EXPONENTIAL SUMS OVER DEFINABLE SUBSETS OF FINITE FIELDS

E. KOWALSKI

Abstract. We prove some general estimates for exponential sums over subsets of finite fields which are definable in the language of rings. This generalizes both the classical exponential sum estimates over varieties over finite fields due to Weil, Deligne and others, and the result of Chatzidakis, van den Dries and Macintyre concerning the number of points of those definable sets. As a first application, there is no formula in the language of rings that defines for infinitely many primes an "interval" in $\mathbf{Z}/p\mathbf{Z}$ that is neither bounded nor with bounded complement.

1. Introduction

Exponential sums are ubiquitous in analytic number theory, in various shape and forms. A basic type is a sum

$$S_f(M,N) = \sum_{M\leqslant n<M+N} e(f(n)), \tag{1}$$

where $e(z) = e^{2i\pi z}$ and f is some real-valued function. These tend to arise naturally in any asymptotic counting problem, as ways to express the secondary terms after isolating a "main term" and the basic goal is to establish some form of cancellation, of the type

$$\sum_{M\leqslant n<M+N} e(f(n)) \ll N\theta(N)^{-1}, \tag{2}$$

where the saving $\theta(N)$ from the trivial bound N is a positive increasing function with $\theta(N)\to +\infty$ as $N\to+\infty$. Evidently, it must be the case that f varies "fast enough" for such an estimate to hold.

Various highly ingenious methods have been developed to deal with the distinct possible types of phase functions f; the names of Weyl, van der Corput and Vinogradov in particular are attached to the most classical ideas (see e.g. [IK, §8]). It was however discovered that this type of analytic questions could sometimes be attacked using highly involved algebraic tools: if the interval of summation is of the type $0\leqslant n<p$, where p is prime, and if $f(n)=g(n)/p$, where g is a polynomial or a rational function, the best general results come from an interpretation as an exponential sum over the finite field $\mathbf{Z}/p\mathbf{Z}$.

Indeed, one introduces the "companion" sums

$$S_\nu = \sum_{x\in\mathbf{F}_{p^\nu}} e\Big(\frac{\operatorname{Tr} g(x))}{p}\Big),$$

for $\nu\geqslant 1$, where $\mathbf{F}_{p^\nu}$ is a field with p^ν elements, $\operatorname{Tr}:\mathbf{F}_{p^\nu}\to\mathbf{F}_p=\mathbf{Z}/p\mathbf{Z}$ being the trace map. Although S_ν, $\nu\geqslant 2$, never (?) has any interpretation in analytic number theory, it is the properties of the generating function

$$Z(T)=\exp\Big(\sum_{\nu\geqslant 1}\frac{S_\nu}{\nu}T^\nu\Big)$$

which are fundamental in understanding the original sums. In this context, this was first recognized and developed by A. Weil, who proved for instance that for a fixed (non-constant)

2000 *Mathematics Subject Classification.* 11T23, 11L03 (Primary); 03C60 (Secondary).

Key words and phrases. Exponential sums, definable sets, finite fields, Riemann Hypothesis over finite fields.

function $g \in \mathbf{Z}[X]$ one has

$$S_\nu(p) \ll p^{\nu/2}$$

for all primes p and $\nu \geqslant 1$ (with possibly few well-understood exceptions), with an implied constant depending only on g. See e.g [IK, §11] for a description of the elementary approach of Stepanov and [IK, §11.11] for a first survey of the more advanced cohomological methods of Grothendieck, Deligne, Katz and others.

In terms of applications to analytic number theory, it is clear that the potential of the more advanced results has not yet been fully exploited; there are a number of reasons for this, not only the complexity of the algebraic geometry involved (although that is certainly a factor), but also the difficulty of bringing a natural problem to a position where the Riemann Hypothesis for varieties over finite fields can be applied successfully: the reader need only look at the proof of the Burgess estimate for short character sums (see e.g. [IK, 12.4]) to see what ingenuity may be required; also the comments in [IK, 11.12] explain how the question of uniformity in parameters and "flexibility" in the shape of the sums can be crucial matters.

In this paper, we describe a new general estimate for exponential sums over finite fields which combines quite efficiently the cohomological methods (as "black-box") and some results and techniques of logic to give estimates where the summation set in the finite field is much more general than the algebraic sets that are usually considered. We hope that this added flexibility will make it suitable for applications to analytic number theory; also the statement is, in itself, quite elementary with very few conditions, and this may also make it appealing to readers without a great experience in algebraic geometry (at the price of learning, or remembering, a few notions of logic...)

See Section 3 for the general statement, which is preceded by a section recalling the precise formulas permitted as summation conditions. As a sample result, for the very important case of a sum in one variable, one gets the following:

Theorem 1. *Let $\varphi(x)$ be a first-order formula in the language $(0, 1, +, -, \cdot)$ of rings.*[1] *For every ring A, let*

$$\varphi(A) = \{x \in A \mid \varphi(x) \text{ holds}\}.$$

Let f, $g \in \mathbf{Q}(X)$ be rational functions with f non-constant. Let $N \geqslant 1$ be the product of primes p such that f modulo p is constant. Then there exists a constant $C \geqslant 0$, depending only on φ and the degree of the numerator and denominator of f and g such that for any prime p and any multiplicative character χ modulo p we have

$$\Big| \sum_{\substack{x \in \varphi(\mathbf{Z}/p\mathbf{Z}) \\ f(x), g(x) \text{ defined}}} \chi(g(x)) e\Big(\frac{f(x)}{p}\Big) \Big| \leqslant C(p, N)^{1/2} \sqrt{p}. \tag{3}$$

Compared to the classical sums above, the point is that the summation condition can be quite complicated, involving arbitrary entanglements of quantifiers (in first-order predicates, i.e., applied to elements of the field). One may also wonder if in fact the bound is really non-trivial (what if the number of points is usually of size $p^{1/4}$, for instance?), but as proved in [CDM] and as we will explain again in detail below, the number of points of summation is either $\leqslant A$ or $\geqslant cp$, for some $A \geqslant 1$ and $c > 0$ depending only on the formula φ. And one should keep in mind that if this were applied to a problem of analytic number theory, whether this is efficient or not would most often be obvious from the final result anyway.

Notation. As already mentioned, we denote $e(z) = e^{2\pi i z}$. We denote by $\mathbf{F}_q$ a finite field with q elements and usually p is its characteristic. For a finite set X, $|X|$ denotes its cardinality. By $f \ll g$ for $x \in X$, or $f = O(g)$ for $x \in X$, where X is an arbitrary set on which f is defined, we mean synonymously that there exists a constant $C \geqslant 0$ such that $|f(x)| \leqslant Cg(x)$ for all $x \in X$. The "implied constant" is any admissible value of C. It may depend on the set X which is always specified or clear in context. For notation and conventions concerning logical

[1] We recall the precise definition in Section 2.

formulas, see the beginning of the next section. We use elementary scheme-theoretic language for our algebraic geometry (see e.g. [Ha, II]); in particular, an algebraic variety over a field F or over $\mathbf{Z}$ is simply a separated scheme of finite type over F or $\mathbf{Z}$, and in fact only affine schemes will occur (so separatedness is automatic); so a variety is not necessarily reduced or irreducible. We write either V_A or V/A to indicate that a scheme is defined over a ring A. (The choice of A is sometimes important to indicate precise dependency for constants that occur.)

Acknowledgment. I wish to thank the referee for a careful reading and for making a number of interesting remarks.

2. Definable sets

Since the paper involves a fairly unusual mixture of analytic number theory and logic (also algebraic geometry, but the latter is kept essentially inside the proofs), we start by recalling what are precisely the formulas which define the summation sets we will consider. Of course logicians can skip this section without loss, unless they wish to make sure that the author does not speak utter nonsense.

A *term* in the language $(0, 1, +, -, \cdot)$ of rings is simply a polynomial $f \in \mathbf{Z}[x_1, \ldots, x_n]$ with integer coefficients, where the x_i are variables; an *atomic formula* φ is a formula of the type $f = g$ where f and g are polynomials (possibly involving distinct sets of variables). Given an atomic formula φ, a ring A, and assignments of elements $x_i = a_i \in A$ to the variables involved, the formula $\varphi(a)$ with $a = (a_i)$ substituted for the variables is *satisfied* in A, denoted

$$A \models \varphi(a)$$

if the equality which "is" φ holds when the variables are given the values a_i.

Next the (first-order) *formulas* in the language of rings are built from atomic formulas by induction using the additional logical symbols $\neg$, $\wedge$, $\vee$, and quantifiers $\exists$, $\forall$: atomic formulas are formulas by definition and if φ and φ_i, $i \in I$, are formulas, with I finite, then

$$\neg\varphi_i \qquad \bigwedge_{i\in I} \varphi_i \qquad \bigvee_{i\in I} \varphi_i$$

are also formulas, and if x is any variable then

$$\exists x\ \varphi \quad \text{and} \quad \forall x\ \varphi$$

are also formulas. Implication $\rightarrow$ and equivalence $\leftrightarrow$ are defined as abbreviations:

$$\varphi_1 \rightarrow \varphi_2 \text{ means } (\neg\varphi_1) \vee \varphi_2,$$
$$\varphi_1 \leftrightarrow \varphi_2 \text{ means } (\varphi_1 \rightarrow \varphi_2) \wedge (\varphi_2 \rightarrow \varphi_1),$$

(and parenthesizing can be introduced for clarity).

In an obvious way, the relation $A \models \varphi(a)$ defined for an atomic formula is extended to any formula by induction using the usual meanings of the symbols: $\wedge$ as "and", $\vee$ as "or", $\neg$ as "not". The quantifiers are always extended to elements of A only (not to subsets, not to elements of other rings than A). For instance the torsion subgroup of invertible elements in A is *not* definable in the first-order language of rings since the exponent can not be bounded a priori.

Given a formula $\varphi(x, y)$, where $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_m)$ are (disjoint) tuples of variables, and given a ring A and $y \in A^m$, we put

$$\varphi(A, y) = \{x \in A^n \mid A \models \varphi(x, y)\}, \tag{4}$$

in other words, $\varphi(A, y)$ is the set of n-tuples in A which satisfy the formula φ for the given value y of the parameter. Such a set is called a *definable set* (with parameters); if $m = 0$ (no parameters), then the set is also called $\emptyset$-definable.

If φ is an atomic formula $f = g$, the assignment $A \mapsto \varphi(A)$ is simply the functor that associates its A-valued points $V(A)$ to the scheme $V = \mathrm{Spec}(\mathbf{Z}[X]/(f - g))$ over $\mathbf{Z}$ given by

the equation $f = g$. So in general definable sets can be seen as a (substantial) generalization of algebraic varieties.

For instance, the set of squares in A is $\emptyset$-definable by the formula $\exists y\ x = y^2$, but the assignment $A \mapsto \varphi(A)$ is not a functor (e.g. because an element can become a square after extension to a larger field, which can not happen to points of schemes). Here is more complicated example: for $d \geqslant 1$ an integer, the set of irreducible polynomials of degree $\leqslant d$ in $A[X]$, identified with a subset of A^{d+1} by the coefficients, is $\emptyset$-definable (for every j, $k \geqslant 1$ with $j + k \leqslant d$, write existential quantifiers on coefficients of two polynomials of degree j and k with product equal to the given one).

See e.g. [Ho, 1.3,2.1] or [FJ, 6.1] for more details (involving more general languages) and more examples.

A final notation: to define a formula $\varphi(x)$, we will sometimes write

$$\varphi(x) = \text{“}x \text{ satisfies such and such property”},$$

(and will either explain or leave to the reader to check that the property thus stated in informal manner can be written as a first-order formula in the language of rings), or

$$\varphi(x)\ :\ \psi_1(x)\dots$$

to indicate that the formula $\varphi(x)$ is defined to be the expression after “:”, which will usually be a combination of various bits and pieces; for instance

$$\varphi(x)\ :\ (\exists y\ x = y^2) \vee (\exists y\ x = y^3) \vee (\forall y\ \exists z\ y^2 + x = z^2).$$

3. Exponential sums over definable sets in finite fields

This section defines the exponential sums we want to consider. We generalize from the context described in the introduction by introducing formulas with parameters $\varphi(x, y)$ where $x = (x_1, \dots, x_n)$, $n \geqslant 1$, are the variables and $y = (y_1, \dots, y_m)$, $m \geqslant 0$, are the parameters. This formula is still assumed to be in the first-order language of rings. As in the previous section, we let

$$\varphi(A, y) = \{x \in A^n \mid A \models \varphi(x, y)\}$$

for any ring A and parameter $y \in A^m$.

We consider especially finite fields $\mathbf{F}_q$ with q elements. Assume that for all q in some subset of the powers of primes we have chosen an additive character

$$\psi\ :\ \mathbf{F}_q \to \mathbf{C}^\times$$

and a multiplicative character

$$\chi\ :\ \mathbf{F}_q^\times \to \mathbf{C}^\times$$

(which of course depend on q, although it is not indicated in the notation). We extend χ to $\mathbf{F}_q$ by putting $\chi(0) = 0$, except when χ is the trivial character, in which case $\chi(0) = 1$.

Let f_1, f_2, g_1, $g_2 \in \mathbf{Z}[X]$ be polynomials in $X = (X_1, \dots, X_n)$, with f_2 and g_2 non-zero, and let $f = f_1/f_2$, $g = g_1/g_2$ (as rational functions). We assume that for all the q under consideration the formula $\varphi(x, y)$ satisfies

$$\mathbf{F}_q \models (\varphi(x, y) \to (f_2(x)g_2(x) \neq 0)), \tag{5}$$

and if necessary, this can be achieved by replacing $\varphi(x, y)$ by the formula

$$\varphi(x, y) \wedge (\neg f_2(x) = 0) \wedge (\neg g_2(x) = 0),$$

which “restricts” to the points which are not poles of f and g. This may introduce a further dependency of the results below on f_2 and g_2, but that is of course not surprising, and it will be clear that such dependency is really only in terms of the degree of f_2 and g_2.

Now finally we introduce the following general exponential sums over a definable set:

$$S(y, \varphi, \mathbf{F}_q) = \sum_{x \in \varphi(\mathbf{F}_q, y)} \psi(f(x))\chi(g(x)), \tag{6}$$

for all q for which the data is defined.

These generalize the more classical exponential sums over the $\mathbf{F}_q$-points of an algebraic variety $V/\mathbf{Z}$, which corresponds to the case where the formula $\varphi(x,y)$ is the conjunction of the atomic formulas which "are" the equations of V. In that situation we also denote

$$S(y,V,\mathbf{F}_q)=\sum_{x\in V(\mathbf{F}_q)}\psi(f(x))\chi(g(x)). \tag{7}$$

The natural goal is to describe a non-trivial upper bound for $S(y,\varphi,\mathbf{F}_q)$ when possible, as explicit as possible in its dependencies. For applications to analytic number theory, it is natural to look primarily at the so-called "horizontal" case, i.e., when $\mathbf{F}_q=\mathbf{F}_p$ is the prime field, and our statements are skewed to this case (assuming for instance that p is large enough, instead of q large enough, for some condition to hold).

Here is a fairly simple example that follows easily from our results.

Theorem 2. *With data as described above, assume that the additive characters ψ are non-trivial. There exist constants $C\geqslant 0$ and $\eta>0$, depending only on the formula $\varphi(x,y)$ and the degrees of the polynomials f_1, f_2, g_1, g_2 such that for any prime p and any parameter $y\in\mathbf{F}_p^m$, we have*

$$\Big|\sum_{x\in\varphi(\mathbf{F}_p,y)}\psi(f(x))\chi(g(x))\Big|\leqslant Cp^{-1/2}\sum_{x\in\varphi(\mathbf{F}_p,y)}1$$

unless there exists $c\in\mathbf{F}_p$ such that

$$|\{x\in\varphi(\mathbf{F}_p,y)\ \mid\ f(x)=c\}|\geqslant\eta|\varphi(\mathbf{F}_p,y)|.$$

The result is stated in this manner in order to make quite clear what the saving is (i.e., about $p^{1/2}$) compared to the trivial estimate. We will also recall during the course of the proof the main theorem of [CDM] which gives the approximate value of the number of points of summation. The condition for the estimate to hold is sufficient but not necessary (see below for examples). It states intuitively that if there is no cancellation, then f must be constant on a subset of $\varphi(\mathbf{F}_p,y)$ which has "positive density".

This condition may seem difficult to check but in applications it should be the case that the "degenerate" cases are fairly obvious, and can be dealt with separately. We give an example in the Section 7.

This theorem will be derived from more precise "structural" results concerning the exponential sum and its companions, which are of independent interest and may be useful for deeper studies in some cases.

Before going into details, a very important remark is that we have *not* found a new source of cancellation in exponential sums: the saving will come by application of the Riemann Hypothesis for varieties over finite fields (Deligne's theorem). However, the point is that we have a very general result, with great flexibility, and with intrinsic uniformity in parameters, so Theorem 2 has the potential of being a very efficient "black-boxing" of Deligne's result. Certainly in tricky cases it might not be easy to perform the reduction to varieties over finite fields explicitly.

For one-variable sums, the exponent $1/2$ in Theorem 1 is well-known to be optimal, but for sums with $n\geqslant 2$ variables, it is natural to expect from general principles about exponential sums that much better bounds should hold for "generic" sums (the exponent should be $n/2$). It is not clear how to define a simple and interesting class of sums with $n\geqslant 2$ for which this principle holds.[2] One very important form of this principle, however, lies in the stratification theorems of Katz and Laumon (see [KL, FK]), which imply (among other things) that if one considers a *family* of "twisted" sums, with non-trivial ψ and $f(x)$ replaced by $f_0(x)+h\cdot x$,

[2]Even for "classical" sums, it often turns out that the statements obtained by algebraic geometers are insufficient for concrete applications in analytic number theory.

where $h \in \mathbf{Z}^n$ and $h \cdot x$ denotes the standard scalar product, then for all h except those in some hypersurface, there is optimal cancellation in

$$\sum_{x \in V(\mathbf{F}_q)} \psi(f_0(x) + h \cdot x)\chi(g(x)).$$

As pointed out by the referee, it is quite likely that it would be possible to obtain an analogue of this stratification theorem for exponential sums over definable subsets of finite fields. It seems, roughly, that two main difficulties arise: understanding the interaction between the tools of Katz-Laumon and the intersection-decomposition procedure (used in the proof of Proposition 9 below), and checking the uniformity of the constants occurring in [KL] with respect to the extra parameters that are required for the geometric analysis of definable sets. We hope to come back to such topics later.

Remark 3. We have not stated results with purely multiplicative sums. Although they can be analyzed by the method of Sections 5 and 6, this tends to reveal trickier aspects which make simple statements for a general summation set hard to state (in other words, it seems one needs a deeper understanding of the structure of $\varphi(\mathbf{F}_q, y)$). We will give a few examples in the next section.

4. Examples

We will now give a few simple examples of the exponential sums we have in mind, and make some general comments. We make forward references to the structural results of the next sections, as the examples illustrate various aspects involved.

Example 4. The simplest example of a formula defining a set which is not a variety is probably the formula

$$\varphi(x) \ : \ \exists y \ x = y^2$$

which characterizes the squares in a ring. Thus, if the characteristic p is odd, we have

$$|\varphi(\mathbf{F}_q)| = \frac{q+1}{2},$$

and since $x \mapsto x^2$ is two-to-one except at 0, for any complex numbers $\beta(x)$ defined for $x \in \mathbf{F}_q$ we have

$$\sum_{x \in \varphi(\mathbf{F}_q)} \beta(x) = \frac{\beta(0)}{2} + \frac{1}{2} \sum_{x \in \mathbf{F}_q} \beta(x^2).$$

If $\beta(x) = \psi(f(x))\chi(g(x))$ where ψ (resp. χ) is an additive (resp. multiplicative) character, and f, g two polynomials, the second sum is still of this type, but over the points in $\mathbf{F}_q$, so it can be analyzed in the standard way.

More generally, one can do similar things for any formula of the type

$$\exists y \ x = h(y)$$

where h is another polynomial, except that one must handle the various possibilities for the number of solutions y in $\mathbf{F}_q$ to the equation $h(y) = x$: this kind of step is very clear in the structure result (Theorem 7).

Example 5. We next show that multiplicative characters can involve rather more delicate issues: consider the formula $\varphi(x)$ in one variable

$$\exists y \, x^2 + 1 = y^2$$

and take $g(x) = x^2+1$ and χ the multiplicative character of order 2 for all finite fields, non-trivial if $p \neq 2$. Clearly

$$\sum_{x \in \varphi(\mathbf{F}_q)} \chi(g(x)) = \sum_{x \in \varphi(\mathbf{F}_q)} 1$$

so there is never cancellation. In this case, the reduction in Theorem 7 below applies with $K = 1$, $s = 0$, $r = 0$, $k = 1$, $\Phi_1(x, y) = \varphi(x)$ and $h_{1,1}(x, z) = x^2 - z^2 + 1$ (see (13)), $e = 2$, so

$V = V_1 = \mathbf{A}^1_{\mathbf{Z}}$, $W = W_{1,1}$ is the affine conic with equation $X^2 - Z^2 + 1 = 0$ and $\tau = \tau_{1,1} : W \to V$ is given by X. The function $g \circ \tau$ is, on W, equal to $X^2 + 1$, and so is the square of the function Z on the conic. This is quite obvious, but indicates that some knowledge of the structure of the definable sets is required to state a precise criterion for cancellation in a multiplicative character sum. Still, this knowledge need only be gained *once* and may then be applied for many different sums.

Another variant is the following: take the formula in two variables

$$\varphi(x, y) \ : \ \exists z \ (x^2 - y^2 + 1)^2 + z^2 = 0,$$

and consider as before the quadratic character sum over $\varphi(x, y)$ with $g(x, y) = y^2 - 1$.

So we introduce the affine variety W with this equation and the projection $W \to \mathbf{A}^2$. This variety is not absolutely irreducible: adjoining a square root ε of -1, it splits as

$$((X^2 - Y^2 + 1) - \varepsilon Z)((X^2 - Y^2 + 1) + \varepsilon Z) = 0.$$

Hence if -1 is a square in $\mathbf{F}_q$, there is always a value of z for each (x, y) and the sum is

$$\sum_{(x,y)\in\mathbf{F}_q} \chi(y^2 + 1) = q \sum_{y\in\mathbf{F}_q} \chi(y^2 + 1) \ll q^{3/2},$$

which gives some cancellation, while on the other hand if -1 is not a square in $\mathbf{F}_q$, the points of $W(\mathbf{F}_q)$ must have $z = 0$, hence $x^2 = y^2 - 1$ and the sum becomes

$$\sum_{\substack{x\in\mathbf{F}_q \\ x^2+1 \text{ is a square}}} \chi(x^2)$$

which is degenerate as in the previous case, although g is not the square of a function on $W_{\overline{\mathbf{F}}_q}$, but only on the intersection of its absolutely irreducible components.

Another amusing example is as follows: consider variables (a, b) and let $\varphi(a, b)$ be the formula

$$\forall x \ x^2 + ax + b \neq 0.$$

For a field F of characteristic $\neq 2$, we have $F \models \varphi(a, b)$ if and only if the discriminant $\Delta(a, b) = a^2 - 4b$ is not a square in F. Hence if we take ψ trivial, χ of order 2 and $g(a, b) = \Delta(a, b)$, the sum

$$\sum_{(a,b)\in\varphi(\mathbf{F}_q)} \chi_2(\Delta(a, b))$$

has no cancellation. This is only "trivial" if one knows about discriminants of quadratic polynomials, and one can guess that situations involving invariants of more complicated algebraic forms will lead to examples which are much less obvious.

Because of this and the lack of current application, we have not tried to give a cancellation criterion for multiplicative character sum in this paper, but we hope to investigate this problem further.

Example 6. Here is a challenging example: let $n \geqslant 1$ and consider the formula $\varphi(a)$, $a = (a_0, a_1, \dots, a_{n-1})$, which expresses that the polynomial

$$X^n + a_{n-1}X^{n-1} + \cdots + a_1X + 1 \tag{8}$$

is irreducible and $a_0a_1 \cdots a_{n-1} = 1$. Consider then the following exponential sum

$$K^*_{n,p} = \sum_{a\in\varphi(\mathbf{F}_p)} e\Big(\frac{a_0 + \cdots + a_{n-1}}{p}\Big)$$

which is thus a subsum of a hyper-Kloosterman $K_{n,p}$ sum in n variables (which only includes the condition $a_0 \cdots a_{n-1} = 1$ in the summation). Then we have

$$|K^*_{n,p}| \ll p^{n-1/2}, \tag{9}$$

where the implied constant depends on n. Compare this with Deligne's estimate ([D1, Sommes trig. §7])

$$|K_{n,p}| \leqslant (n+1)p^{n/2}.$$

To prove (9), it suffices, according to Theorem 2, to show that the function

$$f(a) = a_0 + \cdots + a_{n-1}$$

is not constant for a positive proportion of $a \in \varphi(\mathbf{F}_p)$. This follows from the following two facts: (1) a positive proportion of $a \in \mathbf{F}_p^n$ with $a_0 \cdots a_{n-1} = 1$ define an irreducible polynomial (8); (2) f is not constant on a positive proportion of $a \in \mathbf{F}_p^n$ with $a_0 \cdots a_{n-1} = 1$. Of these, (2) is clear (if one wishes, it is a consequence of Deligne's estimate for hyper-Kloosterman sums!), and (1) follows by interpreting the desired number as $1/n$ times the number of elements in $\mathbf{F}_{p^n}^\times$ which are of norm 1 and are of degree n over $\mathbf{F}_p$ (i.e. do not lie in a smaller field).

Here is a natural question: can the estimate for $K_{n,p}^*$ be made more precise? Is the exponent $n - 1/2$ optimal?

5. Geometric decomposition of exponential sums over definable sets

Given a formula $\varphi(x, y)$, we start by describing a "geometric" decomposition of the definable sets $\varphi(\mathbf{F}_q, y)$ and any sum over $\varphi(\mathbf{F}_q, y)$, following [CDM] with some more details. Then in the next section we will apply the sheaf-theoretic and cohomological methods to express the exponential sums in terms of eigenvalues of the Frobenius operator on suitable cohomology groups.

It will be noticed that the notation is somewhat involved, since a large number of parameters occur here and below. In the Appendix, we give a list of most of them.

Theorem 7. *Let $\varphi(x, y)$ be a first-order formula in the language of rings with variables $x = (x_1, \ldots, x_n)$ and parameters $y = (y_1, \ldots, y_m)$, $n \geqslant 0$, $m \geqslant 0$.*

There exist the following data, depending only on $\varphi(x, y)$:

(i) *Integers $K \geqslant 1$, $s \geqslant 0$, $e \geqslant 1$;*

(ii) *A prime power q_0;*

(iii) *For $\kappa \leqslant K$, formulas $\Phi_\kappa(x, x', y)$ with auxiliary parameters $x' = (x'_1, \ldots, x'_s)$;*

(iv) *For $\kappa \leqslant K$ and $i \leqslant e$, affine schemes $W_{\kappa,i}$ of finite type over $\mathbf{Z}$ with maps*

$$\pi_{\kappa,i} : W_{\kappa,i} \to \mathbf{A}_{\mathbf{Z}}^{s+m}, \quad \tau_{\kappa,i} : W_{\kappa,i} \to \mathbf{A}_{\mathbf{Z}}^{n};$$

with the following properties:

(1) *For every finite field $\mathbf{F}_q$ with $q \geqslant q_0$, there exists $x' \in \mathbf{F}_q^s$ such that*

$$\varphi(x, y) \leftrightarrow (\Phi_1(x, x', y) \vee \cdots \vee \Phi_K(x, x', y)) \tag{10}$$

for every $y \in \mathbf{F}_q^m$.

(2) *For every field F, every $(x', y) \in F^{s+m}$, the sets $\Phi_\kappa(F, x', y)$, $\kappa \leqslant K$, are disjoint.*

(3) *For all finite fields $\mathbf{F}_q$ with $q \geqslant q_0$ and $(x', y) \in \mathbf{F}_q^{s+m}$ with x' chosen so that (10) holds, we have*

$$x \in W_{\kappa,i}(\mathbf{F}_q) \text{ implies } \tau_{\kappa,i}(x) \in \Phi_\kappa(\mathbf{F}_q, x', y) \tag{11}$$

and at most e elements of $W_{\kappa,i}(\mathbf{F}_q)$ satisfy $\tau_{\kappa,i}(x) \in \Phi_\kappa(\mathbf{F}_q, x', y)$.

(4) *For all finite fields $\mathbf{F}_q$ with $q \geqslant q_0$ and $(x', y) \in \mathbf{F}_q^{s+m}$ with x' chosen so that (10) holds, and any complex numbers $\beta(x)$ for $x \in \varphi(\mathbf{F}_q, y)$, we have*

$$\sum_{x \in \Phi_\kappa(\mathbf{F}_q, x', y)} \beta(x) = \sum_{1 \leqslant i \leqslant e} \frac{(-1)^{i+1}}{i!} \sum_{\substack{x \in W_{\kappa,i}(\mathbf{F}_q) \\ \pi_{\kappa,i}(x) = (x', y)}} \beta(\tau_{\kappa,i}(x)). \tag{12}$$

Proof. We follow the reduction steps of [CDM, p. 123]. This provides us with the following data:

• Integers $K \geqslant 0$, $s \geqslant 0$, $r \geqslant 0$, $k \geqslant 0$, $e \geqslant 1$, and a prime power q_0;

• For each integer $\kappa \leqslant K$, polynomials $f_{\kappa,1}, \ldots, f_{\kappa,r} \in \mathbf{Z}[X, X', Y]$ where $X' = (X'_1, \ldots, X'_s)$ is an s-tuple of auxiliary parameters;

• For each integer $\kappa \leqslant K$, polynomials $h_{\kappa,j} \in \mathbf{Z}[X, X', Y, Z_j]$ for $1 \leqslant j \leqslant k$;

which depend only on the formula $\varphi(x, y)$ and have the following properties:

• For every finite field $\mathbf{F}_q$ with $q \geqslant q_0$, the formula $\varphi(x, y)$ is equivalent to the formula

$$\varphi'(x, y) = \Big(\Phi_1(x, x', y) \vee \Phi_2(x, x', y) \vee \cdots \vee \Phi_K(x, x', y)\Big)$$

where $\Phi_\kappa(x, x', y)$ is the formula

$$\Phi_\kappa(x, x', y) = \Big(f_{\kappa,1}(x, x', y) = 0 \wedge \cdots \wedge f_{\kappa,r}(x, x', y) = 0 \wedge (\exists z_1 \cdots \exists z_k \; h_{\kappa,1}(x, x', y, z_1) = 0 \wedge \cdots \wedge h_{\kappa,k}(x, x', y, z_k) = 0)\Big), \tag{13}$$

where $x' \in \mathbf{F}_q^s$ is some value of the auxiliary variables (see below for a short explanation).

• For any field F and parameters (x', y), the sets $\Phi_1(F, x', y), \ldots, \Phi_K(F, x', y)$ are disjoint in F^n;

• For each $\kappa \leqslant K$ and $(x', y) \in \mathbf{F}_q^{s+m}$, the number of $z = (z_1, \ldots, z_k) \in F^k$ such that $F \models \Psi_\kappa(x, x', y, z)$ is bounded by e, where $\Psi_\kappa(x, x', y, z)$ is the formula

$$\Psi_\kappa(x, x', y, z) = \Big(f_{\kappa,1}(x, x', y) = 0 \wedge \cdots \wedge f_{\kappa,r}(x, x', y) = 0 \wedge h_{\kappa,1}(x, x', y, z_1) = 0 \wedge \cdots \wedge h_{\kappa,k}(x, x', y, z_k) = 0\Big). \tag{14}$$

(Precisely, this summarizes the discussion on p. 123 of [CDM]: (13) is the conjunction of the formulas (1) of loc. cit., its precise form given in (3) in loc. cit.; the disjointness of the $\Phi_\kappa(\mathbf{F}_q, x', y)$ is stated after (2) in loc. cit.; the existence and property of e is given in (4) in loc. cit.)

Clearly, all this gives already the data of K, s, q_0 and the auxiliary formulas $\Phi_\kappa(x, x', y)$ such that (1) and (2) of the theorem hold. Before continuing to the second part, we explain the occurrence of the auxiliary parameters x': they correspond to extra symbols c_i in the language of enriched fields discussed in [CDM, §2]. For any field F, those constants are interpreted as coefficients of some irreducible monic polynomial in $F[T]$. To see the relevance with definable sets $\varphi(\mathbf{F}_q, y)$, notice that for instance the universal formula

$$\forall t \; a_0 + a_1 t + a_2 t^2 \neq 0 \tag{15}$$

can be restated, for a finite field $\mathbf{F}_q$, by the existential formula stating that $a_0 + a_1 t + a_2 t^2$ splits in linear factors over the field $\mathbf{F}_{q^2}$, with no root in $\mathbf{F}_q$. This can be expressed in terms of the coefficients of an irreducible monic polynomial $f_2 = c_0 + c_1 T + T^2$ by factorizing $a_2(T - y_1)(T - y_2)$ and then expressing $\mathbf{F}_q$-rationally the equality

$$a_0 + a_1 t + a_2 t^2 = a_2(t - y_1)(t - y_2) \text{ with } y_1, \; y_2 \in \mathbf{F}_{q^2} - \mathbf{F}_q$$

in the basis $(1, \alpha_2)$, where α_2 is a root of f_2.[3] It is also useful to mention that it is in constructing Φ_κ that the restriction to large enough finite fields is introduced, this coming from a result of van den Dries, based on the Lang-Weil estimate and some model theory (see [CDM, 2.4]).

Now, to simplify notation for the proof of (3) and (4) of the theorem, which concern the formulas $\Phi_\kappa(x, x', y)$ individually, we drop the subscript κ and we incorporate the new parameters x' into y (so that $s + m$ is now denoted m).

Let V denote the zero set of the polynomials $f_1, \ldots, f_r \in \mathbf{Z}[X, Y]$, seen as a closed subscheme of $\mathbf{A}_{\mathbf{Z}}^{n+m}$. We have the projection $V \to \mathbf{A}_{\mathbf{Z}}^m$ given by the parameter y, and we denote by V_y the

[3] Alternately, (15) can be approached by Galois theory; this would lead to the use of the Galois stratification method described in [FHJ].

fibers. Let W denote the common zero set in $\mathbf{A}_{\mathbf{Z}}^{n+m+k}$ of the polynomials f_i and the polynomials $h_1, \ldots, h_k$. Denote by $\pi : W \to V$ the obvious projection.

For $j \geqslant 1$, denote

$$W_y(\mathbf{F}_q)_j = \{x \in \Phi(\mathbf{F}_q, y) \mid |\pi^{-1}(x, y) \cap W(\mathbf{F}_q)| = j\}.$$

Let now $\beta(x)$ be arbitrary complex numbers defined for $x \in \Phi(\mathbf{F}_q, y)$. By (13), for any $x \in \Phi(\mathbf{F}_q, y)$, we have $(x, y) \in V(\mathbf{F}_q)$ and $\pi^{-1}(x, y) \cap W(\mathbf{F}_q) \neq \emptyset$, so that

$$\sum_{x \in \Phi(\mathbf{F}_q, y)} \beta(x) = \sum_{j \geqslant 1} \sum_{x \in W_y(\mathbf{F}_q)_j} \beta(x)$$

and from the defining property of e, this reduces to

$$\sum_{x \in \Phi(\mathbf{F}_q, y)} \beta(x) = \sum_{1 \leqslant j \leqslant e} \sum_{x \in W_y(\mathbf{F}_q)_j} \beta(x). \tag{16}$$

To deal with the fact that the fibers of π do not necessarily all have the same cardinality, we now use the same combinatorial procedure as in [CDM, p. 124], although we make the result more explicit.

For $1 \leqslant j \leqslant e$, let W_j denote the intersection in $\mathbf{A}_{\mathbf{Z}}^{n+m+jk}$ of the j-fold fiber product of W over V with the open subscheme U_j consisting of points $(x, y, z_1, \ldots, z_j)$ where all the z_i are distinct k-tuples, i.e. in point terms we have

$$W_j(A) = U_j(A) \cap \{(x, y, z_1, \ldots, z_j) \mid (x, y, z_i) \in W(A) \text{ for } 1 \leqslant i \leqslant k\}$$

for any ring A (this corresponds to the formula $\Psi_j(X, Y, Z^1, \ldots, Z^j)$ of loc. cit.) On W_j we have the maps

$$\pi_j \begin{cases} W_j \to \mathbf{A}_{\mathbf{Z}}^m \\ (x, y, z_1, \ldots, z_j) \mapsto y \end{cases} \qquad \text{and} \qquad \tau_j \begin{cases} W_j \to \mathbf{A}_{\mathbf{Z}}^n \\ (x, y, z_1 \ldots, z_j) \mapsto x; \end{cases}$$

we will denote by $W_{j,y}$ the fiber of π_j over y. All this (with the omitted dependency on κ) gives the data (iv) of the Theorem and (3) is satisfied by construction.

Next we claim that the following combinatorial formulas hold: denoting

$$(i)_j = i(i-1)\cdots(i-j+1) = j!\binom{i}{j},$$

we have for $1 \leqslant j \leqslant e$

$$\sum_{i=j}^{e} (i)_j \sum_{x \in W_y(\mathbf{F}_q)_i} \beta(x) = \sum_{(x, y, z_1, \ldots, z_j) \in W_j(\mathbf{F}_q)} \beta(x) = \sum_{x \in W_{j,y}(\mathbf{F}_q)} \beta(\tau_j(x)). \tag{17}$$

Indeed, for each $x \in W_y(\mathbf{F}_q)_i$, the set $\pi^{-1}(x, y) \cap W(\mathbf{F}_q)$ has i elements and for $j \leqslant i \leqslant e$, any ordered subset of length j naturally gives a point of $W_{j,y}(\mathbf{F}_q)$. All of these points are distinct, and of course there are precisely $(i)_j$ of them.

Now we use the following elementary lemma (presumably standard in combinatorics):

Lemma 8. *Let $e \geqslant 1$. Let x_j, y_i be complex numbers defined for $1 \leqslant i, j \leqslant e$, such that*

$$\sum_{i=j}^{e} (i)_j x_i = y_j, \tag{18}$$

for $1 \leqslant j \leqslant e$. Then we have

$$\sum_{1 \leqslant i \leqslant e} x_i = \sum_{1 \leqslant j \leqslant e} \frac{(-1)^{j+1}}{j!} y_j.$$

Proof. To see this, solve first the triangular system (18) using $(i)_j = i!/(i-j)!$ to get

$$x_i = \sum_{j=i}^{e} \frac{(-1)^{i+j}}{i!(j-i)!} y_j,$$

(as easily checked using the binomial theorem), and then sum over i to get

$$\begin{aligned}\sum_{1\leqslant i\leqslant e} x_i &= \sum_{1\leqslant i\leqslant e}\sum_{i\leqslant j\leqslant e} \frac{(-1)^{i+j}}{i!(j-i)!} y_j = \sum_{1\leqslant j\leqslant e} (-1)^j y_j \Big(\sum_{1\leqslant i\leqslant j} \frac{(-1)^i}{i!(j-i)!}\Big) \\ &= \sum_{1\leqslant j\leqslant e} \frac{(-1)^{j+1}}{j!} y_j\end{aligned}$$

by the binomial theorem again. □

Applied to

$$x_i = \sum_{x\in W_y(\mathbf{F}_q)_i} \beta(x), \quad y_j = \sum_{x\in W_{j,y}(\mathbf{F}_q)} \beta(\tau_j(x)),$$

we get by (16) and (17) that

$$\sum_{x\in\Phi(\mathbf{F}_q,y)} \beta(x) = \sum_{1\leqslant j\leqslant e} \frac{(-1)^{j+1}}{j!} \Big(\sum_{x\in W_{j,y}(\mathbf{F}_q)} \beta(\tau_j(x))\Big),$$

which is the final conclusion (12), taking account the change of notation made before. □

6. Estimates arising from the decomposition of definable sets

For the second part of the reduction of exponential sums over definable sets, recall that given a prime power q and an integer $k \geqslant 0$, a complex number $\alpha \in \mathbf{C}$ is a q-Weil number of weight k if α is an algebraic integer, and any Galois-conjugate α' of α (i.e., any root of the minimal polynomial $P \in \mathbf{Z}[T]$ of α) satisfies $|\alpha'| = q^{k/2}$. It will be convenient to call a *signed* q-Weil number a pair $(\pm 1, \alpha)$ of a sign and a q-Weil number. Usually we just write α and the sign is denoted $\varepsilon(\alpha)$. When a Weil number is written down explicitly as a complex number and claimed to be a signed Weil number, this means that the sign is $+1$. For instance, this applies to $\alpha = q^w$, a q-Weil number of weight $2w$.

To compute and estimate the exponential sums $S(y, \varphi, \mathbf{F}_q)$, we will apply the Grothendieck-Lefschetz trace formula and the Riemann Hypothesis over finite fields proved by Deligne to the auxiliary varieties $\pi_{\kappa,i}^{-1}(x', y) \subset W_{\kappa,i}$ arising from Theorem 7. This naturally falls in two steps: first, we examine the number of points of summation, then we analyze when an exponential sum exhibits cancellation.

We will first perform both steps for a single $W_{\kappa,i,y}$, i.e., for a "classical" exponential sum (in logical terms, one corresponding to a positive quantifier free formula). The only subtlety is that we do not know if $W_{\kappa,i,y}$ is absolutely irreducible or not (the case usually treated in the literature), which affects the precise counting of points and the non-triviality of the estimates.

Proposition 9. *Let $W \subset \mathbf{A}_{\mathbf{Z}}^{n+m}$ be an affine subscheme, let q be a power of the prime p, (ψ, χ, f, g) data defining the exponential sum*

$$S(y, W, \mathbf{F}_q) = \sum_{(x,y)\in W(\mathbf{F}_q)} \psi(f(x))\chi(g(x))$$

for $y \in \mathbf{F}_q^m$ over W.

(i) *There exist an integer $B_1 \geqslant 0$, depending only on W, and for all $y \in \mathbf{F}_q^m$, there exists an integer $\delta(y)$, $0 \leqslant \delta(y) \leqslant n$, and signed q-Weil numbers $\alpha_j(y)$ for $1 \leqslant j \leqslant \beta \leqslant B_1$, where β may depend on y, such that*

$$w(\alpha_j(y)) \leqslant 2n, \quad \max w(\alpha_j(y)) = 2\delta(y), \text{ and } \alpha_j(y) = q^{\delta(y)} \text{ if } w(\alpha_j(y)) = 2\delta(y),$$

and

$$\sum_{(x,y)\in W(\mathbf{F}_q)} 1 = \sum_{1\leqslant j\leqslant\beta} \varepsilon(\alpha_j(y))\alpha_j(y). \tag{19}$$

(ii) *There exist an integer $B_2 \geqslant 0$, depending only on W and the degree of f and g, and for all $y \in \mathbf{F}_q^m$ there exist q-Weil numbers $\beta_j(y)$, for $1 \leqslant j \leqslant \gamma \leqslant B_2$, where γ may depend on y, such that*

$$w(\beta_j(y)) \leqslant 2\delta(y) \text{ for all } j,$$

and

$$\sum_{(x,y)\in W(\mathbf{F}_q)} \psi(f(x))\chi(g(x)) = \sum_{1\leqslant j\leqslant\gamma} \varepsilon(\beta_j(y))\beta_j(y). \tag{20}$$

Moreover, there exists $\eta > 0$, depending only on $W/\mathbf{Z}$ such that if p is large enough, $p \geqslant p_0$ where p_0 depends only on W and the degrees of f_1 and f_2, we have $w(\beta_j(y)) < 2\delta(y)$ for all j unless either ψ is trivial or there exists $c \in \mathbf{F}_q$ such that

$$\sum_{\substack{(x,y)\in W(\mathbf{F}_q)\\ f(x)=c}} 1 \geqslant \eta \sum_{(x,y)\in W(\mathbf{F}_q)} 1. \tag{21}$$

Proof. We denote by W_y the fiber over y of $W/\mathbf{F}_q$. For reasons that will become clear soon, we first replace W_y by the subscheme of $\mathbf{A}^{n+m}_{\mathbf{F}_q}$ obtained by performing the intersection-decomposition process (described in [CDM, §1]), i.e., we replace W_y by V_y such that

(i) $W_y(\mathbf{F}_q) = V_y(\mathbf{F}_q)$;

(ii) The absolutely irreducible components of V_y are defined over $\mathbf{F}_q$.

It follows from [CDM, Pr. 1.7] that V_y can be defined as the zero set of N polynomials in $\mathbf{F}_q[X_1, \dots, X_n]$ of degree $\leqslant E$, and moreover V has at most I absolutely irreducible components, where N, E and I depend only on $W/\mathbf{Z}$ (in particular are independent of y).

By (i), we have for all $y \in \mathbf{F}_q^m$

$$S(y, W, \mathbf{F}_q) = S(V_y, \mathbf{F}_q).$$

Note it is possible that $V_y = \emptyset$ (for instance for $X^2 + 1 = 0$ if -1 is not a square in $\mathbf{F}_q$); if that is the case, we can take $B_1 = B_2 = 0$, and we put $\delta(y) = 0$. So assume V_y is not empty.

Fix a prime $\ell \neq p$, where p is the characteristic of $\mathbf{F}_q$. The formalism of the Lang torsor (see e.g. [D1, Sommes trig. 1.4], [K2, 4.3] or the sketch in [IK, 11.11]) provides us with the lisse $\overline{\mathbf{Q}}_\ell$-adic sheaf of rank 1

$$\mathcal{L} = \mathcal{L}_{\psi(f)} \otimes \mathcal{L}_{\chi(g)}$$

on V_y (which depends on p, ψ, χ, f and g) such that the local trace of a geometric Frobenius element $\mathrm{Fr}_{x,\mathbf{F}_q}$ at a rational point $x \in V_y(\mathbf{F}_q)$ is given by

$$\mathrm{Tr}(\mathrm{Fr}_{x,\mathbf{F}_q} \mid \mathcal{L}) = \psi(f(x))\chi(g(x)) \tag{22}$$

and therefore

$$S(V_y, \mathbf{F}_q) = \sum_{x\in V_y(\mathbf{F}_q)} \mathrm{Tr}(\mathrm{Fr}_{x,\mathbf{F}_q} \mid \mathcal{L}).$$

Let $\overline{V}_y$ denote the base change of V_y to the algebraic closure of $\mathbf{F}_q$. The Grothendieck-Lefschetz trace formula (see e.g. [D1, Rapport]) gives the cohomological expression

$$S(V_y, \mathbf{F}_q) = \sum_{i\geqslant 0} (-1)^i \,\mathrm{Tr}(\mathrm{Fr} \mid H^i_c(\overline{V}_y, \mathcal{L}))$$

where H^i_c are the compactly supported ℓ-adic cohomology groups with coefficient in the sheaf $\mathcal{L}$ and Fr denotes the geometric Frobenius operator over $\mathbf{F}_q$ which acts naturally on those finite dimensional $\overline{\mathbf{Q}}_\ell$-vector spaces. Of course, the sum is in fact finite, and more precisely the space H^i_c vanishes for $i > 2\delta(y)$, where $\delta(y)$ is the maximal dimension of an irreducible component of $\overline{V}_y$. Because V_y is a subset of affine n space, we have $\delta(y) \leqslant n$.

By Deligne's fundamental result (his far-reaching generalization of the Riemann Hypothesis), since the sheaf $\mathcal{L}$ is punctually pure of weight 0 (its local traces being roots of unity), the eigenvalues of Fr acting on $H_c^i(\overline{V}_y, \mathcal{L})$ are q-Weil numbers of weight $\leqslant i$ (see [D2, Th. 3.3.1]).

Thus we obtain (19) in the case $\mathcal{L} = \mathbf{Q}_\ell$ with the family of q-Weil numbers $\alpha_j(y)$ being the eigenvalues (indexed by j, and with multiplicity) of the geometric Frobenius on all the cohomology groups $H_c^i(\overline{V}_y, \mathbf{Q}_\ell)$ for $i \leqslant 2\delta(y)$, those becoming "signed" by the factor $(-1)^i$.

In this case still, for $i = 2\delta(y)$, let $\overline{U}_y$ be an irreducible component of $\overline{V}_y$; by (ii) above, $\overline{U}_y = U_y \times \overline{\mathbf{F}}_q$ for some irreducible $U/\mathbf{F}_q$. By Poincaré duality (see [D1, Sommes trig., Rem. 1.18d]), we have

$$H_c^{2\delta(y)}(\overline{U}_y, \mathbf{Q}_\ell) = (\mathbf{Q}_\ell)_{\pi_1(\overline{U}'_y, \overline{\eta})}(-2\delta(y)) = (\mathbf{Q}_\ell)(-2\delta(y))$$

where $U'_y \subset U_y$ is a smooth, dense open subscheme of U_y, and $\pi_1(\overline{U}'_y, \overline{\eta})$ is the geometric fundamental group of $\overline{V}_y$ with respect to some geometric point $\overline{\eta}$. This precisely means that $H_c^{2\delta(y)}$ is of dimension 1 and the geometric Frobenius Fr of $\mathbf{F}_q$ acts by multiplication by $q^{\delta(y)}$. (The only delicate point is that if we use an irreducible component not defined over $\mathbf{F}_q$, it is the Frobenius Fr^ν of a field on which it is defined that acts by multiplication by $q^{\nu\delta(y)}$).

Since moreover it is known that $H_c^{2\delta(y)}(\overline{V}_y, \mathbf{Q}_\ell)$ is the direct sum of the corresponding cohomology of the irreducible components, it follows that all eigenvalues of weight $2\delta(y)$ are equal to $q^{2\delta(y)}$ and that the multiplicity is the number of irreducible components of dimension $2\delta(y)$ (see [D1, Sommes trig., Remarques 1.18 (d)]. This gives all the properties of α_j stated in the first part of Proposition 9.

Similarly in the general case we obtain (20) with the analogue eigenvalues for $H_c^i(\overline{V}_y, \mathcal{L})$, and the weight of these is $\leqslant 2\delta(y)$ as stated.

A crucial point that remains to be checked is that the total number of eigenvalues (i.e. the numbers denoted β and γ in the statement of the Proposition) is indeed bounded by B_1 or B_2 depending only on W and (in the case of B_2) on the degrees of f_1, f_2, g_1, g_2.

This is precisely given by a very useful result of Katz [K1, Th. 12], because we can embed $\overline{V}_y$ as a closed subscheme of an affine space $\mathbf{A}^M_{\overline{\mathbf{F}}_q}$ where M depends only on $W/\mathbf{Z}$, using equations of degree and number bounded only in terms of $W/\mathbf{Z}$ (by the uniformity of the intersection-decomposition procedure described at the beginning).[4]

Now we analyze when we can get some cancellation in (20). We assume that ψ is non-trivial and that $\max w(\beta_j(y)) = 2\delta(y)$ and will show then that (21) holds for some c.

The hypothesis implies that for some irreducible component $\overline{U}_y = U_y \times \overline{\mathbf{F}}_q$ of $\overline{V}_y$, the cohomology group $H_c^{2\delta(y)}(\overline{U}_y, \mathcal{L})$ does not vanish (since all H_c^i with $i > 2\delta(y)$ do vanish and those with $i < 2\delta(y)$ yield Weil numbers with smaller weight).

If need be, we replace U_y without changing notation by a smooth non-empty open subscheme. Since $\mathcal{L}$ restricted to U_y is a lisse sheaf on a smooth connected scheme, we have by Poincaré duality (as before) the co-invariant formula

$$H_c^{2\delta(y)}(\overline{U}_y, \mathcal{L}) = (\mathcal{L}_\eta)_{\pi_1(\overline{U}_y, \eta)}(-2\delta(y)) \tag{23}$$

for any geometric point η of $\overline{U}_y$, $\mathcal{L}_\eta$ being the fiber of $\mathcal{L}$ at η. Since $\mathcal{L}$ is of rank 1 and the cohomology does not vanish, we must therefore have

$$(\mathcal{L}_\eta)_{\pi_1(\overline{U}_y, \eta)}(-2\delta(y)) = \mathcal{L}_\eta(-2\delta(y)),$$

i.e., the sheaf $\mathcal{L}$ is geometrically trivial. From the exact sequence

$$1 \to \pi_1(\overline{U}_y, \eta) \to \pi_1(U_y, \eta) \to \mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q) \to 1,$$

and (23), it follows that $\mathcal{L}$ on U_y "is" a character of $\pi_1(U_y, \eta)$ which comes from a character of $\mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)$. This means in particular that the local trace of $\mathcal{L}$ at the geometric Frobenius of a

[4] It may seem surprising, but it is indeed true that B_2 is independent of the order of the multiplicative character χ.

point of $U_y(\mathbf{F}_q)$ is constant i.e. (by (22)), for all $x, x_0 \in U_y(\mathbf{F}_q)$ we have

$$\psi(f(x))\chi(g(x)) = \psi(f(x_0))\chi(g(x_0)).$$

Taking the D-th power (where D is the order of χ) yields the equality

$$\psi(D(f(x) - f(x_0))) = 1. \tag{24}$$

We can write $\psi(x) = e(\mathrm{Tr}(ax)/p)$ for some $a \in \mathbf{F}_q^\times$, since ψ is assumed non-trivial. Then (24) and the injectivity of $x \mapsto e(x/p)$ on $\mathbf{F}_p$ mean that for all $x \in U_y(\mathbf{F}_q)$, the element $aDf(x)$ is in a coset of the kernel of the trace from $\mathbf{F}_q$ to $\mathbf{F}_p$. Such a coset has cardinality $p^{-1}|\mathbf{F}_q|$, but on the other hand if f is non-constant on U_y, and if q is large enough, there are at least $q/\max(\deg(f_1), \deg(f_2))$ elements of the form $aDf(x)$ in $\mathbf{F}_q$. (Note $D \equiv 1 \pmod p$.)

So under the hypothesis that $w(y) = 2\delta(y)$, we see that if p is large enough (depending on W and the degrees of f_1 and f_2) it must be the case that $f|\overline{U}_y$ is constant. Since the number $\mu(y)$ of irreducible components of V_y of dimension $\delta(y)$ is bounded in terms of $W/\mathbf{Z}$ only, the standard counting

$$|W_y(\mathbf{F}_q)| = \mu(y)q^{\delta(y)} + O(q^{\delta(y)-1/2})$$

(with absolute constant depending only on $W/\mathbf{Z}$) coming from (19) and its analogue

$$|U_y(\mathbf{F}_q)| = q^{\delta(y)} + O(q^{\delta(y)-1/2})$$

show that (21) holds for c the constant value of f on $U_y(\mathbf{F}_q)$, p large enough in terms of $W/\mathbf{Z}$. (We could also have argued more geometrically using the triviality of the Artin-Schreier covering associated to $\mathcal{L}$, as in [D1, p. 24, last §]). □

Remark 10. There is presumably a cohomological interpretation of the decomposition-intersection process, which means essentially a general analysis of the cohomology of $W/\mathbf{F}_q$ with coefficient (at least) in a sheaf of the type $\mathcal{L}$ above, in the case where W is not absolutely irreducible, explaining how the trace formula boils down to that of the variety obtained by the process. However the author has not found such a result in the literature.

A drawback of using this procedure is that the Weil numbers involved are not uniquely determined by the exponential sum $S(y, W, \mathbf{F}_q)$ and its companions

$$S_\nu(y, W, \mathbf{F}_q) = \sum_{(x,y)\in W(\mathbf{F}_{q^\nu})} \psi(\mathrm{Tr}\, f(x))\chi(Ng(x)) \tag{25}$$

(where Tr and N are the norms from $\mathbf{F}_{q^\nu}$ or $\mathbf{F}_{q^\nu}^\times$ to $\mathbf{F}_q$), rather they are uniquely determined by the sequence of sums

$$S_\nu(V_y, \mathbf{F}_{q^\nu}) = \sum_{x\in V_y(\mathbf{F}_{q^\nu})} \psi(\mathrm{Tr}\, f(x))\chi(Ng(x)) = \sum_{1\leqslant j\leqslant \gamma} \varepsilon(\beta_j(y))\beta_j(y)^\nu$$

for $\nu \geqslant 1$, in the sense that the multiplicity (with signs taken into account)

$$\sum_{\beta_j(y)=\alpha} \varepsilon(\beta_j(y))$$

of any q-Weil number α is determined by $(S_\nu(V_y, \mathbf{F}_q))$. However, those sums for $\nu \geqslant 2$ are not necessarily related to the original sum $S(y, W, \mathbf{F}_q)$.

One can ignore all this, in a sense, and apply the Grothendieck-Lefschetz trace formula and Deligne's Theorem to W_y directly. But then the computation of the eigenvalues for the top-dimensional cohomology is not valid unless $\dim W_y/\mathbf{F}_q = \delta(y)$; note that this will often be the case for a concrete $W/\mathbf{Z}$ (e.g. if $W/\mathbf{Z}$ is generically absolutely irreducible), but in our applications to definable sets, the auxiliary varieties are not so well controlled, especially as they depend on the value of the auxiliary parameters x'.

We come back to a general formula $\varphi(x, y)$ and start with the special case $f = 0$, $g = 1$, $\psi = 1$, $\chi = 1$ that counts the points of the definable sets.

Theorem 11. *Let $\varphi(x,y)$ be a first-order formula in the language of rings and let K and e be given by Theorem 7 for φ. There exists an integer $B_1 \geqslant 0$, depending only on φ, with the following property: for all q large enough and all $y \in \mathbf{F}_q^m$, there exist signed q-Weil numbers*

$$\alpha_{\kappa,i,1}(y), \dots, \alpha_{\kappa,i,\beta}(y), \text{ with } 1 \leqslant \kappa \leqslant K, \quad 1 \leqslant i \leqslant e,$$

with $\beta \leqslant B_1$, β possibly depending on y, such that

$$w(\alpha_{\kappa,i,j}(y)) \leqslant 2n, \quad \max w(\alpha_{\kappa,i,j}(y)) = 2\delta(y) \text{ is even},$$
$$\alpha_{\kappa,i,j}(y) = q^{\delta(y)} \text{ if } w(\alpha_{\kappa,i,j}(y)) = 2\delta(y),$$

and we have

$$|\varphi(\mathbf{F}_q, y)| = \sum_{1\leqslant\kappa\leqslant K} \sum_{1\leqslant i\leqslant e} \frac{(-1)^{i+1}}{i!} \sum_{1\leqslant j\leqslant\beta} \varepsilon(\alpha_{\kappa,i,j}(y))\alpha_{\kappa,i,j}(y). \tag{26}$$

Finally, if $\varphi(\mathbf{F}_q, y)$ is not empty, the multiplicity "up to sign" of $\alpha = q^{2\delta(y)}$ is strictly positive, i.e.

$$\mu(y) = \sum_{\substack{\kappa,\ i,\ j \\ \alpha_{\kappa,i,j}(y)=q^{2\delta(y)}}} \frac{(-1)^{i+1}\varepsilon(\alpha_{\kappa,i,j}(y))}{i!} > 0$$

We thus recover the main theorem of [CDM].

Corollary 12 (Chatzidakis-van den Dries-Macintyre)**.** (1) *For all finite fields $\mathbf{F}_q$ and $y \in \mathbf{F}_q^m$, we have*

$$|\varphi(\mathbf{F}_q, y)| = \mu(y)q^{\delta(y)} + O(q^{\delta(y)-1/2})$$

where

$$\mu(y) = \sum_{\substack{\kappa,i,j \\ w(\alpha_{\kappa,i,j}(y))=2\delta(y)}} \frac{(-1)^{i+1}}{i!} \in \mathbf{Q}$$

is > 0 unless $\varphi(\mathbf{F}_q, y) = \emptyset$, and the implied constant depends only on φ.

(2) *There exist only finitely many pairs (d,μ) with $d \geqslant 0$ and $\mu \in \mathbf{Q}$ which arise as $(\delta(y), \mu(y))$ for some finite field $\mathbf{F}_q$ and $y \in \mathbf{F}_q^m$.*

(3) *For each pair (d,μ), $d \geqslant 0$ an integer and $\mu \in \mathbf{Q}$, that can arise as $(\delta(y), \mu(y))$, there exists a formula $\mathcal{C}_{d,\mu,\varphi}$ in the language of rings, depending only on d, μ and φ, such that for any finite field $\mathbf{F}_q$, we have $\mathbf{F}_q \models \mathcal{C}_{d,\mu,\varphi}$ if and only if $(\delta(y), \mu(y)) = (d,\mu)$.*

Proof. (1) For q large enough, this is obvious from (26) (with $\nu = 1$) and the stated properties of the weights of the $\alpha_{\kappa,i,j}(y)$, recalling that the sign $\varepsilon(q^{2\delta(y)})$ is $+1$ by convention; in fact we get

$$\left| |\varphi(\mathbf{F}_q, y)| - \mu(y)q^{\delta(y)} \right| \leqslant 3KB_1 q^{\delta(y)-1/2}$$

for $q \geqslant q_0$ large enough so that (26) applies.

Replacing the constant $3KB_1$ by $\max(3KB_1, C)$ where $C \geqslant 0$ satisfies

$$\left| |\varphi(\mathbf{F}_q, y)| - \mu(y)q^{\delta(y)} \right| \leqslant Cq^{\delta(y)-1/2}$$

for $q \leqslant q_0$, we obtain the result for all q.

(2) This is clear since we have the trivial bound $|\varphi(\mathbf{F}_q, y)| \leqslant q^n$ for all n which gives $\delta(y) \leqslant n$, and because there are at most 2^{K+e+B_1} choices of subsets of summation of indices (κ, i, j) that can occur in defining $\mu(y)$.

(3) This is proved in [CDM, Prop. 3.8] (and can be guessed from the proof of Theorem 7 and Proposition 9). □

We refer to [CDM, 4.9,4.10] for intrinsic interpretations of the "dimension" $\delta(y)$ and the "measure" $\mu(y)$ in the context of pseudo-finite fields.

We can now come back to the general exponential sums (6) as we are in a position to compare the estimates obtained with the number of points of summation.

Theorem 13. *Let $(f_1, g_1, f_2, g_2, \{\psi\}, \{\chi\})$ be the data defining a family of exponential sums* (6) *over the definable sets $\varphi(\mathbf{F}_q, y)$.*

(1) *There exists an integer $B_2 \geqslant 0$, depending only on φ and the degrees of f_1, g_1, f_2, g_2, with the following property: for all q large enough and all $y \in \mathbf{F}_q^m$, there exist signed q-Weil numbers*

$$\alpha_{\kappa,i,1}(y), \dots, \alpha_{\kappa,i,\beta}(y), \text{ with } 1 \leqslant \kappa \leqslant K, \quad 1 \leqslant i \leqslant e,$$

for $\beta \leqslant B_2$, β depending possibly on y, such that

$$w(\alpha_{\kappa,i,j}(y)) \leqslant 2\delta(y), \text{ for all } \kappa,\ i,\ j$$

and

$$S(y, \varphi, \mathbf{F}_q) = \sum_{1\leqslant\kappa\leqslant K} \sum_{1\leqslant i\leqslant e} \frac{(-1)^{i+1}}{i!} \sum_{1\leqslant j\leqslant\beta} \varepsilon(\alpha_{\kappa,i,j}(y))\alpha_{\kappa,i,j}(y), \tag{27}$$

hence

$$|S(y, \varphi, \mathbf{F}_q)| \leqslant 3KB_2 q^{w(y)/2} = 3K_2 B q^{\delta(y)-\gamma(y)/2}.$$

(2) *Let*

$$w(y) = \max_{\kappa,i,j} w(\alpha_{\kappa,i,j}(y)) \leqslant 2\delta(y),$$

denote the maximal weight of the Weil numbers occurring in this decomposition, and $\gamma(y) = 2\delta(y) - w(y) \geqslant 0$.

There exists $\eta > 0$ depending only on $\varphi(x, y)$ such that for p is large enough, depending only on $\varphi(x, y)$ and the degrees of f_1 and f_2, we have $w(y) < 2\delta(y)$, i.e., $\gamma(y) > 0$, unless ψ is trivial or there exists some $c \in \mathbf{F}_q$ with

$$\sum_{\substack{x\in\varphi(\mathbf{F}_q,y)\\ f(x)=c}} 1 \geqslant \eta \sum_{x\in\varphi(\mathbf{F}_q,y)} 1.$$

Remark 14. (1) We emphasize that in part (2), we must have p large enough, and not only q. This is necessary even for classical sums, since if we fix the additive characters by defining ψ on $\mathbf{F}_{p^\nu}$ as $e(\mathrm{Tr}(x)/p)$, we have $\psi(x^p - x) = 1$ for all $x \in \mathbf{F}_{p^\nu}$, so that for a polynomial f congruent modulo p to a polynomial of the form $g(x)^p - g(x)$, we have

$$\sum_{x\in\mathbf{F}_{p^\nu}} \psi(f(x)) = p^\nu$$

for all $\nu \geqslant 1$. And of course, such congruences can a priori hold for a large number of distinct primes. So our statement only provides a criterion for cancellation in the "horizontal" direction $p \to +\infty$ which is of most interest in analytic number theory.

(2) Note that of course it is only when $\gamma(y) > 0$ that this has any interest. The condition stated to ensure this does not sound particularly convenient, but that is partly because of the generality allowed. Essentially, for additive character sums, it says that there is some cancellation in $S(y, \varphi, \mathbf{F}_q)$, unless it turns out that f is constant for a positive proportion of the points of summation. This is a generic property; one may say that it corresponds to $\varphi(\mathbf{F}_q, y)$ being "transverse" in some sense to the level sets of f. In concrete applications, it should be clearer how to check this condition.

Proof of Theorem 11 and Theorem 13. By (12) with $\beta(x) = \psi(f(x))\chi(g(x))$, we are reduced to the sums over the $\mathbf{F}_q$-rational points of the fibers of $\pi_{\kappa,i} : W_{\kappa,i} \to \mathbf{A}^n$, which are algebraic varieties. We consider each in turn, assuming $q \geqslant q_0$ as in Theorem 7 and always consider that a choice of the auxiliary parameters x' has been performed, which we incorporate into y for clarity. In any case we apply Proposition 9 to each $W_{\kappa,i}$ (with y replaced by (x', y)) in turn; since at most eK such varieties occur, and both e and K are determined by φ only, the total number of Weil numbers that will occur is bounded in terms of φ (for the counting problem) or φ and the degrees of the functions f and g in the general case.

The maximal weight is the maximal value of the $2\delta_{\kappa,i}(y)$ of Proposition 9 applied to $W_{\kappa,i}$. Denoting it $2\delta(y)$ it follows that each of the Weil number occurring with this weight is in fact equal to $q^{\delta(y)}$.

The remainder of the statement of Theorem 11 is clear except maybe that in Theorem 11 the multiplicity

$$\mu(y) = \sum_{\substack{\kappa,i,j \\ w(\alpha_{\kappa,i,j}(y))=2\delta(y)}} \sum \sum \frac{(-1)^{i+1}}{i!}$$

is > 0 if the set $\varphi(\mathbf{F}_q, y)$ is not empty. But otherwise the number of elements of $\varphi(\mathbf{F}_q, y)$ would be $\ll q^{\delta(y)-1/2}$, with implied constant depending on φ only, while, for any κ, i such that $\delta_{\kappa,i}(y) = \delta(y)$, the number of $x \in W_{\kappa,i,y}(\mathbf{F}_q)$ is at least $\frac{1}{2}q^{\delta(y)}$ if q is large enough (in terms of φ only), and the images $\tau_{\kappa,i}(x)$ yield at least $\frac{1}{e}|W_{\kappa,i,y}(\mathbf{F}_q)|$ elements of $\varphi(x, y)$ (see (11) and the property of e following, or look back at the proof of Theorem 7). Hence we do get the result stated in Theorem 11 for all q large enough.

There remains to examine the condition stated in Theorem 13 for the exponential sum to have maximal weight $w(y) < \delta(y)$. For this, assume $w(y) = \delta(y)$. If ψ is non trivial, then (21) must hold for some κ, i (with $\eta > 0$ depending only on $\varphi(x, y)$) with $\delta_{\kappa,i}(y) = \delta(y)$, i.e., with

$$|W_{\kappa,i,y}(\mathbf{F}_q)| \geqslant \eta_1 |\varphi(\mathbf{F}_q, y)|$$

where again $\eta_1 > 0$ depends only on $\varphi(x, y)$. This gives part (2) of Theorem 13. □

We state finally the following corollary:

Corollary 15. *Let $(f_1, g_1, f_2, g_2, \{\psi\}, \{\chi\})$ be the data defining a family of exponential sums (6) over the definable sets $\varphi(\mathbf{F}_q, y)$, and let $\gamma(y)$ be as in the previous statement. There exists $\eta > 0$ depending only on $\varphi(x, y)$ such that for ψ non-trivial we have*

$$S(y, \varphi, \mathbf{F}_p) \ll p^{\delta(y)-1/2}$$

for all primes p and all $y \in \mathbf{F}_p^m$ for which there does not exist $c \in \mathbf{F}_p$ such that

$$\sum_{\substack{x \in \varphi(\mathbf{F}_p, y) \\ f(x)=c}} 1 \geqslant \eta \sum_{x \in \varphi(\mathbf{F}_p, y)} 1.$$

The implied constant depends only on $\varphi(x, y)$ and the degrees of f_1, f_2, g_1, g_2.

Proof. This is immediate after enlarging if necessary the constant arising from estimating the exponential sum using (27) and $\gamma(y) > 0$ for p large enough under the condition stated. □

The sample statements given in the previous sections are special cases of this corollary. In Theorem 1 (with one variable, no parameter, $\psi(x) = e(x/p)$ non trivial), either $\delta(y) = 0$ in which case (3) is trivial, or $\delta(y) = 1$, and if f is a non-constant rational function modulo p, it can not be constant on a set in $\mathbf{Z}/p\mathbf{Z}$ containing $\gg p$ points. If f is constant modulo p, the estimate is again trivial as $p \mid N$ in that case.

Theorem 2 on the other hand is just a rephrasing of the corollary.

Remark 16. The referee has pointed out that it is likely that Corollary 15 itself could be proved without invoking the cohomological formalism or the deep results of Deligne, relying only on the Lang-Weil method (which is what [CDM] depends on). Indeed, for sums over varieties (without parameters), this is done by Deligne [D1, Sommes trig., Prop. 3.8] by reducing to the case of curves, and the latter may be treated by the more elementary method of Weil (for curves which may be singular or not geometrically connected, some analysis of the desingularization morphism would be required, in particular with respect to uniformity in terms of parameters; at least for point counting, this has been done explicitly, e.g. by Aubry and Perret [AP]).

Analytic number theorists (in particular) may find such a proof preferable to the one above which uses the full strength of Deligne's results. Certainly, it gives a valid indication of the

true mathematical depth of Corollary 15 in itself. However, exponential sums are often a tool for further studies and it is much better for this purpose to have stronger structural results available than provided by the Lang-Weil method. They will probably be necessary for further investigations with the aim of obtaining more cancellation, or when sums involving higher-rank sheaves appear (e.g. for families of Kloosterman sums, as discussed by Katz [K2]).

Remark 17. The reduction theorem and the subsequent expansions of exponential sums in terms of Weil numbers suggest an intriguing question: how intrinsic are those decompositions? Can one define some kind of cohomology theory for certain sheaves on definable sets over finite fields in such a way as to obtain formulas like (27) as consequences of a trace formula operating directly at that level? Since it seems that a condition $q \geqslant q_0$ is necessary, this may be better dealt with at the level of pseudo-finite fields. We hope to come back to such foundational issues.

Finally, the author (at least) can't help wondering if this introduction of some ideas of logic and model theory might not be one clue to the hypothetical theory of "exponential sums over $\mathbf{Z}$" that Katz has written about, for instance, in [K3].

More down to earth, one may hope that exponential sums estimates for non-trivial characters could be useful in other areas, noting for instance that Corollary 12 of Chatzidakis, van den Dries and Macintyre has had applications in model theory (but the author doesn't understand those) and, in remarkable work of Hrushovski and Pillay [HP], in the study of algebraic groups over finite fields (in particular the behavior of the reduction modulo p of a group defined over $\mathbf{Z}$ for large p). The referee also mentioned recent applications in logic of estimates for algebraic exponential sums due to I. Tomašić [T].

7. Applications: definable intervals

We come back to general exponential sums (1), still with $f(n) = g(n)/p$ for some prime p, but now over a short interval:

$$S_{p,\vartheta}(g) = \sum_{0<n\leqslant N} e^{2\pi i g(n)/p} \text{ where } N = p^{\vartheta}$$

for some $\vartheta \in]0,1[$, the inequality $\vartheta < 1$ being characteristic of a "short" interval.

As long as $\vartheta > \frac{1}{2}$, a well-known technique of Fourier completion (see e.g. [IK, 12.2]) leads to complete sums (i.e., with $\vartheta = 1$), for which the results of algebraic geometry can often by applied, giving a bound of size roughly $\sqrt{p}(\log p)$, so an estimate for $S_{p,\vartheta}(g)$ with saving $\theta(N) = N^{1-1/(2\vartheta)} \to +\infty$ (see (2)).

However, very few cases have been handled when $\vartheta \leqslant \frac{1}{2}$. Since the most successful high-level approach to exponential sums in general has been the insertion of a given sum in a sort of "family",[5] of sometimes seemingly unrelated sums, and then exploitation of properties of the family as a whole to derive individual results, one may hope to do so by analogy with the case of complete sums over finite fields by extending $S_{p,\vartheta}(g)$ in some way to all finite fields $\mathbf{F}_q$.

So the following question is of interest: can one "lift" the short intervals $0 \leqslant x < p^{\vartheta}$ to subsets of $\mathbf{F}_{p^\nu}$ in such a way that the corresponding companion sums to $S_p(g)$ have a sufficiently rich structure to become more accessible?

There are of course many ways to envision such a lifting, but the most optimistic version is: are short intervals definable by a uniform formula $\varphi(x)$ in one variable in the language of rings?

More generally, let $\varphi(x)$ be such a formula. The question is: when is it the case that $\varphi(\mathbf{F}_p)$ is an *interval* for almost all p, i.e., when is it the case that for all but finitely many p there exist integers $a_p \leqslant b_p$ for which

$$\varphi(\mathbf{F}_p) = \{x \,(\mathrm{mod}\, p) \mid x \equiv i \,(\mathrm{mod}\, p) \text{ for some integer } i,\ a_p \leqslant i \leqslant b_p\}.$$

Of course, given a fixed interval $I = \{n, n+1, \dots, n+m\}$, $n \geqslant 0$, the formula

$$\varphi(x) \,:\, (x-n)\cdot(x-(n+1))\cdots(x-(m+n)) = 0$$

[5] Not only for sums over finite fields: the strategy of the standard methods of Weyl, van der Corput and Vinogradov can also be understood in this manner.

is such that $\varphi(\mathbf{F}_p)$ coincides with the reduction of I modulo p for all $p > m$. So of course similarly the reduction of the interval $\{n, n+1, \dots, p-1\}$ of length $p-n$ is defined by

$$\varphi(x) \,:\, x \cdot (x-1) \cdot (x-(n-1)) \neq 0.$$

We can easily use the tools of the previous sections to show that those are essentially the only possibilities.

Proposition 18. *Let $\varphi(x)$ be a formula in one variable in the language of rings. If neither $\varphi(\mathbf{F}_p)$ nor $\neg\varphi(\mathbf{F}_p)$ are bounded for all primes, there are only finitely many primes such that $\varphi(\mathbf{F}_p)$ is the reduction modulo p of an interval.*

Proof of Proposition 18. By the Main Theorem of [CDM] (or Theorem 11) applied to φ and $\neg\varphi$, there are constants $A \geqslant 1$, $C \geqslant 0$ and finitely many rationals $\mu_i \in]0,1[$, such that for each prime p either

$$|\varphi(\mathbf{F}_p)| \leqslant A \text{ or } |\neg\varphi(\mathbf{F}_p)| \leqslant A$$

or

$$\Big||\varphi(\mathbf{F}_p)| - \mu_i p\Big| \leqslant C\sqrt{p}.$$

for some i. If p runs over a subsequence of primes (tending to $+\infty$) for which $\varphi(\mathbf{F}_p)$ is an interval, and is unbounded, the finiteness of the set of μ_i shows that for some i a further subsequence exists for which $\varphi(\mathbf{F}_p)$ is an interval of length $|\varphi(\mathbf{F}_p)| \sim \mu_i p$. We will show this is impossible.

For this we observe first that by Theorem 1 we have

$$\sum_{x\in\varphi(\mathbf{F}_p)} e\Big(\frac{x}{p}\Big) \ll \sqrt{p}, \tag{28}$$

for all primes, the implied constant depending only on φ.

Let now p be such that $\varphi(\mathbf{F}_p)$ is an interval, say $\varphi(\mathbf{F}_p) = \{m_p, \dots, m_p + n_p - 1\}$. Summing a geometric progression gives

$$\Big|\sum_{x\in\varphi(\mathbf{F}_p)} e\Big(\frac{x}{p}\Big)\Big| = \left|e\Big(\frac{m_p}{p}\Big)\frac{1-e\Big(\frac{n_p}{p}\Big)}{1-e\Big(\frac{1}{p}\Big)}\right| = \left|\frac{\sin\frac{\pi n_p}{p}}{\sin\frac{\pi}{p}}\right|.$$

For the given hypothetical subsequence $p \to +\infty$, we have $n_p = |\varphi(\mathbf{F}_p)| \sim \mu_i p$, so the numerator converges to $\sin\pi\mu_i \neq 0$ (since $\mu_i \notin \{0,1\}$). On the other hand the denominator is equivalent to π/p, hence we find that

$$\Big|\sum_{x\in\varphi(\mathbf{F}_p)} e\Big(\frac{x}{p}\Big)\Big| \sim \pi|\sin\pi\mu_i|p, \tag{29}$$

which contradicts (28). This concludes the proof. □

Remark 19. Theorem 1 shows more generally that as $p \to +\infty$ along any sequence with $|\varphi(\mathbf{F}_p)|$ unbounded, we have

$$\lim_{p\to+\infty} \frac{1}{|\varphi(\mathbf{F}_p)|} \sum_{x\in\varphi(\mathbf{F}_p)} e\Big(\frac{hx}{p}\Big) = 0,$$

for any fixed integer $h \neq 0$.

Hence, using Weyl's equidistribution criterion, it follows that the fractional parts $\{\frac{x}{p}\}$ for $x \in \varphi(\mathbf{F}_p)$ become equidistributed in $\mathbf{R}/\mathbf{Z}$ for Lebesgue measure as p runs over primes with $|\varphi(\mathbf{F}_p)| \to +\infty$, i.e., for every continuous function $f : \mathbf{R}/\mathbf{Z} \to \mathbf{C}$, one has

$$\lim_{p\to+\infty} \frac{1}{|\varphi(\mathbf{F}_p)|} \sum_{x\in\varphi(\mathbf{F}_p)} f\Big(\frac{x}{p}\Big) = \int_{\mathbf{R}/\mathbf{Z}} f(\theta)d\theta.$$

Note that such a result (in stronger forms, see [FK]) is well-known for algebraic sets (i.e., formulas without quantifiers). Clearly this can be extended to formulas in more than one

variable: for a formula $\varphi(x)$ in n variables, and any sequence of primes p for which $\varphi(\mathbf{F}_p)$ is unbounded, either the sets

$$\tilde{\varphi}(\mathbf{F}_p) = \{(\tfrac{x_1}{p}, \dots, \tfrac{x_n}{p}) \in [0,1]^n \mid x = (x_1, \dots, x_n) \in \varphi(\mathbf{F}_p)\}$$

become equidistributed in $[0,1]^n$ as $p \to +\infty$ (with respect to Lebesgue measure), or there exists a non-trivial linear form $h(x) = \sum a_i x_i \in \mathbf{Z}[X]$ such that for infinitely many p, a positive proportion of elements of $\varphi(\mathbf{F}_p)$ lie in an affine hyperplane $h(x) = c$: for some $\eta > 0$ we have

$$|\{x \in \varphi(\mathbf{F}_p) \mid h(x) = c\}| \geqslant \eta |\varphi(\mathbf{F}_p)|,$$

for a subsequence of the primes considered. This follows immediately from Corollary 15 and the Weyl equidistribution criterion.

Also, the proposition extends immediately to general arithmetic progressions : if $\varphi(x)$ is a formula with one variable in the language of rings, then $\varphi(\mathbf{F}_p)$ can be for infinitely many primes of the form

$$A_{a,q,k} = \{a, a+q, \dots, a+n_p q\} \pmod p$$

for some integers $a \geqslant 1$, q (which may depend on p), with $p \nmid q$, only if either $\varphi(\mathbf{F}_p)$ or its complement is bounded for all p (the case of the complement can only occur for $q = 1$ of course). Indeed, one need only compute the exponential sum

$$\sum_{x \in A_{a,q,k}} e\Big(\frac{\bar{q}x}{p}\Big)$$

(where $\bar{q}$ is the inverse of q modulo p), to obtain an analogue of (29).

Appendix: notation index

For the reader's convenience, here is a list of the notation that occur in the reduction theorem and the decomposition theorem for exponential sums, with a brief explanation of their meaning.

n	:	Number $\geqslant 0$ of variables in $\varphi(x,y)$
m	:	Number $\geqslant 0$ of parameters in $\varphi(x,y)$
K	:	Theorem 7 (integer $\geqslant 1$, number of disjunctions expressing φ)
s	:	Theorem 7 (integer $\geqslant 0$, number of auxiliary parameters needed)
x'	:	Value or variables for the auxiliary parameters
κ	:	Index running from 1 to K
Φ_κ	:	Formulas in the disjunction expressing φ
k	:	Proof of Theorem 7 (integer $\geqslant 0$, number of existential terms in Φ_κ)
r	:	Proof of Theorem 7 (integer $\geqslant 0$, number of terms in formulas Φ_κ)
$f_{\kappa,\cdot}$	:	Terms occurring in Φ_κ
$h_{\kappa,\cdot}$	:	Terms occurring in existential form in Φ_κ
Ψ_κ	:	Proof of Theorem 7 (auxiliary quantifier free formulas)
q_0, p_0	:	Generically, value of q or p so that a statement holds for $q \geqslant q_0$ or $p \geqslant p_0$
e	:	Theorem 7 (integer $\geqslant 1$, maximal number of pre-images for a given $x \in \varphi(\mathbf{F}_q, y)$)
i, j	:	Indices running from 1 to e
$W_{\kappa,i}$	:	Affine schemes projecting "to φ"
$\pi_{\kappa,i}$	:	Projection from $W_{\kappa,i}$ to space of parameters
$\tau_{\kappa,i}$	:	Projection from $W_{\kappa,i}$ to definable sets
$\varepsilon(\alpha)$	:	Paragraph before Proposition 9 ("sign" of a Weil number)
B_1	:	Theorem 11 (maximal number of Weil numbers for the counting function)
B_2	:	Theorem 13 (maximal number of Weil numbers for exponential sum)
β	:	Theorems 11 and 13 (number of Weil numbers occurring for given parameter y)
j	:	Theorems 11 and 13 (index running from 1 to β)
$\alpha_{\kappa,i,j}(y)$	:	Theorems 11 and 13 (Weil numbers giving exponential sum)
$\delta(y)$	:	Theorem 11 (maximal weight of Weil numbers in counting points)
$\mu(y)$	:	Theorem 11 (density of point counting)
$w(y)$	:	Theorem 13 (maximal weight of Weil numbers in exponential sum)
$\gamma(y)$	:	Theorem 13 (gain in bound for exponential sum)

References

[AP] Y. Aubry and M. Perret: *A Weil theorem for singular curves*, in Arithmetic, geometry and coding theory (Luminy, 1993), 1–7, de Gruyter, Berlin, 1996.

[CDM] Z. Chatzidakis, L. van den Dries and A. Macintyre: *Definable sets over finite fields*, J. Reine angew. Math. 427 (1992), 107–135

[D1] P. Deligne: *Cohomologie étale*, S.G.A $4\frac{1}{2}$, L.N.M 569, Springer Verlag (1977).

[D2] P. Deligne: *La conjecture de Weil, II*, Publ. Math. IHÉS 52 (1980), 137–252.

[FHJ] M. Fried, D. Haran and M. Jarden: *Effective counting of the points of definable sets over finite fields*, Israel J. of Math. 85 (1994), 103–133.

[FJ] M. Fried and M. Jarden: *Field arithmetic*, Ergebnisse der Math. und ihrer Grenzgebiete, 3 Folge, vol. 11, Springer Verlag (1986).

[FK] É. Fouvry and N. Katz: *A general stratification theorem for exponential sums, and applications*, J. Reine angew. Math. 540 (2001), 115–166.

[Ha] R. Hartshorne: *Algebraic geometry*, Grad. Texts in Math. 52, Springer-Verlag (1977).

[Ho] W. Hodges: *A shorter model theory*, Cambridge University Press (1997).

[HP] E. Hrushovski and A. Pillay: *Definable subgroups of algebraic groups over finite fields*, J. Reine angew. Math 462 (1995), 69–91.

[IK] H. Iwaniec and E. Kowalski: *Analytic Number Theory*, A.M.S Colloq. Publ. 53, A.M.S (2004).

[K1] N. Katz: *Sums of Betti numbers in arbitrary characteristic*, Finite Fields Appl. 7 (2001), no. 1, 29–44.

[K2] N. Katz: *Gauss sums, Kloosterman sums and monodromy*, Annals of Math. Studies, 116, Princeton Univ. Press, 1988.

[K3] N. Katz: *Exponential sums over finite fields and differential equations over the complex numbers: some interactions*, Bull. A.M.S 23 (1990), 269–309.

[KL] N. Katz and G. Laumon: *Transformation de Fourier et majoration de sommes exponentielles*, Publ. Math. I.H.É.S 62 (1985), 145–202.

[T] I. Tomašić: *Exponential sums in pseudofinite fields and applications*, Illinois J. Math. 48 (2004), no. 4, 1235–1257.

Université Bordeaux I - I.M.B. - UMR 5251, 351, cours de la Libération, 33405 Talence Cedex, France

E-mail address: emmanuel.kowalski@math.u-bordeaux1.fr