,\bullet}(1)^{\otimes_{\mathbb{Z}_\ell} i}$ and for $i = 0$ as $\mathbb{Z}_{\ell,\bullet}(0) = (\mathbb{Z}/\ell^{n+1}\mathbb{Z})_{n\in\mathbb{N}} = \mathbb{Z}_{\ell,\bullet}$. For $i < 0$ we set $\mathbb{Z}_{\ell,\bullet}(i) := \mathcal{H}om_{\mathbb{Z}_\ell}(\mathbb{Z}_{\ell,\bullet}(-i), \mathbb{Z}_{\ell,\bullet})$. Now, for every Λ-sheaf $\mathcal{F}_\bullet$ and $i \in \mathbb{Z}$ we define $\mathcal{F}_\bullet(i) := \mathcal{F}_\bullet \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_{\ell,\bullet}(i)$. By definition, the sheaves $\mathcal{F}_\bullet(i)$ coincide with $(\mathcal{F}_n \otimes_{\mathbb{Z}/\ell^{n+1}\mathbb{Z}} \mathbb{Z}/\ell^{n+1}\mathbb{Z}(i))_{n\in\mathbb{N}} = (\mathcal{F}_n(i))_{n\in\mathbb{N}}$. ■

It is natural to expect Λ-sheaves to verify a certain constructibility property similar to the one defined in Definition 1.2.4.1. The following is a precise statement:

PROPOSITION 1.3.1.4 ([**SGA 4½**, Rapport, Proposition 2.5],[**Con**, Theorem 1.4.4.7]). *Let $\mathcal{F}$ be a Λ-sheaf on a noetherian scheme X. There is a finite partition of X into locally closed subsets X_i such that $\mathcal{F}|_{X_i}$ is a lisse Λ-sheaf on each X_i.* □

Given a geometric point $\overline{x}$ of X and $\mathcal{F}_\bullet$ a Λ-sheaf on X, we define the stalk of $\mathcal{F}_\bullet$ at $\overline{x}$ as the inverse limit $\varprojlim(\mathcal{F}_n)_{\overline{x}}$. Since each stalk $(\mathcal{F}_n)_{\overline{x}}$ is a finitely generated Λ_n-module, obviously $(\mathcal{F}_\bullet)_{\overline{x}}$ is a finitely generated Λ-module (using that Λ is complete with respect to the $\mathfrak{m}$-adic topology). Using stalks and Theorem 1.2.4.3 we obtain the theorem:

THEOREM 1.3.1.5 ([**SGA 5**, Exposé VI, Proposition 1.2.5],[**Fu15**, Proposition 10.1.23]). *Let X be a connected noetherian scheme and $\overline{x}$ a geometric point of X. The functor $\mathcal{F}_\bullet \mapsto (\mathcal{F}_\bullet)_{\overline{x}}$ defines an equivalence of categories*

$$\left\{\textit{lisse } \Lambda\textit{-sheaves on } X_{\text{ét}}\right\} \longleftrightarrow \left\{\textit{finitely generated continuous } \Lambda[\pi_1(X,\overline{x})]\textit{-modules}\right\}.$$

Furthermore, if $f : Y \to X$ is a morphism between connected noetherian schemes and $\overline{y}$ is a geometric point of Y with $\overline{x} = f(\overline{y})$ the diagram

$$\begin{array}{ccc} \{\textit{lisse } \Lambda\textit{-sheaves on } Y_{\text{ét}}\} & \longleftrightarrow & \{\textit{finitely generated continuous } \Lambda[\pi_1(Y,\overline{y})]\textit{-modules}\} \\ {\scriptstyle f^*}\uparrow & & \uparrow \\ \{\textit{lisse } \Lambda\textit{-sheaves on } X_{\text{ét}}\} & \longleftrightarrow & \{\textit{finitely generated continuous } \Lambda[\pi_1(X,\overline{x})]\textit{-modules}\} \end{array}$$

is commutative, where the vertical right arrow is precomposition of the action with the homomorphism f_* introduced in Theorem 1.1.0.3.(b). □

REMARK 1.3.1.6. After Example 1.3.1.3 and Theorem 1.3.1.5 we know $\mathbb{Z}_{\ell,\bullet}(1)$ is equivalent to a $\mathbb{Z}_\ell$-module together with an action of $\pi_1(X,\overline{x})$. For our purposes, it is sufficient to describe it when $X = \texttt{Spec}\ k$ is a point with k a finite field. In this case, $\mathbb{Z}_{\ell,\bullet}(1) = (\mu_{\ell^{n+1},\texttt{Spec}\ k})_{n\in\mathbb{N}}$ and $(\mathbb{Z}_{\ell,\bullet}(1))_{\texttt{Spec}\ k^{\texttt{sep}}} = \varprojlim \mu_{\ell^{n+1}}(k^{\texttt{sep}}) \simeq \varprojlim \mathbb{Z}/\ell^{n+1}\mathbb{Z} \simeq \mathbb{Z}_\ell$ is the Tate module of $k^{\texttt{sep}}$. The action of $\texttt{Gal}(k^{\texttt{sep}}/k)$ on each $\mu_{\ell^{n+1}}(k^{\texttt{sep}})$ is the natural one which factors through the finite quotient $\texttt{Gal}(k(\mu_{\ell^{n+1}})/k)$. This last group is (non-canonically) isomorphic to $(\mathbb{Z}/\ell^{n+1}\mathbb{Z})^\times$ and $\texttt{Gal}(k(\mu_{\ell^\infty})/k) = \varprojlim \texttt{Gal}(k(\mu_{\ell^n})/k) \hookrightarrow \mathbb{Z}_\ell^\times$. The action we are considering of $\mathbb{Z}_\ell^\times$ on $\mathbb{Z}_\ell$ is just multiplication. The map

$$\texttt{Gal}(k(\mu_{\ell^\infty})/k) \hookrightarrow \mathbb{Z}_\ell^\times$$

precomposed with the projection (given by restriction)

$$\texttt{Gal}(k^{\texttt{sep}}/k) \to \texttt{Gal}(k(\mu_{\ell^\infty})/k)$$

is called the cyclotomic character. Under this character $\texttt{Frob}_k$ is mapped to $|k|^{-1}$ since $\texttt{Frob}_k$ is $t \mapsto t^{|k|^{-1}}$. By tensoring (or dualizing) we find $\mathbb{Z}_{\ell,\bullet}(n)$ on $\texttt{Spec}\ k$ corresponds to the ℓ-adic character of $\texttt{Gal}(k^{\texttt{sep}}/k)$ that sends $\texttt{Frob}_k$ to $|k|^{-n}$ for $n \in \mathbb{Z}$. ■

The category of K-sheaves has as objects the Λ-sheaves (this time denoted $\mathcal{F}_\bullet \otimes K$) and $\texttt{Hom}_K(\mathcal{F}_\bullet \otimes K, \mathcal{G}_\bullet \otimes K) = \texttt{Hom}_\Lambda(\mathcal{F}_\bullet, \mathcal{G}_\bullet) \otimes_\Lambda K$. The stalk of a K-sheaf $\mathcal{F}_\bullet \otimes K$ at a geometric point $\overline{x}$ of X is the finite dimensional K-vector space $(\mathcal{F}_\bullet)_{\overline{x}} \otimes_\Lambda K$. We say that $\mathcal{F}_\bullet \otimes K$ is a lisse K-sheaf if $\mathcal{F}_\bullet$ is a lisse Λ-sheaf. We denote $\Lambda(r) \otimes K$ by $K(r)$. It should be remarked that, intuitively, the step from Λ-sheaves to K-sheaves corresponds to the deletion of the torsion. We have the following equivalence of categories:

THEOREM 1.3.1.7 ([**Fu15**, Proposition 10.1.23]). *Let X be a connected noetherian scheme and $\overline{x}$ a geometric point of X. The functor $\mathcal{F}_\bullet \otimes K \mapsto (\mathcal{F}_\bullet)_{\overline{x}} \otimes_\Lambda K$ defines an equivalence between the category of lisse K-sheaves on X and the category of continuous K-linear representations of $\pi_1(X,\overline{x})$ on finite dimensional K-vector spaces.*

Furthermore, if $f : Y \to X$ is a morphism between connected noetherian schemes, $\overline{y}$ is a geometric point of Y with $\overline{x} = f(\overline{y})$ and $\mathcal{F}_\bullet \otimes K$ is a lisse K-sheaf on X with associated representation ρ, then the representation associated to $f^*(\mathcal{F}_\bullet \otimes K)$ is $\rho \circ f_*$ where f_* is the homomorphism introduced in Theorem 1.1.0.3.(b). □

If $\mathbb{Q}_\ell \subset K \subset L$ is a tower of finite extensions we can extend scalars and define, for each K-sheaf $\mathcal{F}_\bullet$, the L-sheaf $\mathcal{F}_\bullet \otimes_K L$. Taking this observation into account, we introduce $\overline{\mathbb{Q}}_\ell$-sheaves:

DEFINITION 1.3.1.8 ([**Con**, Definition 1.4.5.6]). Let X be a noetherian scheme, ℓ a prime and $\overline{\mathbb{Q}}_\ell$ an algebraic closure of $\mathbb{Q}_\ell$. The category of $\overline{\mathbb{Q}}_\ell$-sheaves on X is the category whose objects are triples $(\mathcal{F}_\bullet, K, \imath)$ where $\imath : K \hookrightarrow \overline{\mathbb{Q}}_\ell$ is an embedding of a finite extension of $\mathbb{Q}_\ell$ into $\overline{\mathbb{Q}}_\ell$ and $\mathcal{F}_\bullet$ is a K-sheaf, and $\texttt{Hom}_{\overline{\mathbb{Q}}_\ell}((\mathcal{F}_\bullet, K, \imath), (\mathcal{G}_\bullet, L, \jmath)) := \texttt{Hom}_{K''}(\mathcal{F}_\bullet \otimes_K K'', \mathcal{G}_\bullet \otimes_L K'') \otimes_{K''} \overline{\mathbb{Q}}_\ell$, where K'' is any finite extension of $\mathbb{Q}_\ell$ inside $\overline{\mathbb{Q}}_\ell$ containing both $\imath K$ and $\jmath L$. A $\overline{\mathbb{Q}}_\ell$-sheaf $(\mathcal{F}_\bullet, K, \imath)$ is lisse if $\mathcal{F}_\bullet$ is a lisse K-sheaf. We define the stalk of a $\overline{\mathbb{Q}}_\ell$-sheaf $(\mathcal{F}_\bullet, K, \imath)$ at a geometric point $\overline{x}$ of X as $(\mathcal{F}_\bullet)_{\overline{x}} \otimes_K \overline{\mathbb{Q}}_\ell$.

Let X be a connected scheme and $\overline{x}$ a geometric point of X. Let $\rho : \pi_1(X, \overline{x}) \to \mathtt{GL}(r, \overline{\mathbb{Q}}_\ell)$ be a finite dimensional $\overline{\mathbb{Q}}_\ell$-linear representation of $\pi_1(X, \overline{x})$. Since $\pi_1(X, \overline{x})$ is a profinite group, it is in particular a compact group. Hence the image of ρ is a compact subgroup of $\mathtt{GL}(r, \overline{\mathbb{Q}}_\ell)$ and after [**KS99**, Remark 9.0.7] (see also [**Con**, Proof of Theorem 1.4.5.7]) we know that it lies in $\mathtt{GL}(r, K)$ for some finite extension K of $\mathbb{Q}_\ell$ inside $\overline{\mathbb{Q}}_\ell$. Using this observation we obtain the following theorem:

THEOREM 1.3.1.9 ([**Fu15**, Corollary 10.1.24],[**Con**, Theorem 1.4.5.7]). *Let X be a connected noetherian scheme and $\overline{x}$ a geometric point of X. The functor $(\mathcal{F}_\bullet, K, \imath) \mapsto (\mathcal{F}_\bullet)_{\overline{x}} \otimes_K \overline{\mathbb{Q}}_\ell$ defines an equivalence between the category of lisse $\overline{\mathbb{Q}}_\ell$-sheaves on X and the category of continuous linear representations of $\pi_1(X, \overline{x})$ on finite dimensional $\overline{\mathbb{Q}}_\ell$-vector spaces.* □

We say the rank of a lisse $\overline{\mathbb{Q}}_\ell$-sheaf $\mathcal{F}$ on X is d if the associated $\overline{\mathbb{Q}}_\ell$-representation ρ of $\pi_1(X, \overline{x})$ has dimension d, i.e. $\rho : \pi_1(X, \overline{x}) \to \mathtt{GL}(d, \overline{\mathbb{Q}}_\ell)$.

1.3.2. ℓ-adic cohomology. Let X be a noetherian scheme and $\mathcal{F}_\bullet \otimes K$ a K-sheaf on X with $\mathcal{F}_\bullet$ a Λ-sheaf on X. We define its cohomology groups by $\mathtt{H}^i(X, \mathcal{F}_\bullet \otimes K) := (\varprojlim \mathtt{H}^i(X, \mathcal{F}_n)) \otimes_\Lambda K$. More generally, if $\mathcal{F} = (\mathcal{F}_\bullet \otimes K, K, \imath)$ is a $\overline{\mathbb{Q}}_\ell$-sheaf on X, we define

$$\mathtt{H}^i(X, \mathcal{F}) := \mathtt{H}^i(X, \mathcal{F}_\bullet \otimes K) \otimes_K \overline{\mathbb{Q}}_\ell.$$

Analogously, we define cohomology groups with compact support for K-sheaves $\mathcal{F}_\bullet \otimes K$ by $\mathtt{H}^i_{\mathtt{c}}(X, \mathcal{F}_\bullet \otimes K) := (\varprojlim \mathtt{H}^i_{\mathtt{c}}(X, \mathcal{F}_n)) \otimes_\Lambda K$ and for $\overline{\mathbb{Q}}_\ell$-sheaves $\mathcal{F} = (\mathcal{F}_\bullet \otimes K, K, \imath)$ by

$$\mathtt{H}^i_{\mathtt{c}}(X, \mathcal{F}) := \mathtt{H}^i_{\mathtt{c}}(X, \mathcal{F}_\bullet \otimes K) \otimes_K \overline{\mathbb{Q}}_\ell.$$

We are interested in the case X is a separated of finite type scheme over a separably closed field k. In this case, assuming ℓ is invertible on k, we use Corollary 1.2.6.5 to deduce that the cohomology groups of $\overline{\mathbb{Q}}_\ell$-sheaves on X are finitely generated $\overline{\mathbb{Q}}_\ell$-vector spaces vanishing for every degree except for finitely many of them. For cohomology with compact support we use Corollary 1.2.8.5 to find the analogous properties.

In general, for $f : X \to Y$ a separated finite-type morphism between noetherian schemes of finite type over a separably closed field k and $\mathcal{F}_\bullet$ a Λ-sheaf on X such that ℓ is invertible on k, we define $\mathtt{R}^i f_* \mathcal{F}_\bullet = (\mathtt{R}^i f_* \mathcal{F}_n)_{n \in \mathbb{N}}$. By Theorem 1.2.6.4 we find that $\mathtt{R}^i f_* \mathcal{F}_\bullet$ is again a Λ-sheaf on X. Similarly, using Theorem 1.2.8.4, we find the corresponding result for $\mathtt{R}^i f_! \mathcal{F}_\bullet$ (for more details see [**Con**, Theorem 1.4.6.1] or [**Fu15**, Proposition 10.1.18]). We extend our definitions to K-sheaves and $\overline{\mathbb{Q}}_\ell$-sheaves just embedding the result of the previous operations into the corresponding category.

1.3.3. Grothendieck's Lefschetz trace formula. Before stating Grothendieck's Lefschetz trace formula we introduce (following [**KS99**, §9.0 and §9.1]) the actors involved. Recall from Example 1.1.0.4 that if $k = \mathbb{F}_q$ is a finite field with q elements, we have $\mathtt{Gal}(k^{\mathtt{sep}}/k) \simeq \hat{\mathbb{Z}}$ with topological generator $x \mapsto x^q$. We denote the inverse of this generator by $\mathtt{Frob}_k$, called the geometric Frobenius.

Let X be a connected noetherian scheme and ξ a marked geometric point of X. Given a k-valued point $x \in X(k)$ and a geometric point $\overline{x} : \mathtt{Spec}\ k^{\mathtt{alg}} \to X$ lying over x, we obtain a canonical homomorphism

$$x_* : \pi_1(\mathtt{Spec}\ k, k^{\mathtt{alg}}) \to \pi_1(X, \overline{x}).$$

Using the isomorphism $\pi_1(\mathtt{Spec}\ k, k^{\mathtt{alg}}) \simeq \mathtt{Gal}(k^{\mathtt{sep}}/k)$, we consider $x_*(\mathtt{Frob}_k)$. Since the fundamental groups of X at different base points are all conjugate, the conjugacy class of $\mathtt{Frob}_{k,x}$ is well defined in the set of conjugacy classes $\pi_1(X, \xi)^\natural$ of the fundamental group of X based at ξ.

REMARK 1.3.3.1. For general $\overline{\mathbb{Q}}_\ell$-sheaves $\mathcal{F}$ we can define an action of $\mathtt{Frob}_k$ on $\mathcal{F}_{\overline{x}}$ as follows. As before, if X is a connected noetherian scheme, $x : \mathtt{Spec}\ k \to X$ is a k-valued point and $\mathcal{F}$ is a $\overline{\mathbb{Q}}_\ell$-sheaf on X, we consider its inverse image $x^*\mathcal{F}$ that is a $\overline{\mathbb{Q}}_\ell$-sheaf on $\mathtt{Spec}\ k$. Since $\overline{\mathbb{Q}}_\ell$-sheaves on a point $\mathtt{Spec}\ k$ are just finite dimensional $\overline{\mathbb{Q}}_\ell$-vector spaces $(x^*\mathcal{F})_{k^{\mathtt{sep}}} = \mathcal{F}_{\overline{x}}$ ($\overline{x}$ being the composition

of $x : \mathtt{Spec}\ k \to X$ with $\mathtt{Spec}\ k^{\mathtt{sep}} \to \mathtt{Spec}\ k$) endowed with a continuous action of $\mathtt{Gal}(k^{\mathtt{sep}}/k)$, we speak again of the action of $\mathtt{Frob}_k$ on the the stalk $\mathcal{F}_{\overline{x}}$ and its trace $\mathtt{Trace}(\mathtt{Frob}_k|\mathcal{F}_{\overline{x}})$. This action agrees with the action of (a representative of) $\mathtt{Frob}_{k,x}$ when $\mathcal{F}$ is lisse since the inverse image functor is compatible with the functoriality of fundamental groups.

When $\mathcal{F}$ is lisse with associated representation $\rho : \pi_1(X,\xi) \to \mathtt{GL}(r, \overline{\mathbb{Q}}_\ell)$, for every conjugacy class $\gamma \in \pi_1(X,\xi)^\natural$ we write $\mathtt{Trace}(\gamma|\mathcal{F}) := \mathtt{Trace}(\rho(\gamma))$, which is well defined since the trace is invariant under conjugation. ■

Finally for X a separated, connected noetherian scheme of finite type over a finite field k, fix an algebraic closure $k^{\mathtt{sep}}$ of k and let $\mathcal{F}$ be a $\overline{\mathbb{Q}}_\ell$-sheaf on X. We want to describe a $\mathtt{Gal}(k^{\mathtt{sep}}/k)$-module structure on the cohomology groups $\mathtt{H}^i_{\mathtt{c}}(X \otimes_k k^{\mathtt{sep}}, p^*\mathcal{F})$, where $p : X \otimes_k k^{\mathtt{sep}} \to X$ is the canonical projection. Let $\sigma \in \mathtt{Gal}(k^{\mathtt{sep}}/k)$. We consider the morphism $1 \otimes \sigma : X \otimes_k k^{\mathtt{sep}} \to X \otimes_k k^{\mathtt{sep}}$ which verifies $p \circ (1 \otimes \sigma) = p$. Now for $\alpha \in \mathtt{H}^i_{\mathtt{c}}(X \otimes_k k^{\mathtt{sep}}, p^*\mathcal{F})$ we define $\sigma\alpha := (1 \otimes \sigma)^*\alpha \in \mathtt{H}^i_{\mathtt{c}}(X \otimes_k k^{\mathtt{sep}}, (1\otimes\sigma)^*p^*\mathcal{F})$. Taking into account the equality $(1\otimes\sigma)^*p^* = p^*$ we get $\sigma\alpha \in \mathtt{H}^i_{\mathtt{c}}(X \otimes_k k^{\mathtt{sep}}, p^*\mathcal{F})$ and it defines an action of $\mathtt{Gal}(k^{\mathtt{sep}}/k)$. To simplify the notation we always denote $p^*\mathcal{F}$ directly by $\mathcal{F}$. After our construction, $\mathtt{H}^i_{\mathtt{c}}(X \otimes_k k^{\mathtt{sep}}, \mathcal{F})$ can be understood as a lisse $\overline{\mathbb{Q}}_\ell$-sheaf on $\mathtt{Spec}\ k$. Moreover, it can be checked [**Stacks**, tag 03ST] that this action coincides with the $\mathtt{Gal}(k^{\mathtt{sep}}/k)$ action on the stalk $(\mathtt{R}^i\pi_!\mathcal{F})_{k^{\mathtt{sep}}} \cong \mathtt{H}^i_{\mathtt{c}}(X \otimes_k k^{\mathtt{sep}}, \mathcal{F})$ where $\pi : X \to \mathtt{Spec}\ k$ is the structure morphism. Now all the terms in the following theorem have a meaning:

THEOREM 1.3.3.2 ([**KS99**, §9.0.14],[**SGA 4½**, Rapport, Théorème 3.2]). *Let X be a separated, connected noetherian scheme of finite type over a finite field k of dimension d and $\mathcal{F}$ a $\overline{\mathbb{Q}}_\ell$-sheaf on X. Then for every finite extension E/k we have*

$$\sum_{x \in X(E)} \mathtt{Trace}(\mathtt{Frob}_E|\mathcal{F}_{\overline{x}}) = \sum_{i=0}^{2d} (-1)^i \mathtt{Trace}(\mathtt{Frob}_E|\mathtt{H}^i_{\mathtt{c}}(X \otimes_k k^{\mathtt{alg}}, \mathcal{F})).$$ □

If we assume $\mathcal{F}$ to be lisse in the previous theorem, the traces $\mathtt{Trace}(\mathtt{Frob}_E|\mathcal{F}_{\overline{x}})$ are just $\mathtt{Trace}(\mathtt{Frob}_{E,x}|\mathcal{F})$ as already observed above.

1.3.4. Weights and Deligne's theorem. Let p be a prime number, $k/\mathbb{F}_p$ a finite field and $k^{\mathtt{alg}}$ an algebraic closure. We fix an isomorphism $\iota : \overline{\mathbb{Q}}_\ell \to \mathbb{C}$. Following [**Del80**, Définition 1.2.1] we say $\alpha \in \overline{\mathbb{Q}}_\ell$ is *pure of weight $w \in \mathbb{Z}$ relative to q* (q being a prime power) if it is algebraic and all the complex conjugates of $\iota\alpha$ are complex numbers with absolute value $q^{w/2}$. Such an α is also called a q-Weil number of weight w.

DEFINITION 1.3.4.1 ([**Del80**, Définition 1.2.2]). Let X be a separated of finite type scheme over k and $\mathcal{F}$ a $\overline{\mathbb{Q}}_\ell$-sheaf on X.

(a) We say $\mathcal{F}$ is punctually pure of weight w if for every closed point x of X, the eigenvalues of $\mathtt{Frob}_{k(x)}$ acting on $\mathcal{F}_{\overline{x}}$ (for $\overline{x}$ a geometric point of X over x) are $|k(x)|$-Weil numbers of weight w.
(b) We say $\mathcal{F}$ is mixed if it admits a finite filtration whose successive quotients are punctually pure $\overline{\mathbb{Q}}_\ell$-sheaves. If the weights of the non-zero quotients are bounded above by an integer w, we say $\mathcal{F}$ is mixed of weights $\leq w$.

More generally, we say $\alpha \in \overline{\mathbb{Q}}_\ell$ is ι-pure of weight $w \in \mathbb{Z}$ relative to q if it is algebraic and the complex absolute value of $\iota\alpha$ equals $q^{w/2}$. Analogously to the definitions of pure and mixed sheaves, we use the notion of ι-pure algebraic numbers to define [**Del80**, §1.2.6] ι-pure sheaves of weight w and ι-mixed sheaves of weight $\leq w$.

The main theorem of [**Del80**] is the following:

THEOREM 1.3.4.2 ([**Del80**, Théorème 3.3.1]). *Let $f : X \to Y$ be a separated morphism of schemes of finite type over k and $\mathcal{F}$ a $\overline{\mathbb{Q}}_\ell$-sheaf on X. If $\mathcal{F}$ is mixed of weights $\leq w$ then for every $i \in \mathbb{Z}$ the $\overline{\mathbb{Q}}_\ell$-sheaf $\mathtt{R}^i f_!\mathcal{F}$ over Y is mixed of weights $\leq w + i$.* □

This theorem has a direct corollary:

COROLLARY 1.3.4.3 ([**Del80**, Corollaire 3.3.4]). *Let X be a separated scheme of finite type over k and $\mathcal{F}$ a $\overline{\mathbb{Q}}_\ell$-sheaf mixed of weights $\leq w$. Then $\mathtt{H}^i_{\mathtt{c}}(X \otimes k^{\mathtt{alg}}, \mathcal{F})$ is a $\overline{\mathbb{Q}}_\ell$-sheaf on $\mathtt{Spec}\ k$ mixed of weights $\leq w + i$ for every i.* □

The combination of this theorem with Poincaré duality provides us with the following:

COROLLARY 1.3.4.4 ([**Del80**, Corollaire 3.3.5]). *Let X be a smooth scheme of finite type over k and $\mathcal{F}$ a lisse $\overline{\mathbb{Q}}_\ell$-sheaf mixed of weights $\geq w$. Then $\mathtt{H}^i(X \otimes k^{\mathtt{alg}}, \mathcal{F})$ is a $\overline{\mathbb{Q}}_\ell$-sheaf on $\mathtt{Spec}\ k$ mixed of weights $\geq w + i$ for every i.* □

1.3.5. $\mathcal{L}_\psi$, $\mathcal{L}_\chi$ and generalized Tate twists. We follow [**Kat88a**, §4.4.3], [**Kat90**, §7.2] and [**KS99**, §9.0.11]. Using the equivalence of Theorem 1.3.1.9 we give important examples of lisse $\overline{\mathbb{Q}}_\ell$-sheaves. Their relevance is that they will allow us to translate questions about exponential sums into questions about cohomology of $\overline{\mathbb{Q}}_\ell$-sheaves (see §1.4.2 for details).

EXAMPLE 1.3.5.1. Artin–Schreier and Kummer sheaves:

Let G be a smooth and connected commutative group scheme over a finite field $\mathbb{F}_q$. We denote by $F : G \to G$ the absolute Frobenius endomorphism of G relative to $\mathbb{F}_q$, i.e. it is the identity at the level of topological spaces and the q-th power on the structural (Zariski) sheaf of G. We define the *Lang isogeny* of G as $\mathcal{L} : x \in G \mapsto xF(x^{-1}) \in G$. The Lang isogeny is a finite étale Galois covering with Galois group $G(\mathbb{F}_q)$. $\mathcal{L}$ being an étale Galois covering with group $G(\mathbb{F}_q)$, there is a canonical surjection $\pi_1(G, \xi) \to G(\mathbb{F}_q)$. If $\rho : G(\mathbb{F}_q) \to \overline{\mathbb{Q}}_\ell{}^\times$ is a character with ℓ a prime number invertible on $\mathbb{F}_q$ and we precompose it with the previous canonical surjective homomorphism, we obtain a $\overline{\mathbb{Q}}_\ell$-representation of $\pi_1(G, \xi)$ of dimension 1. The associated sheaf $\mathcal{L}_\rho$ verifies the following properties [**Kat88a**, §4.4.3]:

(a) [**SGA 4½**, Sommes trigonométriques, §1.7.7] For any finite extension $k/\mathbb{F}_q$ and $a \in G(k)$, we have
$$\mathtt{trace}(\mathtt{Frob}_{k,a} | \mathcal{L}_\rho) = \rho(\mathtt{N}_{G(k)}(a))$$
where $\mathtt{N}_{G(k)}(a)$ denotes the norm of a in $G(k)$ under the action of $\mathtt{Gal}(k/\mathbb{F}_q)$, i.e. the product in $G(k)$ of all conjugates of a under $\mathtt{Gal}(k/\mathbb{F}_q)$.

(b) [**SGA 4½**, Sommes trigonométriques, §1.8.(ii)] For any finite extension $k/\mathbb{F}_q$, denote by $\pi : G \otimes_{\mathbb{F}_q} k \to G$ the canonical projection and by $\rho \circ \mathtt{trace}$ the composition $(G \otimes_{\mathbb{F}_q} k)(k) = G(k) \xrightarrow{\mathtt{trace}_{k/\mathbb{F}_q}} G(\mathbb{F}_q) \xrightarrow{\rho} \overline{\mathbb{Q}}_\ell{}^\times$. Then we have a canonical isomorphism of lisse $\overline{\mathbb{Q}}_\ell$-sheaves on $G \otimes_{\mathbb{F}_q} k$
$$\pi^*(\mathcal{L}_\rho) \cong \mathcal{L}_{\rho \circ \mathtt{trace}}.$$

(c) [**Lau87**, §1.1.3.2] Denote $\mathcal{H}om_{\overline{\mathbb{Q}}_\ell}(\mathcal{L}_\rho, \overline{\mathbb{Q}}_\ell)$ by $\mathcal{L}_\rho^\vee$. Then $\mathcal{L}_{\rho^{-1}} \cong \mathcal{L}_\rho^\vee$.

(d) [**SGA 4½**, Sommes trigonométriques, Théorème 2.7] If ρ is a non trivial character, then $\mathtt{H}^\bullet_{\mathtt{c}}(G \otimes k^{\mathtt{alg}}, \mathcal{L}_\rho) = 0$.

We specialize the previous construction to the group schemes $\mathbb{A}^1_{\mathbb{F}_q}$ and $\mathbb{G}_{m,\mathbb{F}_q}$. The Lang isogeny can be seen in an exact sequence as follows:

$$\begin{array}{ccccccccccc} 0 & \to & \mathbb{F}_q & \to & \mathbb{A}^1_{\mathbb{F}_q} & \xrightarrow{\mathcal{L}=x-x^q} & \mathbb{A}^1_{\mathbb{F}_q} & \to & 0 & \text{for} & G = \mathbb{A}^1_{\mathbb{F}_q}, \\ 1 & \to & \mu_{q-1} & \to & \mathbb{G}_{m,\mathbb{F}_q} & \xrightarrow{\mathcal{L}=x^{1-q}} & \mathbb{G}_{m,\mathbb{F}_q} & \to & 1 & \text{for} & G = \mathbb{G}_{m,\mathbb{F}_q}. \end{array}$$

If $\psi : \mathbb{F}_q \to \overline{\mathbb{Q}}_\ell{}^\times$ is an additive character, we obtain a lisse rank one $\overline{\mathbb{Q}}_\ell$-sheaf on $\mathbb{A}^1_{\mathbb{F}_q}$ denoted by $\mathcal{L}_\psi$ and called *Artin–Schreier sheaf*. If $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}_\ell{}^\times$ is a multiplicative character, we obtain a lisse rank one $\overline{\mathbb{Q}}_\ell$-sheaf on $\mathbb{G}_{m,\mathbb{F}_q}$ denoted by $\mathcal{L}_\chi$ and called *Kummer sheaf*. More generally, for any morphism of schemes $f : X \to \mathbb{A}^1_{\mathbb{F}_q}$ and additive character $\psi : \mathbb{F}_q \to \overline{\mathbb{Q}}_\ell{}^\times$ (resp. $f : X \to \mathbb{G}_{m,\mathbb{F}_q}$ and multiplicative character $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}_\ell{}^\times$) we denote $\mathcal{L}_{\psi(f)} := f^*\mathcal{L}_\psi$ (resp. $\mathcal{L}_{\chi(f)} := f^*\mathcal{L}_\chi$). ■

EXAMPLE 1.3.5.2. $\overline{\mathbb{Q}}_\ell$-Tate twist and generalized Tate twists:

Let $k = \mathbb{F}_q$ be a finite field and ℓ a prime number invertible in k. For every $n \in \mathbb{Z}$ consider the character of $\mathtt{Gal}(k^{\mathtt{alg}}/k)$ that sends $\mathtt{Frob}_k$ to q^{-n}. It defines a lisse rank one $\overline{\mathbb{Q}}_\ell$-sheaf on $\mathtt{Spec}\ k$ denoted by $\overline{\mathbb{Q}}_\ell(n)$. After Remark 1.3.1.6, our definition of $\overline{\mathbb{Q}}_\ell(n)$ is the natural extension of our previous notions of Tate twist.

In general, let α be a unit in the ring of integers of $\overline{\mathbb{Q}}_\ell$ and denote by $\alpha^{\mathtt{deg}}$ the lisse rank one $\overline{\mathbb{Q}}_\ell$-sheaf on $\mathtt{Spec}\ k$ associated to the representation $\mathtt{Frob}_k \in \mathtt{Gal}(k^{\mathtt{sep}}/k) \mapsto \alpha$. This way, $\overline{\mathbb{Q}}_\ell(-n)$ is just $\alpha^{\mathtt{deg}}$ with $\alpha = q^n$.

More generally, for any morphism $f : X \to \mathtt{Spec}\ k$ we again denote by $\overline{\mathbb{Q}}_\ell(n)$ and $\alpha^{\mathtt{deg}}$ the pullback along f of the corresponding sheaves on $\mathtt{Spec}\ k$. As characters of $\pi_1(X, \xi)$ (assuming X good enough), they take the value $|E|^n$ and $\alpha^{\mathtt{deg}(E/k)}$ respectively on the Frobenius conjugacy class $\mathtt{Frob}_{E,x}$. For any lisse $\overline{\mathbb{Q}}_\ell$-sheaf $\mathcal{F}$ on X, we denote $\mathcal{F}(n) := \mathcal{F} \otimes_{\overline{\mathbb{Q}}_\ell} \overline{\mathbb{Q}}_\ell(n)$ and $\mathcal{F} \otimes \alpha^{\mathtt{deg}} := \mathcal{F} \otimes_{\overline{\mathbb{Q}}_\ell} \alpha^{\mathtt{deg}}$. When $\alpha \in \overline{\mathbb{Q}}_\ell$ is a square root of $1/q$ we write $\mathcal{F}(1/2) := \mathcal{F} \otimes \alpha^{\mathtt{deg}}$ and call it the half-Tate twist.

It should be observed that we can describe the sheaf $\alpha^{\mathtt{deg}}$ just as the $\overline{\mathbb{Q}}_\ell$-sheaf associated to the composition of the mentioned character $\mathtt{Frob}_k \mapsto \alpha$ with the surjective group homomorphism $\mathtt{deg} : \pi_1(X, x) \to \mathtt{Gal}(k^{\mathtt{sep}}/k)$ of Theorem 1.1.0.5. Using the exact sequence of the theorem we see that, as a character, $\alpha^{\mathtt{deg}}$ vanishes on the geometric fundamental group and they are all the "characters" with such property. ■

1.4. Trace functions and exponential sums

1.4.1. Trace functions.

Let $\mathbb{F}_q$ be a finite field and ℓ a prime number invertible on $\mathbb{F}_q$. While stating Grothendieck's Lefschetz trace formula we have seen that, for every $\overline{\mathbb{Q}}_\ell$-sheaf on a good enough $\mathbb{F}_q$-scheme X and $\mathcal{F}$ a $\overline{\mathbb{Q}}_\ell$-sheaf on X, we can define functions from the sets of E-valued points of X to $\overline{\mathbb{Q}}_\ell$ for every finite extension $E/\mathbb{F}_q$ as follows:

> Given $x \in X(E)$ we know $x^*(\mathcal{F})_{E^{\mathtt{alg}}}$ is a $\overline{\mathbb{Q}}_\ell[\mathtt{Gal}(E^{\mathtt{sep}}/E)]$-module. If $\overline{x}$ is defined by the composition of $x : \mathtt{Spec}\ E \to X$ and $\mathtt{Spec}\ E^{\mathtt{alg}} \to \mathtt{Spec}\ E$, then $(x^*\mathcal{F})_{E^{\mathtt{alg}}} = \mathcal{F}_{\overline{x}}$. We define $\mathtt{tr}_{\mathcal{F},E} : X(E) \to \overline{\mathbb{Q}}_\ell$ by $x \mapsto \mathtt{Trace}(\mathtt{Frob}_E | \mathcal{F}_{\overline{x}})$.

The trace function of a $\overline{\mathbb{Q}}_\ell$-sheaf $\mathcal{F}$ is the collection of functions $\mathtt{tr}_{\mathcal{F}} := (\mathtt{tr}_{\mathcal{F},\mathbb{F}_{q^n}})_{n\in\mathbb{N}}$. They verify the following properties [**Lau87**, §1.1]:

(a) For every pair of $\overline{\mathbb{Q}}_\ell$-sheaves $\mathcal{F}$ and $\mathcal{G}$ on X we have $\mathtt{tr}_{\mathcal{F}\oplus\mathcal{G}} = \mathtt{tr}_{\mathcal{F}} + \mathtt{tr}_{\mathcal{G}}$.
(b) For $\mathcal{F}$ and $\mathcal{G}$ $\overline{\mathbb{Q}}_\ell$-sheaves on X we have $\mathtt{tr}_{\mathcal{F}\otimes\mathcal{G}} = \mathtt{tr}_{\mathcal{F}} \cdot \mathtt{tr}_{\mathcal{G}}$.
(c) For every morphism of $\mathbb{F}_q$-schemes $f : X \to Y$ between $\mathbb{F}_q$-schemes of finite type and every $\overline{\mathbb{Q}}_\ell$-sheaf $\mathcal{F}$ on Y we have $\mathtt{tr}_{f^*\mathcal{F}} = \mathtt{tr}_{\mathcal{F}} \circ f$.
(d) Taking $f : X \to Y$ as in the previous item, Grothendieck's Lefschetz trace formula and the properties of $\mathtt{R}^i f_!$ provide us, for every $\overline{\mathbb{Q}}_\ell$-sheaf $\mathcal{F}$ and every point $y \in Y(\mathbb{F}_{q^n})$, with the (integration) identity

$$\begin{aligned}\sum_{i=0}^{\infty}(-1)^i \mathtt{Trace}(\mathtt{Frob}_{\mathbb{F}_{q^n}} | (\mathtt{R}^i f_! \mathcal{F})_{\overline{y}}) &= \sum_{i=0}^{\infty}(-1)^i \mathtt{Trace}(\mathtt{Frob}_{\mathbb{F}_{q^n}} | \mathtt{H}^i_{\mathtt{c}}(X_{\overline{y}}, \mathcal{F}|_{X_{\overline{y}}})) \\ &= \sum_{x \in X_{\overline{y}}(\mathbb{F}_{q^n})} \mathtt{Trace}(\mathtt{Frob}_{\mathbb{F}_{q^n}} | (\mathcal{F}|_{X_{\overline{y}}})_{\overline{x}}) \\ &= \sum_{\substack{x \in X(\mathbb{F}_{q^n}) \\ f(x)=y}} \mathtt{Trace}(\mathtt{Frob}_{\mathbb{F}_{q^n}} | \mathcal{F}_{\overline{x}}).\end{aligned}$$

1.4.2. Exponential sums.

1.4.2.1. *Fourier transform on finite abelian groups.* In order to describe Gauss sums and Kloosterman sums in a convenient way we briefly review the Fourier transform of complex-valued functions on finite abelian groups. Let G be a finite abelian group and define its Pontryagin dual $G^\vee$ as the group of all homomorphisms from G to $\mathbb{S}^1$. It is well known that for every character $\chi : G \to \mathbb{C}^\times$ the sum $\sum_{g\in G}\chi(g) = 0$ if $\chi \neq \mathbf{1}$ and $|G|$ if $\chi = \mathbf{1}$. Dually, if $g \in G$ then $\sum_{\chi\in G^\vee}\chi(g) = 0$ if $g \neq 0$ and $|G|$ if $g = 0$.

Now for any complex-valued function $f : G \to \mathbb{C}$ we define its Fourier transform as the complex-valued function

$$\begin{array}{rccc} \mathtt{FT}_G f: & G^\vee & \to & \mathbb{C} \\ & \chi & \mapsto & \sum_{g\in G} f(g)\chi(g). \end{array}$$

We can recover f from $\mathtt{FT}_G f$ via Fourier inversion formula

$$f(g) = \frac{1}{|G|}\sum_{\chi\in G^\vee}\overline{\chi}(g)(\mathtt{FT}_G f)(\chi).$$

Indeed, if we expand the term on the right we get:

$$\sum_{\chi\in G^\vee}\overline{\chi}(g)\sum_{h\in G} f(h)\chi(h) = \sum_{h\in G} f(h)\sum_{\chi\in G^\vee}\chi(h-g) = |G|f(g).$$

Given two complex-valued functions $f, g : G \to \mathbb{C}^\times$ their convolution product $f * g$ is the complex-valued function defined by $(f*g)(h) = \sum_{x+y=h} f(x)g(y)$. It holds that the Fourier transform of a convolution is the product of the Fourier transform of the functions: $\mathtt{FT}_G(f*g) = (\mathtt{FT}_G f)(\mathtt{FT}_G g)$. By Fourier inversion formula we find

$$\sum_{h\in G} f(h)g(-h) = (f*g)(0) = \frac{1}{|G|}\sum_{\chi\in G^\vee}\overline{\chi}(0)\mathtt{FT}_G(f*g)(\chi) = \frac{1}{|G|}\sum_{\chi\in G^\vee}(\mathtt{FT}_G f)(\chi)(\mathtt{FT}_G g)(\chi).$$

Using in the previous equality the function $g^*(h) = \overline{g(-h)}$ instead of g and noting that $\mathtt{FT}_G(g^*) = \overline{\mathtt{FT}_G g}$, we arrive at *Parseval's identity*

$$\sum_{h\in G} f(h)\overline{g(h)} = \frac{1}{|G|}\sum_{\chi\in G^\vee}(\mathtt{FT}_G f)(\chi)\overline{\mathtt{FT}_G g(\chi)}.$$

1.4.2.2. *Gauss sums, Jacobi sums and Kloosterman sums.* In this section we fix an isomorphism $\iota : \overline{\mathbb{Q}}_\ell \to \mathbb{C}$ and tacitly identify both fields.

Let $k = \mathbb{F}_q$ be a finite field with $\mathtt{char}(k) = p$ and $\psi : k \to \overline{\mathbb{Q}}_\ell^{\times}$ the additive character $\psi(t) = \mathtt{exp}(2\pi i \mathtt{trace}_{k/\mathbb{F}_p}(t)/p)$. We extend every multiplicative character $\chi : k^\times \to \mathbb{C}^\times$ as a complex-valued function $\chi : k \to \mathbb{C}$ by setting $\chi(0) = 0$. We define *Gauss sums* by

$$\tau(\psi,\chi) := -\sum_{t\in k^\times}\psi(t)\chi(t).$$

Clearly, $\tau(\psi,\chi)$ coincides with $-(\mathtt{FT}_k\chi)(\psi)$ and with $-(\mathtt{FT}_{k^\times}\psi|_{k^\times})(\chi)$. Using Fourier inversion formula we find $\chi(t) = \frac{-1}{q}\sum_{\psi'\in k^\vee}\tau(\overline{\psi'},\chi)\psi'(t)$ for $t \in k$ and $\psi(t) = \frac{-1}{q-1}\sum_{\chi'\in(k^\times)^\vee}\tau(\psi,\overline{\chi'})\chi'(t)$ for $t \in k^\times$. The following properties can be verified easily:

(a) If $\chi = \mathbf{1}$ is the trivial character, then $\tau(\psi,\chi) = 1$. If $\psi' = \mathbf{1}$ is the trivial character and χ is non trivial, then $\tau(\psi',\chi) = 0$. If both ψ' and χ are trivial then $\tau(\psi',\chi) = 1 - q$.
(b) If ${}^a\psi, a \in k^\times$, is the additive character ${}^a\psi(x) := \psi(ax)$, then $\tau({}^a\psi,\chi) = \chi(a^{-1})\tau(\psi,\chi)$.
(c) If $\chi \neq \mathbf{1}$ then $\overline{\tau(\psi,\chi)} = \chi(-1)\tau(\psi,\overline{\chi})$. Moreover $\tau(\psi,\chi)\overline{\tau(\psi,\chi)} = q$.
(d) If $\chi \neq \mathbf{1}$ then $\tau(\psi,\chi^p) = \tau(\psi,\chi\circ\mathtt{Frob}_{k/\mathbb{F}_p}) = \tau(\psi,\chi)$.

In a more general way, let $k_r = \mathbb{F}_{q^r}$ and for $\psi : k \to \mathbb{C}^\times$ and $\chi : k \to \mathbb{C}^\times$ two characters (ψ non trivial) denote by $\psi_{k_r} := \psi\circ\mathtt{trace}_{k_r/k}$ (or simply ψ_r) and $\chi_{k_r} := \chi\circ\mathtt{N}_{k_r/k}$ (or simply χ_r). With these notations, we have the following two relations due to Hasse and Davenport:

(a) *Hasse–Davenport lifting identity:* [**DH35**, (0.8)] For every $r \geq 1$,

$$\tau(\psi_r, \chi_r) = \tau(\psi, \chi)^r.$$

(b) *Hasse–Davenport product identity:* [**DH35**, (0.9_1)] Let N be a divisor of $q-1$ and denote by $\rho_1, \dots, \rho_N$ the N multiplicative characters of $k^\times$ of order dividing N. Then for any multiplicative character χ of $k^\times$ the following identity holds:

$$\tau(\psi^N, \chi^N) \prod_{i=1}^{N} \tau(\psi, \rho_i) = \prod_{i=1}^{N} \tau(\psi, \chi\rho_i).$$

Observe that in the last identity ψ^N is just the product of ψ with itself N times, hence $\psi^N(t) = \psi(Nt)$ for all $t \in k$ so $\tau(\psi^N, \chi^N) = \chi^{-N}(N)\tau(\psi, \chi^N)$.

Related to Gauss sums we have *Jacobi sums* which we introduce here: given multiplicative characters $\chi, \eta \in (k^\times)^\vee$ define

$$\mathtt{J}(\chi, \eta) := -\sum_{\substack{x,y \in k^\times \\ x+y=1}} \chi(x)\eta(y) = -\sum_{x \in k^\times \setminus \{1\}} \chi(x)\eta(1-x).$$

They satisfy the following properties:

(a) $\mathtt{J}(\chi, \eta) = \mathtt{J}(\eta, \chi)$.
(b) $\mathtt{J}(\mathbf{1}, \mathbf{1}) = 2 - q$.
(c) If $\chi \neq \mathbf{1}$ then $\mathtt{J}(\chi, \mathbf{1}) = 1$.
(d) If $\chi \neq \mathbf{1}$ then $\mathtt{J}(\chi, \chi^{-1}) = \chi(-1)$.
(e) For every χ, η with $\chi\eta \neq \mathbf{1}$ and $\psi \in k^\vee$ a nontrivial additive character, $\tau(\psi, \chi\eta)\mathtt{J}(\chi, \eta) = \tau(\psi, \chi)\tau(\psi, \eta)$. In particular, if $\chi, \eta, \chi\eta \neq \mathbf{1}$ then $\mathtt{J}(\chi, \eta)\overline{\mathtt{J}(\chi, \eta)} = q$.

We show the last property:

$$\begin{aligned}
\tau(\psi, \chi)\tau(\psi, \eta) &= \Big(-\sum_{x \in k^\times} \psi(x)\chi(x) \Big) \Big(-\sum_{y \in k^\times} \psi(y)\eta(y) \Big) \\
&= \sum_{x,y \in k^\times} \psi(x+y)\chi(x)\eta(y) = \sum_{t \in k} \psi(t) \sum_{\substack{x,y \in k^\times \\ x+y=t}} \chi(x)\eta(y) \\
&= \sum_{t \in k^\times} \psi(t) \sum_{\substack{x,y \in k^\times \\ x+y=1}} \chi(tx)\eta(ty) = \Big(\sum_{t \in k^\times} \psi(t)(\chi\eta)(t) \Big) \Big(\sum_{\substack{x,y \in k^\times \\ x+y=1}} \chi(x)\eta(y) \Big) \\
&= \tau(\psi, \chi\eta)\mathtt{J}(\chi, \eta).
\end{aligned}$$

Combining this with Hasse–Davenport identity we obtain:

(a) Let $\chi, \eta \in (k^\times)^\vee$ with $\chi\eta \neq \mathbf{1}$, then $\mathtt{J}(\chi_r, \eta_r) = \mathtt{J}(\chi, \eta)^r$. If $\chi\eta = \mathbf{1}$ the identity holds trivially.
(b) [**DH35**, (0.9_2)] Let N be a divisor of $q-1$ and $\chi \in (k^\times)^\vee$ such that $\chi^N \neq \mathbf{1}$. If we denote the set of multiplicative characters of k of order dividing N by $\rho_1, \dots, \rho_N$, then $\rho_i\chi \neq \mathbf{1}$ and

$$\prod_{i=1}^{N} \mathtt{J}(\rho_i, \chi) = \frac{\tau(\psi, \chi)^N}{\tau(\psi^N, \chi^N)}.$$

Another famous family of exponential sums are *Kloosterman sums*: For any $n \in \mathbb{N} \setminus \{0\}$ and $a \in k^\times$ we define

$$\mathtt{Kloos}_n(q; a) := \sum_{\substack{x_1, \dots, x_n \in k \\ x_1 \cdots x_n = a}} \psi(x_1 + \cdots + x_n).$$

These sums are further generalized by the expressions

$$\sum_{\substack{x_1,\dots,x_n\in k^\times\\ x_1^{b_1}\cdots x_n^{b_n}=a}} \psi(x_1+\cdots+x_n)\chi_1(x_1)\cdots\chi_n(x_n),$$

where $\chi_1,\dots,\chi_n$ are multiplicative characters of $k^\times$ and $b_1,\dots,b_n\in\mathbb{Z}$ are integers. The relation between this family and Gauss sums is the following:

PROPOSITION 1.4.2.1 ([**Kat88a**, Chapter 4], [**Kat80**, Lemme 2.4.1.1]). *Define the function $f:k^\times\to\overline{\mathbb{Q}}_\ell$ by the expression $f(a)=\sum_{x_1,\dots,x_n\in k^\times;\ x_1^{b_1}\cdots x_n^{b_n}=a}\psi(x_1+\cdots+x_n)\chi_1(x_1)\cdots\chi_n(x_n)$ where χ_i are multiplicative characters of $k^\times$ and b_i integers. Then*

$$(\mathtt{FT}_{k^\times}f)(\chi)=(-1)^n\cdot\prod_{i=1}^n\tau(\psi,\chi^{b_i}\cdot\chi_i)$$

for every multiplicative character χ of $k^\times$.

PROOF. The result follows from the case $n=1$. Indeed, write $f_i(a)=\sum_{x\in k^\times;\ x^{b_i}=a}\psi(x)\chi_i(x)$, and consider the convolution product

$$\begin{aligned}(f_1*\cdots*f_n)(a)&=\sum_{\substack{y_1,\dots,y_n\in k^\times\\ y_1\cdots y_n=a}}\prod_{i=1}^n f_i(y_i)\\
&=\sum_{\substack{y_1,\dots,y_n\in k^\times\\ y_1\cdots y_n=a}}\prod_{i=1}^n\sum_{\substack{x_i\in k^\times\\ x_i^{b_i}=y_i}}\psi(x_i)\chi_i(x_i)\\
&=\sum_{\substack{y_1,\dots,y_n\in k^\times\\ y_1\cdots y_n=a}}\ \sum_{\substack{x_1,\dots,x_n\in k^\times\\ \forall i\ x_i^{b_i}=y_i}}\psi(x_1+\cdots+x_n)\chi_1(x_1)\cdots\chi_n(x_n)\\
&=\sum_{\substack{x_1,\dots,x_n\in k^\times\\ x_1^{b_1}\cdots x_n^{b_n}=a}}\psi(x_1+\cdots+x_n)\chi_1(x_1)\cdots\chi_n(x_n)=f(a).\end{aligned}$$

Hence $\mathtt{FT}_{k^\times}f=\prod_{i=1}^n\mathtt{FT}_{k^\times}f_i$. For $n=1$, let $f(a):=\sum_{x\in k^\times;x^b=a}\psi(x)\chi(x)$. Then

$$\begin{aligned}(\mathtt{FT}_{k^\times}f)(\eta)&=\sum_{a\in k^\times}\eta(a)f(a)=\sum_{a\in k^\times}\eta(a)\sum_{\substack{x\in k^\times\\ x^b=a}}\psi(x)\chi(x)\\
&=\sum_{\substack{a,x\in k^\times\\ x^b=a}}\psi(x)\eta(x^b)\chi(x)=\sum_{x\in k^\times}\psi(x)(\eta^b\cdot\chi)(x)\\
&=-\tau(\psi,\eta^b\cdot\chi).\end{aligned}$$

□

COROLLARY 1.4.2.2. *The functions $\mathtt{Kloos}_n(q;\cdot):k^\times\to{\overline{\mathbb{Q}}_\ell}^\times$ and $(-\tau(\psi,\cdot))^n:(k^\times)^\vee\to{\overline{\mathbb{Q}}_\ell}^\times$ are Fourier transforms of each other. Explicitly, for every $a\in k^\times$ we have the identity*

$$\mathtt{Kloos}_n(q;a)=\frac{(-1)^n}{q-1}\sum_{\chi\in(k^\times)^\vee}\overline{\chi}(a)\tau(\psi,\chi)^n$$

and for every $\chi\in(k^\times)^\vee$ the identity

$$(-\tau(\psi,\chi))^n=\sum_{a\in k^\times}\chi(a)\mathtt{Kloos}_n(q;a).$$

□

We obtain the following estimate for the absolute value of Kloosterman sums due to Carlitz (compare with Deligne's amazing improvement below):

COROLLARY 1.4.2.3 ([**Kat80**, Corollaire 2.4.1.2]). *For every $n \in \mathbb{N} \setminus \{0\}$, we have*

$$\sum_{a \in k^\times} |\mathtt{Kloos}_n(q;a)|^2 = q^n - (q^{n-1} + q^{n-2} + \cdots + q + 1).$$

In particular, for every $a \in k^\times$, we have the bound $|\mathtt{Kloos}_n(q;a)| < q^{n/2}$.

PROOF. Parseval's identity with $f = g = \mathtt{Kloos}_n(q;\cdot)$ gives the equality

$$\sum_{a \in k^\times} |\mathtt{Kloos}_n(q;a)|^2 = \frac{1}{q-1} \sum_{\chi \in (k^\times)^\vee} |\tau(\psi,\chi)|^{2n}.$$

Since $|\tau(\psi,\chi)|^2 = q$ for $\chi \neq \mathbf{1}$ and $|\tau(\psi,\mathbf{1})|^2 = 1$, we find

$$\begin{aligned}\sum_{a \in k^\times} |\mathtt{Kloos}_n(q;a)|^2 &= \frac{1}{q-1}(1 + (q-2)q^n) \\ &= \frac{1}{q-1}((q-1)q^n - (q^n - 1)) \\ &= q^n - (q^{n-1} + \cdots + 1).\end{aligned}$$

□

1.4.2.3. *Cohomological interpretation of exponential sums.* ℓ-adic cohomology has quite concrete applications to the study of exponential sums. Here we show how some classical properties of character and exponential sums have a geometrical interpretation. The key step in constructing this dictionary is to observe that Artin–Schreier and Kummer sheaves are the correct geometric replacement of additive and multiplicative characters. Indeed, for every additive character $\psi : k \to \overline{\mathbb{Q}}_\ell{}^\times$, the Artin–Schreier sheaf $\mathcal{L}_\psi$ on $\mathbb{A}^1_k$ is a lisse $\overline{\mathbb{Q}}_\ell$-sheaf of rank 1 whose trace function is given by $\mathtt{tr}_{\mathcal{L}_\psi,k_r} = \psi_r$. Similarly, for every multiplicative character $\chi : k^\times \to \overline{\mathbb{Q}}_\ell{}^\times$, the Kummer sheaf $\mathcal{L}_\chi$ on $\mathbb{G}_{m,k}$ is a lisse $\overline{\mathbb{Q}}_\ell$-sheaf of rank 1 whose trace function is given by $\mathtt{tr}_{\mathcal{L}_\chi,k_r} = \chi_r$.

Now we can translate the vanishing of the cohomology groups $\mathtt{H}^\bullet_{\mathtt{c}}(\mathbb{A}^1_k \otimes k^{\mathtt{alg}}, \mathcal{L}_\psi)$ and $\mathtt{H}^\bullet_{\mathtt{c}}(\mathbb{G}_{m,k} \otimes k^{\mathtt{alg}}, \mathcal{L}_\chi)$ into the classical orthogonality of characters: $\sum_{t \in k_r} \psi_r(t) = 0$ and $\sum_{t \in k_r^\times} \chi_r(t) = 0$. Indeed,

$$\sum_{t \in k_r} \psi_r(t) = \sum_{t \in \mathbb{A}^1_k(k_r)} \mathtt{tr}_{\mathcal{L}_\psi,k_r}(t) = \sum_{i=0}^{2} (-1)^i \mathtt{Trace}(\mathtt{Frob}_{k_r} | \mathtt{H}^i_{\mathtt{c}}(\mathbb{A}^1_k \otimes k^{\mathtt{alg}}, \mathcal{L}_\psi)).$$

Similarly for χ and $\mathcal{L}_\chi$.

To realize Gauss sums as trace functions we proceed as follows: let $j : \mathbb{G}_{m,k} \to \mathbb{A}^1_k$ be the open inclusion and consider $j^*\mathcal{L}_\psi$ the restriction of $\mathcal{L}_\psi$ to $\mathbb{G}_{m,k}$. Then

$$\begin{aligned}-\tau(\psi_r,\chi_r) &= \sum_{t \in \mathbb{G}_{m,k}(k_r)} \mathtt{tr}_{j^*\mathcal{L}_\psi,k_r}(t) \cdot \mathtt{tr}_{\mathcal{L}_\chi,k_r}(t) = \sum_{t \in \mathbb{G}_{m,k}(k_r)} \mathtt{tr}_{\mathcal{L}_\chi \otimes j^*\mathcal{L}_\psi,k_r}(t) \\ &= \sum_{i=0}^{2} (-1)^i \mathtt{Trace}(\mathtt{Frob}_{k_r} | \mathtt{H}^i_{\mathtt{c}}(\mathbb{G}_{m,k} \otimes k^{\mathtt{alg}}, \mathcal{L}_\chi \otimes j^*\mathcal{L}_\psi))\end{aligned}$$

In fact we know more thanks to the following result of Deligne:

PROPOSITION 1.4.2.4 ([**SGA 4½**, Sommes trigonométriques, Proposition 4.2]). *The cohomology of $\mathbb{G}_{m,k}$ with coefficients in $\mathcal{L}_\chi \otimes j^*\mathcal{L}_\psi$ satisfies*

(a) $\mathtt{H}^i_{\mathtt{c}} = 0$ *for $i \neq 1$ and $\mathtt{H}^1_{\mathtt{c}}$ is a one dimensional $\overline{\mathbb{Q}}_\ell$-vector space.*

(b) *If χ is non trivial then the canonical morphisms $\mathtt{H}^\bullet_{\mathtt{c}} \to \mathtt{H}^\bullet$ are isomorphisms at every degree.* □

Mixing up our previous formula and this proposition we deduce the equality

$$\mathtt{Trace}(\mathtt{Frob}_{k_r}|\mathtt{H}^1_{\mathtt{c}}(\mathbb{G}_{m,k}\otimes k^{\mathtt{alg}},\mathcal{L}_\chi\otimes j^*\mathcal{L}_\psi)) = \tau(\psi_r,\chi_r),$$

which realizes Gauss sums as the trace function of a lisse $\overline{\mathbb{Q}}_\ell$-sheaf on $\mathtt{Spec}\ k$. Since $\mathtt{H}^1_{\mathtt{c}}(\mathbb{G}_{m,k}\otimes k^{\mathtt{alg}},\mathcal{L}_\chi\otimes j^*\mathcal{L}_\psi)$ is one dimensional we obtain the stronger fact that the action of $\mathtt{Frob}_{k_r}$ on $\mathtt{H}^1_{\mathtt{c}}$ is multiplication by $\tau(\psi_r,\chi_r)$. Actually, this allows us to give a geometric proof of Hasse–Davenport lifting identity. Indeed, the action of $\mathtt{Frob}_{k_r}$ on $\mathtt{H}^1_{\mathtt{c}}$ has as unique eigenvalue the number $\tau(\psi_r,\chi_r)$ but $\mathtt{Frob}_{k_r} = \mathtt{Frob}_k^r$ hence it also have the eigenvalue $\tau(\psi,\chi)^r$ and both must coincide. The geometric interpretation of Hasse–Davenport product identity is more involved but possible, see [**Kat88a**, Proposition 5.6.2 and Remark 5.6.3] for details.

To ilustrate one more time how to derive properties of Gauss sums from geometric properties, we translate the identiy $\tau(\psi_r,\chi_r)\overline{\tau(\psi_r,\chi_r)} = q^r$. Since $\mathtt{H}^1_{\mathtt{c}} \simeq \mathtt{H}^1$, by Poincaré duality we deduce that $\mathtt{H}^1_{\mathtt{c}}(\mathbb{G}_{m,k}\otimes k^{\mathtt{alg}},\mathcal{L}_\chi\otimes j^*\mathcal{L}_\psi)$ and $\mathtt{H}^1_{\mathtt{c}}(\mathbb{G}_{m,k}\otimes k^{\mathtt{alg}},\mathcal{L}_{\overline{\chi}}\otimes j^*\mathcal{L}_{\overline{\psi}})$ are in perfect duality with values in $\overline{\mathbb{Q}}_\ell(-1)$. Using again that we know the unique eigenvalue of $\mathtt{Frob}_{k_r}$ acting on these vector spaces, we conclude

$$\tau(\psi_r,\chi_r)\overline{\tau(\psi_r,\chi_r)} = \tau(\psi_r,\chi_r)\tau(\overline{\psi_r},\overline{\chi_r}) = q^r.$$

For Kloosterman sums we also have a very nice geometric picture which we describe here. For $a\in k^{\mathtt{alg}}$ write V_a for the hypersurface of $\mathbb{A}^n_{k^{\mathtt{alg}}}$ with equation $x_1\dots x_n = a$. Let $\sigma : \mathbb{A}^n_{k^{\mathtt{alg}}} \to \mathbb{A}^1_{k^{\mathtt{alg}}}$ be the map $(x_1,\dots,x_n)\mapsto x_1+\dots+x_n$ and $\mu : \mathbb{A}^n_{k^{\mathtt{alg}}} \to \mathbb{A}^1_{k^{\mathtt{alg}}}$ the map $(x_1,\dots,x_n)\mapsto x_1\cdots x_n$. The next theorem due to Deligne describe the sheaves $\mathtt{R}^i\mu_!\mathcal{L}_{\psi(\sigma)}$ for every $i\in\mathbb{N}\cup\{0\}$:

THEOREM 1.4.2.5 ([**SGA 4½**, Sommes trigonométriques, Théorème 7.4]). *Denote by $\mathtt{H}^i_{\mathtt{c}}$ (resp. $\mathtt{H}^i$) the cohomology groups with proper support (resp. ordinary cohomology groups) of V_a with values in $\mathcal{L}_{\psi(\sigma)}$. They verify the following properties:*

(a) The canonical morphisms $\mathtt{H}^i_{\mathtt{c}} \to \mathtt{H}^i$ are isomorphisms for every i.
(b) $\mathtt{H}^i_{\mathtt{c}} = 0$ for $i\neq n-1$.
(c) For $a\neq 0$, $\mathtt{dim}\ \mathtt{H}^{n-1}_{\mathtt{c}} = n$. For $a=0$, $\mathtt{H}^{n-1}_{\mathtt{c}}$ is canonically isomorphic to $\overline{\mathbb{Q}}_\ell$. □

After base change theorem we know $(\mathtt{R}^i\mu_!\mathcal{L}_{\psi(\sigma)})_a = \mathtt{H}^i_{\mathtt{c}}(V_a,\mathcal{L}_{\psi(\sigma)})$ for every i. Hence, $\mathtt{R}^i\mu_!\mathcal{L}_{\psi(\sigma)}$ is zero for every $i\neq n-1$ and only $\mathtt{R}^{n-1}\mu_!\mathcal{L}_{\psi(\sigma)}$ matters. After Grothendieck's Lefschetz trace formula we obtain for $a\in k_r^\times$ the identity

$$\begin{aligned}(-1)^{n-1}\mathtt{Trace}(\mathtt{Frob}_{k_r}|\mathtt{H}^{n-1}_{\mathtt{c}}(V_a,\mathcal{L}_{\psi(\sigma)})) &= \sum_{p\in V_a(k_r)} \mathtt{t}_{\mathcal{L}_{\psi(\sigma)},k_r}(p) = \sum_{\substack{x_1,\dots,x_n\in k_r^\times\\ x_1\cdots x_n=a}} \psi(x_1+\dots+x_n)\\ &= \mathtt{Kloos}_n(q^r;a),\end{aligned}$$

which realizes Kloosterman sums as values of a certain trace function. Moreover, after Deligne's fundamental theorem (Theorem 1.3.4.2 and Corollary 1.3.4.4) we know $\mathtt{R}^{n-1}\mu_!\mathcal{L}_{\psi(\sigma)}$ is a mixed $\overline{\mathbb{Q}}_\ell$-sheaf of weight $\leq n-1$ since $\mathcal{L}_{\psi(\sigma)}$ is pure of weight 0. But the isomorphism $\mathtt{H}^{n-1}_{\mathtt{c}}(V_a,\mathcal{L}_{\psi(\sigma)})\simeq \mathtt{H}^{n-1}(V_a,\mathcal{L}_{\psi(\sigma)})$ and $\mathcal{L}_{\psi(\sigma)}$ being lisse imply $\mathtt{R}^{n-1}\mu_!\mathcal{L}_{\psi(\sigma)}$ is mixed of weight $\geq n-1$. Hence $\mathtt{R}^{n-1}\mu_!\mathcal{L}_{\psi(\sigma)}$ is pure of weight $n-1$ on $\mathbb{G}_{m,k}$. This implies that for every $a\in k_r^\times$ there exists n complex numbers $\alpha_1,\dots,\alpha_n$ (i.e. the eigenvalues of the action of Frobenius on the n-dimensional vector space $\mathtt{H}^{n-1}_{\mathtt{c}}$) with complex absolute value equal to $q^{\frac{n-1}{2}}$ such that

$$\mathtt{Kloos}_n(q^r;a) = (-1)^{n-1}\sum_{i=1}^n \alpha_i^r.$$

In particular,

$$|\mathtt{Kloos}_n(q^r;a)| \leq n(q^r)^{\frac{n-1}{2}}.$$

This bound considerably improves the one given by Carlitz and is a rather concrete application of Deligne's fundamental theorem on weights.

CHAPTER 2

Monodromy groups and their finiteness

In this chapter we start defining the monodromy groups and reviewing classical criteria to establish their finiteness. Later on we describe the families of sheaves that will occupy us until the end together with explicit numeric criteria for the finiteness of their monodromy groups. In the last section we propose an algorithm to decide effectively which local systems within the mentioned families have finite monodromy. We include an experimental analysis of its complexity for small characteristics and expose phenomena observed by means of an actual implementation of the algorithm.

2.1. Monodromy groups

Let X be a smooth geometrically connected scheme of finite type over a finite field $k = \mathbb{F}_q$ of $\mathtt{char}(k) = p > 0$, $\ell \neq p$ a prime number and $\mathcal{F}$ a lisse $\overline{\mathbb{Q}}_\ell$-sheaf of rank r on X. After Theorem 1.3.1.9, $\mathcal{F}$ "is" just a continuous r-dimensional $\overline{\mathbb{Q}}_\ell$-linear representation of the fundamental group $\rho : \pi_1(X) \to \mathtt{GL}(r, \overline{\mathbb{Q}}_\ell)$ (we omit the base point from the notation taking into account fundamental groups are conjugate for different base points). If $k^{\mathtt{alg}}/k$ is an algebraic closure of k, we consider the geometric fundamental group of X which is a normal closed subgroup of the fundamental arithmetic group:

$$\pi_1^{\mathtt{geom}}(X) := \pi_1(X \otimes_k k^{\mathtt{alg}}) \lhd \pi_1^{\mathtt{arith}}(X) := \pi_1(X).$$

We say the lisse sheaf $\mathcal{F}$ is *arithmetically irreducible* (resp. *geometrically irreducible*) if it has no nonzero lisse subsheaves (resp. if its pullback to $X \otimes_k k^{\mathtt{sep}}$ has no nonzero lisse subsheaves). $\mathcal{F}$ is arithmetically (resp. geometrically) irreducible if and only if as a representation of $\pi_1^{\mathtt{arith}}(X)$ (resp. $\pi_1^{\mathtt{geom}}(X)$) is irreducible. The lisse sheaf $\mathcal{F}$ is *arithmetically semisimple* (resp. *geometrically semisimple*) if it is a direct sum of irreducible lisse sheaves (resp. if its pullback to $X \otimes_k k^{\mathtt{sep}}$ is a direct sum of lisse sheaves). $\mathcal{F}$ is arithmetically (resp. geometrically) semisimple if and only if as a representation of $\pi_1^{\mathtt{arith}}(X)$ (resp. $\pi_1^{\mathtt{geom}}(X)$) is semisimple.

We define the *geometric monodromy group of* $\mathcal{F}$, denoted $G_{\mathtt{geom}}$, as the Zariski closure of $\rho(\pi_1^{\mathtt{geom}}(X))$ in the algebraic group $\mathtt{GL}(r, \overline{\mathbb{Q}}_\ell)$. Similarly, we define the *arithmetic monodromy group of* $\mathcal{F}$, denoted $G_{\mathtt{arith}}$, as the Zariski closure of $\rho(\pi_1^{\mathtt{arith}}(X))$ in the algebraic group $\mathtt{GL}(r, \overline{\mathbb{Q}}_\ell)$. Clearly, $G_{\mathtt{geom}}$ is a normal subgroup of $G_{\mathtt{arith}}$. After a deep result of Deligne [**Del80**, Théorème 3.4.1.(iii)], if $\mathcal{F}$ is ι-pure of some weight w for some isomorphism $\iota : \overline{\mathbb{Q}}_\ell \to \mathbb{C}$, then $\mathcal{F}$ is geometrically semisimple and it follows $G_{\mathtt{geom}}$ is a reductive group. After Grothendieck's theorem [**Del80**, Théorème 1.3.8] we know the identity component $G^0_{\mathtt{geom}}$ is semisimple, or equivalently, the Lie algebra of the complex (via ι) Lie group $G_{\mathtt{geom}}(\overline{\mathbb{Q}}_\ell) \sim G_{\mathtt{geom}}(\mathbb{C})$ is semisimple.

2.1.1. Criteria for finiteness of monodromy and geometric irreducibility. Our final goal is to find $\overline{\mathbb{Q}}_\ell$-sheaves on certain k-varieties X whose geometric monodromy groups are finite. Here we review a classical criterion for this phenomenon. The following result uses the hypothesis fixed at the beginning of the section.

THEOREM 2.1.1.1 ([**Kat90**, Theorem 8.14.4],[**KRLT20**, Propostion 2.1 and Remark 2.2]). *Suppose $\mathcal{F}$ is pure of weight zero and consider the conditions:*

(a) $G_{\mathtt{arith}}$ *is finite.*

(b) *For every finite extension k_r/k and $x \in X(k_r)$, $\mathtt{Trace}(\mathtt{Frob}_{k_r,x}|\mathcal{F})$ is an algebraic integer.*
(c) *$G_{\mathtt{geom}}$ is finite.*
(d) *$\det(\mathcal{F})$ is arithmetically of finite order.*

Then we have the implications (a) $\Longrightarrow$ (b) $\Longrightarrow$ (c) *and* (b) $\Longrightarrow$ (d). *If $\mathcal{F}$ is geometrically irreducible, we have* (a) $\Longleftrightarrow$ (b) $\Longleftrightarrow$ (c). □

We include a useful result that allows us to check if a lisse $\overline{\mathbb{Q}}_\ell$-sheaf is geometrically irreducible:

PROPOSITION 2.1.1.2 ([**KT21**, Proposition 2.1]). *Assume further that $\dim(X) > 0$ and $\mathcal{F}$ is ι-pure of weight zero. If a decomposition into pairwise non-isomorphic irreducible lisse $\overline{\mathbb{Q}}_\ell$-sheaves of $\mathcal{F}$ on $X \otimes_k k^{\mathtt{sep}}$ is $\mathcal{F} \simeq \bigoplus_i n_i\mathcal{G}_i$ with $\mathcal{G}_i$ a lisse $\overline{\mathbb{Q}}_\ell$-sheaf on $X \otimes_k k^{\mathtt{sep}}$ for every i (such a decomposition exists after Deligne's theorem on geometric semisimplicity for pure sheaves), we have:*

$$\sum_i n_i^2 = \underset{k_r/k}{\mathtt{limsup}} \left(\sum_{x \in X(k_r)} \frac{|\mathtt{Trace}(\mathtt{Frob}_{k_r,x}|\mathcal{F})|^2}{|k_r|^{\dim(X)}} \right). \qquad \square$$

The quantity $\sum_i n_i^2$ in the previous proposition is called the *second geometric moment of $\mathcal{F}$* and denoted by $\mathtt{M}_2^{\mathtt{geom}}(X, \mathcal{F})$. More generally, we can define (a, b)-th higher geometric moments for a, b non-negative integers. We follow [**Kat05**, §1.15 and 1.16]. Given an algebraically closed field F of characteristic zero (usually $\overline{\mathbb{Q}}_\ell$ or $\mathbb{C}$) and G a group that acts irreducibly on a finite-dimensional F-vector space V, for each pair (a, b) of non-negative integers, we define the *(a, b)-th moment of* (G, V) by

$$\mathtt{M}_{a,b}(G, V) := \dim_F \left(V^{\otimes a} \otimes (V^\vee)^{\otimes b}\right)^G$$

as the dimension of the space of G-invariants in $V^{\otimes a} \otimes (V^\vee)^{\otimes b}$. Moreover, we denote $\mathtt{M}_{2n}(G, V) := \mathtt{M}_{n,n}(G, V)$ and call it the *$2n$-th moment of* (G, V). Observe that $V^{\otimes n} \otimes (V^\vee)^{\otimes n} = \mathcal{E}\backslash\lceil(V^{\otimes n})$, hence $\mathtt{M}_{2n}(G, V)$ is the dimension of $\mathtt{End}_G(V^{\otimes n})$.

Assuming that $\dim X > 0$, since $\mathcal{F}$ is lisse it has an associated representation of $\pi_1^{\mathtt{geom}}(X)$ and we can speak about its higher moments. We denote $\mathtt{M}_{a,b}^{\mathtt{geom}}(X, \mathcal{F}) := \mathtt{M}_{a,b}(\pi_1^{\mathtt{geom}}(X), \mathcal{F})$ and $\mathtt{M}_{2n}^{\mathtt{geom}}(X, \mathcal{F}) := \mathtt{M}_{2n}(\pi_1^{\mathtt{geom}}(X), \mathcal{F})$. If we further assume that $\mathcal{F}$ is ι-pure of some weight ω and geometrically irreducible, we have the *limit formula* [**Kat05**, Theorem 1.17.4.2)]:

$$\mathtt{M}_{a,b}^{\mathtt{geom}}(X, \mathcal{F}) = \underset{k_r/k}{\mathtt{limsup}} \left(\frac{\left|\sum_{x \in X(k_r)} \mathtt{tr}_{\mathcal{F}^{\otimes a},k_r}(x)\overline{\mathtt{tr}_{\mathcal{F}^{\otimes b},k_r}(x)}\right|}{|k_r|^{\dim\, X + (a+b)\omega/2}} \right).$$

2.1.2. Equidistribution and monodromy. Before explaining how monodromy governs the distribution of traces of Frobenius, we introduce the formal notion of equidistribution of sets following [**Kat88a**]. Given a compact topological space X, denote by $C(X)$ the $\mathbb{C}$-vector space of continuous complex valued functions f on X. Let $\mu : C(X) \to \mathbb{C}$ be a linear functional on $C(X)$ such that (1) if $f \in C(X)$ is real and positive then $\mu(f) \in \mathbb{R}_{>0}$ and (2) μ assings 1 to the constant function equal to 1. We will denote $\mu(f)$ by $\int_X f d\mu$.

DEFINITION 2.1.2.1. Let $\{X_n\}_{n\in\mathbb{N}}$ be a sequence of subsets in X. Consider the measures $\mu_{X_n} = \frac{1}{|X_n|}\sum_{x\in X_n} \delta_x$, where δ_p is the Dirac delta measure supported at p. The sequence of sets is said to be μ-equidistributed over X if for every $f \in C(X)$ we have

$$\int_X f(x)d\mu = \lim_{n\to\infty} \int_X f(x)d\mu_{X_n} = \lim_{n\to\infty} \frac{1}{|X_n|} \sum_{x\in X_n} f(x).$$

When our compact topological space is a compact group G we endow it with the normalized Haar measure $\mathtt{Haar}$. Let $\pi : G \to G^\natural$ be the natural projection of G onto the set of its conjugacy classes, the latter endowed with the quotient topology. Denote by $\mathtt{Haar}_\natural$ the push-forward of $\mathtt{Haar}$ on $G^\natural$, i.e. for class functions $f \in C(G^\natural)$ define $\mathtt{Haar}_\natural(f) := \mathtt{Haar}(f \circ \pi)$.

PROPOSITION 2.1.2.2 ([**Kat88a**, Proof of Theorem 3.6]). *A sequence $\{X_n\}_{n\in\mathbb{N}}$ of subsets of $G^\natural$ is $\mathtt{Haar}_\natural$-equidistributed if and only if for every character χ of a non-trivial finite-dimensional irreducible representation of G we have*

$$\lim_{n\to\infty}\frac{1}{|X_n|}\sum_{x\in X_n}\chi(x)=0. \qquad \square$$

This result follows from Peter–Weyl theorem (which tells us that the subspace generated by irreducible characters of G is dense in $C(G^\natural)$) and Schur's orthogonality.

With this notion in mind, we are going to show that Gauss sums are equidistributed in a concrete sense:

EXAMPLE 2.1.2.3. For every prime power q, fix an additive character $\psi:\mathbb{F}_q\to\mathbb{C}^\times$ and consider the set of angles

$$\left\{\theta_q(\chi):=\frac{\tau(\psi,\chi)}{q^{1/2}}\mid\chi\in(\mathbb{F}_q^\times)^\vee\setminus\{\mathbf{1}\}\right\}\subset S^1.$$

Our equidistribution statement is the following:

THEOREM 2.1.2.4 ([**Kat80**, Théorème 1.3.3.1]). *The sets $\{\theta_q(\chi):\chi\neq\mathbf{1}\}$ become equidistributed over S^1 for the normalized Haar measure when q grows to infinity, that is, for every continuous function $f:\mathbb{S}^1\to\mathbb{C}$ we have the equality*

$$\frac{1}{2\pi}\int_0^{2\pi}f(e^{i\theta})d\theta=\lim_{q\to\infty}\frac{1}{q-2}\sum_{\chi\neq\mathbf{1}}f(\theta_q(\chi)).$$

PROOF. $\mathbb{S}^1$ is an abelian group, it follows $(\mathbb{S}^1)^\natural=\mathbb{S}^1$ and $\mu_\natural=\mu$. Since the irreducible characters of $\mathbb{S}^1$ are just the homomorphisms $z\mapsto z^n$ with $n\in\mathbb{Z}\setminus\{0\}$, we are reduced to showing the equalities

$$0=\frac{1}{2\pi}\int_0^{2\pi}e^{in\theta}d\theta=\lim_{q\to\infty}\frac{1}{q^{n/2}(q-2)}\sum_{\chi\neq\mathbf{1}}\tau(\psi,\chi)^n.$$

It is enough to prove this for $n\geq 1$. Indeed, for $n\leq -1$ and χ non trivial we have $\tau(\psi,\chi)\tau(\overline{\psi},\overline{\chi})=q$ hence

$$\left(\frac{\tau(\psi,\chi)}{q^{1/2}}\right)^n=\left(\frac{\tau(\overline{\psi},\overline{\chi})}{q^{1/2}}\right)^{-n}.$$

For $n\geq 1$,

$$\begin{aligned}\sum_{\chi\neq\mathbf{1}}\tau(\psi,\chi)^n&=(-1)^n\cdot\left(-\tau(\psi,\mathbf{1})^n+\sum_\chi\sum_{a\in\mathbb{F}_q^\times}\chi(a)\mathtt{Kloos}_n(q;a)\right)\\&=(-1)^{n+1}+(-1)^n\sum_{a\in\mathbb{F}_q^\times}\mathtt{Kloos}_n(q;a)\sum_\chi\chi(a)\\&=(-1)^{n+1}+(-1)^n(q-1)\mathtt{Kloos}_n(q;1).\end{aligned}$$

After Deligne's bound, $|\mathtt{Kloos}_n(q;1)|\leq nq^{(n-1)/2}$ and this implies

$$\begin{aligned}\left|\frac{1}{(q-2)q^{n/2}}\sum_{\chi\neq\mathbf{1}}\tau(\psi,\chi)^n\right|&=\left|\frac{-1+(q-1)\mathtt{Kloos}_n(q;1)}{q^{n/2}(q-2)}\right|\\&\leq\frac{1}{(q-2)q^{n/2}}+\frac{q-1}{q-2}\frac{1}{q^{1/2}}\cdot n\\&\leq\frac{n(q-1)/(q-2)+1}{q^{1/2}}\leq\frac{2n+1}{q^{1/2}}\end{aligned}$$

for $q \geq 3$. Hence, for $q \to \infty$ we reach 0.

□

If we use Carlitz's bound instead of Deligne's one we would not be able to conclude the proof. Observe also that this equidistribution result is quite strong since the base prime p does not matter. Indeed, $2n+1$ does not depend on p. In general, with the tools of ℓ-adic cohomology we can only prove *vertical* equidistribution results (that is, we only allow higher powers of a fixed prime). ■

Now we describe the general (but easiest) picture for equidistribution of Frobenius conjugacy classes, mainly following [**Kat88a**, Chapter 3] and [**KS99**, §9.2].

Let k be a finite field of characteristic p, X/k a smooth and geometrically connected scheme of dimension $d \geq 0$, ℓ a prime number $\ell \neq p$, $\iota : \overline{\mathbb{Q}}_\ell \to \mathbb{C}$ an embedding. Consider a lisse $\overline{\mathbb{Q}}_\ell$-sheaf $\mathcal{F}$ of rank $n \geq 1$ on X which is ι-pure of weight 0. Denote by $G_{\mathtt{geom}}$ and $G_{\mathtt{arith}}$ the geometric and arithmetic monodromy groups of $\mathcal{F}$. Via the complex embedding ι we can speak of the group $G_{\mathtt{geom}}(\mathbb{C})$. This group, with the classical topology, is a complex semisimple Lie group. Denote by $K \subset G_{\mathtt{geom}}(\mathbb{C})$ a maximal compact subgroup. It is well known that every compact subgroup of $G_{\mathtt{geom}}(\mathbb{C})$ is $G_{\mathtt{geom}}(\mathbb{C})$-conjugate to a subgroup of K. The representation theories of the $\overline{\mathbb{Q}}_\ell$-algebraic group $G_{\mathtt{geom}}$, the complex Lie group $G_{\mathtt{geom}}(\mathbb{C})$ and the compact group K are described by the following diagram of equivalences between categories (see [**Fre19**, Théorème 3.1],[**Kat88a**, page 37]):

$$\begin{array}{c}
\big(\text{Finite-dimensional } \overline{\mathbb{Q}}_\ell\text{-representations of } G_{\mathtt{geom}} \text{ as } \overline{\mathbb{Q}}_\ell\text{-algebraic group}\big) \\
\Big\downarrow \text{extension of scalars via } \iota \\
\Big(\text{Finite-dimensional } \mathbb{C}\text{-representations of } G_{\mathtt{geom}} \otimes_{\overline{\mathbb{Q}}_\ell} \mathbb{C} \text{ as } \mathbb{C}\text{-algebraic group}\Big) \\
\Big\downarrow \text{evaluation on } \mathbb{C}\text{-valued points} \\
\big(\text{Finite-dimensional holomorphic representations of } G_{\mathtt{geom}}(\mathbb{C}) \text{ as complex Lie group}\big) \\
\Big\downarrow \text{restriction to } K \\
\text{(Finite-dimensional continuous representations of } K \text{ as compact group)}\,.
\end{array}$$

From now on in this subsection we assume the representation $\rho : \pi_1^{\mathtt{arith}}(X) \to \mathtt{GL}(n, \overline{\mathbb{Q}}_\ell)$ associated to $\mathcal{F}$ factors through $G_{\mathtt{geom}}(\overline{\mathbb{Q}}_\ell)$. With the notation introduced above and this hypothesis, the angles of Gauss sums we used before can be generalized as follows. Let E/k be any finite extension of k and $x \in X(E)$. For any choice of Frobenius element $\mathtt{Frob}_{E,x} \in \pi_1^{\mathtt{arith}}(X)$, the element $\iota\rho(\mathtt{Frob}_{E,x}) \in G_{\mathtt{geom}}(\mathbb{C})$ has all its eigenvalues on $\mathbb{S}^1$. Let $\rho(\mathtt{Frob}_{E,x})^{\mathtt{ss}}$ be the semisimple part (in the sense of Jordan decomposition) of $\rho(\mathtt{Frob}_{E,x})$. Then $\iota(\rho(\mathtt{Frob}_{E,x})^{\mathtt{ss}})$ is semisiple and all its eigenvalues are roots of unity, hence $\langle \iota(\rho(\mathtt{Frob}_{E,x})^{\mathtt{ss}})\rangle$ is a compact subgroup of $G_{\mathtt{geom}}(\mathbb{C})$. In particular, $\iota(\rho(\mathtt{Frob}_{E,x})^{\mathtt{ss}})$ is $G_{\mathtt{geom}}(\mathbb{C})$-conjugate to an element of K. Using that $G_{\mathtt{geom}}(\mathbb{C})$ and K have the "same" finite-dimensional representation theory and the Peter–Weyl theorem, it can be shown [**Del80**, Proof of 2.2.2] that the $G_{\mathtt{geom}}(\mathbb{C})$-conjugacy class of $\iota(\rho(\mathtt{Frob}_{E,x})^{\mathtt{ss}})$ meets K in a single K-conjugacy class. Denote this K-conjugacy class by $\theta(E,x)$, thought as the generalized "angle" of $\iota\rho(\mathtt{Frob}_{E,x})$.

With all these ingredients we can state Deligne's equidistribution theorem

THEOREM 2.1.2.5 ([**Del80**, Théorème 3.5.3],[**KS99**, Theorem 9.2.6 (1)]). *With the notations and hypothesis introduced above, the Frobenius conjugacy classes $\theta(E,x)$ are equidistributed in the space of conjugacy clases of K. Explicitly, for any continuous $\mathbb{C}$-valued class function $f : K \to \mathbb{C}$,*

we have the formula:

$$\int_{K_\natural} f d\mathtt{Haar}_\natural = \lim_{|E|\to\infty} \frac{1}{|X(E)|} \sum_{x\in X(E)} f(\theta(E,x)),$$

the limit taken over finite extensions E of k large enough so that $X(E)$ is nonempty. □

Consider the Kloosterman sheaf given by $\mathtt{R}^{n-1}\mu_!\mathcal{L}_{\psi(\sigma)}$ on $\mathbb{G}_{m,k}$, where $\mu : \mathbb{G}_{m,k}^n \to \mathbb{G}_{m,k}$ is the product map and $\sigma : \mathbb{G}_{m,k}^n \to \mathbb{A}_k^1$ is the sum. This is a lisse $\overline{\mathbb{Q}}_\ell$-sheaf of rank n on $\mathbb{G}_{m,k}$ and pure of weight $n-1$. Hence, $\mathtt{R}^{n-1}\mu_!\mathcal{L}_{\psi(\sigma)}(\frac{n-1}{2})$ is lisse of rank n and pure of weight 0 (fixing some square root of $\sqrt{q} \in \overline{\mathbb{Q}}_\ell$.) After the previous theorem, we know the conjugacy classes of Frobenius elements are equidistributed in the space of conjugacy classes of any maximal compact subgroup K of $G_{\mathtt{geom}}(\mathbb{C})$. We combine this equidistribution result with Katz' computation of $G_{\mathtt{geom}}$ for $\mathtt{R}^{n-1}\mu_!\mathcal{L}_{\psi(\sigma)}(\frac{n-1}{2})$:

THEOREM 2.1.2.6 ([**Kat88a**, Main Theorem 11.1 and Remark 11.2.(1)]). *The geometric monodromy group $G_{\mathtt{geom}}$ of $\mathtt{R}^{n-1}\mu_!\mathcal{L}_{\psi(\sigma)}(\frac{n-1}{2})$ as an algebraic group over $\overline{\mathbb{Q}}_\ell$ is given, for $n \geq 2$, by:*

$$G_{\mathtt{geom}} = \begin{cases} \mathtt{Sp}(n) & n \text{ even}, \\ \mathtt{SL}(n) & pn \text{ odd}, \\ \mathtt{SO}(n) & p = 2, n \text{ odd}, n \neq 7, \\ \mathtt{G}_2 & p = 2, n = 7. \end{cases}$$

□

Hence, for $p \neq 2$, the Frobenius traces of $\mathtt{R}^{n-1}\mu_!\mathcal{L}_{\psi(\sigma)}(\frac{n-1}{2})$ at points $a \in k^\times$, i.e. the Kloosterman sums $\frac{(-1)^{n-1}}{\sqrt{q}^{n-1}}\mathtt{Kloos}_n(q;a)$ for $a \in k^\times$, are distributed as the traces of random matrices for big powers of the base prime p, since in both cases the maximal compact subgroup can be described by

$$K = \begin{cases} \mathtt{USp}(n) & n \text{ even} \\ \mathtt{SU}(n) & n \text{ odd} \end{cases} = G_{\mathtt{geom}}(\mathbb{C}) \cap \mathtt{U}(n).$$

2.2. Families of exponential sums and numeric criteria for finite monodromy

In this section we introduce the "parametric" exponential sums we will be working with and give concrete (i.e. numeric) criteria for the finiteness of the monodromy groups of the associated $\overline{\mathbb{Q}}_\ell$-sheaves.

We fix a prime p, and ℓ a prime number different from p. We choose a square root of p, denoted $p^{1/2} \in \overline{\mathbb{Q}}_\ell{}^\times$, for the rest of the chapter. Whenever we refer to a half-Tate twist we are taking $\alpha = p^{-1/2}$ for the generalized Tate twist. We further fix a finite prime field $k = \mathbb{F}_p$, the non-trivial additive character $\psi : \mathbb{F}_p \to \overline{\mathbb{Q}}_\ell{}^\times$ given by $\psi(t) = \mathtt{exp}(2\pi it/p)$. We identify $\overline{\mathbb{Q}}_\ell$ with $\mathbb{C}$ implicitly. Recall our notation $\psi_r := \psi \circ \mathtt{trace}_{k_r/k}$, where $k_r = \mathbb{F}_{p^r}$.

2.2.1. The $\overline{\mathbb{Q}}_\ell$-sheaves of interest for us and their monodromy. Given a polynomial $f \in k[x]$ of degree coprime to p, we are interested in the parametric exponential sums

$$\sum_{x\in k_r} \psi_r(sf(x) + tx) \text{ for } s,t \in k_r^\times \times k_r.$$

To realize these sums as the values of a trace function, we consider the following geometric situation:

$$\begin{array}{ccc} \mathbb{G}_{m,k} \times \mathbb{A}_k^1 \times \mathbb{A}_k^1 & \xrightarrow{\varphi} & \mathbb{A}_k^1 \\ \downarrow{\scriptstyle \pi_{12}} & & \\ \mathbb{G}_{m,k} \times \mathbb{A}_k^1 & & \end{array}$$

where $\varphi(s,t,x) = sf(x) + tx$. Then our sums are just

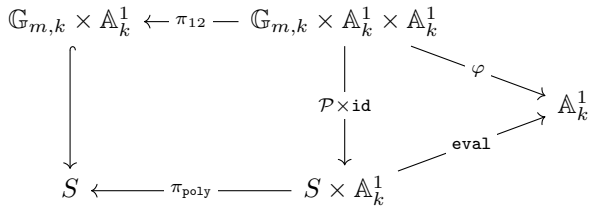
$$\sum_{i=0}^{2} \mathtt{Trace}(\mathtt{Frob}_{k_r} | (\mathtt{R}^i \pi_{12!} \mathcal{L}_{\psi(\varphi)})_{(s,t)})$$

and we must understand the sheaves $\mathtt{R}^i \pi_{12!} \mathcal{L}_{\psi(\varphi)}$.

PROPOSITION 2.2.1.1. *The sheaves $\mathtt{R}^i \pi_{12!} \mathcal{L}_{\psi(\varphi)}$ are zero for $i \neq 1$ and for $i = 1$ the sheaf is lisse of rank $\mathtt{deg}\ f - 1$ and pure of weight 1. Furthermore, the sheaf $\mathtt{R}^1 \pi_{12!} \mathcal{L}_{\psi(\varphi)}(1/2)$ is geometrically irreducible.*

PROOF.

(a) *Vanishing, smoothness and purity:* We use Deligne's idea from [**Del80**, §3.7.2], and in order to do so, we introduce some convenient notation. We denote the variable for polynomials by X, so $f \in k[X]$. Let S be the affine space over k parametrizing polynomials of degree $\mathtt{deg}\ f$, that is, we allow arbitrary coefficients for monomials of degree less than $\mathtt{deg}\ f$ and non-zero coefficients for the leading term of the polynomials (this guarantees the *non-singular hypersurface* condition is fullfilled). Observe that S is isomorphic to $\mathbb{G}_{m,k} \times \mathbb{A}_k^{\mathtt{deg}\ f}$. Let $f_S(X)$ denote the universal polynomial over S. Denote by $\mathtt{eval} : S \times \mathbb{A}_k^1 \to \mathbb{A}_k^1$ the evaluation morphism sending (g, x) to $g(x)$. We denote the lisse $\overline{\mathbb{Q}}_\ell$-sheaf $\mathtt{eval}^* \mathcal{L}_\psi$ by $\mathcal{L}_{\psi(f_S)}$ for notational coherence. Now consider the projection $\pi_{\mathtt{poly}} : S \times \mathbb{A}_k^1 \to S$. Then our polynomial $f(X)$ corresponds to a rational point of S, and the $\overline{\mathbb{Q}}_\ell$-sheaf $\mathcal{L}_{\psi(f)}$ on $\mathbb{A}_k^1$ is just the stalk of $\mathcal{L}_{\psi(f_S)}$ at $f(X)$ under $\pi_{\mathtt{poly}}$. Finally, consider the closed immersion $\mathcal{P} : \mathbb{G}_{m,k} \times \mathbb{A}_k^1 \to S$ defined by $(s,t) \mapsto sf(X) + tX \in S$ ($\mathcal{P}$ standing for parametrization). With this notation we have the enhanced diagram:



where the leftmost vertical arrow is such that the square is commutative. We have the following identity between lisse $\overline{\mathbb{Q}}_\ell$-sheaves:

$$\left(\mathtt{R}^i \pi_{\mathtt{poly}!} \mathcal{L}_{\psi(f_S)}\right)_{|\mathbb{G}_{m,k} \times \mathbb{A}_k^1} = \mathtt{R}^i \pi_{12!} \mathcal{L}_{\psi(\varphi)}.$$

Indeed, since $\varphi = \mathtt{eval} \circ (\mathcal{P} \times \mathtt{id})$, we know $\mathcal{L}_{\psi(\varphi)} = (\mathcal{P} \times \mathtt{id})^* \mathcal{L}_{\psi(f_S)}$. Now we apply the functor $\mathtt{R}^i \pi_{12!}$ and invoke base change theorem for cohomology with compact support:

$$\mathtt{R}^i \pi_{12!} \mathcal{L}_{\psi(\varphi)} = \mathtt{R}^i \pi_{12!} (\mathcal{P} \times \mathtt{id})^* \mathcal{L}_{\psi(f_S)} \simeq \left(\mathtt{R}^i \pi_{\mathtt{poly}!} \mathcal{L}_{\psi(f_S)}\right)_{|\mathbb{G}_{m,k} \times \mathbb{A}_k^1}.$$

After [**Del80**, Lemme 3.7.3 and §3.7.2.3], we know the sheaves $\mathtt{R}^i \pi_{\mathtt{poly}!} \mathcal{L}_{\psi(f_S)}$ are lisse and only $\mathtt{R}^1 \pi_{\mathtt{poly}!} \mathcal{L}_{\psi(f_S)}$ is not trivial, since for $i \neq 1$ they have trivial stalks. Moreover, from the argument in *loc. cit.* it follows that $\mathtt{R}^1 \pi_{\mathtt{poly}!} \mathcal{L}_{\psi(\varphi)}$ has rank $\mathtt{deg}\ f - 1$ and is pure of weight 1.

(b) *Geometric irreducibility:* After the previous item, we know the sheaf $\mathtt{R}^i \pi_{12!} \mathcal{L}_{\psi(\varphi)}(1/2)$ is lisse and pure of weight 0. Denote this sheaf by $\mathcal{F}$ and suppose it can be decomposed as $\bigoplus_{i=1}^{e} n_i \mathcal{G}_i$ into pairwise non-isomorphic irreducible lisse sheaves on $(\mathbb{G}_{m,k} \times \mathbb{A}_k^1) \otimes_k k^{\mathtt{sep}}$. Applying Proposition 2.1.1.2, we get

$$\sum_{i=1}^{e} n_i^2 = \underset{k_r/k}{\mathtt{limsup}} \sum_{s \in k_r^\times, t \in k_r} \frac{\left|\mathtt{Trace}(\mathtt{Frob}_{k_r,(s,t)} | \mathcal{F})\right|^2}{|k_r|^2}.$$

We compute the right hand term of the previous equation using orthogonality of characters:

$$\sum_{s\in k_r^\times, t\in k_r} \left|\mathtt{Trace}(\mathtt{Frob}_{k_r,(s,t)}|\mathcal{F})\right|^2 = \frac{1}{|k_r|}\sum_{s\neq 0,t}\left(\sum_{x\imath k_r}\psi_r(sf(x)+tx)\right)\left(\sum_{y\in k_r}\psi_r^{-1}(sf(y)+ty)\right)$$
$$= \frac{1}{|k_r|}\sum_{s\neq 0,t}\sum_{x,y}\psi_r\big(s(f(x)-f(y))\big)\psi_r\big(t(x-y)\big)$$
$$= \frac{1}{|k_r|}\sum_{x,y}\left(\sum_{s\neq 0}\psi_r\big(s(f(x)-f(y))\big)\right)\left(\sum_{t}\psi_r\big(t(x-y)\big)\right)$$
$$= \frac{1}{|k_r|}\sum_{x}|k_r|\left(-\psi_r(0)+\sum_{s}\psi_r\big(s(f(x)-f(x))\big)\right) = \sum_x(|k_r|-1) = |k_r|(|k_r|-1).$$

Hence $\sum_{i=1}^{e} n_i^2 = \underset{r\in\mathbb{N}}{\mathtt{limsup}}\ (1-\frac{1}{|k_r|}) = 1$. This implies $e=1$ and $n_1=1$, i.e. $\mathcal{F}$ is geometrically irreducible.

□

This proposition shows we can use Theorem 2.1.1.1 to decide the finiteness of $G_{\mathtt{geom}}$ for $\mathtt{R}^1\pi_{12!}\mathcal{L}_{\psi(\varphi)}(1/2)$ by checking the algebraicity of its traces. Moreover, observe that we can further restrict ourselves to the variety $\mathbb{G}_{m,k}\times\mathbb{G}_{m,k}$. This follows because $\mathbb{G}_{m,k}\times\mathbb{G}_{m,k}$ is dense in $\mathbb{G}_{m,k}\times\mathbb{A}^1_k$, so $\pi_1^{\mathtt{geom}}(\mathbb{G}_{m,k}\times\mathbb{G}_{m,k})$ maps onto $\pi_1^{\mathtt{geom}}(\mathbb{G}_{m,k}\times\mathbb{A}^1_k)$. This way, the finiteness of $G_{\mathtt{geom}}$ for the pullback of $\mathtt{R}^1\pi_{12!}\mathcal{L}_{\psi(\varphi)}(1/2)$ to $\mathbb{G}_{m,k}\times\mathbb{G}_{m,k}$ is equivalent to the finiteness of $G_{\mathtt{geom}}$ for the original sheaf. We usually work with the lisse $\overline{\mathbb{Q}}_\ell$-sheaf $\mathtt{R}^1\pi_{12!}\mathcal{L}_{\psi(\varphi)}(1/2)$ on $\mathbb{G}_{m,k}\times\mathbb{G}_{m,k}$, with trace function given by

$$(s,t)\in k_r^\times\times k_r^\times \longmapsto -\frac{1}{|k_r|^{1/2}}\sum_{x\in k_r}\psi_r(sf(x)+tx).$$

Finally we further reduce the study of algebraicity to the study of the p-adic valuation of the traces. Fix a primitive 4-th root of unity ζ_4 and a primitive p-th root of unity ζ_p for $p\neq 2$. Write

$$K = \begin{cases}\mathbb{Q}(\zeta_4) & \text{if } p=2,\\ \mathbb{Q}(\zeta_p) & \text{if } p\neq 2.\end{cases}$$

In both cases, K contains a square root of p. Indeed, $1+\zeta_4$ is such a square root up to multiplication by an unit for $p=2$. For $p\neq 2$, the Gauss sum $\tau(\psi,\chi)\in K$ with χ the Legendre character is a square root of p up to multiplication by an unit. To simplify the exposition, assume that our fixed square root of p in $\overline{\mathbb{Q}}_\ell$ is this Gauss sum if $p\neq 2$ and $1+\zeta_4$ if $p=2$. With this convention, it follows that the traces of $\mathtt{R}^1\pi_{12!}\mathcal{L}_{\psi(\varphi)}(1/2)$ can be realized in K for every prime p.

Taking into account that K is a number field, we know its ring of integers is a Dedekind domain, in particular it is a Krull domain. Therefore an element of K is in its ring of integers if and only if it is in the valuation ring associated to every prime ideal. Now we distinguish the prime ideals according to the characteristic of their residue fields. For any rational prime $\ell\neq p$, observe that $\sum_{x\in k_r}\psi_r(sf(x)+tx)$ is an algebraic integer because it is a sum of roots of unity and we divide by $|k_r|^{1/2}$ (which is not divisible by ℓ), so we already know the traces are integers with respect to every prime with residue characteristic ℓ. For p we argue as follows. Observe that the extension $K/\mathbb{Q}$ is totally ramified at p and unramified outside p, so there is only one prime ideal with residue characteristic p. Let $\mathtt{ord}_{p^r}$ be the unique p-adic valuation of K normalized such that

$\mathtt{ord}_{p^r}(p^r) = 1$. Then the values of the traces on k_r are algebraic integers if and only if

$$\mathtt{ord}_{p^r}\left(\frac{1}{|k_r|^{1/2}}\sum_{x\in k_r}\psi_r(sf(x)+tx)\right) \geq 0 \text{ for every } r\geq 1, \text{ and } s,t\in k_r^\times,$$

i.e. $\mathtt{ord}_{p^r}\sum_{x\in k_r}\psi_r(sf(x)+tx) \geq 1/2$ for every $r\geq 1$ and $s,t\in k_r^\times$. This way we get a numerical criterion for the finitenes of $G_{\mathtt{geom}}$ for $\mathtt{R}^1\pi_{12!}\mathcal{L}_{\psi(\varphi)}(1/2)$ considered either as a $\overline{\mathbb{Q}}_\ell$-sheaf on $\mathbb{G}_{m,k}\times\mathbb{G}_{m,k}$ or $\mathbb{G}_{m,k}\times\mathbb{A}^1_k$.

2.2.1.1. *The sheaves $\mathcal{B}_{(p;a,b)}(\alpha,\beta)$.* Now we specialize the previous discussion to polynomials of the form $f(x)=(x-\alpha)^a(x-\beta)^b$ where $a,b\in\mathbb{N}$ and $\alpha,\beta\in k$ with $a,b,a+b$ coprime to p and $\alpha\neq\beta$. We denote $\mathcal{B}_{(p;a,b))}(\alpha,\beta) := \mathtt{R}^1\pi_{12!}\mathcal{L}_{\psi(sf(x)+tx)}(1/2)$, a $\overline{\mathbb{Q}}_\ell$-sheaf on $\mathbb{G}_{m,k}\times\mathbb{G}_{m,k}$ whose trace function at $(s,t)\in k_r^\times\times k_r^\times$ is

$$-\frac{1}{|k_r|^{1/2}}\sum_{x\in k_r}\psi_r(s(x-\alpha)^a(x-\beta)^b+tx).$$

We do a reduction step before giving an explicit form to our finiteness criterion of monodromy for the sheaf $\mathcal{B}_{(p;a,b)}(\alpha,\beta)$. It suffices to understand the geometric monodromy group of the sheaf $\mathcal{B}_{(p;a,b)} := \mathcal{B}_{(p;a,b)}(0,1)$ on $\mathbb{G}_{m,k}\times\mathbb{G}_{m,k}$. Indeed, write $f(x)=(x-\alpha)^a(x-\beta)^b$ and, for every $r\geq 1, s,t\in k_r^\times$, observe that

$$\sum_{x\in k_r}\psi_r(sf(x+\alpha)+tx) = \sum_{x\in k_r}\psi_r(sf(x)+tx-t\alpha) = \psi_r(-t\alpha)\sum_{x\in k_r}\psi_r(sf(x)+tx).$$

Since $\psi_r(-t\alpha)$ is a root of unity, it does not matter while studying the integrality of the traces. We can assume without loss of generality $\alpha=0$. Also, since

$$\sum_{x\in k_r}\psi_r(sf(x)+tx) = \sum_{x\in k_r}\psi_r(sf(\beta x)+t\beta x) = \sum_{x\in k_r}\psi_r(s\beta^{a+b}x^a(x-1)^b+t\beta x),$$

we see $\mathcal{B}_{(p;a,b)}(0,\beta)$ is the pullback of $\mathcal{B}_{(p;a,b)}$ via the isomorphism $(s,t)\mapsto(\beta^{a+b}s,\beta t)$.

We state the following explicitation of Theorem 2.1.1.1 for the sheaves $\mathcal{B}_{(p;a,b)}(\alpha,\beta)$:

Theorem 2.2.1.2 (Private communication by Antonio Rojas-León). *Let $a,b\in\mathbb{N}$ be natural numbers and $\alpha,\beta\in k$ with $\alpha\neq\beta$. The $\overline{\mathbb{Q}}_\ell$-sheaf $\mathcal{B}_{(p;a,b)}(\alpha,\beta)$ has finite $G_{\mathtt{geom}}$ if and only if for every $r\geq 1$ and multiplicative characters $\chi,\eta\in(k_r^\times)^\vee, \chi\neq\mathbf{1}$ the following inequalities hold:*

(a) *If $\chi^{a+b}\eta\neq\mathbf{1}$,*

$$\mathtt{ord}_{p^r}\big(\tau(\psi_r,\chi)\big)+\mathtt{ord}_{p^r}\big(\tau(\psi_r,\eta)\big) + \mathtt{ord}_{p^r}\big(\tau(\psi_r,\overline{\chi}^a\overline{\eta})\big)+\mathtt{ord}_{p^r}\big(\tau(\psi_r,\overline{\chi}^b)\big)-\mathtt{ord}_{p^r}\big(\tau(\psi_r,\overline{\chi}^{a+b}\overline{\eta})\big)\geq\frac{1}{2}.$$

(b) *If $\chi^{a+b}\eta=\mathbf{1}$,*

$$\mathtt{ord}_{p^r}\big(\tau(\psi_r,\chi)\big)+\mathtt{ord}_{p^r}\big(\tau(\psi_r,\eta)\big)\geq\frac{1}{2}.$$

Proof. We already know $G_{\mathtt{geom}}$ is finite for $\mathcal{B}_{(p;a,b)}(\alpha,\beta)$ on $\mathbb{G}_{m,k}\times\mathbb{A}^1_k$ if and only if $G_{\mathtt{geom}}$ is finite for $\mathcal{B}_{(p;a,b)}$ on $\mathbb{G}_{m,k}\times\mathbb{G}_{m,k}$, if and only if for every $r\geq 1$ and $s,t\in k_r^\times$ the inequality $\mathtt{ord}_{p^r}\big(\sum_{x\in k_r}\psi_r(sx^a(x-1)^b+tx)\big)\geq 1/2$ is satisfied. Now we use Mellin transform and inverse Mellin transform as in [**KRLT20**, Theorem 2.7].

For every $r\geq 1$ the trace function of $\mathcal{B}_{(p;a,b)}$ is defined on the finite abelian group $k_r^\times\times k_r^\times$. Taking the Fourier transform (and the inverse Fourier transform) of this function on the group $k_r^\times\times k_r^\times$ we find $\mathtt{ord}_{p^r}(\mathtt{t}_{\mathcal{B}'_{(p;a,b)},k_r}(s,t))\geq 1/2$ for every $s,t\in k_r^\times$ if and only if the values of its Fourier transform satisfy the same inequality (because inverse Fourier transform involves a division

by $(p^r-1)^2$ which is coprime to p^r). Since the character group $(k_r^\times \times k_r^\times)^\vee$ is $(k_r^\times)^\vee \times (k_r^\times)^\vee$, we are reduced to study whether the inequality

$$\mathtt{ord}_{p^r}\Big(\sum_{s,t\in k_r^\times}\chi(s)\eta(t)\sum_{x\in k_r}\psi_r(sx^a(x-1)^b+tx)\Big)\geq\frac{1}{2}\text{ with }\chi,\eta\in(k_r^\times)^\vee\text{ and }r\geq 1$$

holds or not. We rewrite the Mellin transform as follows:

$$\begin{aligned}\sum_{s,t\in k_r^\times}\chi(s)\eta(t)\sum_{x\in k_r}\psi_r(sx^a(x-1)^b+tx)&=\sum_{x\in k_r}\Big(\sum_{s\in k_r^\times}\psi_r(sx^a(x-1)^b)\chi(s)\Big)\Big(\sum_{t\in k_r^\times}\psi_r(tx)\eta(t)\Big)\\&=\Big(\sum_{s\in k_r^\times}\chi(s)\Big)\Big(-\tau(\psi_r,\eta)+\sum_{t\in k_r^\times}\eta(t)\Big)+\tau(\psi_r,\chi)\tau(\psi_r,\eta)\sum_{x\in k_r^\times\setminus\{1\}}\overline{\chi}(x^a(x-1)^b)\overline{\eta}(x)\\&=\Big(\sum_{s\in k_r^\times}\chi(s)\Big)\Big(-\tau(\psi_r,\eta)+\sum_{t\in k_r^\times}\eta(t)\Big)-\overline{\chi}^b(-1)\tau(\psi_r,\chi)\tau(\psi_r,\eta)\mathtt{J}(\overline{\chi}^a\overline{\eta},\overline{\chi}^b).\end{aligned}$$

If $\chi=\mathbf{1}$, the Mellin transform becomes

$$(p^r-1)\Big(-\tau(\psi_r,\eta)+\sum_{t\in k_r^\times}\eta(t)\Big)-\tau(\psi_r,\eta)\mathtt{J}(\overline{\eta},\mathbf{1}).$$

But

$$\begin{aligned}\tau(\psi_r,\eta)\mathtt{J}(\overline{\eta},\mathbf{1})&=\tau(\psi_r,\eta)\Big(-1+\sum_{y\in k_r^\times}\overline{\eta}(x)\Big)=-\tau(\psi_r,\eta)-\Big(\sum_{x\in k_r^\times}\psi_r(x)\eta(x)\Big)\Big(\sum_{y\in k_r^\times}\overline{\eta}(y)\Big)\\&=-\tau(\psi_r,\eta)-\sum_{x,y\in k_r^\times}\psi_r(x)\eta(xy^{-1})=-\tau(\psi_r,\eta)-\sum_{x,t\in k_r^\times}\psi_r(xt)\eta(t)\\&=-\tau(\psi_r,\eta)-\sum_{t\in k_r^\times}\eta(t)\sum_{x\in k_r^\times}\psi_r(xt)=-\tau(\psi_r,\eta)+\sum_{t\in k_r^\times}\eta(t),\end{aligned}$$

and our Mellin transform is just $p^r\Big(-\tau(\psi_r,\eta)+\sum_{t\in k_r^\times}\eta(t)\Big)$, which is always divisible by p^r (Gauss sums are algebraic integers).

If $\chi\neq\mathbf{1}$, the Mellin transform becomes

$$-\overline{\chi}^b(-1)\tau(\psi_r,\chi)\tau(\psi_r,\eta)\mathtt{J}(\overline{\chi}^a\overline{\eta},\overline{\chi}^b).$$

We distinguish between different cases:

(a) If $\chi^{a+b}\eta\neq\mathbf{1}$. In this case $\mathtt{J}(\overline{\chi}^a\overline{\eta},\overline{\chi}^b)=\tau(\psi_r,\overline{\chi}^a\overline{\eta})\tau(\psi_r,\overline{\chi}^b)/\tau(\psi_r,\overline{\chi}^{a+b}\overline{\eta})$ and the Mellin transform is

$$-\overline{\chi}^b(-1)\tau(\psi_r,\chi)\tau(\psi_r,\eta)\tau(\psi_r,\overline{\chi}^a\overline{\eta})\tau(\psi_r,\overline{\chi}^b)\tau(\psi_r,\overline{\chi}^{a+b}\overline{\eta}).$$

We have to impose the inequality

$$\begin{aligned}&\mathtt{ord}_{p^r}\big(\tau(\psi_r,\chi)\big)+\mathtt{ord}_{p^r}\big(\tau(\psi_r,\eta)\big)\\&\qquad+\mathtt{ord}_{p^r}\big(\tau(\psi_r,\overline{\chi}^a\overline{\eta})\big)+\mathtt{ord}_{p^r}\big(\tau(\psi_r,\overline{\chi}^b)\big)-\mathtt{ord}_{p^r}\big(\tau(\psi_r,\overline{\chi}^{a+b}\overline{\eta})\big)\geq\frac{1}{2}.\end{aligned}$$

(b) If $\chi^{a+b}\eta=\mathbf{1}$. If $\chi^b\neq\mathbf{1}$ then $\mathtt{J}(\overline{\chi}^a\overline{\eta},\overline{\chi}^b)=\overline{\chi}^b(-1)$ and we impose the inequality

$$\mathtt{ord}_{p^r}\Big(\tau(\psi_r,\chi)\Big)+\mathtt{ord}_{p^r}\Big(\tau(\psi_r,\eta)\Big)\geq\frac{1}{2}.$$

If $\chi^a\eta=\chi^b=\mathbf{1}$ then $\mathtt{J}(\overline{\chi}^a\overline{\eta},\overline{\chi}^b)=(2-p^r)$. The inequality takes the form

$$\mathtt{ord}_{p^r}\big(\tau(\psi_r,\chi)\big)+\mathtt{ord}_{p^r}\big(\tau(\psi_r,\eta)\big)+\mathtt{ord}_{p^r}(2-p^r)\geq\frac{1}{2}.$$

If $p \neq 2$ then $\mathtt{ord}_{p^r}(2-p^r) = 0$ and we obtain the same inequality. If $p = 2$ then

$$\mathtt{ord}_{p^r}(2-p^r) = \frac{\mathtt{ord}_p(2-p^r)}{r} = \frac{1}{r},$$

and the inequality is

$$\mathtt{ord}_{p^r}\big(\tau(\psi_r,\chi)\big) + \mathtt{ord}_{p^r}\big(\tau(\psi_r,\eta)\big) + \frac{1}{r} \geq \frac{1}{2}.$$

We impose this inequality for every $r \geq 1$ and every pair of characters χ and η satisfying $\chi^a\eta = \chi^b = \mathbf{1}$. In particular, for every $n \in \mathbb{N}$ the same inequality holds for k_{nr} and χ_n, η_n. Then for every $n \in \mathbb{N}$ we impose

$$\begin{aligned}\frac{1}{2} &\leq \mathtt{ord}_{p^{rn}}\big(\tau(\psi_{rn},\chi_n)\big) + \mathtt{ord}_{p^{rn}}\big(\tau(\psi_{nr},\eta_n)\big) + \frac{1}{rn} \\ &= n\mathtt{ord}_{p^{rn}}\big(\tau(\psi_r,\chi)\big) + n\mathtt{ord}_{p^{rn}}\big(\tau(\psi_r,\eta)\big) + \frac{1}{rn} \\ &= \mathtt{ord}_{p^r}\big(\tau(\psi_r,\chi)\big) + \mathtt{ord}_{p^r}\big(\tau(\psi_r,\eta)\big) + \frac{1}{rn}.\end{aligned}$$

Taking $n \to \infty$ we again get the same inequality.

□

2.2.1.2. *The sheaves $\mathcal{M}(p;d,1)$ and $\mathcal{M}_{\mathtt{big}}(p;d,1)$.* Let $d > 1$ be an integer and consider the polynomial $f(x) = x^d \in k[x]$. Denote by $\mathcal{M}_{\mathtt{big}}(p;d,1)$ either the sheaf $\mathtt{R}^1\pi_{12!}\mathcal{L}_{\psi(sx^d+tx)}(1/2)$ on $\mathbb{G}_{m,k} \times \mathbb{A}^1_k$ or on $\mathbb{G}_{m,k} \times \mathbb{G}_{m,k}$. The trace function of $\mathcal{M}_{\mathtt{big}}(p;d,1)$ in both cases is given by $-\frac{1}{|k_r|^{1/2}}\sum_{x\in k_r}\psi_r(sx^d+tx)$, with $s \in k_r^\times$ and $t \in k_r$ or $k_r^\times$. We can assume without loss of generality that d is coprime to p, otherwise an Artin–Schreier reduction would bring us back to this assumption.

The following lemma shows that the finiteness of $G_{\mathtt{geom}}$ for $\mathcal{M}_{\mathtt{big}}(p;d,1)$ is equivalent to the finiteness of $G_{\mathtt{geom}}$ when we restrict our sheaf to the slice $s = 1$.We denote it by $\mathcal{M}(p;d,1) := \mathcal{M}_{\mathtt{big}}(p;d,1)_{|s=1}$. As in Proposition 2.2.1.1, it can be shown that $\mathcal{M}(p;d,1)$ is lisse of rank $d-1$, pure of weight zero and geometrically irreducible. Its trace function on $\mathbb{A}^1_k$ (resp. $\mathbb{G}_{m,k}$) is given by

$$t \in k_r \text{ (resp. } t \in k_r^\times) \longmapsto -\frac{1}{|k_r|^{1/2}}\sum_{x\in k_r}\psi_r(x^d+tx).$$

Lemma 2.2.1.3 ([**KRLT20**, Lemma 2.6]). *The $\overline{\mathbb{Q}}_\ell$-sheaf $\mathcal{M}_{\mathtt{big}}(p;d,1)$ on $\mathbb{G}_{m,k}\times\mathbb{G}_{m,k}$ has finite $G_{\mathtt{geom}}$ if and only if the sheaf $\mathcal{M}(p;d,1)$ on $\mathbb{G}_{m,k}$ has finite $G_{\mathtt{geom}}$.*

Proof. Since $\mathcal{M}(p;d,1)$ is a pullback of $\mathcal{M}_{\mathtt{big}}(p;d)$, the finiteness of $G_{\mathtt{geom}}$ for the latter clearly implies the finiteness of $G_{\mathtt{geom}}$ for the former.

Conversely, let k_r/k be a finite extension and $t \in k_r^\times$. For $s \in k_r^\times$ we have

$$\sum_{x\in k_r}\psi_r(x^d+tx) = \sum_{x\in k_r}\psi_r(s^dx^d+tsx).$$

Making the change of variable $t' = st$, the sum becomes $\sum_{x\in k_r}\psi_r(s^dx^d+t'x)$, which (after a normalization) is still an algebraic integer. Hence the pullback of $\mathcal{M}_{\mathtt{big}}(p;d,1)$ via the finite étale Galois map $\theta(s,t) = (s^d,t)$ has all its traces algebraic integers. After Theorem 2.1.1.1 we know this pullback has finite $G_{\mathtt{arith}}$. Since the image of $\theta_* : \pi_1^{\mathtt{arith}}(\mathbb{G}_{m,k}\times\mathbb{G}_{m,k}) \to \pi_1^{\mathtt{arith}}(\mathbb{G}_{m,k}\times\mathbb{G}_{m,k})$ is a subgroup of index d, the group $G_{\mathtt{arith}}$ for $\mathcal{M}_{\mathtt{big}}(p;d,1)$ contains a finite group as a subgroup of finite index, so it must be finite as well. To conclude recall that the finiteness of $G_{\mathtt{geom}}$ is equivalent to the finiteness of $G_{\mathtt{arith}}$ for the sheaf $\mathcal{M}_{\mathtt{big}}(p;d,1)$.

□

An explicit version of Theorem 2.1.1.1 for the sheaf $\mathcal{M}_{\mathtt{big}}(p;d,1)$ is the following:

THEOREM 2.2.1.4 ([**KRLT20**, Theorem 2.7]). *Let $d > 1$ be an integer coprime to p. The $\overline{\mathbb{Q}}_\ell$-sheaf $\mathcal{M}_{\mathtt{big}}(p; d, 1)$ on $\mathbb{G}_{m,k} \times \mathbb{G}_{m,k}$ has finite $G_{\mathtt{geom}}$ if and only if for every pair of multiplicative characters $\rho, \chi \in (k_r^\times)^\vee$ such that not both are trivial and $\rho\chi^d = \mathbf{1}$ the following inequality is satisfied:*

$$\mathtt{ord}_{p^r}\big(\tau(\psi_r, \rho)\big) + \mathtt{ord}_{p^r}\big(\tau(\psi_r, \chi)\big) \geq \frac{1}{2}.$$

PROOF. As we argued before, for the Frobenius traces to be algebraic integers it is sufficient for them to be so with respect to the unique p-adic valuation of the field K where the traces live.

Now we invoke Mellin transform as we did earlier. The Mellin transform of our trace function on k_r is, evaluated at $\rho, \chi \in (k_r^\times)^\vee$, the following sum

$$\mathtt{Mellin}(\mathtt{t}_{\mathcal{M}_{\mathtt{big}},k_r})(\rho, \chi) := \sum_{s,t \in k_r^\times} \rho(t)\chi(s) \sum_{x \in k_r} \psi_r(sx^d + tx).$$

We rewrite it as follows:

$$\begin{aligned}
\mathtt{Mellin}(\mathtt{t}_{\mathcal{M}_{\mathtt{big}},k_r})(\rho, \chi) &= \sum_{x \in k_r} \Big(\sum_{s \in k_r^\times} \psi_r(sx^d)\chi(s) \Big) \Big(\sum_{t \in k_r^\times} \psi_r(tx) \Big) \\
&= \Big(\sum_{s \in k_r^\times} \chi(s) \Big) \Big(\sum_{t \in k_r^\times} \rho(t) \Big) + \sum_{x \in k_r^\times} \Big(\sum_{s \in k_r^\times} \psi_r(sx^d)\chi(s) \Big) \Big(\sum_{t \in k_r^\times} \psi_r(tx)\rho(t) \Big) \\
&= \Big(\sum_{s \in k_r^\times} \chi(s) \Big) \Big(\sum_{t \in k_r^\times} \rho(t) \Big) + \tau(\psi_r, \chi)\tau(\psi_r, \rho) \sum_{x \in k_r^\times} (\overline{\chi}^d \overline{\rho})(x).
\end{aligned}$$

We distinguish two cases:

(a) If $\rho = \chi = \mathbf{1}$. Then

$$\mathtt{Mellin}(\mathtt{t}_{\mathcal{M}_{\mathtt{big}},k_r})(\mathbf{1}, \mathbf{1}) = (p^r - 1)^2 + p^r - 1 = (p^r - 1)p^r,$$

which is divisible by p^r.

(b) If $\rho \neq \mathbf{1}$ or $\chi \neq \mathbf{1}$. Then

$$\mathtt{Mellin}(\mathtt{t}_{\mathcal{M}_{\mathtt{big}},k_r})(\rho, \chi) = \tau(\psi_r, \rho)\tau(\psi_r, \chi) \sum_{x \in k_r^\times} (\overline{\rho\chi}^d)(x).$$

If $\rho\chi^d \neq \mathbf{1}$ the Mellin transform vanish. If $\rho\chi^d = \mathbf{1}$ then the Mellin transform equals $(q^r - 1)\tau(\psi_r, \rho)\tau(\psi_r, \chi)$. The inequality we impose is

$$\mathtt{ord}_{p^r}\big(\tau(\psi_r, \rho)\big) + \mathtt{ord}_{p^r}\big(\tau(\psi_r, \chi)\big) \geq \frac{1}{2}.$$

□

REMARK 2.2.1.5. The sheaves $\mathcal{M}(p; d_n, \ldots, d_1)$ and $\mathcal{M}_{\mathtt{big}}(p; d_n, \ldots, d_1)$. As a generalization of the sheaves $\mathcal{M}_{\mathtt{big}}(p; d, 1)$ we can consider, for $d_{n+1} > d_n > d_{n-1} > \cdots > d_2 > d_1 = 1$ a sequence of integers coprime to p, the $\overline{\mathbb{Q}}_\ell$-sheaf on $\mathbb{G}_{m,k}^{n+1}$ with trace function

$$\boldsymbol{t} = (t_1, \ldots, t_{n+1}) \in k_r^{n+1} \mapsto -1 \frac{1}{|k_r|^{1/2}} \sum_{x \in k_r} \psi_r\Big(\sum_{i=1}^{n+1} t_i x^{d_i} \Big).$$

As we did in Proposition 2.2.1.1, we can show that these sheaves are lisse, pure of weight zero and geometrically irreducible. Moreover, we can further consider them as sheaves on $\mathbb{A}_k^n \times \mathbb{G}_{m,k}$ and the finiteness of $G_{\mathtt{geom}}$ for both is equivalent. In both cases we can consider the slice $\mathcal{M}(p; d_{n+1}, d_n, \ldots, d_1) := \mathcal{M}_{\mathtt{big}}(p; d_{n+1}, \ldots, d_1)_{|t_{n+1}=1}$, and the finiteness of $G_{\mathtt{geom}}$ for these sheaves can be shown to be equivalent to the finiteness of $G_{\mathtt{geom}}$ for the original sheaves as in Lemma 2.2.1.3. The corresponding explicitation of Theorem 2.1.1.1 for these sheaves is the following, which we include because it will be needed later:

THEOREM 2.2.1.6 ([**KRLT20**, Theorem 2.7]). *Let $d_{n+1} > d_n > \cdots > d_2 > d_1 = 1$ be a sequence of integers coprime to p. The sheaf $\mathcal{M}(p; d_{n+1}, \ldots, d_1)$ (equivalently $\mathcal{M}_{\mathtt{big}}(p; d_{n+1}, \ldots, d_1)$ on $\mathbb{A}^n_k$ or $\mathbb{G}^n_{m,k}$ (equivalently on $\mathbb{A}^n_k \times \mathbb{G}_{m,k}$ or $\mathbb{G}^{n+1}_{m,k}$) has finite $G_{\mathtt{geom}}$ if and only if for every $n+1$-tuple of multiplicative characters $\rho_1, \ldots, \rho_{n+1} \in (k_r^\times)^\vee$ such that there exists an index i with $\rho_i \neq \mathbf{1}$ and $\rho_1^{d_1} \cdots \rho_n^{d_n} \rho_{n+1}^{d_{n+1}} = \mathbf{1}$ the following inequality is satisfied:*

$$\sum_{i=1}^{n+1} \mathtt{ord}_{p^r}\Big(\tau(\psi_r, \rho_i)\Big) \geq \frac{1}{2}. \qquad \square$$

■

2.2.2. Kubert's `V` function and sums of digits. In Theorems 2.2.1.2 and 2.2.1.4 the valuation of Gauss sums naturally arised. In this subsection we define Kubert's `V` function which, together with sums of p-adic digits, allows us to work with valuations of Gauss sums, reformulate our explicit criteria and study finiteness of monodromy effectively.

2.2.2.1. *Kubert's `V` function.* We follow [**Kat90**, §8.14] and [**Kat07**, §13]. Let p be a prime number. For every $N \in \mathbb{N}$ denote by $\zeta_N \in \overline{\mathbb{Q}}$ a primitive N-th root of unity. Let $K = \mathbb{Q}(\{\zeta_p\} \cup \{\zeta_N : (N,p) = 1\})$ with a fixed embedding into $\overline{\mathbb{Q}}_\ell$. Denote by $\mathcal{O}_K = \mathbb{Z}[\{\zeta_p\} \cup \{\zeta_N : (N,p) = 1\}]$ the subring of all algebraic integers in K. We write $K_{\mathtt{ur}} = \mathbb{Q}(\{\zeta_N : (N,p) = 1\}) \subset K$ and $\mathcal{O}_{\mathtt{ur}} = \mathbb{Z}[\{\zeta_N : (N,p) = 1\}]$ for the subring of all algebraic integers in $K_{\mathtt{ur}}$. Every multiplicative character $\chi : \mathbb{F}_{p^r} \to \overline{\mathbb{Q}}_\ell{}^\times$ takes values in $\mathcal{O}_{\mathtt{ur}}$ and the Gauss sums $\tau(\psi, \chi) \in \mathcal{O}_K$. Fix an embedding $\jmath : K_{\mathtt{ur}} \hookrightarrow \overline{\mathbb{Q}}_p$.

For any $n \in \mathbb{N}$ coprime to p we can identify the groups of n-th roots of unity $\mu_n(\overline{\mathbb{Q}}_p) \sim \mu_n(\mathbb{F}_p^{\mathtt{alg}})$ via reduction modulo a prime $\wp$ of $\overline{\mathbb{Q}}_p$ lying over p. We have

$$\mu_n(\overline{\mathbb{Q}}_\ell) = \mu_n(\mathcal{O}_{\mathtt{ur}}) = \mu_n(\overline{\mathbb{Q}}_p) \sim \mu_n(\mathbb{F}_p).$$

For $n = q - 1$ with $q = p^r$ a p-power we have

$$\mu_n(\mathcal{O}_{\mathtt{ur}}) \sim \mu_n(\mathbb{F}_p^{\mathtt{alg}}) = \mu_{q-1}(\mathbb{F}_p^{\mathtt{alg}}) = \mathbb{F}_q^\times.$$

The isomorphism from $\mathbb{F}_q^\times \to \mu_{q-1}(\mathcal{O}_{\mathtt{ur}})$ is the *Teichmüller character* $\mathtt{Teich}_{\mathbb{F}_q}$. Observe that, after our construction, $\mathtt{Teich}_{\mathbb{F}_q}(t) + \wp = t$ and in particular $\mathtt{Teich}_{\mathbb{F}_q}(\zeta_{q-1} + \wp) + \wp = \zeta_{q-1} + \wp$ so $\mathtt{Teich}_{\mathbb{F}_q}$ has order $q-1$ and is a generator of the character group $(\mathbb{F}_q^\times)^\vee$. Observe the compatibility $\mathtt{Teich}_{\mathbb{F}_{p^s}}|_{\mathbb{F}_{p^r}^\times} = \mathtt{Teich}_{\mathbb{F}_{p^r}}$ if $\mathbb{F}_{p^s}/\mathbb{F}_{p^r}$.

Using $\mathtt{Teich}_{\mathbb{F}_q}$ we can construct for every p-power q a group isomorphism

$$\begin{array}{rccc} \Lambda_{\mathbb{F}_q} : & \left(\frac{1}{q-1}\mathbb{Z}\right)/\mathbb{Z} & \longrightarrow & (\mathbb{F}_q^\times)^\vee \\ & x & \longmapsto & \mathtt{Teich}_{\mathbb{F}_q}^{-x\cdot(q-1)}. \end{array}$$

To avoid confusions, the group $(\frac{1}{q-1}\mathbb{Z})/\mathbb{Z} = \{i/(q-1) \mod \mathbb{Z} : i = 0, \ldots, q-2\}$ is just the group of integer multiples of $1/(q-1)$ modulo $\mathbb{Z}$ and we use indistinguishibly $x \mod \mathbb{Z}$ and $x \in \mathbb{Q}$. If $\mathbb{F}_{p^s}/\mathbb{F}_{p^r}$ the following diagram commutes:

$$\begin{array}{ccc} \left(\frac{1}{p^r-1}\mathbb{Z}\right)/\mathbb{Z} & \hookrightarrow & \left(\frac{1}{p^s-1}\mathbb{Z}\right)/\mathbb{Z} \\ \Lambda_{\mathbb{F}_{p^r}}\downarrow & & \Lambda_{\mathbb{F}_{p^s}}\downarrow \\ (\mathbb{F}_{p^r}^\times)^\vee & \xrightarrow{(\cdot)\circ \mathtt{N}_{\mathbb{F}_{p^s}/\mathbb{F}_{p^r}}} & (\mathbb{F}_{p^s}^\times)^\vee. \end{array}$$

Indeed, for every $x \in (\frac{1}{p^s-1}\mathbb{Z})/\mathbb{Z}$ and $t \in \mathbb{F}_{p^s}$ we have the following equalities

$$\begin{aligned}\mathtt{Teich}_{\mathbb{F}_{p^s}}^{-x(p^s-1)}(t) &= \left(\mathtt{Teich}_{\mathbb{F}_{p^s}}^{-x(p^r-1)}\right)^{(p^s-1)/(p^r-1)}(t)\\ &= \mathtt{Teich}_{\mathbb{F}_{p^s}}^{-x(p^r-1)}(\mathtt{N}_{\mathbb{F}_{p^s}/\mathbb{F}_{p^r}}(t))\\ &= \mathtt{Teich}_{\mathbb{F}_{p^r}}^{-x(p^r-1)} \circ \mathtt{N}_{\mathbb{F}_{p^s}/\mathbb{F}_{p^r}}(t).\end{aligned}$$

Now for q a p-power we denote by $\mathtt{ord}_q$ the p-adic valuation of $\overline{\mathbb{Q}}_p$ normalized by $\mathtt{ord}_q(q) = 1$. Observe that if $r|s$ then $\mathtt{ord}_{p^s} = (r/s)\mathtt{ord}_{p^r}$. Let $\psi \in \mathbb{F}_p^\vee$ be a non trivial additive character and denote by ψ_r the additive character of $\mathbb{F}_{p^r}$ given by $\psi \circ \mathtt{trace}_{\mathbb{F}_{p^r}/\mathbb{F}_p}$. For every $r \in \mathbb{N}$ we define the function

$$\begin{array}{rccc}\mathtt{V}_r: & \left(\frac{1}{p^r-1}\mathbb{Z}\right)/\mathbb{Z} & \longrightarrow & [0,1)\\ & x & \longmapsto & \mathtt{ord}_{p^r}(\tau(\psi_r, \Lambda_{\mathbb{F}_{p^r}}(x))).\end{array}$$

If $r|s$ and $x \in \left(\frac{1}{p^s-1}\mathbb{Z}\right)/\mathbb{Z}$ then, after Hasse–Davenport lifting identity,

$$\begin{aligned}\mathtt{V}_s(x) &= \mathtt{ord}_{p^s}\left(\tau(\psi_s, \Lambda_{\mathbb{F}_{p^s}}(x))\right)\\ &= \mathtt{ord}_{p^s}\left(\tau(\psi_s, \Lambda_{\mathbb{F}_{p^r}}(x) \circ \mathtt{N}_{\mathbb{F}_{p^s}/\mathbb{F}_{p^r}})\right)\\ &= (r/s)\mathtt{ord}_{p^r}\left(\tau(\psi_r, \Lambda_{\mathbb{F}_{p^r}}(x))^{s/r}\right)\\ &= \mathtt{V}_r(x).\end{aligned}$$

Hence, all these functions can be "glued" together via an inverse limit. We denote the limit function by $\mathtt{V} : (\mathbb{Q}/\mathbb{Z})_{\mathtt{not}\ p} \to [0,1)$ and call it *Kubert's* $\mathtt{V}$ *function*. Here $(\mathbb{Q}/\mathbb{Z})_{\mathtt{not}\ p}$ denotes the group of rational numbers with denominator coprime to p modulo $\mathbb{Z}$, i.e. $\mathbb{Z}_{p\mathbb{Z}}/\mathbb{Z}$ with $\mathbb{Z}_{p\mathbb{Z}}$ the localization of $\mathbb{Z}$ at the prime ideal $p\mathbb{Z}$.

The properties of Gauss sums §1.4.2.2 translate into properties of the $\mathtt{V}$ function [**Kat07**, page 37]:

(a) $\mathtt{V}(x) = 0$ *if and only if* $x = 0$ *in* $(\mathbb{Q}/\mathbb{Z})_{\mathtt{not}\ p}$. This follows from the fact $\tau(\psi_r, \chi)$ has absolute value $p^{r/2}$ if χ is non trivial.

(b) *For* $x \in (\mathbb{Q}/\mathbb{Z})_{\mathtt{not}\ p}$ *nonzero,* $\mathtt{V}(x) + \mathtt{V}(-x) = 1$. This again follows from the norm formula $\tau(\psi_r, \chi)\overline{\tau(\psi_r, \chi)} = p^r$.

(c) $\mathtt{V}(1/2) = 1/2$ *if* $p \neq 2$. This is (b) with $x = 1/2$ since $1/2 = -1/2$ in $\mathbb{Q}/\mathbb{Z}$.

(d) *For any* $x \in (\mathbb{Q}/\mathbb{Z})_{\mathtt{not}\ p}$, $\mathtt{V}(x) = \mathtt{V}(px)$. Indeed, $\tau(\psi_r, \chi \circ \mathtt{Frob}_{k_r/\mathbb{F}_p}) = \tau(\psi_r, \chi)$.

(e) *For any* $x, y \in (\mathbb{Q}/\mathbb{Z})_{\mathtt{not}\ p}$, $\mathtt{V}(x) + \mathtt{V}(y) \geq \mathtt{V}(x+y)$. This is the integrality of Jacobi sums [**Was97**, Corllary 6.3].

(f) *For any* $x \in (\mathbb{Q}/\mathbb{Z})_{\mathtt{not}\ p}$ *and any integer* $N \geq 1$ *prime to* p, $\sum_{i=0}^{N-1} \mathtt{V}(x + i/N) = \mathtt{V}(Nx) + (N-1)/2$. This follows from Hasse–Davenport product identity. Indeed, let r be the smallest integer with $(p^r - 1)x \in \mathbb{Z}$ and $p^r \equiv 1 \pmod N$. The multiplicative characters of $\mathbb{F}_{p^r}$ of order N are precisely the characters $\Lambda_{\mathbb{F}_{p^r}}(x)$ with $x \in \{i/N : i = 0, \ldots, N-1\}$. By Hasse-Davenport product identity:

$$\tau(\psi_r^N, \Lambda_{\mathbb{F}_{p^r}}(Nx)) \prod_{i=0}^{N-1} \tau(\psi_r, \Lambda_{\mathbb{F}_{p^r}}(i/N)) = \prod_{i=0}^{N-1} \tau(\psi_r, \Lambda_{\mathbb{F}_{p^r}}(x + i/N)).$$

Taking $\mathtt{ord}_{p^r}$ of both terms we find $\mathtt{V}(Nx) + \sum_{i=0}^{N-1} \mathtt{V}(i/N) = \sum_{i=0}^{N-1} \mathtt{V}(x + i/N)$. Using (b) it follows $\sum_{i=0}^{N-1} \mathtt{V}(i/N) = (N-1)/2$.

All these properties show that $\mathtt{V}$ is a Kubert distribution (see [**Lan78**] for a survey) and it is an interesting question to decide if the relationships written above are essentially the unique ones that $\mathtt{V}$ verifies. Relationships for $\mathtt{V}$ come from multiplicative identities between Gauss sums (omitting

the information coming from roots of unity). There are results [**Yam66, Yam75**] showing that all multiplicative identities between Gauss sums up to multiplication by roots of unity can be derived from Hasse–Davenport identities together with the norm relationship under (mild) restrictions. An analogous result, proven this time using equidistribution techniques, in a different but closely related direction can be found in [**RL23b**].

It is hard to work computationally with $\mathtt{V}$ function, and we would like to have an expression for it as explicit as possible. Stickelberger's theorem provides us with such an expression. Before stating the result we fix some notation. Let $\pi \in \overline{\mathbb{Q}}_p$ such that $\pi^{p-1} = -p$ and $\mathtt{ord}_\pi$ is the p-adic valuation normalized such that $\mathtt{ord}_\pi(\pi) = 1$. It follows that $\mathtt{ord}_\pi = (p-1)\mathtt{ord}_p$. Write $[a]_p$ for the sum of the p-adic digits of $a \in \mathbb{Z}$, i.e., if $a = a_0 + a_1 p + \cdots a_{f-1}p^{f-1}$ is the base-p-expansion of a, then

$$[a]_p = a_0 + a_1 + \cdots + a_{f-1}.$$

It is well known that $[a]_p$, with $0 \leq a < p^f - 1$, can be computed as follows [**Was97**, Lemma 6.14]:

$$[a]_p = (p-1)\sum_{i=0}^{f-1} \left\{ \frac{p^i a}{p^f - 1} \right\}.$$

Let $f \in \mathbb{N}$ and $\psi : \mathbb{F}_{p^f} \to \overline{\mathbb{Q}}_\ell^{\times}$ be a non trivial additive character. Stickelberger's theorem [**Was97**, Proposition 6.13] gives us the p-adic valuation of Gauss sums:

$$\mathtt{ord}_\pi(\tau(\psi, \mathtt{Teich}_{\mathbb{F}_{p^f}}^{-a})) = [a]_p \text{ for every } a \in \mathbb{Z}/(p^f - 1)\mathbb{Z}.$$

For $x \in (\mathbb{Q}/\mathbb{Z})_{\mathtt{not}\ p}$, let $f \in \mathbb{N}$ such that $(p^f - 1)x = 0$, then

$$\mathtt{V}(x) = \mathtt{ord}_{p^f}(\tau(\psi, \Lambda_{\mathbb{F}_{p^f}}(x)) = \frac{1}{f}\mathtt{ord}_p(\tau(\psi, \Lambda_{\mathbb{F}_{p^f}}(x))) = \frac{[(p^f-1)x]_p}{(p-1)f}.$$

Equivalently,

$$\mathtt{V}(x) = \frac{1}{f}\sum_{i=0}^{f-1}\{p^i x\}.$$

We introduce a variant of Kubert's $\mathtt{V}$ function. Define Rojas-León's $\mathtt{V}_{\mathtt{RL}}$ function by

$$\mathtt{V}_{\mathtt{RL}}(x) = \mathtt{V}(x) \quad \text{for } x \neq 0,$$
$$\mathtt{V}_{\mathtt{RL}}(0) = 1.$$

Now equality $\mathtt{V}(x) + \mathtt{V}(-x) = 1$ for $x \neq 0$ becomes $\mathtt{V}(x) + \mathtt{V}_{\mathtt{RL}}(-x) = 1$ for all x and this implies $\mathtt{V}_{\mathtt{RL}}$ verifies:

(a) $\mathtt{V}_{\mathtt{RL}}(x) = 1$ if and only if $x = 0$.
(b) $\mathtt{V}_{\mathtt{RL}}(1/2) = 1/2$ if $p \neq 2$.
(c) $\mathtt{V}_{\mathtt{RL}}(x) = \mathtt{V}_{\mathtt{RL}}(px)$ for every $x \in (\mathbb{Q}/\mathbb{Z})_{\mathtt{not}\ p}$.
(d) For any $x \in (\mathbb{Q}/\mathbb{Z})_{\mathtt{not}\ p}$ and any integer $N \geq 1$ prime to p, $\sum_{i=0}^{N-1}\mathtt{V}_{\mathtt{RL}}(x + i/N) = \mathtt{V}_{\mathtt{RL}}(Nx) + (N-1)/2$.

2.2.2.2. *Sums of p-adic digits.* After Stickelberger's theorem it is natural to study sums of p-adic digits and their properties, where p is as always a prime number. We have Kummer's theorem on sums of p-adic digits:

LEMMA 2.2.2.1 ([**Kum52**, Lehrsatz, pages 115 and 116]). *Let $x, y \in \mathbb{Z}$ be positive integers. Then*

$$[x+y]_p = [x]_p + [y]_p - (p-1)(\#\textit{carries while adding } x \textit{ and } y \textit{ in base } p).$$

PROOF. Let $x = \sum_{i=0}^{l} x_i p^i, y = \sum_{i=0}^{l} y_i p^i$ be the base-p-expansions of x and y. Write $x + y = \sum_{i=0}^{l+1} z_i p^i$. Set $\epsilon_{-1} = 0$ and define $\epsilon_i \in \{0, 1\}$ for $0 \leq i \leq l$ by:

$$z_i = x_i + y_i + \epsilon_{i-1} - p\epsilon_i.$$

Observe that, with this definition $\epsilon_i = 1$ $(0 \leq i \leq l)$ if and only if a carry occurs at i-th digit while adding x and y in base p. In particular, $z_{l+1} = \epsilon_l$. Now the lemma follows from the following manipulations:

$$\begin{aligned}[x+y]_p &= \sum_{i=0}^{l+1} z_i = \sum_{i=0}^{l}(x_i + y_i + \epsilon_{i-1} - p\epsilon_i) + \epsilon_l \\ &= [x]_p + [y]_p + \sum_{i=0}^{l+1}\epsilon_{i-1} - p\sum_{i=0}^{l}\epsilon_i = [x]_p + [y]_p - (p-1)\sum_{i=0}^{l}\epsilon_i.\end{aligned}$$

□

Strictly speaking, this is not Kummer's result. He proved, using Legendre's identity $\mathtt{ord}_p(n!) = (n-[n]_p)/(p-1)$, that the number of carries that occur while adding x and y in base p is $\mathtt{ord}_p\binom{x+y}{x}$. Indeed, $[x+y]_p = x + y - (p-1)\mathtt{ord}_p\left((x+y)!\right) = [x]_p + [y]_p - (p-1)\mathtt{ord}_p\left((x+y)!/(x!y!)\right)$.

Now we introduce a function that will simplify our statements later. For every $r \in \mathbb{N}$, denote $q = p^r$. For any x with $1 \leq x \leq q-1$ we define [**RL19**] $[x]_{p,r} := [x]_p$ and extend this definition to all integers by periodicity, that is, for $x \in \mathbb{Z}$ we consider its residue modulo $q-1$ in the set of residue classes $\{1, 2, \ldots, q-1\}$. Observe that for $1 \leq x \leq q-2$, $[x]_{p,r} = (p-1)\sum_{i=0}^{r}\{p^i x/(q-1)\}$. Using Kummer's theorem 2.2.2.1 we can describe $[x]_{p,r}$ in terms of $[x]_p$ for $x \not\equiv 0 \pmod{q-1}$ as follows:

Lemma 2.2.2.2. *Let x such that $x \not\equiv 0 \pmod{q-1}$. Then*

$$[x]_{p,r} = [x]_p - (p-1)\mathtt{ord}_p\binom{x + \left\lfloor \frac{x}{q-1} \right\rfloor}{x}.$$

Proof. By Euclidean division write $x = \left\lfloor \frac{x}{q-1} \right\rfloor (q-1) + \overline{x}$ with $0 < \overline{x} < q-1 < q$. Then $x + \left\lfloor \frac{x}{q-1} \right\rfloor = \left\lfloor \frac{x}{q-1} \right\rfloor q + \overline{x}$. Applying $[\cdot]_p$ to both sides we get: $\left[x + \left\lfloor \frac{x}{q-1} \right\rfloor\right]_p = \left[\left\lfloor \frac{x}{q-1} \right\rfloor q + \overline{x}\right]_p$. Since $\overline{x} < q$, there is no carry while adding $\left\lfloor \frac{x}{q-1} \right\rfloor q$ and $\overline{x}$ in base p. Also, by definition $[\overline{x}]_p = [x]_{p,r}$. After Lemma 2.2.2.1 and using that $[p \cdot n]_p = [n]_p$:

$$[x]_p + \left[\left\lfloor \frac{x}{q-1} \right\rfloor\right]_p - (p-1)\mathtt{ord}_p\binom{x + \left\lfloor \frac{x}{q-1} \right\rfloor}{x} = \left[\left\lfloor \frac{x}{q-1} \right\rfloor\right]_p + [x]_{p,r}.$$

□

The functions $[\cdot]_p, [\cdot]_{p,r}$ satisfy the properties:

Proposition 2.2.2.3. *For every integers $x, y > 0$ and every $r, s \in \mathbb{N}$ we have the following properties:*

(a) $[x+y]_p \leq [x]_p + [y]_p$.
(b) $[x]_{p,r} \leq [x]_p$.
(c) $[x+y]_{p,r} \leq [x]_{p,r} + [y]_{p,r}$.
(d) $[px]_{p,r} = [x]_{p,r}$.
(e) $\left[\frac{p^{rs}-1}{p^r-1}x\right]_{p,rs} = s[x]_{p,r}$.

Proof. (a) This follows immediately from Kummer's theorem.

(b) This is obvious after Lemma 2.2.2.2 since $\binom{x+\left\lfloor \frac{x}{p^r-1} \right\rfloor}{x} \in \mathbb{Z}$.

(c) We reproduce the argument of [**KRL19**, Proof of Proposition 2.2]. Assume $x, y < p^r$. Then $[x+y]_{p,r} \leq [x+y]_p \leq [x]_p + [y]_p = [x]_{p,r} + [y]_{p,r}$.

(d) Following *loc. cit.*: Assume $x < p^r$ and write $x = \sum_{i=0}^{r-1} a_i p^i$. Then $px \pmod{p^r-1} = a_0 p + a_1 p^2 + \cdots + a_{r-2}p^{r-1} + a_{r-1}$. Hence, $[px]_{p,r} = \sum_{i=0}^{r-1} a_i = [x]_{p,r}$.

(e) It is proven in [**KRLT20**, Lemma 2.10].

□

We introduce a slight variant of $[\cdot]_{p,r}$. For $0 \leq x < p^r - 1$ define $[x]_{p,r,-} := [x]_p$ and extend the definition to $\mathbb{Z}$ by periodicity, i.e. $[x]_{p,r,-} = [x \pmod{p^r - 1}]_{p,r,-}$. With this definition, Lemma 2.2.2.2 holds for every integer $x \in \mathbb{Z}$ and not only for $x \not\equiv 0 \pmod{p^r - 1}$. The corresponding properties of Proposition 2.2.2.3 hold true for $[\cdot]_{p,r,-}$.

2.2.2.3. *Relationships between* $\mathtt{V}$ *functions and sums of digits.* As we observed above,

$$\mathtt{V}\left(\frac{a}{p^r-1}\right) = \frac{1}{r}\sum_{i=0}^{r-1}\left\{\frac{p^i a}{p^r-1}\right\} = \frac{[a]_{p,r,-}}{r(p-1)}$$

for $0 \leq a < p^r - 1$. In general, if $x \in (\mathbb{Q}/\mathbb{Z})_{\mathtt{not}\ p}$ and $r \in \mathbb{N}$ is such that $(p^r-1)x = 0$ then $\mathtt{V}(x) = \frac{[(p^r-1)x]_{p,r,-}}{r(p-1)}$. For $\mathtt{V}_{\mathtt{RL}}$ we have the following:

$$\mathtt{V}_{\mathtt{RL}}\left(\frac{a}{p^r-1}\right) = 1 - \mathtt{V}\left(\frac{-a}{p^r-1}\right) = \frac{r(p-1) - [-a]_{p,r,-}}{r(p-1)} = \frac{r(p-1) - r(p-1) + [a]_{p,r}}{r(p-1)} = \frac{[a]_{p,r}}{r(p-1)}$$

for $0 \leq a < p^r - 1$. In general, if $x \in (\mathbb{Q}/\mathbb{Z})_{\mathtt{not}\ p}$ is such that $(p^r-1)x = 0$ then $\mathtt{V}_{\mathtt{RL}}(x) = \frac{[(p^r-1)x]_{p,r}}{r(p-1)}$.

2.2.3. Reformulation of criteria for finite monodromy. We rewrite Theorems 2.2.1.2 and 2.2.1.4 using $\mathtt{V}$ functions and sums of digits. We keep the notations fixed in section 1.

Corollary 2.2.3.1 ([**KRLT20**, Theorems 2.8 and 2.9]). *Let $d_{n+1} > d_n > \cdots > d_1 = 1$ be a sequence of integers coprime to p. The $\overline{\mathbb{Q}}_\ell$-sheaf $\mathcal{M}(p; d_{n+1}, d_n, \ldots, d_1)$ has finite $G_{\mathtt{geom}}$ if and only if*

$$\frac{1}{2} + \sum_{i=2}^{n+1} \mathtt{V}(x_i) \geq \mathtt{V}_{\mathtt{RL}}\left(\sum_{i=2}^{n+1} d_i x_i\right)$$

for every $x_2, \ldots, x_{n+1} \in (\mathbb{Q}/\mathbb{Z})_{\mathtt{not}\ p}$ which are not all 0. Equivalently, if and only if

$$\frac{r(p-1)}{2} + \sum_{i=2}^{n+1} [x_i]_{p,r,-} \geq \left[\sum_{i=2}^{n+1} d_i x_i\right]_{p,r}$$

for every $r \geq 1$ and $0 \leq x_2, \ldots, x_{n+1} < p^r - 1$ which are not all 0.

Proof. Let $x_1, \ldots, x_{n+1} \in (\mathbb{Q}/\mathbb{Z})_{\mathtt{not}\ p}$ (not all 0) and $r \geq 1$ such that $(p^r-1)x_i = 0$ for all $i = 1, \ldots, n+1$. Consider the characters $\rho_i := \Lambda_{\mathbb{F}_{p^r}}(x_i)$. There is at least one index i with $\rho_i \neq \mathbf{1}$. After Theorem 2.2.1.4 we know $\mathcal{M}(p; D, d_n, \ldots, d_1)$ has finite $G_{\mathtt{geom}}$ if and only if the inequality $\sum_{i=1}^{n+1} \mathtt{ord}_{p^r}\big(\tau(\psi_r, \rho_i)\big) \geq 1/2$ holds whenever $\rho_1^{d_1} \cdots \rho_{n+1}^{d_{n+1}} = \mathbf{1}$. Hence, $G_{\mathtt{geom}}$ is finite if and only if $\sum_{i=1}^{n+1} \mathtt{V}(x_i) \geq 1/2$ whenever $\sum_{i=1}^{n+1} d_i x_i = 0$. Since $d_1 = 1$, we know the equality $\sum_{i=1}^{n+1} d_i x_i = 0$ is equivalent to $x_1 = -\sum_{i=2}^{n+1} d_i x_i$. If we substitute this in the last inequality we find

$$\mathtt{V}\Big(-\sum_{i=2}^{n+1} d_i x_i\Big) + \sum_{i=2}^{n+1} \mathtt{V}(x_i) \geq \frac{1}{2}$$

must hold for arbitrary $x_2, \ldots, x_{n+1} \in (\mathbb{Q}/\mathbb{Z})_{\mathtt{not}\ p}$ (not all 0) for $G_{\mathtt{geom}}$ to be finite. Using the relationship $\mathtt{V}(-t) + \mathtt{V}_{\mathtt{RL}}(t) = 1$ we conclude our criterion is equivalent to the inequality

$$\sum_{i=2}^{n+1} \mathtt{V}(x_i) + \frac{1}{2} \geq \mathtt{V}_{\mathtt{RL}}\left(\sum_{i=2}^{n+1} d_i x_i\right)$$

for every $x_2, \ldots, x_{n+1} \in \overline{\mathbb{Q}}_\ell$ not all equal to 0.

The second part of the statement follows easily using the formulas relating $\mathtt{V}$ functions and sums of digits.

□

COROLLARY 2.2.3.2. *Let $a, b \in \mathbb{N}$ be natural numbers and $\alpha, \beta \in k$ with $\alpha \neq \beta$. The $\overline{\mathbb{Q}}_\ell$-sheaf $\mathcal{B}_{(p;a,b)}(\alpha, \beta)$ has finite $G_{\mathtt{geom}}$ if and only if*

$$\mathtt{V}\big(x\big) + \mathtt{V}\big(y - (a+b)x\big) + \mathtt{V}\big(bx - y\big) + \mathtt{V}\big(-bx\big) + \mathtt{V}\big(y\big) \geq \frac{3}{2}$$

for every $x, y \in (\mathbb{Q}/\mathbb{Z})_{\mathtt{not}\ p} \setminus \{0\}$ and

$$\mathtt{V}\big(x\big) + \mathtt{V}\big(-(a+b)x\big) \geq \frac{1}{2}$$

for every $x \in (\mathbb{Q}/\mathbb{Z})_{\mathtt{not}\ p} \setminus \{0\}$. Equivalently, if and only if

$$[x]_{p,r,-} + [y - (a+b)x]_{p,r,-} + [bx - y]_{p,r,-} + [-bx]_{p,r,-} + [y]_{p,r,-} \geq \frac{3r(p-1)}{2}$$

for every $r \geq 1$, $0 < x, y < p^r - 1$ and

$$[x]_{p,r,-} + [-(a+b)x]_{p,r,-} \geq \frac{1}{2}$$

for every $r \geq 1$, $0 < x < p^r - 1$.

PROOF. Let $x, y \in (\mathbb{Q}/\mathbb{Z})_{\mathtt{not}\ p}$ with $x \neq 0$ and $r \geq 1$ such that $(p^r - 1)x = (p^r - 1)y = 0$ in $(\mathbb{Q}/\mathbb{Z})_{\mathtt{not}\ p}$. Consider the characters $\chi := \Lambda_{\mathbb{F}_{p^r}}(x)$ and $\eta := \Lambda_{\mathbb{F}_{p^r}}(y)$. Since $x \neq 0$, it is $\chi \neq \mathbf{1}$. After Theorem 2.2.1.2 we know $\mathcal{B}_{(p;a,b)}(\alpha, \beta)$ has finite $G_{\mathtt{geom}}$ if and only if the following inequalities hold:

(a) If $(a+b)x + y \neq 0$ then $\mathtt{V}\big(x\big) + \mathtt{V}\big(y\big) + \mathtt{V}\big(-ax - y\big) + \mathtt{V}\big(-bx\big) - \mathtt{V}\big(-(a+b)x - y\big) \geq 1/2$ must be true. If we make the change of variable $y \mapsto y - (a+b)x$ (so now $y \neq 0$) we rewrite the inequality as

$$\mathtt{V}\big(x\big) + \mathtt{V}\big(y - (a+b)x\big) + \mathtt{V}\big(bx - y\big) + \mathtt{V}\big(-bx\big) - \mathtt{V}\big(-y\big) \geq 1/2.$$

Finally we rewrite this using the relationship $\mathtt{V}(-t) + \mathtt{V}(t) = 1$ for $t \neq 0$:

$$\mathtt{V}\big(x\big) + \mathtt{V}\big(y - (a+b)x\big) + \mathtt{V}\big(bx - y\big) + \mathtt{V}\big(-bx\big) + \mathtt{V}\big(y\big) \geq 3/2.$$

(b) If $(a+b)x + y = 0$ then $\mathtt{V}\big(x\big) + \mathtt{V}\big(y\big) \geq 1/2$. Since $y = -(a+b)x$ this is equivalent to

$$\mathtt{V}\big(x\big) + \mathtt{V}\big(-(a+b)x\big) \geq 1/2.$$

The second part of the statement follows trivially using the known formula relating Kubert's $\mathtt{V}$ function and $[\cdot]_{p,r,-}$.

□

We will mostly work with the sehaves $\mathcal{M}(p; a, 1)$ and $\mathcal{M}(p; a, b, 1)$, that is, with $n = 1$ or $n = 2$. For $n = 1$ the criterion is just

$$\mathtt{V}(x) + 1/2 \geq \mathtt{V}_{\mathtt{RL}}(ax) \text{ for every } x \in (\mathbb{Q}/\mathbb{Z})_{\mathtt{not}\ p} \setminus \{0\}.$$

For $n = 2$ it is

$$\mathtt{V}(x) + \mathtt{V}(y) + 1/2 \geq \mathtt{V}_{\mathtt{RL}}(ax + by) \text{ for every } x, y \in (\mathbb{Q}/\mathbb{Z})_{\mathtt{not}\ p} \text{ with } (x, y) \neq (0, 0).$$

As it is expected, we can see from these inequalities that the finiteness of $G_{\mathtt{geom}}$ for $\mathcal{M}(p; a, b, 1)$ implies the finiteness of $G_{\mathtt{geom}}$ for both $\mathcal{M}(p; a, 1)$ and $\mathcal{M}(p; b, 1)$.

There are also some relations between the sheaves $\mathcal{B}$ and $\mathcal{M}$ for $n = 1$. Namely, if $\mathcal{B}_{(p;a,b)}$ has finite monodromy then we know that for every $x \in (\mathbb{Q}/\mathbb{Z})_{\mathtt{not}\ p} \setminus \{0\}$ the inequality $\mathtt{V}(x) + \mathtt{V}(-(a+b)x) \geq 1/2$ holds. Using that $\mathtt{V}(-t) + \mathtt{V}_{\mathtt{RL}}(t) = 1$, the previous inequality would imply the inequality

$$\mathtt{V}(x) + 1/2 \geq \mathtt{V}_{\mathtt{RL}}((a+b)x)$$

for every $x \in (\mathbb{Q}/\mathbb{Z})_{\mathtt{not}\ p} \setminus \{0\}$. This means that the finiteness of $G_{\mathtt{geom}}$ for $\mathcal{B}_{(p;a,b)}$ implies the finiteness of $G_{\mathtt{geom}}$ for $\mathcal{M}(p; a+b, 1)$. A bit more surprising is the following:

LEMMA 2.2.3.3. *Let $a, b \in \mathbb{N}$ be natural numbers. Then the finiteness of $G_{\mathtt{geom}}$ for $\mathcal{B}_{(p;a,b)}$ implies the finiteness of $G_{\mathtt{geom}}$ for both $\mathcal{M}(p; a, 1)$ and $\mathcal{M}(p; b, 1)$.*

PROOF. Assume $\mathcal{B}_{(p;a,b)}$ has finite $G_{\mathtt{geom}}$. Then, for every $x, y \in (\mathbb{Q}/\mathbb{Z})_{\mathtt{not}\ p} \setminus \{0\}$ we have the inequality

$$\mathtt{V}(x) + \mathtt{V}(y - (a+b)x) + \mathtt{V}(bx - y) + \mathtt{V}(-bx) + \mathtt{V}(y) \geq 3/2$$

and

$$\mathtt{V}(x) + 1/2 \geq \mathtt{V}_{\mathtt{RL}}((a+b)x).$$

Now we particularize these at points of the form (x, bx) with $x \neq 0$, i.e. $y = bx$ and $x \neq 0$. We consider two cases.

If x is such that $bx \neq 0$ then the first inequality applies and we get

$$3/2 \leq \mathtt{V}(x) + \mathtt{V}(-ax) + \mathtt{V}(0) + \mathtt{V}(-bx) + \mathtt{V}(bx) = \mathtt{V}(x) + \mathtt{V}(-ax) + 1$$

since $bx \neq 0$ and $\mathtt{V}(t) + \mathtt{V}(-t) = 1$ for $t \neq 0$. Rearranging and rewriting with $\mathtt{V}_{\mathtt{RL}}$ we reach the inequality $\mathtt{V}(x) + 1/2 \geq \mathtt{V}_{\mathtt{RL}}(ax)$ for x such that $bx \neq 0$.

If x is such that $bx = 0$, since $x \neq 0$, the second inequality applies and we get

$$\mathtt{V}(x) + 1/2 \geq \mathtt{V}_{\mathtt{RL}}((a+b)x) = \mathtt{V}_{\mathtt{RL}}(ax).$$

In summary, it does not matter if $bx = 0$ or not, we get the same inequality and it implies that $\mathcal{M}(p; a, 1)$ has finite $G_{\mathtt{geom}}$. To deduce the same for $\mathcal{M}(p; b, 1)$ observe that $\mathcal{B}_{(p;a,b)}$ has finite $G_{\mathtt{geom}}$ if and only if $\mathcal{B}_{(p;b,a)}$ does since we can just reindex the defining exponential sums.

□

From this lemma we see that the problem of deciding if $\mathcal{M}(p; a, 1)$ has finite $G_{\mathtt{geom}}$ is more fundamental than studying the same for the sheaves $\mathcal{B}$ or the sheaves $\mathcal{M}$ for higher $n > 1$.

We know some cases for which $\mathcal{M}(p; a, 1)$ and $\mathcal{M}(p; d_{n+1}, d_n, \ldots, 1)$ have finite $G_{\mathtt{geom}}$. These results are due, independtly, to Kubert [**Kat07**, §13] (for $n = 1$) and Rojas-León [**RL19**] (for arbitrary n) :

PROPOSITION 2.2.3.4 ([**Kat18**, Theorem 4.1],[**RL19**, Corollary 4]). *Let $a_n > \cdots > a_1 \geq 0$ be a sequence of non-negative integers. Then $\mathcal{M}(p; p^{a_n} + 1, \ldots, p^{a_1} + 1, 1)$ has finite $G_{\mathtt{geom}}$.*

PROOF. We use the idea of [**RL19**, Proof of Corollary 4]. We want to show that for every $r \geq 1$ and $0 \leq x_1, \ldots, x_n < p^r - 1$ the inequality

$$\left[\sum_{i=1}^{n} (p^{a_i} + 1)x_i\right]_{p,r} \leq \sum_{i=1}^{n} [x_i]_{p,r,-} + \frac{r(p-1)}{2}$$

holds true. We can assume without loss of generality that $x_i \neq 0$ for every i, so $[x_i]_{p,r,-} = [x_i]_{p,r}$. Observe that if $\sum_{i=1}^{n} [x_i]_{p,r} \geq \frac{r(p-1)}{2}$ then the inequality is trivially satisfied since the function $[\cdot]_{p,r}$ takes values less than $r(p-1)$. Assume that $\sum_{i=1}^{n} [x_i]_{p,r} < r(p-1)/2$. Then

$$\left[\sum_{i=1}^{n} (p^{a_i} + 1)x_i\right]_{p,r} \leq \sum_{i=1}^{n} [(p^{a_i} + 1)x_i]_{p,r} \leq 2 \cdot \sum_{i=1}^{n} [x_i]_{p,r} < \sum_{i=1}^{n} [x_i]_{p,r} + \frac{r(p-1)}{2}.$$

□

PROPOSITION 2.2.3.5 ([**Kat18**, Theorems 4.2 and 4.3],[**RL19**, Corollary 5]). *Let $a_n > \cdots > a_1 \geq 1$ be a sequence of non-negative integers and $m \in \mathbb{Z}_{\geq 0}$.*

(a) *If $m = 0$ and p is odd, then*

$$\mathcal{M}(p; (p^{a_n} + 1)/2, \ldots, (p^{a_1} + 1)/2, 1)$$

has finite $G_{\mathtt{geom}}$.

(b) *If $m > 0$ and a_i is odd for every $i = 1, \dots, n$ then*

$$\mathcal{M}(p; (p^{ma_n}+1)/(p^m+1), \dots, (p^{ma_1}+1)/(p^m+1), 1)$$

has finite $G_{\texttt{geom}}$.

PROOF. Assume $m = 0$. Let $r \geq 1$ and $0 \leq x_1, \dots, x_n < p^r - 1$ not all equal to 0. Actually, without loss of generality, we assume all $x_i \neq 0$ so $[x_i]_{p,r} = [x_i]_{p,r-}$. We use the idea of [**RL19**, Proof of Corollary 5].

$$r(p-1) - \left[\sum_{i=1}^{n}(p^{a_i}+1)x_i\right]_{p,r} = r(p-1) - \left[2\sum_{i=1}^{n}\frac{p^{a_i}+1}{2}x_i\right]_{p,r} = \left[-2\sum_{i=1}^{n}\frac{p^{a_i}+1}{2}x_i\right]_{p,r}$$
$$\leq 2\left[-\sum_{i=1}^{n}\frac{p^{a_i}+1}{2}x_i\right]_{p,r} = 2r(p-1) - 2\left[\sum_{i=1}^{n}\frac{p^{a_i}+1}{2}x_i\right]_{p,r}.$$

Rearranging we get

$$\left[\sum_{i=1}^{n}\frac{p^{a_i}+1}{2}x_i\right]_{p,r} \leq \frac{1}{2}\left[\sum_{i=1}^{n}(p^{a_i}+1)x_i\right]_{p,r} + \frac{r(p-1)}{2} \leq \frac{1}{2}\sum_{i=1}^{n}\left[(p^{a_i}+1)x_i\right]_{p,r} + \frac{r(p-1)}{2}$$
$$\leq \sum_{i=1}^{n}[x_i]_{p,r,-} + \frac{r(p-1)}{2}.$$

Notice the same argument works for the second case, since $2 = p^0 + 1$ and the only property we use of this number is that $[(p^0+1)x]_{p,r} \leq 2[x]_{p,r}$. The distinction in the statement is just to assure that $(p^{a_i}+1)/2$ or $(p^{ma_i}+1)/(p^m+1)$ is an integer for every $i = 1, \dots, n$ (see [**RL19**, Remark 1]).

□

REMARK 2.2.3.6. *Kubert's types and finiteness of $G_{\texttt{geom}}$:*

The numbers appearing in the previous corollaries have a quite particular base-p-expansion.

The numbers $p^a + 1$ for $a > 0$ are those with base-p-expansion given by $(10\dots01)_p$, with $a-1$ zeroes between the 1 digits. If $a = 0$ and p is odd, then $2 = (2)_p$.

For p an odd prime we have

$$\frac{p^m+1}{2} = 1 + \frac{p^m-1}{2} = \left(\left(\frac{p-1}{2}\right)\dots\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)\right)_p,$$

with the digit $(p-1)/2$ repeated $m-1$ times.

For l an odd integer and $m \geq 1$, denoting $q = p^m$, we have

$$\frac{q^l+1}{q+1} = \sum_{i=0}^{l-1}(-1)^i q^i = 1 + q(q-1) + q^3(q-1) + \dots + q^{l-2}(q-1)$$
$$= 1 + (q-1)\sum_{i=1}^{(l-1)/2} q^{2i-1} = 1 + (p-1)\Big(\sum_{i=0}^{m-1}p^i\Big)\Big(\sum_{i=1}^{(l-1)/2}p^{m(2i-1)}\Big)$$
$$= \Bigg(\underbrace{\underbrace{(p-1)\dots(p-1)}_{m\text{-times}}\underbrace{0\dots0}_{m\text{-times}}\dots\underbrace{(p-1)\dots(p-1)}_{m\text{-times}}\underbrace{0\dots0}_{m\text{-times}}}_{(l-1)/2\text{-times}}\Bigg)_p + (1)_p.$$

The corollaries above tell us that if we do not mix Kubert types the monodromy groups keep finite. Our interest will be in finding new integers giving finite monodromy for $n = 1$ that do not pertain to a Kubert type and/or integers that mix Kubert types but still give finite monodromy for $n > 1$.

■

Despite the second formulation of Corollary 2.2.3.1 is the useful one for computations, we need a further formulation suitable for inductive proofs:

COROLLARY 2.2.3.7 ([**KRLT20**, Theorem 2.12]). *Let $D := d_{n+1} > d_n > \cdots > d_1 = 1$ be a sequence of integers coprime to p. The $\overline{\mathbb{Q}}_\ell$-sheaf $\mathcal{M}(p; d_{n+1}, d_n, \ldots, d_1)$ has finite $G_{\mathtt{geom}}$ if and only if there exists some real $A \geq 0$ such that for every positive integer r and every $0 \leq x_2, \ldots, x_{n+1} < q^r - 1$ which are not all 0, we have the inequality*

$$\frac{r(p-1)}{2} + A + \sum_{i=2}^{n+1} [x_i]_p \geq \left[\sum_{i=2}^{n+1} d_i x_i \right]_p .$$

PROOF. We show that the inequality of this corollary is equivalent to the inequality of the previous one.

Suppose there is some $A \geq 0$ such that $r(p-1)/2 + A + \sum_{i=2}^{n+1} [x_i]_p \geq \left[\sum_{i=2}^{n+1} d_i x_i \right]_p$ holds for every $r \geq 1$ and every $0 \leq x_2, \ldots, x_{n+1} < q^r - 1$ which are not all zero. Then $\sum_{i=2}^{r+1} d_i x_i > 0$, and

$$\begin{aligned} \left[\sum_{i=2}^{n+1} d_i x_i \right]_{p,r} &\leq \left[\sum_{i=2}^{n+1} d_i x_i \right]_p \leq \sum_{i=2}^{n+1} [x_i]_p + \frac{r(p-1)}{2} + A \\ &= \sum_{i=2}^{n+1} [x_i]_{p,r,-} + \frac{r(p-1)}{2} + A. \end{aligned}$$

Hence, for every $m \geq 1$

$$\left[\sum_{i=2}^{r+1} d_i \frac{p^{mr}-1}{p^r-1} x_i \right]_{p,mr} \leq \sum_{i=2}^{n+1} \left[\frac{p^{mr}-1}{p^r-1} x_i \right]_{p,mr,-} + \frac{mr(p-1)}{2} + A.$$

Using Proposition 2.2.2.3 and dividing by m we get

$$\left[\sum_{i=2}^{r+1} d_i x_i \right]_{p,r} \leq \sum_{i=2}^{n+1} [x_i]_{p,r,-} + \frac{r(p-1)}{2} + \frac{A}{m}$$

for every $m \geq 1$. Taking $m \to \infty$ we get our seeked inequality.

Conversely, assume

$$\frac{r(p-1)}{2} + \sum_{i=2}^{n+1} [x_i]_{p,r,-} \geq \left[\sum_{i=2}^{n+1} d_i x_i \right]_{p,r}$$

is satisfied for every $r \geq 1$ and every $0 \leq x_2, \ldots, x_{n+1} < p^r - 1$ which are not all 0. Let l be an integer such that $\sum_{i=2}^{n+1} d_i < p^l$. Then, if $0 \leq x_2, \ldots, x_{n+1} < p^r - 1$, $\sum_{i=2}^{n+1} d_i x_i < p^{r+l} - 1$, so

$$\begin{aligned} \left[\sum_{i=2}^{n+1} d_i x_i \right]_p = \left[\sum_{i=2}^{n+1} d_i x_i \right]_{p,r+l} &\leq \sum_{i=2}^{n+1} [x_i]_{p,r+l,-} + \frac{(r+l)(p-1)}{2} \\ &= \sum_{i=2}^{n+1} [x_i]_p + \frac{r(p-1)}{2} + \frac{l(p-1)}{2}. \end{aligned}$$

Taking $A = l(p-1)/2$ we get the inequality from the statement.

□

2.3. Computational approach and numeric explorations

In this section we explain how to use effectively the criteria given above, compare the consequent algorithm with previous ones and present some experimental phenomena obtained by use of these ideas. We mostly focus on the sheaves $\mathcal{M}(p; a, 1)$, $\mathcal{M}(p; a, b, 1)$ and $\mathcal{B}_{(p;a,b)}$.

2.3.1. The sheaves $\mathcal{M}(p,a,1)$. Recall that the monodromy group $G_{\mathtt{geom}}$ of the $\overline{\mathbb{Q}}_\ell$-sheaf $\mathcal{M}(p;a,1)$ on $\mathbb{A}^1_{\mathbb{F}_p}$ is finite if and only if for every $r \geq 1$ and every $0 < x < p^r - 1$ we have

$$[ax]_{p,r} \leq [x]_{p,r,-} + \frac{r(p-1)}{2}.$$

Our approach is to decide if a does not have finite monodromy by checking the inequality against every $x \in (0, p^r - 1) \cap \mathbb{Z}$ with r running through some finite set of integers, usually $[1, L] \cap \mathbb{Z}$. Just doing this we get the naive algorithm:

Algorithm 1 Naive algorithm for finding candidates with finite $G_{\mathtt{geom}}$ for $\mathcal{M}(p;\cdot,1)$

Input: $p > 0$ prime number; $L > 0$ an integer
  for $1 \leq a \leq p^L - 1$ **do**
    if $a \pmod p = 0$ **then**
      continue a's loop
    end if
    for $1 \leq r \leq L$ **do**
      $t \leftarrow 0$
      for $1 \leq x < p^r - 1$ **do**
        $t \leftarrow [x]_{p,r,-} - [ax]_{p,r} + r(p-1)/2$
        if $t < 0$ **then**
          break x's loop
        end if
      end for
      if $t < 0$ **then**
        break r's loop
      end if
    end for
    if $t \geq 0$ **then**
      print a
    end if
  end for

We will use this algorithm as our basic layout and incorporate some simplifications to it. In general, to improve the naive approach we can reduce the sets where we look for witnesses ($(0, p^r - 1) \cap \mathbb{Z}$ for $1 \leq r \leq L$ above) and obtain from just one a such that $\mathcal{M}(p;a,1)$ does not have finite $G_{\mathtt{geom}}$ as many new b's as possible such that $\mathcal{M}(p;b,1)$ does also not have finite $G_{\mathtt{geom}}$. The following observations go in this direction:

1. For every $r \geq 1$, both $[\cdot]_{p,r,-}$ and $[\cdot]_{p,r}$ are periodic functions of period $p^r - 1$. This has two consequences.

   First of all, if $a \in \mathbb{Z}_{>0}$, to evaluate $[x]_{p,r-} - [ax]_{p,r}$ against every $x \in (0, p^r - 1) \cap \mathbb{Z}$, we only have to consider $ax \pmod{p^r - 1} = \Big(\big(a \pmod{p^r - 1}\big)x\Big) \pmod{p^r - 1}$. This reduces the number of operations needed to perform the multiplication of integers a, x.

   Second, if there exists $x \in (0, p^r - 1) \cap \mathbb{Z}$ such that $[ax]_{p,r} > [x]_{p,r,-} + r(p-1)/2$ (i.e. x is a whitness for the non-finiteness of monodromy for $\mathcal{M}(p;a,1)$), then $\big[(a + k(p^r - 1))x\big]_{p,r} > [x]_{p,r,-} + r(p-1)/2$ for every $k \in \mathbb{Z}$. In particular, $\mathcal{M}(p; a + k(p^r - 1), 1)$ does not have finite $G_{\mathtt{geom}}$ for every $k \geq 0$.
2. For every $r \geq 1$ both $[\cdot]_{p,r,-}$ and $[\cdot]_{p,r}$ are invariant under multiplication by p. This again has two practical implications.

   In the first place, if $x \in (0, p^r - 1) \cap \mathbb{Z}$ then x satisfies the inequality $[ax]_{p,r} \leq [x]_{p,r,-} + r(p-1)/2$ if and only if $px \pmod{p^r - 1}$ satisfies the same inequality. Moreover,

since we can consider arguments modulo p^r-1, we see x satisfies the inequality at "level" r if and only if any rotation of its base-p-expansion does. This allows us to restrict the search for witnesses at each level r to the set of orbits of $\mathbb{Z}/(p^r-1)\mathbb{Z}$ under the action by multiplication of $p \pmod{p^r-1}$. These orbits are well-known in combinatorics, they are *$(p-1)$-ary necklaces of length r*.

Second, if we find that $x \in (0, p^r-1) \cap \mathbb{Z}$ is a witness for the non-finiteness of $G_{\texttt{geom}}$ for $\mathcal{M}(p;a,1)$ at level r, then $\mathcal{M}(p;p^i a \pmod{p^r-1},1)$ does not also has finite $G_{\texttt{geom}}$ for any $i = 0,\dots,r-1$.

3. Observe that the inequality $[ax]_{p,r} \leq [x]_{p,r,-} + r(p-1)/2$ is an empty condition whenever $[x]_{p,r,-} \geq r(p-1)/2$ since $[ax]_{p,r} \leq r(p-1)$ always holds. This restrict us further to those orbits such that each (or any) representative verifies $[x]_{p,r,-} < r(p-1)/2$.
4. We introduce a bit of notation that will simplify our algorithms. We write $a \circlearrowleft_r p$ for the orbit of $a \pmod{p^r-1}$ under multiplication by p. Observe that each orbit $a \circlearrowleft_r p$ can be well-ordered by considering the lexicographic order on the base-p-expansions of its elements (starting from the right). Using this order, we denote the set of smallest representatives of $(p-1)$-ary necklaces of length r by $\texttt{Necks}_r(p)$.

These remarks lead to an improvement of the naive approach. We collect them in Algorithm 2.

Algorithm 2 Algorithm for finding candidates with finite $G_{\texttt{arith}}$ for $\mathcal{M}(p;\cdot,1)$

Input: $p > 0$ prime number; $L > 0$ an integer
  $A \leftarrow$ Boolean array indexed from 1 to p^L-1 with all its entries equal to `True`
  for $1 \leq a \leq p^L-1$ **do**
    if $a \pmod p = 0$ **then**
      a-th entry of $A \leftarrow$ `False`
    end if
  end for
  for $1 \leq a \leq p^L-1$ **do**
    if a-th entry of $A =$ `False` **then**
      continue a's loop
    end if
    for $1 \leq r \leq L$ **do**
      $a' \leftarrow a \pmod{p^r-1} \in \{1,\dots,p^r-1\}$
      $t \leftarrow 0$
      for $x \in \texttt{Necks}_r(p)$ **do**
        if $[x]_{p,r,-} \geq r(p-1)/2$ **then**
          continue x's loop
        end if
        $t \leftarrow [x]_{p,r,-} - \left[a'x \pmod{p^r-1}\right]_{p,r} + r(p-1)/2$
        if $t < 0$ **then**
          for $i = 0,\dots,r-1$ **do**
            $a' \leftarrow pa' \pmod{p^r-1}$
            for $0 \leq k \leq \left\lfloor \frac{(p^L-1)-a'}{p^r-1} \right\rfloor$ **do**
              $\big(a' + k(p^r-1)\big)$-th entry of $A \leftarrow$ `False`
            end for
          end for
          break x's loop
        end if
      end for

```
        if t < 0 then
            break r's loop
        end if
    end for
    if t ≥ 0 then
        print a
    end if
end for
```

Remarks 2.3.1.1.

1. Observe that in both algorithms we only print integers $a \geq 1$ for which we have not been able to find a witness for the non-finiteness of $G_{\texttt{geom}}$ for $\mathcal{M}(p; a, 1)$ at any level $r = 1, \ldots, L$. Clearly, this does not mean $\mathcal{M}(p; a, 1)$ has finite $G_{\texttt{geom}}$. The utility of these algorithms is to find strong candidates, that is, find integers a that satisfies all our inequalities up to some big level L. At this point it is natural to ask if there are upper bounds to the number of levels we have to check in order to establish if certain $\mathcal{M}(p; a, 1)$ has finite monodromy or not. This question is addressed in Rojas-León's paper [**RL23a**] using the notion of complexity for lisse $\overline{\mathbb{Q}}_\ell$-sheaves introduced by Sawin (see the paper for more details). For the moment being, it seems the bounds these methods can provide us are impractical for computational purposes.
2. It should be observed that our algorithm has some resemblence to classic sieve algorithms such as Eratosthenes' sieve. The main differences are that we have to check the inequalities which are by no means trivial, and that we have for each $r \geq 1$ a whole set of exclusions that we "propagate" modulo $p^r - 1$.
3. As we have seen, our algorithm makes essential usage of necklaces. In fact, it needs the smallest representative in each orbit with respect to lexicographic order on base-p expansions. We make use of Cattell–Ruskey–Sawada–Serra–Miers algorithm [**CRS$^+$00**, Algorithm 2.1 and Table 1] for our purpose. This algorithm generates lexicographically minimal necklaces of arbitrary length and on arbitrary finite alphabets in constant amortized time. Moreover, if desired, the algorithm can output the period of the corresponding necklace, that is, the size of its orbit. Essentially, the algorithm computes efficiently the permutation p induces on $S_{p^r-1} = \{0, \ldots, p^r - 2\}$ acting by multiplication modulo $p^r - 1$.
4. This algorithm has been implemented succesfully with *Julia Programming Language* [**BEKS17**]. In practice we precompute a few things for the code to be practical. Since powers of the base prime p are needed frequently, it is more efficient to keep the values $\{1, p, p^2, \ldots, p^L\}$ in memory rather than computing them each time. Also, since we make several loops on representatives of necklaces, we precompute once and for all the sets $\texttt{Necks}_r(p)$ for $r = 1, \ldots, L$ using the algorithm from previous item. The same philosophy applies to the computation of digital sums, so our code previously computes an array where all values of $[t]_p$ for $t = 1, \ldots, p^L - 1$ are saved. For details, see the Appendix. These precomputations are an important limitation to the performance of the code for big values of L.

2.3.1.1. *Experimental comparison of algorithms.* Here we present some tables showing the performance of the naive approach and the algorithm with our improvements. We include the column *Checks* which counts the number of integers a that were tested checking inequalities and not using congruences or rotations. As we remarked above, even for Algorithm 1 we precompute and save in memory some values that are used several times during the execution. This explains the *Memory* column for Algorithm 1. The following benchmarks were obtained in a machine with an *Intel Core i7-11700* and *16 GB of RAM*.

TABLE 1. Experimental comparison of algorithms with $p = 2$.

	Algorithm 1			Algorithm 2		
L	Memory	Time (secs)	Checks	Memory	Time (secs)	Checks
1	416 bytes	0.000003	2^0	944 bytes	0.000007	1
2	496 bytes	0.000003	2^1	1.281 KiB	0.000007	2
3	528 bytes	0.000004	2^2	1.625 KiB	0.000007	4
4	656 bytes	0.000004	2^3	2.031 KiB	0.000008	8
5	800 bytes	0.000005	2^4	2.484 KiB	0.000009	13
6	1.078 KiB	0.000007	2^5	3.062 KiB	0.000010	22
7	1.641 KiB	0.000015	2^6	4.609 KiB	0.000014	34
8	2.953 KiB	0.000039	2^7	6.875 KiB	0.000020	55
9	4.984 KiB	0.000098	2^8	9.906 KiB	0.000031	75
10	9.047 KiB	0.000258	2^9	14.969 KiB	0.000052	113
11	17.047 KiB	0.000624	2^{10}	26.891 KiB	0.000091	163
12	33.031 KiB	0.001353	2^{11}	46.859 KiB	0.000149	205
13	65.062 KiB	0.002805	2^{12}	94.297 KiB	0.000249	276
14	129.125 KiB	0.005688	2^{13}	174.297 KiB	0.000411	357
15	257.125 KiB	0.011601	2^{14}	347.703 KiB	0.000740	455
16	513.453 KiB	0.024495	2^{15}	651.406 KiB	0.001326	596
17	1.001 MiB	0.050667	2^{16}	1.249 MiB	0.002566	746
18	2.002 MiB	0.109405	2^{17}	2.502 MiB	0.004871	940
19	4.002 MiB	0.223869	2^{18}	5.171 MiB	0.009905	1122
20	8.002 MiB	0.483419	2^{19}	9.871 MiB	0.020577	1291
21	16.002 MiB	1.196611	2^{20}	19.582 MiB	0.049972	1521
22	32.002 MiB	3.324997	2^{21}	39.487 MiB	0.120472	1786
23	64.002 MiB	7.585174	2^{22}	77.900 MiB	0.277792	2094
24	128.002 MiB	17.896381	2^{23}	153.354 MiB	0.613388	2456
25	265.002 MiB	39.491887	2^{24}	302.916 MiB	1.315770	2876
26	512.002 MiB	91.082204	2^{25}	582.478 MiB	2.686707	3198
27	1.000 GiB	219.994560	2^{26}	1.149 GiB	6.546916	3532
28	?	?	?	2.237 GiB	19.373952	3938
29	?	?	?	4.413 GiB	46.468393	4552
30	?	?	?	8.762 GiB	102.230161	5397

TABLE 2. Experimental comparison of algorithms with $p = 3$.

	Algorithm 1			Algorithm 2		
L	Memory	Time (secs)	Checks	Memory	Time (secs)	Checks
1	416 bytes	0.000003	$2 \cdot 3^0$	944 bytes	0.000007	2
2	528 bytes	0.000003	$2 \cdot 3^1$	1.312 KiB	0.000006	6
3	672 bytes	0.000004	$2 \cdot 3^2$	1.766 KiB	0.000008	15
4	1.172 KiB	0.000008	$2 \cdot 3^3$	3.234 KiB	0.000011	35
5	2.438 KiB	0.000041	$2 \cdot 3^4$	5.484 KiB	0.000019	72
6	6.391 KiB	0.000141	$2 \cdot 3^5$	13.250 KiB	0.000040	127
7	17.750 KiB	0.000537	$2 \cdot 3^6$	28.562 KiB	0.000093	230
8	52.188 KiB	0.001894	$2 \cdot 3^7$	78.422 KiB	0.000210	370
9	154.718 KiB	0.005798	$2 \cdot 3^8$	226.047 KiB	0.000651	521
10	462.344 KiB	0.018401	$2 \cdot 3^9$	645.922 KiB	0.001177	765
11	1.353 MiB	0.058771	$2 \cdot 3^{10}$	1.7848 MiB	0.003614	1102
12	4.056 MiB	0.186331	$2 \cdot 3^{11}$	5.166 MiB	0.008290	1515
13	12.165 MiB	0.659928	$2 \cdot 3^{12}$	14.989 MiB	0.026610	2086
14	36.492 MiB	2.726438	$2 \cdot 3^{13}$	45.609 MiB	0.119359	2671
15	109.475 MiB	9.682236	$2 \cdot 3^{14}$	130.186 MiB	0.397085	3397
16	328.442 MiB	35.711725	$2 \cdot 3^{15}$	390.363 MiB	1.326211	4296
17	985.263 MiB	132.235027	$2 \cdot 3^{16}$	1.105 GiB	4.999794	5663
18	?	?	?	3.204 GiB	21.931799	7924
19	?	?	?	9.514 GiB	77.184047	11336

TABLE 3. Experimental comparison of algorithms with $p = 5$.

	Algorithm 1			Algorithm 2		
L	Memory	Time (secs)	Checks	Memory	Time (secs)	Checks
1	432 bytes	0.000005	$4 \cdot 5^0$	960 bytes	0.000007	4
2	656 bytes	0.000004	$4 \cdot 5^1$	1.438 KiB	0.000008	14
3	1.453 KiB	0.000010	$4 \cdot 5^2$	3.234 KiB	0.000013	43
4	5.516 KiB	0.000077	$4 \cdot 5^3$	11.109 KiB	0.000031	103
5	24.938 KiB	0.000510	$4 \cdot 5^4$	45.734 KiB	0.000112	263
6	122.688 KiB	0.003043	$4 \cdot 5^5$	188.406 KiB	0.000360	466
7	611.000 KiB	0.015977	$4 \cdot 5^6$	927.953 KiB	0.001292	745
8	2.981 MiB	0.087240	$4 \cdot 5^7$	3.965 MiB	0.005960	1266
9	14.902 MiB	0.543751	$4 \cdot 5^8$	19.727 MiB	0.034570	2259
10	74.507 MiB	3.850998	$4 \cdot 5^9$	90.717 MiB	0.221591	4274

⟶

Table 3 *(continued).*

	Algorithm 1			Algorithm 2		
L	Memory	Time (secs)	Checks	Memory	Time (secs)	Checks
11	372.530 MiB	23.994012	$4 \cdot 5^{10}$	431.206 MiB	1.177317	6107
12	1.819 GiB	165.095751	$4 \cdot 5^{11}$	2.043 GiB	9.309871	8106
13	?	?	?	10.389 GiB	57.875320	11906

TABLE 4. Experimental comparison of algorithms with $p = 7$.

	Algorithm 1			Algorithm 2		
L	Memory	Time (secs)	Checks	Memory	Time (secs)	Checks
1	448 bytes	0.000003	$6 \cdot 7^0$	976 bytes	0.000007	6
2	848 bytes	0.000005	$6 \cdot 7^1$	2.281 KiB	0.000008	21
3	3.203 KiB	0.000026	$6 \cdot 7^2$	8.484 KiB	0.000021	67
4	19.312 KiB	0.000257	$6 \cdot 7^3$	39.719 KiB	0.000075	154
5	131.812 KiB	0.002181	$6 \cdot 7^4$	197.453 KiB	0.000358	395
6	919.750 KiB	0.019089	$6 \cdot 7^5$	1.612 MiB	0.001976	874
7	6.284 MiB	0.138650	$6 \cdot 7^6$	8.668 MiB	0.011353	1430
8	43.983 MiB	1.703619	$6 \cdot 7^7$	57.410 MiB	0.127027	2315
9	307.874 MiB	14.556409	$6 \cdot 7^8$	363.234 MiB	0.915330	4277
10	2.105 GiB	147.667029	$6 \cdot 7^9$	2.474 GiB	9.157338	11754
11	?	?	?	16.624 GiB	423.844096	23087

2.3.1.2. *Some numerical phenomena observed.* We start looking at some of the outputs the algorithm returns. We use the following notation. For a fixed prime p, we write $n_{\mathtt{I}}$ to indicate n has Kubert type of the form $p^r + 1$ for some $r \geq 1$. Similarly, if p is odd, we write $n_{\mathtt{II}}$ if n has Kubert type $(p^r+1)/2$ for some $r \geq 0$. Finally, we write $n_{\mathtt{III},m}$ if n has Kubert type $(q^r+1)/(q+1)$ for some $r \geq 1$ odd and $q = p^m$. Whenever a number n can be realized using different Kubert types, we use the subindex attending to the ordering $\mathtt{I} > \mathtt{II} > \mathtt{III}$.

$\boxed{\boldsymbol{p = 2}}$ Running our algorithm for $L = 30$ we get the numbers:

$$\begin{array}{lllll}
\{3_{\mathtt{I}}, & 5_{\mathtt{I}}, & 9_{\mathtt{I}}, & 11_{\mathtt{III},1}, & 13_{\mathtt{III},2}, \\
17_{\mathtt{I}}, & 33_{\mathtt{I}}, & 43_{\mathtt{III},1}, & 57_{\mathtt{III},3}, & 65_{\mathtt{I}}, \\
129_{\mathtt{I}}, & 171_{\mathtt{III},1}, & 205_{\mathtt{III},2}, & 241_{\mathtt{III},4}, & 257_{\mathtt{I}}, \\
513_{\mathtt{I}}, & 683_{\mathtt{III},1}, & 993_{\mathtt{III},5}, & 1025_{\mathtt{I}}, & 2049_{\mathtt{I}}, \\
2731_{\mathtt{III},1}, & 3277_{\mathtt{III},2}, & 3641_{\mathtt{III},3}, & 4033_{\mathtt{III},6}, & 4097_{\mathtt{I}}, \\
8193_{\mathtt{I}}, & 10923_{\mathtt{III},1}, & 16257_{\mathtt{III},7}, & 16385_{\mathtt{I}}, & 32769_{\mathtt{I}}, \\
43691_{\mathtt{III},1}, & 52429_{\mathtt{III},2}, & 61681_{\mathtt{III},4}, & 65281_{\mathtt{III},8}, & 65537_{\mathtt{I}}, \\
131073_{\mathtt{I}}, & 174763_{\mathtt{III},1}, & 233017_{\mathtt{III},3}, & 261633_{\mathtt{III},9}, & 262145_{\mathtt{I}}, \\
524289_{\mathtt{I}}, & 699051_{\mathtt{III},1}, & 838861_{\mathtt{III},2}, & 1016801_{\mathtt{III},5}, & 1047553_{\mathtt{III},10},
\end{array}$$

1048577_{I}, 2097153_{I}, $2796203_{\mathrm{III},1}$, $4192257_{\mathrm{III},11}$, 4194305_{I},
8388609_{I}, $11184811_{\mathrm{III},1}$, $13421773_{\mathrm{III},2}$, $14913081_{\mathrm{III},3}$, $15790321_{\mathrm{III},4}$,
$16519105_{\mathrm{III},6}$, $16773121_{\mathrm{III},12}$, 16777217_{I}, 33554433_{I}, $44739243_{\mathrm{III},1}$,
$67100673_{\mathrm{III},13}$, 67108865_{I}, 134217729_{I}, $178956971_{\mathrm{III},1}$, $214748365_{\mathrm{III},2}$,
$266354561_{\mathrm{III},7}$, $268419073_{\mathrm{III},14}$, 268435457_{I}, 536870913_{I}, $715827883_{\mathrm{III},1}$,
$954437177_{\mathrm{III},3}$, $1041204193_{\mathrm{III},5}$, $1073709057_{\mathrm{III},15}\}$.

As we can see, every number a for which the algorithm is not able to decide if $\mathcal{M}(2;a,1)$ has non-finite $G_{\mathtt{geom}}$ is actually of Kubert type, i.e. they verify $\mathcal{M}(p;a,1)$ has finite $G_{\mathtt{geom}}$. Since, up to $2^{30}-1 > 10^9$ we have checked only numbers of Kubert type have associated sheaf with finite $G_{\mathtt{geom}}$, it is natural to conjecture that $\mathcal{M}(2;a,1)$ has finite $G_{\mathtt{geom}}$ if and only if a is of Kubert type. This is precisely what Katz (see [**Kat18**]) and Rojas-León (see [**RL19**, Conjecture 1]) conjectured independently in 2017, using much less computational evidence than us. In fact, with our implementation we were able to check this conjecture up to 10^9. A much stronger theorem has been recently proved by Katz and Tiep in [**KT23**, Theorem 10.2.6] which implies this conjecture in particular (see the analysis for primes $p = 3, 5$ and 7 below to get a taste of the content of this recent theorem).

$\boxed{\boldsymbol{p=3}}$ For $L = 16$ we obtain the following:

$\{2_{\mathrm{I}}$, 4_{I}, 5_{II}, $7_{\mathrm{III},1}$, 10_{I},
14_{II}, 28_{I}, 41_{II}, $61_{\mathrm{III},1}$, $73_{\mathrm{III},2}$,
82_{I}, 122_{II}, 244_{I}, 365_{II}, $547_{\mathrm{III},1}$,
$703_{\mathrm{III},3}$, 730_{I}, 1094_{II}, 2188_{I}, 3281_{II},
$4921_{\mathrm{III},1}$, $5905_{\mathrm{III},2}$, $6481_{\mathrm{III},4}$, 6562_{I}, 9842_{II},
19684_{I}, 29525_{II}, $44287_{\mathrm{III},1}$, $58807_{\mathrm{III},5}$, 59050_{I},
88574_{II}, 177148_{I}, 265721_{II}, $398581_{\mathrm{III},1}$, $478297_{\mathrm{III},2}$,
$512461_{\mathrm{III},3}$, $530713_{\mathrm{III},6}$, 531442_{I}, 797162_{II}, 1594324_{I},
2391485_{II}, $3587227_{\mathrm{III},1}$, $4780783_{\mathrm{III},7}$, 4782970_{I}, $\mathbf{4782971}$,
7174454_{II}, 14348908_{I}, 21523361_{II}, $32285041_{\mathrm{III},1}$, $38742049_{\mathrm{III},2}$,
$42521761_{\mathrm{III},4}$, $43040161_{\mathrm{III},8}\}$.

Every number is of Kubert type except $4782971 = (100000000000002)_3$. This tells us that $a = 4782971$ is a strong candidate for $\mathcal{M}(3;a,1)$ to have finite $G_{\mathtt{geom}}$. However, this is illusory. Once we reach $L = 17$ we find that $x = 773005 = (1110021100211)_3$ is a witness with $r = 17$ of the non-finiteness of $G_{\mathtt{geom}}$ for $\mathcal{M}(3;a,1)$. With our algorithm we can check only Kubert types arise up to $L = 19$ and again it is natural to expect that only Kubert types give $\mathcal{M}(3;a,1)$ with finite $G_{\mathtt{geom}}$. This is the case and it follows from Katz–Tiep result.

$\boxed{\boldsymbol{p=5}}$ For $L = 13$ the algorithm returns the following:

$\{2_{\mathrm{I}}$, 3_{II}, 6_{I}, $\mathbf{7}$, 13_{II},
$21_{\mathrm{III},1}$, 26_{I}, 63_{II}, 126_{I}, 313_{II},
$521_{\mathrm{III},1}$, $601_{\mathrm{III},2}$, 626_{I}, 1563_{II}, 3126_{I},
7813_{II}, $13021_{\mathrm{III},1}$, $15501_{\mathrm{III},3}$, 15626_{I}, 39063_{II},
78126_{I}, 195313_{II}, $325521_{\mathrm{III},1}$, $375601_{\mathrm{III},2}$, $390001_{\mathrm{III},4}$,
390626_{I}, 976563_{II}, 1953126_{I}, 4882813_{II}, $8138021_{\mathrm{III},1}$,

$9762501_{\mathrm{III},5}$, 9765626_{I}, 24414063_{II}, 48828126_{I}, 122070313_{II}, $203450521_{\mathrm{III},1}$, $234750601_{\mathrm{III},2}$, $242203001_{\mathrm{III},3}$, $244125001_{\mathrm{III},6}$, 244140626_{I}, $610351563_{\mathrm{II}}\}$.

Again, every number except $7 = (12)_5$ is of Kubert type. This time, in contrast to what we observed for $p = 3$, it does not matter how far we go with higher values of L, $a = 7$ will always satisfy the inequalities. We show $G_{\mathtt{geom}}$ for $\mathcal{M}(5; 7, 1)$ is finite in two steps:

LEMMA 2.3.1.2 ([**KRL19**, Lemma 2.3]). *Let $r \geq 1$ be a positive integer and $x \in \{0, \ldots, 5^r - 1\}$ an integer such that $x \pmod 5 \neq 2$. Then $[7x]_5 \leq [x]_5 + 2r$.*

PROOF. We proceed by induction. For $r \leq 2$ it is checked manually. For $r \geq 3$ we proceed as follows. Let $x = \sum_{i=0}^{r-1} x_i 5^i$ be the base-5-expansion of x and split the proof in two cases:

Case 1: There exists $j \in \{1, \ldots, r-1\}$ such that $x_j \neq 2$. We write $x_{<j} = \sum_{i=0}^{j-1} x_i 5^i$ and $x_{\geq j} = \sum_{i=0}^{r-j-1} x_{i+j} 5^i$. Then

$$[7x]_5 = [7x_{<j} + 5^j \cdot 7x_{\geq j}]_5 \leq [7x_{<j}]_5 + [7x_{\geq j}]_5 \leq [x_{<j}]_5 + 2j + [x_{\geq j}]_5 + 2(r-j) = [x]_5 + 2r.$$

Case 2: $x_j = 2$ for all $j \in \{1, \ldots, r-1\}$. Write $x_{\geq 1} = \sum_{i=0}^{r-2} x_{i+1} 5^i = 2 \sum_{i=0}^{r-2} 5^i$. We evaluate $[7x_{\geq 1}]_5$ explicitly. Observe that

$$7x_{\geq 1} = 5x_{\geq 1} + 2x_{\geq 1} = \sum_{i=1}^{r-1} 2 \cdot 5^i + \sum_{i=0}^{r-2} 4 \cdot 5^i = 4 + 5 + \sum_{i=2}^{r-2} 2 \cdot 5^i + 3 \cdot 5^{r-1},$$

hence $[7x_{\geq 1}]_5 = 4 + 1 + 2(r-3) + 3 = 2(r+1)$. From this we find:

$$\begin{aligned}[7x]_5 &\leq [7x_0]_5 + [7x_{\geq 1}]_5 = [7x_0]_5 + 2(r+1) \leq [x_0]_5 + 2 + 2(r+1) \\ &= [x]_5 + 2(r-1) + 2 \cdot 3 = [x]_5 + 2 \cdot 3 \leq [x]_5 + 2r.\end{aligned}$$

□

THEOREM 2.3.1.3 ([**KRL19**, Theorem 2.5]). *The lisse $\overline{\mathbb{Q}}_\ell$-sheaf $\mathcal{M}(5; 7, 1)$ has finite $G_{\mathtt{geom}}$.*

PROOF. We show Corollary 2.2.3.7 holds with $A = 2$. Let $r \geq 1$ and $0 \leq x < 5^r$. If $x \pmod 5 \neq 2$, after our previous lemma we know $[7x]_5 \leq [x]_5 + 2r < [x]_5 + 2r + 2$. If $x \pmod 5 = 2$ then

$$[7x]_5 = [7 \cdot 5x]_5 \leq [5x]_5 + 2(r+1) = [x]_5 + 2r + 2.$$

□

The sheaf $\mathcal{M}(5; 7, 1)$ merits to be called sporadic for two reasons. First, it is a sheaf of type $\mathcal{M}$ with finite $G_{\mathtt{geom}}$ not of Kubert type. It was found for the first time by Rojas-León after extensive computer calculations. Moreover, we can also call it sporadic since the mondromy groups $G_{\mathtt{geom}}$ and $G_{\mathtt{arith}}$ of $\mathcal{M}(5; 7, 1)$ are both equal to a sporadic simple group (see [**KRL19**, Corollary 3.5] for a precise statement). After that the problem of deciding (and realizing) which sporadic simple groups can arise as monodromy groups of hypergeometric and related classes of sheaves started and became an active area, still active today.

$\boxed{\boldsymbol{p = 7}}$ For $L = 11$ we find:

$\{2_{\mathrm{I}}$, 4_{II}, 8_{I}, 25_{II}, $43_{\mathrm{III},1}$, 50_{I}, 172_{II}, 344_{I}, 1201_{II}, $2101_{\mathrm{III},1}$, $2353_{\mathrm{III},2}$, 2402_{I}, 8404_{II}, 16808_{I}, 58825_{II}, $102943_{\mathrm{III},1}$, $117307_{\mathrm{III},3}$, 117650_{I}, 411772_{II}, 823544_{I}, 2882401_{II}, $5044201_{\mathrm{III},1}$, $5649505_{\mathrm{III},2}$, $5762401_{\mathrm{III},4}$, 5764802_{I}, 20176804_{II}, 40353608_{I}, 141237625_{II}, $247165843_{\mathrm{III},1}$, $282458443_{\mathrm{III},5}$,

$282475250_{\mathtt{I}}, \quad 988663372_{\mathtt{II}}\}$.

One more time, the only values a that survive all the tests up to $L = 11$ are of Kubert types, which we already know would give a sheaf with finite monodromy. It follows from the theorem of Katz–Tiep that only numbers of Kubert type for $p = 7$ are the ones associated to sheaves with finite monodromy group.

The question of whether for bigger primes p there are "sporadic" values of a, not of Kubert type, such that $\mathcal{M}(p; a, 1)$ has finite $G_{\mathtt{geom}}$ is known to have the answer: it only occurs for $p = 5$ and $a = 7$. This is the strong consequence that follows from Katz and Tiep's theorem referenced above (which further settles this question for other related sheaves we have not considered in this work, namely, sheaves further tensored with a Kummer sheaf).

Now we report on the next phenomenon observed. If for each $L > 0$ we pay attention to the biggest $r \in \{1, 2, \ldots, L\}$ where a witness was found, we would see we are far from using all the information within the range $\{1, 2, \ldots, L\}$. Explicitly, Figures 1, 2, 3 below show the maximum r where we have found a witness during the execution of the algorithm for input L.

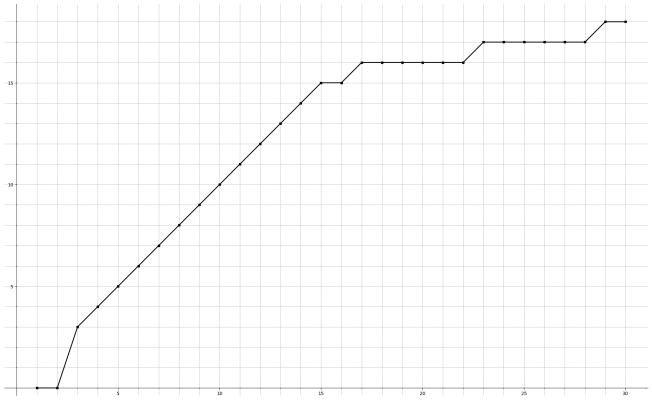


FIGURE 1. The biggest value of r needed for $L \in \{1, \ldots, 30\}$ and $p = 2$.

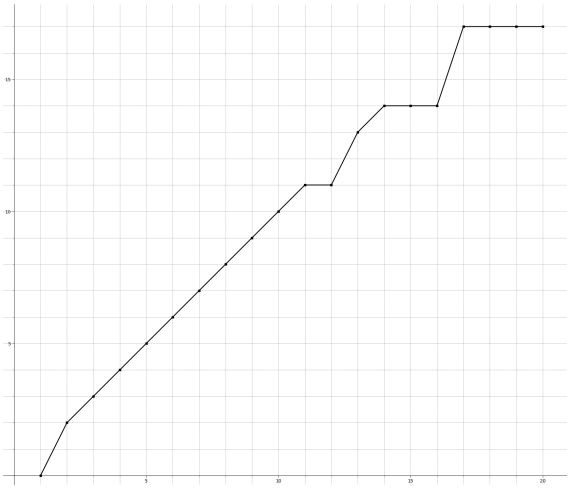


FIGURE 2. The biggest value of r needed for $L \in \{1, \ldots, 20\}$ and $p = 3$.

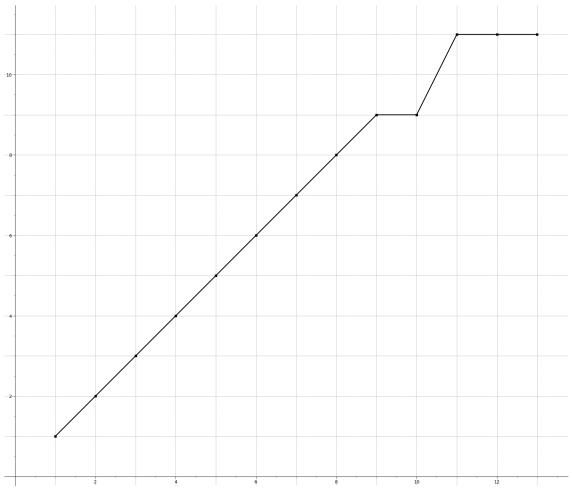


FIGURE 3. The biggest value of r needed for $L \in \{1, \dots, 13\}$ and $p = 5$.

This might be misleading. We are not saying that we have not used the information from all the values of $r \in \{1, \dots, L\}$, we say that we have used much less information while determining the non-finiteness of monodromy for the associated sheaves. Observe that whenever our algorithm reaches an integer of Kubert type it is going to test all the inequalities since that number verifies all of them. As a side remark, we see that running times of our algorithm are much longer than actually needed since we spend most of the time checking that numbers of Kubert type pass the tests, and we already know they do. Moreover, practical knowledge on the maximum value of r needed for each L (which we still do not have) would be useful in reducing the memory consumption of our implementation.

Finally, these observations suggest us to take a look at the size of the sets of integers within the interval $(0, p^r) \cap \mathbb{Z}$ that verify the r-th inequality. More precisely, write

$$S_r := \left\{ a \in (0, p^r) \cap \mathbb{Z} \ : \ [ax]_{p,r} \leq [x]_{p,r,-} + r(p-1)/2, \ \forall\ 0 < x < p^r \right\}.$$

Figure 4 shows the quantities $|S_r|/(p^r - 1)$ in black and $1 - |S_r|/(p^r - 1)$ in red for different primes.

2.3.2. The sheaves $\mathcal{M}(p; a, b, 1)$. Proceeding similarly as with $\mathcal{M}(p; a, 1)$, we first study what really matters while checking the non-finiteness of $G_{\texttt{arith}}$ for $\mathcal{M}(p; a, b, 1)$. Let $r \geq 1$ be a positive integer, $a, b \in \mathbb{N}$ and $i, j \in \{0, 1, \dots, r-1\}$. We refer to the inequality $[ax + by]_{p,r} \leq [x]_{p,r,-} + [y]_{p,r,-} + r(p-1)/2$ as the r-th inequality associated to the pair (a, b) specialized at $(x, y) \in (\mathbb{Z}/(p^r - 1)\mathbb{Z})^2$. We have the following:

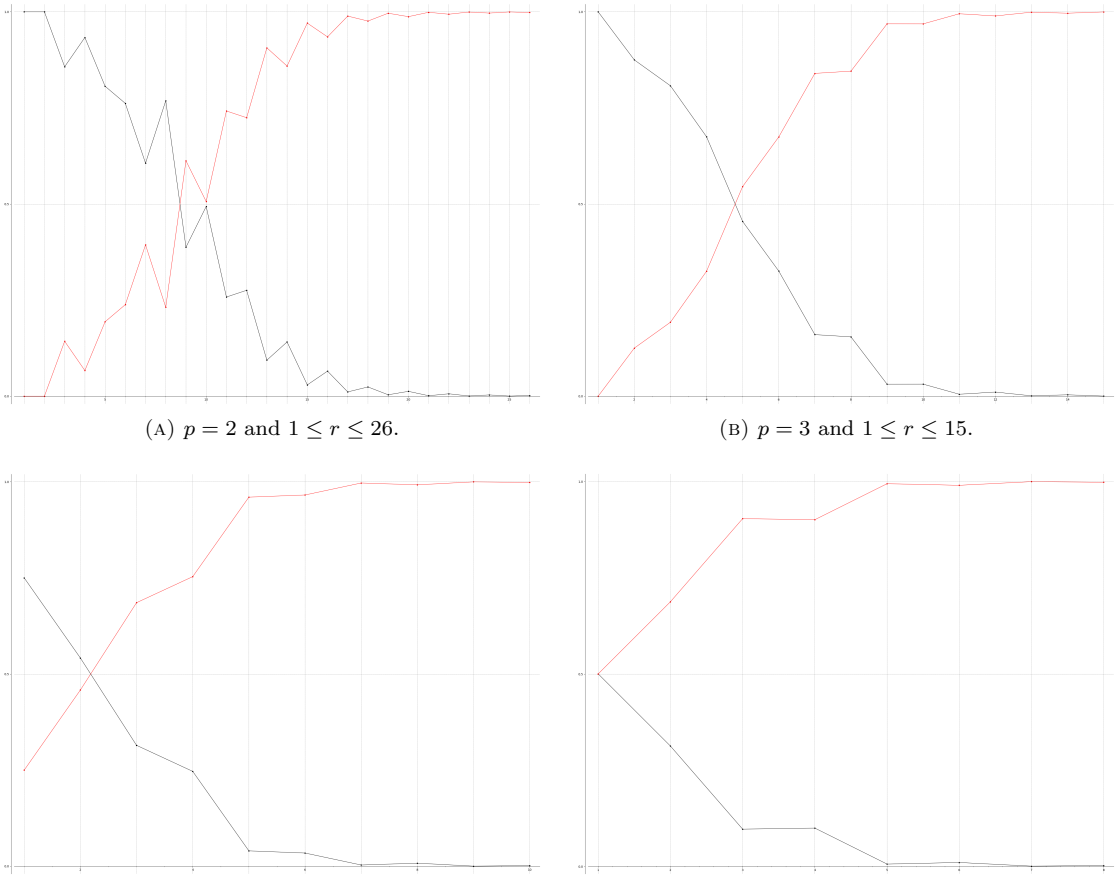
1. *The pair (a, b) satisfies the r-th inequality $[ax + by]_{p,r} \leq [x]_{p,r,-} + [y]_{p,r,-} + r(p-1)/2$ for every $0 \leq x, y < p^r - 1$ not both 0, if and only if the pair $(p^i a \pmod{p^r - 1}, p^j b \pmod{p^r - 1})$ satisfies the same inequality for every $0 \leq x, y < p^r - 1$ not both 0.* Indeed, observe

$$\begin{aligned}[ax + by]_{p,r} - [x]_{p,r,-} - [y]_{p,r,-} &= [p^r(ax + by)]_{p,r} - [x]_{p,r,-} - [y]_{p,r,-} \\ &= [p^i a \cdot p^{r-i} x + p^j b \cdot p^{r-j} y]_{p,r} - [p^{r-i} x]_{p,r,-} - [p^{r-j} y]_{p,r,-}.\end{aligned}$$

   To finish the argument use the bijectivity of the map

$$(x, y) \in (\mathbb{Z}/(p^r - 1)\mathbb{Z})^2 \mapsto (p^{r-i} x, p^{r-j} y) \in (\mathbb{Z}/(p^r - 1)\mathbb{Z})^2$$

   and that it sends $(0, 0)$ to $(0, 0)$.



(A) $p = 2$ and $1 \leq r \leq 26$.

(B) $p = 3$ and $1 \leq r \leq 15$.

(C) $p = 5$ and $1 \leq r \leq 10$.

(D) $p = 7$ and $1 \leq r \leq 8$.

FIGURE 4. Graphs showing the density of the subsets $S_r \subset (0, p^r) \cap \mathbb{Z}$.

2. *For every* $0 \leq x, y < p^r - 1$, *to specialize the* r*-th inequality associated to the pair* (a, b) *at* $(p^i x, p^j y)$ *is equivalent to specialize the same inequality at* $(x, p^{j-i} y \pmod{p^r - 1})$. Assume without loss of generality that $j > i$. The statement follows from the following equality:

$$\begin{aligned}[a \cdot p^i x + b \cdot p^j y]_{p,r} - [p^i x]_{p,r,-} - [p^j y]_{p,r,-} &= [p^i(ax + b \cdot p^{j-i} y)]_{p,r} - [x]_{p,r,-} - [p^{j-i} y]_{p,r,-} \\ &= [ax + b \cdot p^{j-i} y]_{p,r} - [x]_{p,r,-} - [p^{j-i} y]_{p,r,-}.\end{aligned}$$

After these two observations, we can propagate pairs (a, b) for which their associated r-th inequality is not satisfied via rotations and congruences modulo $p^r - 1$. Moreover, we can test r-th inequalities up to rotations on the first component x. Using these observations an algorithm analogous to Algorithm 2 can be designed (see the Appendix). This approach is not as performant as its one-parametric analog, nevertheless, it is the best approach we have at our disposal at this moment. For this reason, we do not give a detailed analysis of this approach and just proceed to describe its output for small values of p and L.

2.3.2.1. *Results for small characteristics.* Running the algorithm for small values of p and L, the only unexpected pairs of exponents (a, b) for which we can not decide if $\mathcal{M}(p; a, b, 1)$ has

non-finite $G_{\texttt{geom}}$ are:

$$\begin{aligned}&\text{for } p=2 \text{ and } (a,b)=(13_{\texttt{III},2},3_{\texttt{I}})=(13_{\texttt{III},2},3_{\texttt{III},1});\\&\text{for } p=3 \text{ and } (a,b)\in\{(7_{\texttt{III},1},4_{\texttt{I}}),(7_{\texttt{III},1},2_{\texttt{I}}),(5_{\texttt{II}},4_{\texttt{I}}),(5_{\texttt{II}},2_{\texttt{I}}),(4_{\texttt{I}},2_{\texttt{I}})\};\\&\text{for } p=5 \text{ and } (a,b)=(3_{\texttt{II}},2_{\texttt{I}}).\end{aligned}$$

Observe that, for $p=3$, $2=3^0+1=(3+1)/2$ has Kubert types `I` and `II`, so the pair $(4,2)$ may be interpreted as a mixture of types. Actually, from all these pairs a sheaf with finite $G_{\texttt{geom}}$ arises. In fact, for $p=3$ we can say more, the sheaves $\mathcal{M}(3;7,4,2,1)$ and $\mathcal{M}(3;5,4,2,1)$ have finite $G_{\texttt{geom}}$. All these results have been already proven by Katz, Rojas-León and Tiep in [**KRLT23**]. More precisely, the corresponding results from *loc. cit.* for $\mathcal{M}(2;13,3,1)$ are Theorems 32.3 and 32.4, for $\mathcal{M}(3;7,4,2,1)$ are Theorems 32.1 and 32.2, for $\mathcal{M}(3;5,4,2,1)$ are Theorems 32.5 and 32.6 and for $\mathcal{M}(5;3,2,1)$ are Theorems 32.7 and 32.8.

After Katz and Tiep's theorem [**KT23**, Theorem 11.2.3] we know that these are all the unexpected tuples of exponents with finite $G_{\texttt{geom}}$ for $\mathcal{M}$.

2.3.3. The sheaves $\mathcal{B}_{(p;a,b)}$. As before, let us start with a brief comment on computational simplifications. Let $r\geq 1$ be a positive integer, $a,b\in\mathbb{N}$ and $i,j\in\{0,1,\dots,r-1\}$. Again, we refer to inequality

$$[x]_{p,r,-}+[y-(a+b)x]_{p,r,-}+[bx-y]_{p,r,-}+[-bx]_{p,r,-}+[y]_{p,r,-}\geq 3r(p-1)/2$$

as the r-th inequality associated to the pair (a,b) specialized at (x,y) with $0<x,y<p^r-1$. We have:

1. *The r-th inequality associated to (a,b) is satisfied for every $0<x,y<p^r-1$, if and only if the r-the inequality associated to $(p^ia \pmod{p^r-1}, p^jb \pmod{p^r-1})$ is satisfied for every $0<x,y<p^r-1$.* It follows from the equality

$$\begin{aligned}&[x]_{p,r,-}+[y-(a+b)]_{p,r,-}+[bx-y]_{p,r,-}+[-bx]_{p,r,-}+[y]_{p,r,-}\\&\qquad=[x]_{p,r,-}+[p^iy-p^i(a+b)x]_{p,r,-}+[p^ibx-p^iy]_{p,r,-}+[-p^ibx]_{p,r,-}+[p^iy]_{p,r,-},\end{aligned}$$

   and the fact that the map $(x,y)\in\mathbb{Z}/(p^r-1)\mathbb{Z}\longmapsto(x,p^iy)$ is a bijection sending $(0,0)$ to $(0,0)$.
2. *For every $0<x,y<p^r-1$, to specialize the r-th inequality associated to the pair (a,b) at (p^ix,p^jy) is equivalent to specialize the same inequality at $(x,p^{j-i}y \pmod{p^r-1})$.* Assuming $j>i$, it follows from the equality:

$$\begin{aligned}&[p^ix]_{p,r,-}+[p^jy-(a+b)\cdot p^ix]_{p,r,-}+[b\cdot p^ix+p^jy]_{p,r,-}+[-b\cdot p^ix]_{p,r,-}+[p^jy]_{p,r,-}\\&\qquad=[x]_{p,r,-}+[p^{j-i}y-(a+b)x]_{p,r,-}+[bx-p^{j-i}y]_{p,r,-}+[-bx]_{p,r,-}+[p^{j-i}y]_{p,r,-}.\end{aligned}$$

In costrast to the situation for the sheaves $\mathcal{M}$, we see that the propagation of pairs with non-finite $G_{\texttt{geom}}$ for the sehaves $\mathcal{B}$ can only be done only multiplicating by the same power of p. This makes our approach for this family of sheaves even less performant than the same strategy for the sheaves $\mathcal{M}$. For this reason we do not analyze here the performance of our approach, we just describe some of the pairs not discarded by the algorithm and study if they really give rise to a sheaf with finite monodromy group. An implementation is presented in the Appendix.

Fix the morphisms

$$\begin{aligned}\varphi:\ \mathbb{G}_{m,k}^2&\longrightarrow\mathbb{G}_{m,k}^3\\(s,t)&\longmapsto(s,-s,t);\\\phi:\ \mathbb{G}_{m,k}^2&\longrightarrow\mathbb{G}_{m,k}^5\\(s,t)&\longmapsto(s,-s,-s,s,t).\end{aligned}$$

For any arbitrary prime p, we find after computer calculations the following family:

- $(p^n, 1)$ for $n = 0, 1, \ldots$. Observe that the trace function of $\mathcal{B}_{(p;p^n,1)}$ at some rational point $(s,t) \in \mathbb{G}^2_{m,k}(k_r)$ with $k_r = \mathbb{F}_{p^r}$ is

$$-\frac{1}{\sqrt{p^r}} \sum_{x \in k_r} \psi_r(sx^{p^n}(x-1) + tx) = -\frac{1}{\sqrt{p^r}} \sum_{x \in k_r} \psi_r(sx^{p^n+1} - sx^{p^n} + tx).$$

  Then $\mathcal{B}_{(p;p^n,1)} = \varphi^* \mathcal{M}_{\mathtt{big}}(p; p^n+1, p^n, 1)$. Since the latter has finite $G_{\mathtt{geom}}$ after an Artin–Schreier reduction, we conclude $\mathcal{B}_{(p;p^n,1)}$ has finite $G_{\mathtt{geom}}$. From this also follows that the exponents $(1, p^n)$ give rise to a sheaf with finite $G_{\mathtt{geom}}$.

Now we report the further families found for some small primes p :

$p = 2$ By executing some code we get the following families and special cases:

- $(2^n + 1, 1)$ for $n = 1, 2, \ldots$. The trace function of $\mathcal{B}_{(2;2^n+1,1)}$ at $(s,t) \in \mathbb{G}^2_{m,k}(k_r)$ with $k_r = \mathbb{F}_{2^r}$ is

$$-\frac{1}{\sqrt{2^r}} \sum_{x \in k_r} \psi_r(sx^{2^n+1}(x+1) + tx) = -\frac{1}{\sqrt{2^r}} \sum_{x \in k_r} \psi_r(sx^{2(2^{n-1}+1)} + sx^{2^n+1} + tx).$$

  Then $\mathcal{B}_{(2;2^n+1,1)} = \varphi^* \mathcal{M}_{\mathtt{big}}(2; 2(2^{n-1}+1), 2^n+1, 1)$. The latter has finite $G_{\mathtt{geom}}$ after an Artin–Schreier reduction, hence our original sheaf has finite $G_{\mathtt{geom}}$ too. We also deduce $(1, 2^n+1)$ gives rise to a sheaf with finite $G_{\mathtt{geom}}$.
- $(2^n + 1, 2^n)$ for $n = 1, 2, \ldots$. The trace function of $\mathcal{B}_{(2;2^n+1,2^n)}$ at $(s,t) \in \mathbb{G}^2_{m,k}(k_r)$ with $k_r = \mathbb{F}_{2^r}$ is

$$-\frac{1}{\sqrt{2^r}} \sum_{x \in k_r} \psi_r(sx^{2^n+1}(x^{2^n}+1) + tx) = -\frac{1}{\sqrt{2^r}} \sum_{x \in k_r} \psi_r(sx^{2^{n+1}+1)} + sx^{2^n+1} + tx).$$

  Then $\mathcal{B}_{(2;2^n+1,1)} = \varphi^* \mathcal{M}_{\mathtt{big}}(2; 2^{n+1}+1, 2^n+1, 1)$. The latter has finite $G_{\mathtt{geom}}$ hence our original sheaf has finite $G_{\mathtt{geom}}$ too. We also deduce $(2^n, 2^n+1)$ gives rise to a sheaf with finite $G_{\mathtt{geom}}$.
- $\left(\frac{2^{2n+1}+1}{2+1}, 1\right)$ for $n = 1, 2 \ldots$. Observe that $\frac{2^{2n+1}+1}{2+1} + 1 = 2^2 \frac{2^{2n-1}+1}{2+1}$. The trace function of $\mathcal{B}_{\left(2;\frac{2^{2n+1}+1}{2+1},1\right)}$ at $(s,t) \in \mathbb{G}^2_{m,k}(k_r)$ with $k_r = \mathbb{F}_{2^r}$ is

$$-\frac{1}{\sqrt{2^r}} \sum_{x \in k_r} \psi_r\Big(sx^{\frac{2^{2n+1}+1}{2+1}}(x+1) + tx\Big) = -\frac{1}{\sqrt{2^r}} \sum_{x \in k_r} \psi_r\Big(sx^{2^2 \frac{2^{2n-1}+1}{2+1}} + sx^{\frac{2^{2n+1}+1}{2+1}} + tx\Big).$$

  Then $\mathcal{B}_{\left(2;\frac{2^{2n+1}+1}{2+1},1\right)} = \varphi^* \mathcal{M}_{\mathtt{big}}\big(2; 2^2 \frac{2^{2n+1}+1}{2+1}, \frac{2^{2n+1}+1}{2+1}, 1\big)$. The latter has finite $G_{\mathtt{geom}}$ after an Artin–Schreier reduction, hence our original sheaf has finite $G_{\mathtt{geom}}$ too. We also deduce $\big(1, \frac{2^{2n+1}+1}{2+1}\big)$ gives rise to a sheaf with finite $G_{\mathtt{geom}}$.
- $\left(\frac{2^{2n+1}+1}{2+1}, 2^{2n+1}\right)$ for $n = 1, 2 \ldots$. Observe that $(2^{2n+1}+1)/(2+1) + 2^{2n+1} = (2^{2n+3}+1)/(2+1)$. The trace function of $\mathcal{B}_{\left(2;\frac{2^{2n+1}+1}{2+1},2^{2n+1}\right)}$ at $(s,t) \in \mathbb{G}^2_{m,k}(k_r)$ with $k_r = \mathbb{F}_{2^r}$ is

$$-\frac{1}{\sqrt{2^r}} \sum_{x \in k_r} \psi_r\Big(sx^{\frac{2^{2n+1}+1}{2+1}}(x^{2^{2n+1}}+1) + tx\Big) = -\frac{1}{\sqrt{2^r}} \sum_{x \in k_r} \psi_r\Big(sx^{\frac{2^{2n+3}+1}{2+1}} + sx^{\frac{2^{2n+1}+1}{2+1}} + tx\Big).$$

  Then $\mathcal{B}_{\left(2;\frac{2^{2n+1}+1}{2+1},1\right)} = \varphi^* \mathcal{M}_{\mathtt{big}}\big(2; \frac{2^{2n+3}+1}{2+1}, \frac{2^{2n+1}+1}{2+1}, 1\big)$. The latter has finite $G_{\mathtt{geom}}$, hence our original sheaf has finite $G_{\mathtt{geom}}$ too. We also deduce $\big(2^{2n+1}, \frac{2^{2n+1}+1}{2+1}\big)$ gives rise to a sheaf with finite $G_{\mathtt{geom}}$.

- $\big(\frac{2^{2n+1}+1}{2+1}, 2^{2n+1}+1\big)$ for $n = 1, 2\ldots$. The trace function of $\mathcal{B}_{\big(2;\frac{2^{2n+1}+1}{2+1},2^{2n+1}+1\big)}$ at $(s,t) \in \mathbb{G}^2_{m,k}(k_r)$ with $k_r = \mathbb{F}_{2^r}$ is

$$-\frac{1}{\sqrt{2^r}}\sum_{x\in k_r}\psi_r\Big(sx^{\frac{2^{2n+1}+1}{2+1}}(x^{2^{2n+1}}+1)(x+1)+tx\Big)$$
$$= -\frac{1}{\sqrt{2^r}}\sum_{x\in k_r}\psi_r\Big(sx^{2^2\frac{2^{2n+1}+1}{2+1}} + sx^{\frac{2^{2n+3}+1}{2+1}} + sx^{2^2\frac{2^{2n-1}+1}{2+1}} + sx^{\frac{2^{2n+1}+1}{2+1}} + tx\Big).$$

  Then $\mathcal{B}_{\big(2;\frac{2^{2n+1}+1}{2+1},1\big)} = \phi^*\mathcal{M}_{\mathtt{big}}\big(2; 2^2\frac{2^{2n+1}+1}{2+1}, \frac{2^{2n+3}+1}{2+1}, 2^2\frac{2^{2n-1}+1}{2+1}, \frac{2^{2n+1}+1}{2+1}, 1\big)$. The latter has finite $G_{\mathtt{geom}}$ after an Artin–Schreier reduction, hence our original sheaf has finite $G_{\mathtt{geom}}$ too. We also deduce $\big(2^{2n+1}+1, \frac{2^{2n+1}+1}{2+1}\big)$ gives rise to a sheaf with finite $G_{\mathtt{geom}}$.
- (a,a) for a such that $\mathcal{M}(2;a,1)$ has finite $G_{\mathtt{geom}}$. The trace function of $\mathcal{B}_{(2;a,a)}$ at $(s,t) \in \mathbb{G}_{m,k}(k_r)\times\mathbb{A}^1_k(k_r)$ with $k_r = \mathbb{F}_{2^r}$ is

$$-\frac{1}{\sqrt{2^r}}\sum_{x\in k_r}\psi_r(s(x^2+x)^a+tx).$$

  This case requires some work. Rewrite the exponential sum appearing in the trace function as follows:

$$\sum_{x\in k_r}\psi_r(s(x^2+x)^a+tx) = \sum_{y\in k_r}\psi_r(sy^a)\sum_{\substack{x\in k_r\\ x^2+x=y}}\psi_r(tx) \overset{(*)}{=} \sum_{y\in k_r}\psi_r(sy^a)\sum_{\substack{u\in k_r\\ u^2+u=t^2}}\psi_r(uy)$$
$$= \sum_{\substack{u\in k_r\\ u^2+u=t^2}}\sum_{y\in k_r}\psi_r(sy^a+uy).$$

  Assume momentarily the validity of $(*)$. If we consider the finite morphisms $\alpha : \mathbb{G}_{m,k}\times\mathbb{A}^1_k \to \mathbb{G}_{m,k}\times\mathbb{A}^1_k$ and $\beta : \mathbb{G}_{m,k}\times\mathbb{A}^1_k \to \mathbb{G}_{m,k}\times\mathbb{A}^1_k$ given by $\alpha(s,u) = (s, u^2+u)$ and $\beta(s,t) = (s,t^2)$, then $\mathcal{B}_{(2;a,a)} = \beta^*\alpha_!\mathcal{M}_{\mathtt{big}}(2;a,1)$. Indeed, observe that α is an étale covering, hence the functor $\alpha_!$ is exact and the stalk at any geometric point $\overline{pt} \in \mathbb{G}_{m,k}\times\mathbb{A}^1_k$ of $\alpha_!\mathcal{M}_{\mathtt{big}}(2;a,1)$ equals

$$\big(\alpha_!\mathcal{M}_{\mathtt{big}}(2;a,1)\big)_{\overline{pt}} = \bigoplus_{\substack{\overline{pt}'\in\mathbb{G}_{m,k}\times\mathbb{A}^1_k\\ \alpha(\overline{pt}')=\overline{pt}}}\mathcal{M}_{\mathtt{big}}(2;a,1)_{\overline{pt}'}.$$

  Moreover, since the morphism α is defined over k, we know the action of Frobenius on the stalk of $\alpha_!\mathcal{M}_{\mathtt{big}}(2;a,1)$ is fiberwise. In conclusion, we see that the trace function of $\alpha_!\mathcal{M}_{\mathtt{big}}(2;a,1)$ is obtained by integration of the trace function of $\mathcal{M}_{\mathtt{big}}(2;a,1)$ over fibers:

$$\mathtt{tr}_{\alpha_!\mathcal{M}_{\mathtt{big}}(2;a,1),k_r}(s,t) = \sum_{\substack{u\in k_r\\ u^2+u=t}}\mathtt{tr}_{\mathcal{M}_{\mathtt{big}}(2;a,1),k_r}(s,u).$$

  Now we just take the pullback by β of $\alpha_!\mathcal{M}_{\mathtt{big}}(2;a,1)$ and obtain $\mathcal{B}_{(2;a,a)}$. Since both α and β are finite morphisms and we assume $\mathcal{M}_{\mathtt{big}}(2;a,1)$ with finite monodromy, the monodromy remains finite.

  We still have to show equality $(*)$, i.e. $\sum_{x^2+x=y}\psi_r(tx) = \sum_{u^2+u=t^2}\psi_r(uy)$ for every $t,y\in k_r$. If $x\in k_r$ satisfies that $x^2+x=y$ then $(x+1)^2+(x+1)=y$ as well. Hence, $(1-\psi_r(t))\cdot\sum_{x^2+x=y}\psi_r(tx) = 0$. Analogously, $(1-\psi_r(y))\cdot\sum_{u^2+u=t^2}\psi_r(uy) = 0$. Hence if $\psi_r(t) = -1$, i.e. $\mathtt{trace}_{k_r/k}(t) = 1$, then $\sum_{x^2+x=y}\psi_r(tx) = 0$. But $\mathtt{trace}_{k_r/k}(t^2) = \mathtt{trace}_{k_r/k}(t) = 1$ hence the equation $u^2+u=t^2$ has no solutions in k_r (see [**LN94**, Theorem 2.25]) and $\sum_{u^2+u=t^2}\psi_r(uy) = 0$ as well. Analogously, if $\psi_r(y) = -1$ then

both $\sum_{x^2+x=y}\psi_r(tx)=\sum_{u^2+u=t^2}\psi_r(uy)=0$. Assume from now on that $\mathtt{trace}_{k_r/k}(t)=\mathtt{trace}_{k_r/k}(y)=0$ and let $x_1,u_1\in k_r$ be solutions of the equations $x^2+x=y$ and $u^2+u=t^2$ respectively (invoking *loc. cit.*). Then

$$\sum_{x^2+x=y}\psi_r(tx)=\psi_r(tx_1)+\psi_r(t(x_1+1))=(1+\psi_r(t))\psi_r(tx_1)=2\psi_r(tx_1)$$

and analogously

$$\sum_{u^2+u=t^2}\psi_r(uy)=2\psi_r(yu_1).$$

We need the equality $\psi_r(tx_1)=\psi_r(yu_1)$, which follows from the manipulations:

$$\begin{aligned}\psi_r(tx_1)&=\psi_r(t^2x_1^2)=\psi_r((u_1^2+u_1)x_1^2)=\psi_r(u_1^2x_1^2)\psi_r(u_1x_1^2)\\&=\psi_r(u_1x_1)\psi_r(u_1(x_1+y))=\psi_r(u_1x_1)^2\psi_r(yu_1)=\psi_r(yu_1).\end{aligned}$$

- $(12,1)$. The trace function of $\mathcal{B}_{(2;12,1)}$ at $(s,t)\in\mathbb{G}^2_{m,k}(k_r)$ with $k_r=\mathbb{F}_{2^r}$ is

$$-\frac{1}{\sqrt{2^2}}\sum_{x\in k_r}\psi_r(sx^{13}+sx^{12}+tx).$$

Then $\mathcal{B}_{(2;12,1)}=\varphi^*\mathcal{M}_{\mathtt{big}}(2;13,12,1)$. The latter has finite $G_{\mathtt{geom}}$ after an Artin–Schreier reduction, hence our original sheaf has finite $G_{\mathtt{geom}}$ too. We also deduce $(1,12)$ gives rise to a sheaf with finite $G_{\mathtt{geom}}$.

$p=3$ We have:

- $\left(\frac{3^n+1}{2},1\right)$ for $n=1,2,\dots$. Observe that $\frac{3^n+1}{2}+1=3\frac{3^{n-1}+1}{2}$. The trace function of $\mathcal{B}_{\left(3;\frac{3^n+1}{2},1\right)}$ at $(s,t)\in\mathbb{G}^2_{m,k}(k_r)$ with $k_r=\mathbb{F}_{3^r}$ is

$$-\frac{1}{\sqrt{3^r}}\sum_{x\in k_r}\psi_r\Big(sx^{\frac{3^n+1}{2}}(x-1)+tx\Big)=-\frac{1}{\sqrt{3^r}}\sum_{x\in k_r}\psi_r\Big(sx^{3\frac{3^{n-1}+1}{2}}-sx^{\frac{3^n+1}{2}}+tx\Big).$$

Then $\mathcal{B}_{\left(3;\frac{3^n+1}{2},1\right)}=\varphi^*\mathcal{M}_{\mathtt{big}}\big(3;3\frac{3^{n-1}+1}{2},\frac{3^n+1}{2},1\big)$. The latter has finite $G_{\mathtt{geom}}$ after an Artin–Schreier reduction, hence our original sheaf has finite $G_{\mathtt{geom}}$ too. We also deduce $\big(1,\frac{3^n+1}{2}\big)$ gives rise to a sheaf with finite $G_{\mathtt{geom}}$.
- $\left(\frac{3^n+1}{2},3^n\right)$ for $n=0,1,\dots$. Observe that $\frac{3^n+1}{2}+3^n=\frac{3^{n+1}+1}{2}$. The trace function of $\mathcal{B}_{\left(3;\frac{3^n+1}{2},3^n\right)}$ at $(s,t)\in\mathbb{G}^2_{m,k}(k_r)$ with $k_r=\mathbb{F}_{3^r}$ is

$$-\frac{1}{\sqrt{3^r}}\sum_{x\in k_r}\psi_r\Big(sx^{\frac{3^n+1}{2}}(x^{3^n}-1)+tx\Big)=-\frac{1}{\sqrt{3^r}}\sum_{x\in k_r}\psi_r\Big(sx^{\frac{3^{n+1}+1}{2}}-sx^{\frac{3^n+1}{2}}+tx\Big).$$

Then $\mathcal{B}_{\left(3;\frac{3^n+1}{2},3^n\right)}=\varphi^*\mathcal{M}_{\mathtt{big}}\big(3;\frac{3^{n+1}+1}{2},\frac{3^n+1}{2},1\big)$. The latter has finite $G_{\mathtt{geom}}$, hence our original sheaf has finite $G_{\mathtt{geom}}$ too. We also deduce $\big(3^n,\frac{3^n+1}{2}\big)$ gives rise to a sheaf with finite $G_{\mathtt{geom}}$.
- $\left(\frac{3^n+1}{2},3^n+1\right)$ for $n=1,2,\dots$. The trace function of $\mathcal{B}_{\left(3;\frac{3^n+1}{2},3^n+1\right)}$ at $(s,t)\in\mathbb{G}^2_{m,k}(k_r)$ with $k_r=\mathbb{F}_{3^r}$ is

$$\begin{aligned}&-\frac{1}{\sqrt{3^r}}\sum_{x\in k_r}\psi_r\Big(sx^{\frac{3^n+1}{2}}(x^{3^n}-1)(x-1)+tx\Big)\\&\qquad=-\frac{1}{\sqrt{3^r}}\sum_{x\in k_r}\psi_r\Big(sx^{3\frac{3^n+1}{2}}-sx^{\frac{3^{n+1}+1}{2}}-sx^{3\frac{3^{n-1}+1}{2}}+sx^{\frac{3^n+1}{2}}+tx\Big).\end{aligned}$$

Then $\mathcal{B}_{\left(3;\frac{3^n+1}{2},3^n+1\right)} = \phi^*\mathcal{M}_{\mathtt{big}}\big(3;3\frac{3^n+1}{2},\frac{3^{n+1}+1}{2},3\frac{3^{n-1}+1}{2},\frac{3^n+1}{2},1\big)$. The latter has finite $G_{\mathtt{geom}}$ after an Artin–Schreier reduction, hence our original sheaf has finite $G_{\mathtt{geom}}$ too. We also deduce $\big(3^n+1,\frac{3^n+1}{2}\big)$ gives rise to a sheaf with finite $G_{\mathtt{geom}}$.

- $(4,1)$. The trace function of $\mathcal{B}_{(3;4,1)}$ at $(s,t)\in\mathbb{G}^2_{m,k}(k_r)$ with $k_r=\mathbb{F}_{3^r}$ is
$$-\frac{1}{\sqrt{3^r}}\sum_{x\in k_r}\psi_r\Big(sx^4(x-1)+tx\Big)=-\frac{1}{\sqrt{3^r}}\sum_{x\in k_r}\psi_r\Big(sx^5-sx^4+tx\Big).$$
Then $\mathcal{B}_{(3;4,1)}=\varphi^*\mathcal{M}_{\mathtt{big}}(3;5,4,1)$. The latter has finite $G_{\mathtt{geom}}$, hence our original sheaf has finite $G_{\mathtt{geom}}$ too. We also deduce $(1,4)$ gives rise to a sheaf with finite $G_{\mathtt{geom}}$.
- $(6,1)$. The trace function of $\mathcal{B}_{(3;6,1)}$ at $(s,t)\in\mathbb{G}^2_{m,k}(k_r)$ with $k_r=\mathbb{F}_{3^r}$ is
$$-\frac{1}{\sqrt{3^r}}\sum_{x\in k_r}\psi_r\Big(sx^6(x-1)+tx\Big)=-\frac{1}{\sqrt{3^r}}\sum_{x\in k_r}\psi_r\Big(sx^7-sx^6+tx\Big).$$
Then $\mathcal{B}_{(3;4,1)}=\varphi^*\mathcal{M}_{\mathtt{big}}(3;7,6,1)$. The latter has finite $G_{\mathtt{geom}}$ after an Artin–Schreier reduction, hence our original sheaf has finite $G_{\mathtt{geom}}$ too. We also deduce $(1,6)$ gives rise to a sheaf with finite $G_{\mathtt{geom}}$.
- $(2,2)$. The trace function of $\mathcal{B}_{(3;2,2)}$ at $(s,t)\in\mathbb{G}^2_{m,k}(k_r)$ with $k_r=\mathbb{F}_{3^r}$ is
$$-\frac{1}{\sqrt{3^r}}\sum_{x\in k_r}\psi_r\Big(sx^2(x-1)^2+tx\Big)=-\frac{1}{\sqrt{3^r}}\sum_{x\in k_r}\psi_r\Big(sx^4+sx^3+sx^2+tx\Big).$$
Then $\mathcal{B}_{(3;2,2)}=\Phi^*\mathcal{M}_{\mathtt{big}}(3;4,3,2,1)$, where $\Phi:(s,t)\in\mathbb{G}^2_m\mapsto(s,s,s,t)\in\mathbb{G}^4_m$. The latter has finite $G_{\mathtt{geom}}$ after an Artin–Schreier reduction, hence our original sheaf has finite $G_{\mathtt{geom}}$ too.
- $(4,3)$. The trace function of $\mathcal{B}_{(3;4,3)}$ at $(s,t)\in\mathbb{G}^2_{m,k}(k_r)$ with $k_r=\mathbb{F}_{3^r}$ is
$$-\frac{1}{\sqrt{3^r}}\sum_{x\in k_r}\psi_r\Big(sx^4(x^3-1)+tx\Big)=-\frac{1}{\sqrt{3^r}}\sum_{x\in k_r}\psi_r\Big(sx^7-sx^4+tx\Big).$$
Then $\mathcal{B}_{(3;4,3)}=\varphi^*\mathcal{M}_{\mathtt{big}}(3;7,4,1)$. The latter has finite $G_{\mathtt{geom}}$, hence our original sheaf has finite $G_{\mathtt{geom}}$ too. We also deduce $(3,4)$ gives rise to a sheaf with finite $G_{\mathtt{geom}}$.

$\boxed{\boldsymbol{p=5}}$ We have:

- $(2,1)$. The trace function of $\mathcal{B}_{(5;2,1)}$ at $(s,t)\in\mathbb{G}^2_{m,k}(k_r)$ with $k_r=\mathbb{F}_{5^r}$ is
$$-\frac{1}{\sqrt{5^r}}\sum_{x\in k_r}\psi_r\Big(sx^2(x-1)+tx\Big)=-\frac{1}{\sqrt{5^r}}\sum_{x\in k_r}\psi_r\Big(sx^3-sx^2+tx\Big).$$
Then $\mathcal{B}_{(5;2,1)}=\phi^*\mathcal{M}_{\mathtt{big}}(5;3,2,1)$. The latter has finite $G_{\mathtt{geom}}$, hence our original sheaf has finite $G_{\mathtt{geom}}$ too. We also deduce $(1,2)$ gives rise to a sheaf with finite $G_{\mathtt{geom}}$.

Remark 2.3.3.1. In all the proofs above we claimed that we have an equality between lisse $\overline{\mathbb{Q}}_\ell$-sheaves just from an equality between trace functions. This result is not trivial and it follows from [**Lau87**, Proposition 1.1.2.1] which assures us that the equality of trace functions for every extension k_r/k implies that the underlying lisse sheaves are isomorphic. ■

CHAPTER 3

Applications to coding theory and cryptography

In this chapter we expose some topics from coding theory and cryptography which are related to the $\overline{\mathbb{Q}}_\ell$-sheaves $\mathcal{M}$ from the previous chapter. The *Handbook* [**MP13**] was useful while learning about the theory to be exposed below and deciding which aspects are included here.

3.1. Review of coding theory

Let p be a prime and $\mathbb{F}_q$ be a finite field of characteristic p. Given a vector $\boldsymbol{x} = (x_1, \dots, x_n) \in \mathbb{F}_q^n$, define the *Hamming weight* of $\boldsymbol{x}$ by the formula $\mathtt{wt}(\boldsymbol{x}) = |\{i \in \{1, \dots, n\} : x_i \neq 0\}|$. Given two vectors $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^n$ we define the distance between them as $\mathtt{dist}(\boldsymbol{x}, \boldsymbol{y}) = \mathtt{wt}(\boldsymbol{x} - \boldsymbol{y})$.

3.1.1. Linear codes. Let $\mathcal{C} \subset \mathbb{F}_q^n$ be a linear subspace. We say that $\mathcal{C}$ is a *linear code of length n over $\mathbb{F}_q$*. If $\mathcal{C}$ has dimension k and the minimum distance between vectors of $\mathcal{C}$ is d^*, we say that $\mathcal{C}$ is a $(n, k, d^*)_q$ code. The vectors $\boldsymbol{c} \in \mathcal{C}$ are called *codewords* of $\mathcal{C}$.

Given a $(n, k, d^*)_q$ code $\mathcal{C}$, a $k \times n$ matrix G with entries in $\mathbb{F}_q$ is called a *generator matrix* of $\mathcal{C}$ if its row space is $\mathcal{C}$. A $(n-k) \times n$ matrix H with entries in $\mathbb{F}_q$ is said to be a *parity check matrix* of $\mathcal{C}$ if $H\boldsymbol{c}^t = 0$ for every $\boldsymbol{c} \in \mathcal{C}$.

Given a $(n, k, d^*)_q$ linear code $\mathcal{C}$, we define the dual linear code as follows:

$$\mathcal{C}^\perp = \left\{ \boldsymbol{x} \in \mathbb{F}_q^n : \langle \boldsymbol{x}, \boldsymbol{c} \rangle = \sum_{i=1}^{n} x_i c_i = 0 \ \forall \boldsymbol{c} \in \mathcal{C} \right\}.$$

The dimension of $\mathcal{C}^\perp$ is $n - k$. Moreover, if H is a parity check matrix of $\mathcal{C}$, then H is a generator matrix of $\mathcal{C}^\perp$.

3.1.2. Cyclic codes. Given a vector $\boldsymbol{x} = (x_0, \dots, x_{n-1}) \in \mathbb{F}_q^n$, the *cyclic shift of $\boldsymbol{x}$* is defined by $\sigma\boldsymbol{x} = (x_{n-1}, x_0, \dots, x_{n-2})$. A linear $(n, k, d^*)_q$ code $\mathcal{C}$ is said to be *cyclic* if for every codeword $\boldsymbol{c} \in \mathcal{C}$ then $\sigma\boldsymbol{c} \in \mathcal{C}$ too.

We identify the $\mathbb{F}_q$-vector spaces $\mathbb{F}_q^n$ and $\mathbb{F}_q[x]/(x^n - 1)$ via the $\mathbb{F}_q$-linear isomorphism

$$\begin{array}{ccc} \mathbb{F}_q^n & \longleftrightarrow & \mathbb{F}_q[x]/(x^n - 1) \\ \boldsymbol{v} = (v_0, \dots, v_{n-1}) & \longmapsto & \mathtt{pol}(\boldsymbol{v})(x) = \sum_{i=0}^{n-1} v_i x^i \\ \mathtt{vec}(p) = (p_0, \dots, p_{n-1}) & \longleftarrow & p(x) = \sum_{i=0}^{n-1} p_i x^i. \end{array}$$

Despite we have named explicitly both isomorphisms, for the ease of notation, we usually identify both sides and it will be always clear from the context which one we refer to.

Under this bijection, a linear code $\mathcal{C}$ is cyclic if and only if it is an ideal in $\mathbb{F}_q[x]/(x^n - 1)$ (observe that cyclically shifting a codeword correspond to multiplication by x on the polynomial side). Since $\mathbb{F}_q[x]$ is a principal ideal domain, it follows that every ideal of $\mathbb{F}_q[x]/(x^n - 1)$ is a principal ideal. Assume that $\mathcal{C}$ is a cyclic code (i.e. an ideal) and let $g \in \mathbb{F}_q[x]/(x^n - 1)$ be a generator of the ideal. If g is monic, we say that g is the *generator polynomial* of the code. The following properties of cyclic codes and generators are known [**MS77**, Chapter 7, Theorem 1]:

(a) g is a divisor of $x^n - 1$.
(b) If $k = \mathtt{deg}\ g$ then $\mathcal{C}$ has dimension $n - k$.

(c) Write $g(x) = \sum_{i=0}^{k} g_i x^i$. Then the matrix

$$\begin{pmatrix} g_0 & g_1 & g_2 & \dots & g_k & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_{k-1} & g_k & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & g_0 & g_1 & g_2 & \dots & g_k \end{pmatrix}$$

is a generator matrix of $\mathcal{C}$.

Consider the polynomial $h(x) := (x^n - 1)/g(x) = \sum_{i=0}^{n-k} h_i x^i$, which has $\mathtt{deg}\ h = n - k$. It is called the *parity check polynomial* of $\mathcal{C}$. Observe that, if $c(x) = \sum_{i=0}^{n-1} c_i x^i \in \mathcal{C}$ then $c(x)h(x) = 0$ in $\mathbb{F}_q[x]/(x^n - 1)$. Looking at the coefficients of the polynomial $c(x)h(x)$, we obtain the equalities $\sum_{i=0}^{n-1} c_i h_{j-i \pmod n} = 0$ for $j = 0, 1, \dots, n-1$. Consider

$$H = \begin{pmatrix} 0 & \dots & 0 & 0 & h_{n-k} & \dots & h_2 & h_1 & h_0 \\ 0 & \dots & 0 & h_{n-k} & h_{n-k-1} & \dots & h_1 & h_0 & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ h_{n-k} & \dots & h_2 & h_1 & h_0 & \dots & 0 & 0 & 0 \end{pmatrix}.$$

We have seen that, if $\boldsymbol{c} \in \mathcal{C}$ then $H\boldsymbol{c}^t = 0$. But H has rank k, then the condition $H\boldsymbol{x}^t = 0$ is sufficient for $\boldsymbol{x}$ to be in $\mathcal{C}$. In conclusion, H is a parity check matrix for $\mathcal{C}$. Moreover, with this we show that $\mathcal{C}^\perp$ is again a cyclic code with a generator (not monic in general) given by $x^{n-k}h(x^{-1})$, the reverse polynomial of h.

3.1.3. $\mathbb{F}_q$ codes from $\mathbb{F}_{q^m}$ codes. Fix an integer $m \geq 1$. If $\mathcal{C}$ is a $(n, k, d^*)_{q^m}$ linear code over $\mathbb{F}_{q^m}$, we can construct linear codes of length n over $\mathbb{F}_q$ in the following ways:

1. *Subfield subcodes*: Define
$$\mathcal{C}(\mathbb{F}_q) = \{\boldsymbol{c} \in \mathcal{C} : \boldsymbol{c} \in \mathbb{F}_q^n\} = \mathcal{C} \cap \mathbb{F}_q^n.$$
It is called the $\mathbb{F}_q$-subfield subcode of $\mathcal{C}$. Our notation $\mathcal{C}(\mathbb{F}_q)$ is not standard, it tries to recall that we are just looking at $\mathbb{F}_q$-rational points of a scheme defined over $\mathbb{F}_{q^m}$.
2. *Trace code*: Define
$$\mathtt{trace}_{\mathbb{F}_{q^m}/\mathbb{F}_q}\ \mathcal{C} = \left\{(\mathtt{trace}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(c_1), \dots, \mathtt{trace}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(c_n)) : (c_1, \dots, c_n) \in \mathcal{C}\right\}.$$
It is called the trace code of $\mathcal{C}$ over $\mathbb{F}_q$.

Delsarte's theorem relates these two constructions:

THEOREM 3.1.3.1 ([**MS77**, Chapter 7, Theorem 11]). *Let $\mathcal{C}$ be a $\mathbb{F}_{q^m}$-linear code. Then the dual of the $\mathbb{F}_q$-subfield subcode is the trace code of the dual of the original code over $\mathbb{F}_{q^m}$. In symbols:*

$$\mathcal{C}(\mathbb{F}_q)^\perp = \mathtt{trace}_{\mathbb{F}_{q^m}/\mathbb{F}_q}\ \mathcal{C}^\perp. \qquad \square$$

3.2. M-sequences and cyclic binary codes

We begin by introducing the so-called *maximal length sequences* (*m-sequences* for short). As before, p is a prime number and $n \in \mathbb{Z}_{>0}$.

DEFINITION 3.2.0.1 ([**GG05**, Definition 4.6 and Corollary 4.6]). Let $\alpha \in \mathbb{F}_{p^n}$ be a primitive element and $\beta \in \mathbb{F}_{p^n}^\times$ an arbitrary non-zero element. A (p-ary) m-sequence is any sequence $(s_i)_{i=0,1,\dots}$ with values in $\mathbb{F}_p$ of the form

$$s_i = \mathtt{trace}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\beta\alpha^i).$$

Every m-sequence is periodic of period $p^n - 1$ since we choose $\alpha \in \mathbb{F}_{p^n}$ to be a primitive element, i.e. with order $p^n - 1$.

3.2.1. Autocorrelation of m-sequences and simplex codes. One of the most interesting properties of m-sequences is that they allow us to produce in a deterministic way p-ary sequences which simulate randomness (see [**GG05**, Chapter 5] for more details). The property of interest for us is the one concerning the auto-correlation function. We fix the additive character $\psi : \mathbb{F}_p \to \mathbb{C}^\times$ given by $\psi(a) = \mathtt{exp}(2\pi i a/p)$, and denote by $\psi_n : \mathbb{F}_{p^n} \to \mathbb{C}^\times$ the additive character obtained from ψ by precomposition with $\mathtt{trace}_{\mathbb{F}_{p^n}/\mathbb{F}_p}$.

DEFINITION 3.2.1.1. Let $\boldsymbol{s} = (s_i)_i$ be a periodic sequence with values in $\mathbb{F}_p$ of period P. The auto-correlation function associated to the periodic sequence $\boldsymbol{s}$ is defined at the phase shift $t \in \mathbb{Z}_{\geq 0}$ by the formula

$$\mathtt{AC}_{\boldsymbol{s}}(t) := \sum_{i=0}^{P-1} \psi(s_{i+t})\overline{\psi}(s_i) = \sum_{i=0}^{P-1} \psi(s_{i+t} - s_i).$$

The auto-correlation function of a m-sequence $\boldsymbol{s} = (\mathtt{trace}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\beta\alpha^i))_i$ can only take two values due to the orthogonality of characters:

$$\begin{aligned}\mathtt{AC}_{\boldsymbol{s}}(t) &= \sum_{i=0}^{p^n-2} \psi_n(\beta\alpha^{i+t} - \beta\alpha^i) = \sum_{x\in\mathbb{F}_{p^n}^\times} \psi_n\big((\beta\alpha^t - 1)x\big) \\ &= -1 + \sum_{x\in\mathbb{F}_{p^n}} \psi_n\big((\beta\alpha^t - 1)x\big) = \begin{cases} p^n - 1 & \text{if } \alpha^t = \beta^{-1}, \\ -1 & \text{otherwise.}\end{cases}\end{aligned}$$

3.2.1.1. *Simplex codes.* Let $\alpha \in \mathbb{F}_{p^n}$ be a primitive element. We begin by making some easy observations about the set

$$\mathcal{C}(\mathbb{F}_p)^\perp := \left\{ \left(\mathtt{trace}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\beta\alpha^i)\right)_{i=0}^{p^n-2} \ : \ \beta \in \mathbb{F}_{p^n} \right\}.$$

First of all, observe that for $\beta = 0$ we get the zero vector of length $p^n - 1$. Moreover, since the trace is $\mathbb{F}_p$-linear we know the set $\mathcal{C}(\mathbb{F}_p)^\perp$ is a $\mathbb{F}_p$-linear subspace of $\mathbb{F}_p^{p^n-1}$. Finally, observe that this lineal code is cyclic because if we rotate cyclically the codeword $\left(\mathtt{trace}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\beta\alpha^i)\right)_i$, we get $\left(\mathtt{trace}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\beta\alpha\alpha^i)\right)_i$ which is again in $\mathcal{C}(\mathbb{F}_p)^\perp$. From this last observation we get the description

$$\mathcal{C}(\mathbb{F}_p)^\perp = \{(\mathtt{trace}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\alpha^{i+t}))_{i=0}^{p^n-2} \ : \ t = 0, \ldots, p^n - 2\} \cup \{\mathbf{0}\},$$

i.e. the set of the first $p^n - 1$ terms of all rotations of the m-sequence with $\beta = 1$ together with the zero vector of length $p^n - 1$.

When $p = 2$ we can easily understand the consequence of the fact that any two nonzero codewords of $\mathcal{C}(\mathbb{F}_2)^\perp$ are uncorrelated. Indeed, observe that now $\psi(\cdot) = (-1)^{(\cdot)}$ and, if we write $u_i = \mathtt{trace}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\alpha^i), v_i = \mathtt{trace}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\alpha^{i+t})$ with $t \not\equiv 0 \pmod{2^n - 1}$ for $i = 0, \ldots, 2^n - 2$, we see that

$$\begin{aligned}-1 &= \sum_{i=0}^{2^n-2} \psi_n(\alpha^i + \alpha^{i+t}) \\ &= \left|\{i \in \{0, \ldots, 2^n - 2\} : \mathtt{trace}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\alpha^i) = \mathtt{trace}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\alpha^{i+t})\}\right| \\ &\qquad - \left|\{i \in \{0, \ldots, 2^n - 2\} : \mathtt{trace}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\alpha^i) \neq \mathtt{trace}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\alpha^{i+t})\}\right| \\ &= 2^n - 1 - 2 \cdot \mathtt{dist}(\boldsymbol{u}, \boldsymbol{v})\end{aligned}$$

where $\boldsymbol{u} = (u_i)_{i=0}^{2^n-2}, \boldsymbol{v} = (v_i)_{i=0}^{2^n-2}$ and $\mathtt{dist}(\boldsymbol{u}, \boldsymbol{v})$ is the Hamming distance between these two binary codewords. From the previous identity it follows that $\mathtt{dist}(\boldsymbol{u}, \boldsymbol{v}) = 2^{n-1}$, i.e. any two rotations of a fixed m-sequence differ at exactly 2^{n-1} indices within a period. Taking into account that every nonzero codeword of $\mathcal{C}(\mathbb{F}_2)^\perp$ has precisely 2^{n-1} nonzero entries (this follows easily from the orthogonality of characters), we see that any two codewords of $\mathcal{C}(\mathbb{F}_2)^\perp$ differ at exactly 2^{n-1}

indices, and this justifies why these codes are called *simplex codes*. This same property is satisfied for every prime p in general (see [**PW72**, §8.5] for further details).

To explain our notation, consider the $1 \times (p^n - 1)$ matrix with entries in $\mathbb{F}_{p^n}$ given by:

$$\mathcal{H}_1 := \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{p^n-2} \end{pmatrix}.$$

Let $\mathcal{C}$ be the $\mathbb{F}_{p^n}$-linear code with parity check matrix $\mathcal{H}_1$. Now consider the $\mathbb{F}_p$-subfield subcode of $\mathcal{C}$, i.e.

$$\mathcal{C}(\mathbb{F}_p) := \{(c_0, \ldots, c_{p^n-2}) \in \mathcal{C} \ : \ c_i \in \mathbb{F}_p \ \forall i\}.$$

Now we use the identification between $\mathbb{F}_p^{p^n-1}$ and $\mathbb{F}_p[x]/(x^{p^n-1}-1)$ such that $\boldsymbol{c} = (c_0, \ldots, c_{p^n-2})$ is identified with its associated polynomial $\mathtt{pol}(\boldsymbol{c})(x) := \sum_{i=0}^{p^n-2} c_i x^i$, and every polynomial modulo $x^{p^n-1} - 1$ is identified with the word obtained from its coefficients. Then $\boldsymbol{c} \in \mathcal{C}(\mathbb{F}_p)$ if and only if $\sum_{i=0}^{p^n-2} c_i \alpha^i = 0$, which is equivalent to $\mathtt{pol}(\boldsymbol{c})(\alpha) = 0$. Hence, under this bijection, we se that $\mathcal{C}(\mathbb{F}_p)$ is the ideal in $\mathbb{F}_p[x]/(x^{p^n-1} - 1)$ generated by the minimal (primitive) monic polinomial $m_1(x)$ of α. In particular, $\mathcal{C}(\mathbb{F}_p)$ is a cyclic code. To show that the code $\mathcal{C}(\mathbb{F}_p)^\perp$ is precisely the dual code of $\mathcal{C}(\mathbb{F}_p)$ as the notation suggests we invoke Delsarte's theorem 3.1.3.1 to deduce that the codewords of $\mathcal{C}(\mathbb{F}_p)^\perp$ are obtained from the codewords of $\mathcal{C}^\perp$ by applying the trace function componentwise. Since a generator matrix of $\mathcal{C}^\perp$ is $\mathcal{H}_1$, the codewords of $\mathcal{C}^\perp$ are the $\mathbb{F}_{p^n}$-multiples of $(1, \alpha, \ldots, \alpha^{p^n-2})^t$. It follows that

$$\mathcal{C}(\mathbb{F}_p)^\perp = \{(\mathtt{trace}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\beta\alpha^i))_{i=0}^{p^n-2} : \beta \in \mathbb{F}_{p^n}\}.$$

This code is a cyclic code with parity check polynomial $x^n m_1(1/x)$, which coincides with $m_{-1}(x)$ the minimal primitive polynomial of α^{-1}.

3.2.2. Cross-correlation of m-sequences and cyclic binary codes. As we saw before, the auto-correlation of m-sequences can be computed explicitly, so it is natural to ask if we can compute the correlation between two different m-sequences. We introduce the concept of cross-correlation here:

DEFINITION 3.2.2.1. Let $\boldsymbol{r} = (r_i)_i$ and $\boldsymbol{s} = (s_i)_i$ be two periodic sequences with values in $\mathbb{F}_p$ and both of period P. The cross-correlation function associated to $\boldsymbol{r}$ and $\boldsymbol{s}$ is defined at the phase shift $t \in \mathbb{Z}_{\geq 0}$ by the formula

$$\mathtt{CC}_{\boldsymbol{r},\boldsymbol{s}}(t) := \sum_{i=0}^{P-1} \psi(r_{i+t})\overline{\psi}(s_i) = \sum_{i=0}^{P-1} \psi(r_{i+t} - s_i).$$

Now let $\alpha, \alpha' \in \mathbb{F}_{p^n}$ be two primitive elements and $\beta, \beta' \in \mathbb{F}_{p^n}^\times$. Since α and α' are primitive elements, there exists an integer $0 \leq d < p^n - 1$ such that $\mathtt{gcd}(d, p^n - 1) = 1$ and $\alpha' = \alpha^d$. With this notation we can express the cross-correlation between the m-sequences $\left(\mathtt{trace}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\beta\alpha^i)\right)_i$ and $\left(\mathtt{trace}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\beta'\alpha'^i)\right)_i$ as follows:

$$\begin{aligned} \sum_{i=0}^{p^n-2} \psi_n(\beta\alpha^{i+t} - \beta'\alpha'^i) &= \sum_{i=0}^{p^n-2} \psi_n(\beta\alpha^{i+t} - \beta'\alpha^{di}) \\ &= \sum_{x \in \mathbb{F}_{p^n}} \psi_n(\beta\alpha^t x - \beta' x^d) \\ &= -1 + \sum_{x \in \mathbb{F}_{p^n}} \psi_n(\beta\alpha^t x - \beta' x^d), \end{aligned}$$

an expression that involves the trace function of $\mathcal{M}_{\mathtt{big}}(p; d, 1)$ on $\mathbb{G}_{m,\mathbb{F}_p} \times \mathbb{G}_{m,\mathbb{F}_p}$ at the rational point $(-\beta', \beta\alpha^t) \in \mathbb{F}_{p^n}^\times \times \mathbb{F}_{p^n}^\times$.

It is known [**Hel76**, Theorem 4.1] that, as soon as $d \notin \{1, p, p^2, \dots, p^{n-1}\}$, i.e. α^d is not a root of the minimal polynomial $m_1(x)$ of α over $\mathbb{F}_p$, then the cross-correlation function between any two m-sequences constructed with α and α^d takes at least three different values. It is an interesting problem to study which values of d give a cross-correlation that has exactly three different values. For example, let $k \in \mathbb{N}$ be a positive integer such that $n/\mathtt{gcd}(n,k)$ is odd. For $p = 2$, the exponents $d = 2^k + 1$ (Gold numbers) and $d = 2^k(2^k - 1) + 1$ (Kasami–Welch numbers) give three valued crosscorrelation functions [**HK98**, Theorem 5.3]. Observe that $2^k + 1$ has Kubert type I and $2^k(2^k - 1) + 1 = (2^{3k} + 1)/(2^k + 1)$ has Kubert type III, k for $p = 2$.

3.2.2.1. *Cyclic codes with two zeroes.* Now we proceed as in §3.2.1.1 and show how the cross-correlation of m-sequences is useful to study the weight distribution of codewords for certain cyclic codes. Let $\alpha \in \mathbb{F}_{p^n}$ be a primitive element and denote by $m_i(x) \in \mathbb{F}_p[x]$ the minimal polynomial of α^i. We fix an integer $0 \leq d < p^n - 1$ coprime with $p^n - 1$ (so α^d is a primitive element as well). Now consider the $2 \times (p^n - 1)$ matrix with entries in $\mathbb{F}_{p^n}$ given by

$$\mathcal{H}_{1,d} := \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{p^n-2} \\ 1 & \alpha^d & \alpha^{2d} & \cdots & \alpha^{d(p^n-2)} \end{pmatrix}.$$

$\mathcal{C}_{1,d}$ is defined as the $\mathbb{F}_{p^n}$-linear code with parity check matrix $\mathcal{H}_{1,d}$. Define $\mathcal{C}_{1,d}(\mathbb{F}_p)$ as the $\mathbb{F}_p$-subfield subcode of $\mathcal{C}_{1,d}$ which consists of those codewords of $\mathcal{C}_{1,d}$ whose entries lie in $\mathbb{F}_p$. Observe that $\boldsymbol{c} = (c_0, \dots, c_{p^n-2}) \in \mathcal{C}_{1,d}(\mathbb{F}_p)$ if and only if $\sum_{i=0}^{p^n-2} c_i\alpha^i = \sum_{i=0}^{p^n-2} c_i\alpha^{di} = 0$ and $c_i \in \mathbb{F}_p$ for every index i. Equivalently, if and only if $\mathtt{pol}(\boldsymbol{c})(\alpha) = \mathtt{pol}(\boldsymbol{c})(\alpha^d) = 0$. Hence, $\mathcal{C}_{1,d}(\mathbb{F}_p)$ is, seen as a subset of $\mathbb{F}_p[x]/(x^{p^n-1} - 1)$, the ideal generated by the polynomial $m_1(x)m_d(x)$ and it is a cyclic code.

Its dual is a cyclic code with parity check polynomial $x^{2n}m_1(1/x)m_d(1/x) = m_{-1}(x)m_{-d}(x)$. Using Delsarte's theorem 3.1.3.1, we know that this dual consists of the codewords obtained from the codewords of $\mathcal{C}_{1,d}^{\perp}$ by applying the trace componentwise. Since

$$\mathcal{C}_{1,d}^{\perp} = \left\langle (1, \alpha, \dots, \alpha^{p^n-2})^t, (1, \alpha^d, \dots, \alpha^{d(p^n-2)})^t \right\rangle_{\mathbb{F}_{p^n}}$$

because it has $\mathcal{H}_{1,d}$ as generator matrix, we obtain the equality

$$\mathcal{C}_{1,d}(\mathbb{F}_p)^{\perp} = \left\{ \left(\mathtt{trace}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\beta_1\alpha^{i+t} - \beta_2\alpha^{di})\right)_{i=0}^{p^n-2} \ : \ \beta_1, \beta_2 \in \mathbb{F}_{p^n} \right\}.$$

When $p = 2$, we can relate the Hamming weight of codewords in $\mathcal{C}_{1,d}(\mathbb{F}_2)^{\perp}$ with the cross-correlation of two m-sequences. Explictly, observe that for $\beta_1, \beta_2 \neq 0$

$$\begin{aligned} \sum_{i=0}^{2^n-2} \psi_n(\beta_1\alpha^{i+t} + \beta_2\alpha^{di}) &= \left|\left\{i \in \{0, \dots, 2^n - 2\} : \mathtt{trace}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\beta_1\alpha^{i+t} + \beta_2\alpha^{di}) = 0\right\}\right| \\ &\quad - \left|\left\{i \in \{0, \dots, 2^n - 2\} : \mathtt{trace}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\beta_1\alpha^{i+t} + \beta_2\alpha^{di}) = 1\right\}\right| \\ &= 2^n - 1 - 2 \cdot \mathtt{wt}(\boldsymbol{u}) \end{aligned}$$

where $\boldsymbol{u} = (\mathtt{trace}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\beta_1\alpha^{i+t} + \beta_2\alpha^{di}))_{i=0}^{2^n-2}$ and $\mathtt{wt}(\boldsymbol{u})$ is the Hamming weight of the binary codeword $\boldsymbol{u}$. If we fix a square root $\sqrt{2}$ of 2, the left-hand side of the previous equality can be expressed as $-1-2^{n/2}\cdot\mathtt{tr}_{\mathcal{M}_{\mathtt{big}}(2;d,1),\mathbb{F}_{2^n}}(-\beta_2, \beta_1\alpha^t)$, considering the $\overline{\mathbb{Q}}_\ell$-sheaf $\mathcal{M}_{\mathtt{big}}(2; d, 1)$ as defined on the variety $\mathbb{G}_{m,\mathbb{F}_2} \times \mathbb{G}_{m,\mathbb{F}_2}$.

3.3. Almost Perfect Nonlinear (APN) functions

We review some concepts in order to explain the relation between cryptography and the study of monodromy groups of the lisse $\overline{\mathbb{Q}}_\ell$-sheaves $\mathcal{M}(2; d, 1)$.

3.3.1. Rinjdael cipher and the differential attack. In 2001, the U.S. National Institute of Standards and Technology (NIST) established the *Advanced Encryption Standard* (AES) based on the Rijndael cipher. Here we explain the most basic setup for Rijndael, namely with block length 128 and key length 128, which is actually the most common one. We follow closely Lenstra's well-written notes [**Len**] and Smart's textbook [**Sma**, §8.3].

Rijndael is a block cipher which applies certain operations on some given plaintext a prescribed number of rounds (usually 10) involving certain keys obtained following some key schedule. Any element of $\mathbb{F}_2$ is called *bit* and any element of $\mathbb{F}_2^8$ is called *byte*. We identify $\mathbb{F}_2^8$ with the finite field $\mathbb{F}_{2^8}$ defined by the primitive polynomial $x^8 + x^4 + x^3 + x + 1$. Rijndael operates on an internal 4×4 matrix of bytes S, i.e. with entries in $\mathbb{F}_{2^8}$, called the *state matrix* and each round key K_i is held analogously. The four operations that take place within an encryption round are the following (observe that we do not describe decryption since it is analogous):

- *SubBytes*: Write
$$S = \begin{pmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{pmatrix}.$$
We associate to every nonzero byte $s_{ij} \in \mathbb{F}_{2^8}^\times$ its inverse and associate $0 \in \mathbb{F}_{2^8}$ to 0. Rewrite the bytes obtained this way as vectors of 8 bits, say $x_7x_6 \dots x_1x_0$. Now apply the affine transformation
$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix},$$
where $\oplus$ denotes *xor* addition, and save the result as a byte $y \in \mathbb{F}_{2^8}$.
- *ShiftRows*: This operation performs cyclic shifts on rows of the state matrix. For our version of Rijndael it can be described as follows:
$$\begin{pmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{pmatrix} \mapsto \begin{pmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{11} & s_{12} & s_{13} & s_{10} \\ s_{22} & s_{23} & s_{20} & s_{21} \\ s_{33} & s_{30} & s_{31} & s_{32} \end{pmatrix}.$$
- *MixColumns*: Let $(a_0, a_1, a_2, a_3)^t$ be a column of the state matrix S. Then we can define the operation as the matrix product
$$\begin{pmatrix} \alpha & 1+\alpha & 1 & 1 \\ 1 & \alpha & 1+\alpha & 1 \\ 1 & 1 & \alpha & 1+\alpha \\ 1+\alpha & 1 & 1 & \alpha \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix},$$

where α is a root of the primitive polynomial $x^8+x^4+x^3+x+1$, i.e. a primitive element of $\mathbb{F}_{2^8}$. This operation is **not** applied at the 10th round.
- *AddRoundKey*: This is just componentwise xor addition between the state matrix and the key matrix corresponding to the round.

The operation SubBytes is usually known as the S-box of Rijndael cipher. It should be observed that it is the only operation which involves a non-linear transformation, namely the map $a \in \mathbb{F}_{2^8}^{\times} \mapsto a^{-1}$. For this reason this operation have to be properly choosen. This motivates the next topic.

3.3.1.1. *APN functions.* In 1991 Biham and Shamir [**BS91**] described the *differential cryptanalysis* for breaking iterated block cryptosystems. This statistical attack consists in the study of the non-linearity properties of the corresponding S-box with the aim of identifying pairs of texts on which the S-box is particularly weak. Specifically, given a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and $a \in \mathbb{F}_{2^n}$ we define the derivative of F with respect to a as the function

$$\begin{array}{ccc} \mathtt{D}_aF : \mathbb{F}_{2^n} & \longrightarrow & \mathbb{F}_{2^n} \\ x & \longmapsto & F(x+a)+F(x). \end{array}$$

For any pair of elements $a, b \in \mathbb{F}_{2^n}$ we consider the quantity $\delta(a,b) = |\{x \in \mathbb{F}_{2^n} : \mathtt{D}_aF(x) = b\}|$. The *differential uniformity* of F is defined by the formula

$$\delta(F) = \mathtt{max}_{a\neq 0,b}\ \delta(a,b).$$

If we use F in the design of our S-boxes we want F to not be as linear as possible, which can be formalized by requiring $\delta(F)$ to be as small as posible.

Since $\mathbb{F}_{2^n}$ has characteristic 2, $\delta(a,b)$ is even for every $a, b \in \mathbb{F}_{2^n}$ with $a \neq 0$. Indeed, if $t \in \{x \in \mathbb{F}_{2^n} : \mathtt{D}_aF(x) = b\}$, then $F(t+a)+F(t) = b$ and hence $F((t+a)+a)+F(t+a) = F(t)+F(t+a) = b$, so $t+a \in \{x \in \mathbb{F}_{2^n} : \mathtt{D}_aF(x) = b\}$. It follows that the differential uniformity of F, $\delta(F)$, is an even number and bigger or equal than 2. This motivates the following definition:

DEFINITION 3.3.1.1. A function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called *almost perfect nonlinear* if its differential uniformity $\delta(F)$ takes its least possible value, i.e. $\delta(F) = 2$.

Observe that this definition is equivalent to the condition $|\{\mathtt{D}_aF(x) : x \in \mathbb{F}_{2^n}\}| = 2^{n-1}$ for every $a \neq 0$. Indeed, note that $\mathtt{im}(\mathtt{D}_aF) = \{\mathtt{D}_aF(x) : x \in \mathbb{F}_{2^n}\}$ and, for $b \in \mathbb{F}_{2^n}$, $(\mathtt{D}_aF)^{-1}(b) = \{x \in \mathbb{F}_{2^n} : \mathtt{D}_aF(x) = b\}$. Taking into account that

$$2^n = |\mathbb{F}_{2^n}| = \left|\cup_{b\in\mathbb{F}_{2^n}} (\mathtt{D}_aF)^{-1}(b)\right| = \left|\cup_{b\in\mathtt{im}(\mathtt{D}_aF)} (\mathtt{D}_aF)^{-1}(b)\right| = \sum_{b\in\mathtt{im}(\mathtt{D}_aF)} \left|(\mathtt{D}_aF)^{-1}(b)\right|,$$

we see that both conditions are equivalent. Hence, this implies that we do not obtain any statistical information by fixing the difference of two plaintexts and analyzing the difference of the corresponding outputs.

For example, we can ask if the function $x \in \mathbb{F}_{2^n}^{\times} \mapsto x^{-1}, 0 \mapsto 0$, used in the implementation of Rijndael with $n = 8$ is APN or not. This question was answered by Kaisa Nyberg [**Nyb94**, §4], and the answer is that the inversion mapping given by $x \in \mathbb{F}_{2^n} \mapsto x^{2^n-2}$ is APN if and only if n is odd. When n is even, this power transformation is not too far from being APN since its differential uniformity equals 4.

3.3.2. APN polynomials and binary codes. In [**CCZ98**, Theorem 5] the APN polynomial functions $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are characterized using coding theory. We review here this result which will allow us to find connections between monomial APN functions, cyclic codes and m-sequences.

THEOREM 3.3.2.1 ([**CCZ98**, Theorem 5.(i) and (ii)]). *Let $F \in \mathbb{F}_{2^n}[x]$ be a polynomial of degree less than 2^n-1 such that $F(0) = 0$ and consider it as a function from $\mathbb{F}_{2^n}$ to itself. Let $\alpha \in \mathbb{F}_{2^n}$ be*

a primitive element. Define $\mathcal{C}_F(\mathbb{F}_2)$ to be the binary code of length 2^n-1 defined as the $\mathbb{F}_2$-subfield subcode of the $\mathbb{F}_{2^n}$-linear code with parity check matrix

$$\mathcal{H}_F := \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^n-2} \\ F(1) & F(\alpha) & F(\alpha^2) & \cdots & F(\alpha^{2^n-2}) \end{pmatrix}.$$

Denote by d_F^* its minimum distance. Then

(a) *$d_F^* \in \{3,4,5\}$.*
(b) *F is APN if and only if $d_F^* = 5$.*

PROOF. We only prove part (b) of the theorem to illustrate the sort of ideas involved. Observe that a codeword $\boldsymbol{c} = (c_0, \ldots, c_{2^n-2}) \in \mathbb{F}_2^{2^n-1}$ is in $\mathcal{C}_F(\mathbb{F}_2)$ if and only if $\sum_{i=0}^{2^n-2} c_i\alpha^i = \sum_{i=0}^{2^n-2} c_i F(\alpha^i) = 0$. Since the minimum distance of a linear binary code is equal to the minimum Hamming weight of a codeword, we only need to see what means for $\mathcal{C}_F(\mathbb{F}_2)$ to have codewords with Hamming weight 3 or 4.

This way, assume that there exists four distinct elements $x, y, x', y' \in \mathbb{F}_{2^n}$ such that

$$x + y + x' + y' = 0 \text{ and } F(x) + F(y) + F(x') + F(y') = 0.$$

If we write $a := x' + y'$ and $b := F(x') + F(y')$, observe that $a \neq 0$ and $x + y = a, F(x) + F(y) = b$. Since both (x, y) and (x', y') satisfies these two relations, we conclude $|(\mathtt{D}_a F)^{-1}(b)| \geq 4$, so F is not APN. The converse is analogous. In conclusion, $\mathcal{C}_F(\mathbb{F}_2)$ does not contain codewords of weight < 5 if and only if F is APN, hence $5 \leq d_F^* \leq 5$ if and only if F is APN.

□

When $F(x) \in \mathbb{F}_{2^n}[x]$ is an APN polynomial with $F(0) = 0$, then the code $\mathcal{C}_F(\mathbb{F}_2)$ has dimension $2^n - 1 - 2n$ (see [**CCZ98**, §3.2, Corollary 1]).

3.3.2.1. *APN monomials, cyclic binary codes and m-sequences.* In general, while implementing the S-box of a block cipher like AES we use a table with precomputed values of the non-linear function F. However, if the function is a power function, i.e. $F(x) = x^d$ for some $1 < d < 2^n - 1$, then it is easy to implement it directly with electronic circuits. For this reason, APN monomials or APN power functions are so interesting and a lot of research have been developed around them.

After Theorem 3.3.2.1 we know that $F(x) = x^d$ is APN if and only if the code $\mathcal{C}_F(\mathbb{F}_2)$ has minimum distance 5. In this case, we know that $\mathcal{C}_F(\mathbb{F}_2)$ has dimension 2^n-1-2n. Since $\mathcal{H}_F = \mathcal{H}_{1,d}$ it follows that $\mathcal{C}_F = \mathcal{C}_{1,d}(\mathbb{F}_2)$. Hence its dual has dimension $2n$ and parity check polynomial $m_{-1}(x)m_{-d}(x)$, it follows that α^d is a primitive element of $\mathbb{F}_{2^n}$ and in particular $\mathtt{gcd}(d, 2^n-1) = 1$.

The combination of §3.5 Theorem 10, §3.2 Theorem 5.(ii) and Corollary 1.(iii) from [**CCZ98**] shows that Gold numbers $d = 2^k + 1$ with $\mathtt{gcd}(k, n) = 1$ and Kasami numbers $d = 2^k(2^k - 1) + 1$ with $\mathtt{gcd}(k, n) = 1$ give rise to an APN power function, the same numbers that give special cross-correlation functions if we further assume n odd.

3.3.3. Exceptional APN monomials and geometry. We are interested in knowing if a power function $F = x^d \in \mathbb{F}_2[x]$, when understood as a transformation $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, can be APN for infinitely many values of n. We name those special monomial functions:

DEFINITION 3.3.3.1. Let $F(x) = x^d$. The exponent d is called *exceptional* if F is APN on infinitely many extensions of $\mathbb{F}_2$.

Lets see that exceptionality is a geometric property [**HM11**]. Recall that $F(x) = x^d$ is APN over $\mathbb{F}_{2^n}$ if and only if, for any fixed primitive element $\alpha \in \mathbb{F}_{2^n}$, the $\mathbb{F}_2$-subfield cyclic code $\mathcal{C}_{1,d}(\mathbb{F}_2)$ with parity check matrix $\mathcal{H}_{1,d}$ has minimum distance equal to 5. As we saw above, this is equivalent to $\mathcal{C}_{1,d}(\mathbb{F}_2)$ not having codewords of Hamming weight less than 5. We already know that codewords of $\mathcal{C}_{1,d}(\mathbb{F}_2)$ with Hamming weight 3 or 4 correspond to rational points over $\mathbb{F}_{2^n}$ of the zero locus of the polynomial

$$f_d(x, y, z) := x^d + y^d + z^d + (x + y + z)^d$$

with distinct coordinates. Observe that the polynomial f_d is divisible by $x+y, x+z, y+z$ and we are interested in $\mathbb{F}_{2^n}$-rational points outside the union of the varieties they define, hence we consider the polynomial

$$g_d(x,y,z) := \frac{f_d(x,y,z)}{(x+y)(x+z)(y+z)}.$$

We are requiring $g_d = 0$ to not have $\mathbb{F}_{2^n}$-rational points for infinitely many extensions $\mathbb{F}_{2^n}/\mathbb{F}_2$. The following Theorem is the key result to establish the relation between exceptional APN monomials and monodromy:

THEOREM 3.3.3.2 ([**JW93**, Propostion 1 and Corollary]). *If the polynomial $g_d(x,y,z)$ is absolutely irreducible, i.e. if it is irreducible in $\mathbb{F}_2^{\mathtt{alg}}[x]$ with $\mathbb{F}_2^{\mathtt{alg}}$ an algebraic closure of $\mathbb{F}_2$, then the monomial $x \mapsto x^d$ is APN only for finitely many extensions $\mathbb{F}_{2^n}$.* □

The previous discussion can be carried out more generally for polynomials $p(x) \in \mathbb{F}_2[x]$ such that $p(0) = 0$ because $p : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is APN if and only if the associated code has minimum distance equal to 5. In this more general case, we consider $f_p(x,y,z) := p(x)+p(y)+p(z)+p(x+y+z) \in \mathbb{F}_2[x,y,z]$ and $g_p(x,y,z) := \frac{f_p(x,y,z)}{(x+y)(x+z)(y+z)} \in \mathbb{F}_2[x,y,z]$. In order for the transformation defined by p to be APN for infinitely many extensions $\mathbb{F}_{2^n}$ the polynomial g_p should not be absolutely irreducible.

3.4. Exceptional APN polynomials and monodromy

For a given polynomial $p \in \mathbb{F}_2[x]$ such that $p(0) = 0$, denote by $\mathcal{F}_p$ the $\overline{\mathbb{Q}}_\ell$-sheaf on $\mathbb{G}_{m,\mathbb{F}_2} \times \mathbb{A}^1_{\mathbb{F}_2}$ constructed in Proposition 2.2.1.1, i.e. $\mathtt{R}^1\pi_{12!}\mathcal{L}_{\psi(sp(x)+tx)}$ where $\pi_{12} : \mathbb{G}_{m,\mathbb{F}_2} \times \mathbb{A}^1_{\mathbb{F}_2} \times \mathbb{A}^1_{\mathbb{F}_2} \to \mathbb{G}_{m,\mathbb{F}_2} \times \mathbb{A}^1_{\mathbb{F}_2}$ is the projection onto the first two factors (observe that we do not Tate twist the sheaf). We already know that $\mathcal{F}_p$ is a lisse geometrically irreducible $\overline{\mathbb{Q}}_\ell$-sheaf and pure of weight 1. Denote the trace function of $\mathcal{F}_p$ at the rational point $(s,t) \in \mathbb{F}_{2^n}^\times \times \mathbb{F}_{2^n}$ by $\varphi_n(s,t)$. Applying formula 2.1.1 we find that

$$\mathtt{M}_4(\mathbb{G}_{m,\mathbb{F}_2} \times \mathbb{A}^1_{\mathbb{F}_2}, \mathcal{F}_p) = \mathtt{lim}_{n\to\infty} \frac{\left|\sum_{s\neq 0, t\in\mathbb{F}_{2^n}} \varphi_n(s,t)^2 \overline{\varphi_n(s,t)}^2\right|}{2^{4n}} = \mathtt{M}_4(\mathbb{G}_{m,\mathbb{F}_2} \times \mathbb{A}^1_{\mathbb{F}_2}, \mathcal{M}_{\mathtt{big}}(2;d,1)).$$

Taking into account that we are working in characteristic 2, the sum in the previous formula can be written as follows:

$$\begin{aligned}
\sum_{s\neq 0, t\in\mathbb{F}_{2^n}} |\varphi_n(s,t)|^4 &= \sum_{x,y,z,w\in\mathbb{F}_{2^n}} \left(\sum_{s\in\mathbb{F}_{2^n}^\times} \psi_n\big(s(p(x)+\cdots+p(w))\big)\right)\left(\sum_{t\in\mathbb{F}_{2^n}} \psi_n\big(t(x+\cdots+w)\big)\right)\\
&= \sum_{\substack{x,y,z,w\in\mathbb{F}_{2^n}\\ p(x)+\cdots+p(w)=0}} (2^n-1)\sum_{t\in\mathbb{F}_{2^n}} \psi_n\big(t(x+y+z+w)\big)\\
&\qquad - \sum_{\substack{x,y,z,w\in\mathbb{F}_{2^n}\\ p(x)+\cdots+p(w)\neq 0}} \sum_{t\in\mathbb{F}_{2^n}} \psi_n\big(t(x+y+z+w)\big)\\
&= 2^n\cdot \sum_{\substack{x,y,z,w\in\mathbb{F}_{2^n}\\ p(x)+\cdots+p(w)=0}} \sum_{t\in\mathbb{F}_{2^n}} \psi_n\big(t(x+y+z+w)\big)\\
&\qquad - \sum_{x,y,z,w\in\mathbb{F}_{2^n}} \sum_{t\in\mathbb{F}_{2^n}} \psi_n\big(t(x+y+z+w)\big)\\
&= 2^{2n}\cdot \left|\left\{(x,y,z,w)\in\mathbb{F}_{2^n}^4 : \substack{x+\cdots+w=0,\\ p(x)+\cdots+p(w)=0}\right\}\right|\\
&\qquad - 2^n\left|\{(x,y,z,w)\in\mathbb{F}_{2^n}^4 : x+\cdots+w=0\}\right|\\
&= 2^{2n}\left|\{(x,y,z)\in\mathbb{F}_{2^n}^3 : f_p(x,y,z)=0\}\right| - 2^{4n}\\
&= 2^{2n}\left|\{(x,y,z)\in\mathbb{F}_{2^n}^3 : (x+y)(x+z)(y+z)g_p(x,y,z)=0\}\right| - 2^{4n}\\
&= (2+C)2^{4n} + O\left(2^{\frac{7}{2}n}\right),
\end{aligned}$$

where C is equal to the number of absolutely irreducible components of the algebraic variety $\{(x,y,z)\in\mathbb{F}_{2^n}^3 : g_p(x,y,z)=0\}$, equality that is valid for n divisible enough and such that all the absolutely irreducible factors of $g_p(x,y,z)$ over $\mathbb{F}_2^{\mathtt{alg}}$ are defined over $\mathbb{F}_{2^n}$. In conclusion, we obtain the formula

$$\mathtt{M}_4(\mathbb{G}_{m,\mathbb{F}_2}\times\mathbb{A}^1_{\mathbb{F}_2},\mathcal{F}_p) = 2 + \#\text{ abs. irr. comp. of } \{g_p=0\}.$$

Therefore, information about the geometric monodromy representation associated to $\mathcal{F}_p$, i.e. knowing the geometric monodromy group $G_{\mathtt{geom}}(\mathbb{C})$ and in which representation $G_{\mathtt{geom}}(\mathbb{C})\to\mathtt{GL}(r,\mathbb{C})$, we can obtain the number of absolutely irreducible components of $g_p=0$ and study the APN-ness exceptionality of p.

3.4.1. Exceptional APN monomials and $\mathcal{M}(2;d,1)$. Using the ideas introduced above and the determination of the monodromy groups for the sheaves $\mathcal{M}(2;d,1)$ due to Šuch [**Š00**] (but also see [**RL19**, Corollary 6]), we are able to rule out several exponents d which does not give rise to an APN exceptional power function. Specifically, when $p=2$, if the monodromy group $G_{\mathtt{geom}}$ of $\mathcal{M}(2;d,1)$ is not finite, then it is $\mathtt{Sp}(d-1)$ in its standard representation (we always assume d coprime to the prime p). This means that the representation $\rho:\pi_1^{\mathtt{geom}}(\mathbb{A}^1_{\mathbb{F}_2})\to\mathtt{GL}(d-1,\mathbb{C})$ associated to $\mathcal{M}(2;d,1)$ factors through $G_{\mathtt{geom}}(\mathbb{C})=\mathtt{Sp}(d-1,\mathbb{C})\to\mathtt{GL}(d-1,\mathbb{C})$ where the last arrow is the standard representation, which we denote by $\mathtt{std}:\mathtt{Sp}(d-1,\mathbb{C})\to\mathtt{GL}(d-1,\mathbb{C})$.

Write $G^{\mathtt{big}}_{\mathtt{geom}}$ to denote the geometric monodromy group of $\mathcal{M}_{\mathtt{big}}(2;d,1)$ as a sheaf over $\mathbb{G}_{m,\mathbb{F}_2}\times\mathbb{A}^1_{\mathbb{F}_2}$ and keep the notation $G_{\mathtt{geom}}$ for the geometric monodromy group of $\mathcal{M}(2;d,1)$ as a sheaf over $\mathbb{A}^1_{\mathbb{F}_2}$. Recall that $\mathcal{M}(2;d,1)=\iota^*\mathcal{M}_{\mathtt{big}}(2;d,1)$ where $\iota:\mathbb{A}^1_{\mathbb{F}_2}\hookrightarrow\mathbb{G}_{m,\mathbb{F}_2}\times\mathbb{A}^1_{\mathbb{F}_2}$ is the slice $t\mapsto(1,t)$. It follows that $G_{\mathtt{geom}}\subset G^{\mathtt{big}}_{\mathtt{geom}}$. Since we assume $G_{\mathtt{geom}}$ non-finite, it is equal (via the standard representation) to $\mathtt{Sp}(d-1)$. But the trace function of $\mathcal{M}_{\mathtt{big}}(2;d,1)$ assume real values as well, hence it is self-dual and it follows that $G^{\mathtt{big}}_{\mathtt{geom}}$ can be realized inside $\mathtt{Sp}(d-1)$ via the standard representation too. We conclude that $\mathtt{M}_{\mathtt{big}}(2;d,1)$ has geometric monodromy group $\mathtt{Sp}(d-1)$ in its standard representation.

In conclusion, when $\mathcal{M}(2;d,1)$ has not finite geometric monodromy group, we know that the 4-th geometric moment $\mathtt{M}_4(\mathbb{G}_{m,\mathbb{F}_2}\times\mathbb{A}^1_{\mathbb{F}_2},\mathcal{M}_{\mathtt{big}}(2;d,1))$ is actually the 4-th moment $\mathtt{M}_4(\mathtt{Sp}(d-1,\mathbb{C}),\mathtt{std})$. This moment is easily computed as follows. We want to compute $\mathtt{dim}_{\mathbb{C}}\,\mathtt{End}_{\mathtt{Sp}(d-1,\mathbb{C})}(\mathtt{std}\otimes\mathtt{std})$. It is well-known that $\mathtt{std}\otimes\mathtt{std}=\bigwedge^2(\mathtt{std})\oplus\mathtt{Sym}^2(\mathtt{std})$, and for the standard representation of $\mathtt{Sp}(d-1,\mathbb{C})$ we know $\bigwedge^2(\mathtt{std})=\mathbf{1}\oplus\bigwedge^2(\mathtt{std})/\mathbf{1}$, where $\bigwedge^2(\mathtt{std})/\mathbf{1}$ is an irreducible representation and $\mathbf{1}$ the trivial one. Using Schur's lemma we conclude that $\mathtt{M}_4(\mathtt{Sp}(d-1,\mathbb{C}),\mathtt{std})=3$ since $\mathtt{dim}_{\mathbb{C}}\,\mathtt{End}_{\mathtt{Sp}(d-1,\mathbb{C})}(\mathtt{std}\otimes\mathtt{std})$ equals the sum of the squares of the multiplicities of the irreducible constituents of $\mathtt{std}$ and all $\mathbf{1},\bigwedge^2(\mathtt{std})$ and $\mathtt{Sym}^2(\mathtt{std})$ are irreducible representations of $\mathtt{Sp}(d-1,\mathbb{C})$ with multiplicity 1. Combining all these observations we arrive at

Proposition 3.4.1.1 ([**RL19**]). *Let $d\in\mathbb{Z}_{>0}$ be a positive integer. If the $\overline{\mathbb{Q}}_\ell$-sheaf $\mathcal{M}(2;d,1)$ does not have finite geometric monodromy group, then the monomial function $x\mapsto x^d$ is not APN exceptional.*

Proof. Indeed, after Šuch and the previous discussion, if $G_{\mathtt{geom}}$ is infinite for $\mathcal{M}(2;d,1)$ then $G^{\mathtt{big}}_{\mathtt{geom}}(\mathbb{C})=\mathtt{Sp}(d-1,\mathbb{C})$ in its standard representation. We obtain the equality

$$3=2+\#\text{ abs. irr. comp. of }\{g_d=0\},$$

i.e. the polynomial $g_d(x,y,z)=x^d+y^d+z^d+(x+y+z)^d$ is absolutely irreducible. After Theorem 3.3.3.2 we see that $x\mapsto x^d$ is APN for finitely many extensions $\mathbb{F}_{2^n}/\mathbb{F}_2$, hence it is not APN exceptional.

□

APPENDIX

Implementations with Julia Programming Language

In this appendix we present the full implementation of our algorithms (even the ones not explictly described in Section 2.3) using Julia Programming Language.

The first two routines are used in all the programs.

The following piece of code is used to (pre)compute the smallest representatives of necklaces (see [**CRS$^+$00**]):

```
function necks(k::Int64,
        n::Int64,
        C::Float64,
        a::Vector{Int64},
        pows::Vector{Int64},
        t::Int64=1,
        p::Int64=1,
        res::Vector{Tuple{Int64,Int64,Int64}}=empty([(0,0,0)]))
    @inbounds begin
        if t>n
            s=sum(a)
            if n%p == 0 && s<C
                push!(res,(sum(@view(a[n+1-i])[1]*@view(pows[i+1])[1] for i=0:n-1),s,p))
            end
        else
            @view(a[t+1])[1]=@view(a[t-p+1])[1]
            necks(k,n,C,a,pows,t+1,p,res)
            for j=(@view(a[t-p+1])[1]+1):(k-1)
                @view(a[t+1])[1]=j
                necks(k,n,C,a,pows,t+1,t,res)
            end
        end
    end
    return res
end
```

The next piece of code is used to compute the sum of digits in base p and with expansion of length at most l :

```
function sd(p::Int64,l::Int64)
    @inbounds begin
        res::Array{Int64,1}=fill(0,p^l)
        for i = 1:p^(l-1)
            view(res,p*(i-1)+1:p*i) .+= res[i]:(res[i]+p-1)
        end
    end
    return res
end
```

Code for $\mathcal{M}(p; a, 1)$

```
function main_monomial(p::Int64,l::Int64)
    @time begin
        @inbounds begin
            #pre-computations:
            digitsum=sd(p,l) # list with [i]_p for i=0,1,...,p^l-1
            pows=cumprod(p for i = 1:l)
            mod=pows.-fill(1,l) # list with p^i for i=1,2,...,l
            pushfirst!(pows,1) # list with p^i for i=0,1,...,l
            modl=@view(mod[l])[1] # p^l-1
            Cs=cumsum((p-1)/2 for i=1:l) # list with i(p-1)/2 for i=1,...,l
            dtjs=fill(0,l+1) # auxiliary array

            good=falses(modl) # boolean array for sieving
            fill!(view(good,p:p:modl),true) # discarding indices divisible by p

            # array with smallest representatives of necklaces
            necklaces=[necks(p,r,@view(Cs[r])[1],fill!(dtjs,0),pows) for r=1:l]

            # actual program
            checks=0
            for d = 1:modl
                if !@view(good[d])[1]
                    checks+=1
                    for r = 1:l
                        tmod=@view(mod[r])[1]
                        dt=(d-1)%tmod+1 # d (mod p^r-1) with representative in {1,...,p^r-1}
                        C=@view(Cs[r])[1]
                        t::Float64=0
                        for (x,s) in @view(@view(necklaces[r])[1][2:end])
                            # t = [dx]_{p,r}-[x]_{p,r,-}-r(p-1)/2
                            t=@view(digitsum[((dt*x-1)%tmod)+1+1])[1]-s-C
                            if t>0
                                for j = 1:r
                                    dt=(p*dt-1)%tmod+1
                                    # propagate 'p^j*a' modulo p^r-1
                                    fill!(view(good,dt:tmod:modl),true)
                                end
                                break
                            end
                        end
                        if t>0
                            break
                        end
                    end
                end
            end
        end
    end
    println("I checked $(checks) numbers.")
    println("There are $(length(findall(!,good))) bad numbers.  They are the following:")
    println(findall(!,good))
end
```

Code for $\mathcal{M}(p;a,b,1)$

```
function main_binomial(p::Int64,l::Int64)
    @time begin
        @inbounds begin
            #pre-computations:
            digitsum=sd(p,l)
            pows=cumprod(p for i = 1:l)
            modulos=pows.-fill(1,l)
            modl=@view(modulos[l])[1]
            pushfirst!(pows,1)
            Cs=cumsum((p-1)/2 for i=1:l-1)
            atjs=fill(0,l)
            btjs=fill(0,l)

            goods=trues(modl,modl)
            fill!(view(goods,p:p:modl,:),false)
            fill!(view(goods,:,p:p:modl),false)

            necklaces=[necks(p,r,r*(p-1)+1.0,atjs,pows) for r=1:l-1]

            # actual program
            checks=0
            for ind in CartesianIndices((modl,modl))
                if @view(goods[ind])[1]
                    checks+=1
                    for r = 1:l-1
                        tmod=@view(modulos[r])[1]
                        at=(ind[1]-1)%tmod+1
                        bt=(ind[1]-2)%tmod+1
                        pa=r
                        pb=r
                        @view(atjs[1])[1]=at
                        @view(btjs[1])[1]=bt
                        for k = 2:r
                            @view(atjs[k])[1] = (@view(atjs[k-1])[1]*p-1)%tmod+1
                            if @view(atjs[k])[1]==@view(atjs[1])[1]
                                pa=k
                                break
                            end
                        end
                        for k = 2:r
                            @view(btjs[k])[1] = (@view(btjs[k-1])[1]*p-1)%tmod+1
                            if @view(btjs[k])[1]==@view(btjs[1])[1]
                                pb=k
                                break
                            end
                        end
                        at=minimum(view(atjs,1:pa))
                        bt=minimum(view(btjs,1:pb))
                        C=@view(Cs[r])[1]
                        t::Float64=0
```

```
                        for (m,sm) in @view(@view(necklaces[r])[1][2:end]),
                             (n,sn) in @view(@view(necklaces[r])[1][1:end-1])
                            if m==tmod && n==0
                                continue
                            else
                                t=@view(digitsum[mod(at*m-bt*n,tmod)+1])[1]-sm+sn+C
                            end
                            if t<0
                                if m==tmod
                                    for j = 1:pb
                                        fill!(view(goods,
                                            :,
                                            @view(btjs[j])[1]:tmod:modl),
                                           false)
                                        fill!(view(goods,
                                            @view(btjs[j])[1]:tmod:modl),
                                            :),
                                           false)
                                    end
                                elseif n==0
                                    for j = 1:pa
                                        fill!(view(goods,
                                            @view(atjs[j])[1]:tmod:modl),
                                            :),
                                           false)
                                        fill!(view(goods,
                                            :,
                                            @view(atjs[j])[1]:tmod:modl),
                                           false)
                                    end
                                else
                                    for ja = 1:pa, jb = 1:pb
                                        fill!(view(goods,
                                            @view(atjs[ja])[1]:tmod:modl),
                                            @view(btjs[jb])[1]:tmod:modl),
                                           false)
                                        fill!(view(goods,
                                            @view(btjs[jb])[1]:tmod:modl),
                                            @view(atjs[ja])[1]:tmod:modl),
                                           false)
                                    end
                                end
                                break
                            end
                        end
                        if t<0
                            break
                        end
                    end
                end
            end
        end
    end
    println("I checked $(checks) numbers.")
    println("There are $(length(findall(goods))) bad numbers.  They are the following:")
    println([(d[1],d[2]) for d in findall(good)])
end
```

Code for $\mathcal{B}_{(p;d,e)}$

```
function main_tworoots(p::Int64,l::Int64)
    @time begin
        @inbounds begin
            #pre-computations:
            digitsum=sd(p,l)
            pows=cumprod(p for i = 1:l)
            modulos=pows.-fill(1,l)
            modl=@view(modulos[l])[1]
            pushfirst!(pows,1)
            Cs=cumsum((p-1)/2 for i=1:l-1)
            dtjs=fill(0,l)
            etjs=fill(0,l)

            goods=trues(modl,modl)
            fill!(view(goods,p:p:modl,p:p:modl),false)

            # actual program
            checks=0
            for ind in CartesianIndices((modl,modl))
                if @view(goods[ind])[1]
                    checks+=1
                    for r = 1:l-1
                        tmod=@view(modulos[r])[1]
                        dt=(ind[1]-1)%tmod+1
                        et=(ind[1]-2)%tmod+1
                        C=@view(Cs[r])[1]
                        t::Float64=0
                        s::Float64=0
                        for x = 0:tmod-1, y = 0:tmod-1
                            t=(@view(digitsum[x+1])[1]+
                                @view(digitsum[y+1])[1]+
                                @view(digitsum[mod(y-dt*x-et*x,tmod)+1])[1]+
                                @view(digitsum[mod(et*x-y,tmod)+1])[1]+
                                @views(digitsum[mod(-et*x,tmod)+1])[1]-
                                3*C)
                            s=(@view(digitsum[x+1])[1]+
                                @view(digitsum[mod(-(dt+et)*x,tmod)+1])[1]-
                                C)
                            if t<0 || s<0
                                for j = 1:r
                                    dt=(p*dt-1)%tmod+1
                                    et=(p*et-1)%tmod+1
                                    fill!(view(goods,
                                        dt:tmod:modl),
                                        et:tmod:modl),
                                       false)
                                end
                                break
                            end
                        end
```

```
                        if t<0 || s<0
                            break
                        end
                    end
                end
            end
        end
    end
    println("I checked $(checks) numbers.")
    println("There are $(length(findall(goods))) bad numbers.  They are the following:")
    println([(d[1],d[2]) for d in findall(goods)])
end
```

Bibliography

[Art62] Michael Artin, *Grothendieck topologies: notes on a seminar*, 1962.

[BEKS17] Jeff Bezanson, Alan Edelman, Stefan Karpinski, and Viral B. Shah, *Julia: A Fresh Approach to Numerical Computing*, SIAM Review **59** (2017), no. 1, 65–98.

[BS91] Eli Biham and Adi Shamir, *Differential cryptanalysis of DES-like cryptosystems*, J. Cryptology **4** (1991), no. 1, 3–72.

[CCZ98] Claude Carlet, Pascale Charpin, and Victor Zinoviev, *Codes, bent functions and permutations suitable for DES-like cryptosystems*, Des. Codes Cryptogr. **15** (1998), no. 2, 125–156.

[Con] Brian Conrad, *Étale Cohomology*, Available online at:`virtualmath1.stanford.edu/~conrad/Weil2seminar/Notes/etnotes.pdf`.

[Con07] ———, *Deligne's notes on Nagata compactifications*, J. Ramanujan Math. Soc. (2007), no. 3, 205–257.

[CRS+00] Kevin Cattell, Frank Ruskey, Joe Sawada, Micaela Serra, and C. Robert Miers, *Fast algorithms to generate necklaces, unlabeled necklaces, and irreducible polynomials over* GF(2), Journal of Algorithms **37** (2000), no. 2, 267–282.

[Del80] Pierre Deligne, *La conjecture de Weil. II*, Inst. Hautes Études Sci. Publ. Math. (1980), no. 52, 137–252.

[DH35] Harold Davenport and Helmut Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. **172** (1935), 151–182.

[FFK23] Arthur Forey, Javier Fresán, and Emmanuel Kowalski, *Arithmetic Fourier transforms over finite fields: generic vanishing, convolution, and equidistribution*, 2023.

[Fre19] Javier Fresán, *Équirépartition de Sommes exponentielles [travaux de Katz]*, Astérisque (2019), no. 414, Séminaire Bourbaki. Vol. 2017/2018. Exposés 1136–1150, 205–250.

[Fu15] Lei Fu, *Etale cohomology theory*, revised ed., Nankai Tracts in Mathematics, vol. 14, World Scientific Publishing Co. Pte. Ltd., 2015.

[GG05] Solomon W. Golomb and Guang Gong, *Signal design for good correlation*, Cambridge University Press, Cambridge, 2005, For wireless communication, cryptography, and radar.

[Hel76] Tor Helleseth, *Some results about the cross-correlation function between two maximal linear sequences*, Discrete Math. **16** (1976), no. 3, 209–232.

[HK98] Tor Helleseth and P. Vijay Kumar, *Sequences with low correlation*, Handbook of coding theory, Vol. II, North-Holland, Amsterdam, 1998, pp. 1765–1853.

[HM11] Fernando Hernando and Gary McGuire, *Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions*, J. Algebra **343** (2011), 78–92.

[Ill87] Luc Illusie, *Deligne's l-adic Fourier transform*, Algebraic geometry, Bowdoin, 1985 (Brunswick, Maine, 1985), Proc. Sympos. Pure Math., vol. 46, Amer. Math. Soc., Providence, RI, 1987, pp. 151–163.

[Ill06] ———, *Old and new in étale cohomology*, Available online at: `https://www.imo.universite-paris-saclay.fr/~luc.illusie/wolfson2.pdf`, 2006.

[JW93] H. Janwa and R. M. Wilson, *Hyperplane sections of Fermat varieties in* $\mathbf{P}^3$ *in* char. 2 *and some applications to cyclic codes*, Applied algebra, algebraic algorithms and error-correcting codes (San Juan, PR, 1993), Lecture Notes in Comput. Sci., vol. 673, Springer, Berlin, 1993, pp. 180–194.

[Kat80] Nicholas M. Katz, *Sommes exponentielles*, Astérisque, vol. 79, Société Mathématique de France, Paris, 1980, Course taught at the University of Paris, Orsay, Fall 1979, With a preface by Luc Illusie, Notes written by Gérard Laumon, With an English summary.

[Kat88a] ———, *Gauss sums, Kloosterman sums, and monodromy groups*, Annals of Mathematics Studies, vol. 116, Princeton University Press, Princeton, NJ, 1988.

[Kat88b] ———, *Travaux de Laumon*, no. 161-162, 1988, Séminaire Bourbaki, Vol. 1987/88, pp. Exp. No. 691, 4, 105–132 (1989).

[Kat90] ———, *Exponential sums and differential equations*, Annals of Mathematics Studies, vol. 124, Princeton University Press, Princeton, NJ, 1990.

[Kat94] ———, *Review of l-adic cohomology*, Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math., vol. 55, Amer. Math. Soc., Providence, RI, 1994, pp. 21–30.

[Kat01] ———, *L-functions and monodromy: four lectures on Weil II*, Adv. Math. **160** (2001), no. 1, 81–132.

[Kat05] ———, *Moments, monodromy, and perversity: a Diophantine perspective*, Annals of Mathematics Studies, vol. 159, Princeton University Press, Princeton, NJ, 2005.

[Kat07] ———, *G_2 and hypergeometric sheaves*, Finite Fields Appl. **13** (2007), no. 2, 175–223.

[Kat18] ———, *Rigid local systems on $\mathbb{A}^1$ with finite monodromy*, Mathematika **64** (2018), no. 3, 785–846, With an appendix by Pham Huu Tiep.

[KR20] Lars Kindler and Kay Rülling, *Introductory course on ℓ-adic sheaves and their ramification theory on curves*, Amplitudes, Hodge theory and ramification—from periods and motives to Feynman amplitudes, Clay Math. Proc., vol. 21, Amer. Math. Soc., Providence, RI, 2020, pp. 103–229.

[KRL19] Nicholas M. Katz and Antonio Rojas-León, *A rigid local system with monodromy group $2.J_2$*, Finite Fields Appl. **57** (2019), 276–286.

[KRLT20] Nicholas M. Katz, Antonio Rojas-León, and Pham Huu Tiep, *Rigid local systems with monodromy group the Conway group Co_3*, J. Number Theory **206** (2020), 1–23.

[KRLT23] ———, *Rigid local systems and sporadic simple groups*, Preprint available online at: `https://web.math.princeton.edu/~nmk/krlt26.pdf`, 2023, To appear in Memoirs of the AMS.

[KS99] Nicholas M. Katz and Peter Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications, vol. 45, American Mathematical Society, Providence, RI, 1999.

[KT21] Nicholas M. Katz and Pham Huu Tiep, *Exponential sums and total Weil representations of finite symplectic and unitary groups*, Proc. Lond. Math. Soc. (3) **122** (2021), no. 6, 745–807.

[KT23] ———, *Exponential sums, hypergeometric sheaves, and monodromy groups*, Preprint available online at: `https://web.math.princeton.edu/~nmk/kt18_141.pdf`, 2023.

[Kum52] Ernst E. Kummer, *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen*, J. Reine Angew. Math. **44** (1852), 93–146.

[Lan78] Serge Lang, *Relations de distributions et exemples classiques*, Séminaire Delange-Pisot-Poitou. Théorie des nombres **19** (1977-1978), no. 2 (fr), talk:40.

[Lau87] Gérard Laumon, *Transformation de Fourier, constantes d'équations fonctionnelles et conjecture de Weil*, Inst. Hautes Études Sci. Publ. Math. (1987), no. 65, 131–210.

[Len] Hendrik W. Lenstra, *Rijndael for algebraists*, Available online at: `https://math.berkeley.edu/~hwl/`.

[LN94] Rudolf Lidl and Harald Niederreiter, *Introduction to finite fields and their applications*, first ed., Cambridge University Press, Cambridge, 1994.

[Mil80] James S. Milne, *Étale cohomology*, Princeton Mathematical Series, No. 33, Princeton University Press, Princeton, N.J., 1980.

[MP13] Gary L. Mullen and Daniel Panario (eds.), *Handbook of finite fields*, Discrete Mathematics and its Applications, CRC Press, Boca Raton, FL, 2013.

[MS77] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland Mathematical Library, Vol. 16, North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977.

[Nag62] Masayoshi Nagata, *Imbedding of an abstract variety in a complete variety*, J. Math. Kyoto Univ. **2** (1962), 1–10.

[Ngo17] Bao Chau Ngo, *Perverse sheaves and fundamental lemmas*, Geometry of moduli spaces and representation theory, IAS/Park City Math. Ser., vol. 24, Amer. Math. Soc., Providence, RI, 2017, pp. 217–250.

[Nyb94] Kaisa Nyberg, *Differentially uniform mappings for cryptography*, Advances in cryptology—EUROCRYPT '93 (Lofthus, 1993), Lecture Notes in Comput. Sci., vol. 765, Springer, Berlin, 1994, pp. 55–64.

[PW72] W. Wesley Peterson and E. J. Weldon, Jr., *Error-correcting codes*, second ed., The M.I.T. Press, Cambridge, Mass.-London, 1972.

[RL19] Antonio Rojas-León, *Finite monodromy of some families of exponential sums*, J. Number Theory **197** (2019), 37–48.

[RL23a] ———, *An Effective Criterion for Finite Monodromy of ℓ-Adic Sheaves*, Vietnam J. Math. **51** (2023), no. 3, 703–713.

[RL23b] ———, *Equidistribution and independence of gauss sums*, 2023.

[SGA 1] *Revêtements étales et groupe fondamental (SGA 1)*, Documents Mathématiques (Paris), vol. 3, Société Mathématique de France, Paris, 2003, Séminaire de géométrie algébrique du Bois Marie 1960–61., Directed by A. Grothendieck, With two papers by M. Raynaud, Updated and annotated reprint of the 1971 original [Lecture Notes in Math., 224, Springer, Berlin].

[SGA 4_1] *Théorie des topos et cohomologie étale des schémas. Tome 1: Théorie des topos*, Lecture Notes in Mathematics, Vol. 269, Springer-Verlag, Berlin-New York, 1972, Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4), Dirigé par M. Artin, A. Grothendieck, et J. L. Verdier. Avec la collaboration de N. Bourbaki, P. Deligne et B. Saint-Donat.

[SGA 4_2] *Théorie des topos et cohomologie étale des schémas. Tome 2*, Lecture Notes in Mathematics, Vol. 270, Springer-Verlag, Berlin-New York, 1972, Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964

(SGA 4), Dirigé par M. Artin, A. Grothendieck et J. L. Verdier. Avec la collaboration de N. Bourbaki, P. Deligne et B. Saint-Donat.

[SGA 4_3] *Théorie des topos et cohomologie étale des schémas. Tome 3*, Lecture Notes in Mathematics, Vol. 305, Springer-Verlag, Berlin-New York, 1973, Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4), Dirigé par M. Artin, A. Grothendieck et J. L. Verdier. Avec la collaboration de P. Deligne et B. Saint-Donat.

[SGA 4½] Pierre Deligne, *Cohomologie étale*, Lecture Notes in Mathematics, vol. 569, Springer-Verlag, Berlin, 1977, Séminaire de géométrie algébrique du Bois-Marie SGA 4½.

[SGA 5] *Cohomologie l-adique et fonctions L*, Lecture Notes in Mathematics, Vol. 589, Springer-Verlag, Berlin-New York, 1977, Séminaire de Géometrie Algébrique du Bois-Marie 1965–1966 (SGA 5), Edité par Luc Illusie.

[Sma] Nigel P. Smart, *Cryptography: An introduction*, Available online at: `https://homes.esat.kuleuven.be/~nsmart/Crypto_Book/`.

[Stacks] The Stacks Project Authors, *Stacks Project*, `https://stacks.math.columbia.edu`, 2018.

[Š00] Ondrej Šuch, *Monodromy of Airy and Kloosterman sheaves*, Duke Math. J. **103** (2000), no. 3, 397–444.

[Was97] Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.

[Yam66] Koichi Yamamoto, *On a conjecture of Hasse concerning multiplicative relations of Gaussian sums*, J. Combinatorial Theory **1** (1966), 476–489.

[Yam75] ———, *The gap group of multiplicative relationships of Gaussian sums*, Symposia Mathematica, Vol. XV, Academic Press, London, 1975, Convegno di Strutture in Corpi Algebrici, INDAM, Rome, 1973,, pp. 427–440.