SHIFTED VARIETIES AND DISCRETE NEIGHBORHOODS AROUND VARIETIES

JOACHIM VON ZUR GATHEN[1], GUILLERMO MATERA[2,3,4]

Abstract. In the area of symbolic-numerical computation within computer algebra, an interesting question is how "close" a random input is to the "critical" ones. Examples are the singular matrices in linear algebra or the polynomials with multiple roots for Newton's root-finding method. Bounds, sometimes very precise, are known for the volumes over $\mathbb{R}$ or $\mathbb{C}$ of such neighborhoods of the varieties of "critical" inputs; see the references below.

This paper deals with the discrete version of this question: over a finite field, how many points lie in a certain type of neighborhood around a given variety? A trivial upper bound on this number is given by the product (size of the variety) · (size of a neighborhood of a point). It turns out that this bound is usually asymptotically tight, in particular for the singular matrices, polynomials with multiple roots, and pairs of non-coprime polynomials.

The interesting question then is: for which varieties does this bound not hold? We show that these are precisely those that admit a shift, that is, where one absolutely irreducible component is a shift (translation by a fixed nonzero point) of another such component. Furthermore, the shift-invariant absolutely irreducible varieties are characterized as being cylinders over some base variety.

Computationally, determining whether a given variety is shift-invariant turns out to be intractable, namely NP-hard even in simple cases.

1. Introduction

In computer algebra, the area of symbolic-numerical computation has gained a lot of attention in the past decades. One question here is how "close" an input is to a set of "critical" instances. Iterative numerical methods may not work on specific "critical" (or "ill-posed") inputs, and may work badly on inputs "close" to these critical ones. Sometimes this is described by *condition numbers*, large values of which indicate closeness to criticality. For some tasks of linear algebra, the singular (square) matrices are critical and the condition number is essentially

Date: October 14, 2020.

Key words and phrases. Finite fields, polynomial systems, neighborhoods around varieties, neighborhoods of varieties.

GM is partially supported by the grants PIP CONICET 11220130100598 and PIO CONICET-UNGS 14420140100027.

1/|determinant|. In the Newton method for finding roots of (univariate) polynomials, inputs with multiple roots are critical, and one might consider 1/|discriminant| as a condition number. A well-studied issue, starting with Schönhage (1985) and Hribernig and Stetter (1997), is the *approximate gcd* of a pair of univariate polynomials: how close is a given polynomial to the true gcd of a pair of non-coprime polynomials, with 1/|resultant| as a condition number. Such condition numbers indicate the accuracy of solutions and the number of iterations until convergence.

Much work about this question has focussed on individual inputs. A more global question is: what is the probability for a uniformly random input (say, a random matrix) to be ϵ-close to some critical (that is, singular) one?

The general question of the measure (over $\mathbb{R}$ or $\mathbb{C}$) of such ϵ-neighborhoods (or ϵ-tubes, tubular neighborhoods) of varieties is first considered in Hotelling (1939) and Weyl (1939). In Smale's (1981) work on the efficiency of Newton's method, the size of ϵ-neighborhoods around polynomials with multiple roots plays a major role. Renegar (1987) extends this to solving general complex polynomial systems. Demmel (1988) provides upper and lower bounds on the size of such neighborhoods of varieties, and in particular, for singular matrices and for polynomials with multiple roots, over $\mathbb{R}$ and $\mathbb{C}$. Beltrán and Pardo (2007) generalize and improve these findings. The most precise result for matrices is the exact determination by Edelman (1988, 1992) of the distribution function of the condition number. Von zur Gathen & Matera (2017) present upper and lower bounds on the size of ϵ-neighborhoods of the variety of decomposable univariate polynomials over $\mathbb{R}$ and $\mathbb{C}$.

Such results may be viewed as continuous analogs of the corresponding counting problem over finite fields, replacing the probability for a uniformly random input being "in" by being "close to" the variety in question.

The present paper turns this question around by determining the asymptotic size of *discrete neighborhoods* of varieties over a finite field. This might be called *discretizing a continuous version of a discrete problem.* It turns out that this size is usually asymptotically close to a trivial upper bound. Interestingly, the exceptions can be characterized as *shifted varieties.* Alas, the computational problem of determining whether a given variety belongs to this class is intractable for growing input size. This holds already for the simple case of a linear hyperplane and neighborhoods consisting of three points.

In more detail, we start with an odd prime p, the field $\mathbb{F}_p = \{-(p-1)/2, \ldots, (p-1)/2\}$ with p elements considered as a subset of the integers $\mathbb{Z}$ with arithmetic modulo p, positive integers n and h with $h < p/2$, the ∞-norm $||a|| = \max_{1 \leq i \leq n} |a_i|$ for $a = (a_1, \ldots, a_n) \in \mathbb{F}_p^n$ and the ball $U_h = \{a \in \mathbb{F}_p^n : ||a|| \le h\}$ of radius h and with $\#U_h = (2h+1)^n$ elements.

Given a system f of polynomials in $\mathbb{F}_p[x_1, \ldots, x_n]$, we consider its affine variety $X = \{f = 0\} \subseteq \overline{\mathbb{F}}_p^n$, its rational points $X(\mathbb{F}_p)$ that lie in $\mathbb{F}_p^n$, and the "discrete neighborhood" $X(\mathbb{F}_p) + U_h = \{a + u \in \mathbb{F}_p^n : a \in X(\mathbb{F}_p), u \in U_h\}$ around $X(\mathbb{F}_p)$ of radius h. Then

$$\#(X(\mathbb{F}_p) + U_h) \le \#X(\mathbb{F}_p) \cdot \#U_h. \tag{1.1}$$

This paper addresses the question:

(Q) Is the neighborhood's size close to this upper bound?

Thus we ask for upper bounds on the (non-negative) difference

$$\Delta = \#X(\mathbb{F}_p) \cdot \#U_h - \#(X(\mathbb{F}_p) + U_h). \tag{1.2}$$

A small such bound implies a lower bound on $\#(X(\mathbb{F}_p) + U_h)$.

The central notion for understanding (Q) turns out to be the *shift* of a variety, which is the translation by a nonzero constant vector of the coordinates. If no absolutely irreducible component with maximal dimension of X is a shift of another component, then the answer to (Q) is "yes". For the opposite case, we exhibit examples where the answer is "no". When X is absolutely irreducible, the condition on shifts turns out to be necessary and sufficient (Corollary 4.5). Examples of *shift-free* absolutely irreducible varieties include: square matrices of rank bounded by some fixed number, non-squarefree polynomials, pairs of non-coprime polynomials, decomposable polynomials, and graphs of polynomials.

2. Preliminaries

Let q be a power of a prime p and $\mathbb{F}_q$ a finite field with q elements. We denote the algebraic closure of $\mathbb{F}_q$ by $\overline{\mathbb{F}}_q$ and the affine n-dimensional space over $\overline{\mathbb{F}}_q$ by $\mathbb{A}^n = \mathbb{A}^n(\overline{\mathbb{F}}_q)$. A nonempty subset $X \subset \mathbb{A}^n$ is an affine subvariety of $\mathbb{A}^n$ (a variety for short) if it is the set of common zeros in $\mathbb{A}^n$ of some set of polynomials in $\overline{\mathbb{F}}_q[x_1, \ldots, x_n]$. Furthermore, X is an $\mathbb{F}_q$-variety (or $\mathbb{F}_q$-definable) if it can be defined by polynomials in $\mathbb{F}_q[x_1, \ldots, x_n]$. We will use the notations $\{f_1 = \cdots = f_s = 0\}$ and $\mathcal{V}(f_1, \ldots, f_s)$ to denote the $\mathbb{F}_q$-variety defined by $f_1, \ldots, f_s$.

An $\mathbb{F}_q$-variety $X \subset \mathbb{A}^n$ is $\mathbb{F}_q$-irreducible if it cannot be expressed as a finite union of proper $\mathbb{F}_q$-subvarieties of X. Furthermore, X is absolutely irreducible if it is $\overline{\mathbb{F}}_q$–irreducible as an $\overline{\mathbb{F}}_q$–variety. Any $\mathbb{F}_q$-variety X can be expressed as a non-redundant union $X = X_1 \cup \cdots \cup X_m$ of irreducible $\mathbb{F}_q$-varieties, unique up to reordering, which are called the *irreducible* $\mathbb{F}_q$-components of X. Some of them may be absolutely irreducible.

For an $\mathbb{F}_q$-variety $X \subset \mathbb{A}^n$, its defining ideal $I(X)$ is the set of polynomials in $\mathbb{F}_q[x_1, \ldots, x_n]$ vanishing on X. The *dimension* $\dim X$ of an

$\mathbb{F}_q$-variety X is the length r of a longest chain $X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_r$ of nonempty irreducible $\mathbb{F}_q$-varieties contained in X.

The degree $\deg X$ of an irreducible $\mathbb{F}_q$-variety X is the maximum number of points lying in the intersection of X with a linear space $L \subseteq \overline{\mathbb{F}}_q^n$ of codimension $\dim X$, for which $X \cap L$ is finite. More generally, following Heintz (1983) (see also Fulton (1984)), if $X = X_1 \cup \cdots \cup X_m$ is the decomposition of X into irreducible $\mathbb{F}_q$-components, then the degree of X is

$$\deg X = \sum_{1 \leq i \leq m} \deg X_i.$$

The following *Bézout inequality* holds (see Heintz (1983), Fulton (1984), Vogel (1984)): if X and Y are $\mathbb{F}_q$-varieties, then

$$\deg(X \cap Y) \leq \deg X \cdot \deg Y. \tag{2.1}$$

In the following, we usually state explicit inequalities, but the spirit is that the field size q is (much) larger than the geometric quantities like n, $\deg X$, and h, so that our bounds should be taken as asymptotics in q. Thus an upper bound on Δ is "small" if it is of smaller order in q than the arguments of Δ.

We denote by $X(\mathbb{F}_q)$ the set of $\mathbb{F}_q$-rational points of an $\mathbb{F}_q$-variety $X \subseteq \mathbb{A}^n$, namely, $X(\mathbb{F}_q) = X \cap \mathbb{F}_q^n$. For X of dimension r and degree d, we let $X = X_1 \cup \cdots \cup X_m$ be the decomposition of X into irreducible $\mathbb{F}_q$-components, and suppose that $X_1, \ldots, X_\sigma$ are absolutely irreducible of dimension r and that $X_{\sigma+1}, \ldots, X_m$ are not. Then $X_1, \ldots, X_\sigma$ provide the main contribution to $\#X(\mathbb{F}_q)$ and we call them the *essential components*. We write

$$d_i = \deg X_i \text{ for } 1 \leq i \leq m \text{ and } D = \sum_{1 \leq i \leq \sigma} d_i.$$

Then the following bounds on $\#X(\mathbb{F}_q)$ hold.

Fact 2.1. (i) $\#X(\mathbb{F}_q) \leq dq^r$.

(ii) *If* $q > d$ *and* $\sigma > 0$*, then*

$$|\#X(\mathbb{F}_q) - \sigma q^r| \leq (D-1)(D-2)q^{r-1/2} + (5D^{13/3} + d^2)q^{r-1}.$$

(iii) *If* X *is an irreducible* $\mathbb{F}_q$*-variety and not absolutely irreducible, then*

$$\#X(\mathbb{F}_q) \leq d^2 q^{r-1}/4.$$

Proofs of (ii) and (iii) are in Cafure and Matera (2006), Theorem 5.7 and Lemma 2.3.

3. Neighborhoods around varieties

Given a polynomial sequence $f = (f_1, \ldots, f_s)$ in $\mathbb{F}_p[x_1, \ldots, x_n]^s$ and the affine $\mathbb{F}_p$-variety $X = \{f = 0\} \subseteq \mathbb{A}^n$, question (Q) is concerned with the size of the "standard neighborhood"

$$X(\mathbb{F}_p) + U_h = \{a + u \in \mathbb{F}_p^n : a \in X(\mathbb{F}_p), u \in U_h\}.$$

As $\#X(\mathbb{F}_p) \cdot \#U_h$ is an optimal upper bound, we concentrate on lower bounds, or, equivalently, on upper bounds on the difference Δ from (1.2).

3.1. **Generalized neighborhoods around varieties.** Most of this paper deals with the following more general problem: given an $\mathbb{F}_q$-variety $X = \{f = 0\} \subseteq \mathbb{A}^n$, and a nonempty set $U \subset \mathbb{F}_q^n$, find lower bounds on

$$X(\mathbb{F}_q) + U = \{a + u \in \mathbb{F}_q^n : a \in X(\mathbb{F}_q), u \in U\}.$$

Since

$$\Delta = \#X(\mathbb{F}_q)\cdot\#U - \#(X(\mathbb{F}_q)+U) \leq \sum_{a \neq b \in X(\mathbb{F}_q)} \#((a+U)\cap(b+U)), \tag{3.1}$$

it is sufficient to show upper bounds on the sum.

We fix the following notation for an irreducible decomposition of an $\mathbb{F}_q$-variety $X = X_1 \cup \cdots \cup X_m \subset \mathbb{A}^n$ of dimension r:

$$\begin{aligned} X_1, \ldots, X_m &: \text{irreducible } \mathbb{F}_q\text{-components}, \\ X_1, \ldots, X_\sigma &: \text{absolutely irreducible of dimension } r, \\ X_{\sigma+1}, \ldots, X_\rho &: \text{absolutely irreducible of dimension less than } r, \\ X_{\rho+1}, \ldots, X_m &: \text{not absolutely irreducible}, \end{aligned} \tag{3.2}$$

with $0 \leq \sigma \leq \rho \leq m$. The ordering inside each type of components is arbitrary and only done to simplify notation. Recall that $X_1, \ldots, X_\sigma$ are the *essential components*. According to Fact 2.1, the cardinality of the set $X_j(\mathbb{F}_q)$ for an essential component X_j is of order q^r, while that of the other components is at most of order q^{r-1}. The following notions of shifts are central to our considerations.

Definition 3.1.

(i) For $0 \neq u = (u_1, \ldots, u_n) \in \mathbb{A}^n$ and $g \in \mathbb{F}_q[x_1, \ldots, x_n]$, $g^{(u)} = g(x_1 - u_1, \ldots, x_n - u_n)$ is g *shifted by* u.

(ii) For $f \in \mathbb{F}_q[x_1, \ldots, x_n]^s$ and $X = \{f = 0\} \subseteq \mathbb{A}^n$, $f^{(u)}$ consists of the polynomials in f shifted by u, and $X^{(u)} = \{f^{(u)} = 0\} = \{a + u : a \in X\}$ is X *shifted by* u.

(iii) X with decomposition (3.2) is *essentially* u*-shift-free* if none of its components X_i equals $X_j^{(u)}$ for any i, j with $1 \leq i, j \leq \sigma$. (The case $i = j$ is included, and if $\sigma = 0$, then X is essentially u-shift-free.)

(iv) For $U \subseteq \mathbb{F}_q^n$, X is *essentially* U*-shift-free* if it is essentially u-shift-free for all $u \in U$.

Thus $X^{(u)}$ is isomorphic to X, and if $X = Y^{(u)}$, then $X^{(-u)} = (Y^{(u)})^{(-u)} = Y$. When X is absolutely irreducible, so that $\sigma = m = 1$ in (3.2), we leave out the word "essentially".

Lemma 3.2. *We have*

$$\sum_{a\neq b\in X(\mathbb{F}_q)} \#((a+U)\cap(b+U)) \leq \#U\cdot \sum_{0\neq u\in U-U} \#(X(\mathbb{F}_q)\cap X^{(u)}(\mathbb{F}_q)).$$

Proof. For $a, b \in X(\mathbb{F}_q)$ with $a \neq b$, $v, w \in U$ with $a + v = b + w$, and $u = v - w$, we have $u \neq 0$ and $b = a + u \in X(\mathbb{F}_q) \cap X^{(u)}(\mathbb{F}_q)$. Since any $u \in U - U$ can be expressed in at most $\#U$ ways as $u = v - w$ with $v, w \in U$, the lemma follows. □

The following result first establishes an upper bound on the difference Δ from (3.1) in terms of intersections of shifted varieties. Then we state, under a shift-freeness assumption, a bound which is small compared to the two arguments of Δ.

Theorem 3.3. *Let $X \subset \mathbb{A}^n$ be an $\mathbb{F}_q$-variety of dimension r, degree $d < q$, and decomposition (3.2).*

(i)

$$\Delta \leq \#U\cdot\Big(\sum_{\substack{0\neq u\in U-U\\ 1\leq i,j\leq\sigma}} \#\big(X_i(\mathbb{F}_q)\cap X_j^{(u)}(\mathbb{F}_q)\big) + 2(\#(U-U)-1)\sum_{\sigma<i\leq m}\#X_i(\mathbb{F}_q)\Big).$$

(ii) *If furthermore X is essentially $(U - U)$-shift-free, then*

$$\Delta \leq \#U(\#(U-U)-1)\cdot d^2q^{r-1}.$$

Proof. Inequality (3.1) and Lemma 3.2 imply that

$$\Delta \leq \#U \sum_{0\neq u\in U-U} \#(X(\mathbb{F}_q)\cap X^{(u)}(\mathbb{F}_q)).$$

Given $0 \neq u \in U - U$, we expand each summand as

$$\#(X(\mathbb{F}_q)\cap X^{(u)}(\mathbb{F}_q)) = \#\big(\bigcup_{1\leq i,j\leq m} X_i(\mathbb{F}_q)\cap X_j^{(u)}(\mathbb{F}_q)\big).$$

For $\sigma < i \leq m$ and $1 \leq j \leq m$, we have $X_i(\mathbb{F}_q) \cap X_j^{(u)}(\mathbb{F}_q) \subseteq X_i(\mathbb{F}_q)$. Similarly, $X_i(\mathbb{F}_q) \cap X_j^{(u)}(\mathbb{F}_q) \subseteq X_j^{(u)}(\mathbb{F}_q)$ holds for $\sigma < j \leq m$ and all i. Thus all these intersections are contained in $\bigcup_{\sigma<i\leq m}(X_i(\mathbb{F}_q)\cup X_i^{(u)}(\mathbb{F}_q))$. Together with $\#X_i(\mathbb{F}_q) = \#X_i^{(u)}(\mathbb{F}_q)$ this yields the bound claimed in (i).

For (ii), we first have $2\#X_i(\mathbb{F}_q) \leq d_i d q^{r-1}$ for $\sigma < i \leq m$ by Fact 2.1. It remains to consider $1 \leq i, j \leq \sigma$. By hypothesis X_i and $X_j^{(u)}$ are distinct absolutely irreducible varieties and their intersection has dimension at most $r-1$ and degree at most $d_i d_j$ by the Bézout inequality (2.1). By Fact 2.1 (i) we have for any $0 \neq u \in U - U$ that

$$\begin{aligned}\#\big(\bigcup_{1\leq i,j\leq\sigma} X_i(\mathbb{F}_q)\cap X_j^{(u)}(\mathbb{F}_q)\big) &\leq \sum_{1\leq i,j\leq\sigma} \#(X_i(\mathbb{F}_q)\cap X_j^{(u)}(\mathbb{F}_q))\\ &\leq \sum_{1\leq i,j\leq\sigma} d_i d_j q^{r-1}.\end{aligned}$$

□

For $\sigma = 0$ we have the following less precise result, which follows from Fact 2.1 (i) and (iii), and (1.1) (for general U).

Corollary 3.4. *With hypotheses and notations as in Theorem 3.3, assume further that $\sigma = 0$. Then*

$$\#(X(\mathbb{F}_q)+U) \leq \#U \cdot d^2 q^{r-1}/2.$$

When X is not shift-free, then Δ may be large, as in the following example.

Example 3.5. Let $p > d+2h$, $h \geq 1$, $n \geq 2$, $f = x_1\cdot(x_1-1)\cdots(x_1-(d-1)) \in \mathbb{F}_p[x_1,\ldots,x_n]$, so that $d = \deg f$ and $X = \{f = 0\}$ is the union of d parallel hyperplanes $H_i = \{x_1 = i\}$ for $0 \leq i < d$ with distance 1 between "neighbors", and $X(\mathbb{F}_p)+U_h = \bigcup_{-h\leq i<d+h} H_i(\mathbb{F}_p)$. X is invariant under many shifts. Namely, $X = X^{(u)}$ for any $u \in \{0\}\times\mathbb{F}_p^{n-1}$, and for $0 \leq i < j \leq d$, $X_j = X_i^{(u)}$ for any $u \in \{j-i\}\times\mathbb{F}_p^{n-1}$. We have $\#X(\mathbb{F}_p) = dp^{n-1}$, $\#(X(\mathbb{F}_p)+U_h) = (d+2h)p^{n-1}$, and

$$\Delta = p^{n-1}(d(2h+1)^n - (d+2h)).$$

Since $\Delta \neq 0$, there is no "small" upper bound on Δ, namely of order less than $n-1 = \dim X$ in p. In particular, if X is a single hyperplane, then $\#(X(\mathbb{F}_p)+U_h) = (2h+1)p^{n-1}$. Its difference $\Delta = ((2h+1)^n - (2h+1))p^{n-1}$ with $\#X(\mathbb{F}_p)\cdot\#U_h$ is of the same order of magnitude in p as its two arguments, that is, not "small". ♢

Example 3.6. Generalizing Example 3.5, we consider a variety $Y \subset \mathbb{A}^n$ whose defining polynomials are independent of the variables $x_{n-m+1}, \ldots, x_n$, for some m with $1 \leq m < n$. We may also consider them as elements of $\mathbb{F}_q[x_1,\ldots,x_{n-m}]$, they define a variety $Y' \subseteq \mathbb{A}^{n-m}$, and $Y(\mathbb{F}_q) = Y'(\mathbb{F}_q)\times\mathbb{F}_q^m$. We consider the embedding

$$\begin{aligned} e\colon \mathbb{A}^{n-m} &\hookrightarrow \mathbb{A}^n \\ a' &\mapsto (a', 0, \ldots, 0), \end{aligned} \tag{3.3}$$

take some $V \subseteq \mathbb{F}_q^n$, and let $V' = e^{-1}(V)$. Then $Y+V = (Y'+V')\times\mathbb{A}^m$.

If we write $\Delta' = \#Y'(\mathbb{F}_q)\#V' - \#(Y'(\mathbb{F}_q)+V')$ and assume that $V = V'\times V''$ for some $V'' \subseteq \mathbb{F}_q^m$ with $\#V'' \geq 2$, then

$$\Delta = q^m\big(\#(Y'(\mathbb{F}_q)+V')\cdot(\#V''-1) + \Delta'\#V''\big). \tag{3.4}$$

We will modify this reasoning in Theorem 4.4 to show that under a certain condition, no "small" upper bound on Δ exists. $\Diamond$

Example 3.7. For $m, n \in \mathbb{N}$ and $s < \min\{m, n\}$, we consider the "determinantal" $\mathbb{F}_q$-variety M_s of matrices in $\mathbb{A}^{m\times n}$ of rank at most s. It is well-known that M_s is absolutely irreducible with

$$r = \dim M_s = s(m+n-s), \quad d = \deg M_s = \prod_{0\leq i<n-s} \frac{\binom{m+i}{s}}{\binom{s+i}{s}};$$

see, e.g., Bruns and Vetter (1988), Proposition 1.1, for the first assertion and Harris (1992), Example 19.10, for the second one. A simple calculation reveals that the factors decrease monotonically with growing i, so that the term for $i = 0$ dominates and $d \leq \binom{m}{s}^{n-s}$.

In view of Theorem 3.3, we check that M_s is not shift-invariant. Let $u \in \mathbb{F}_q^{m\times n} \setminus \{0\}$ and consider $M_s^{(u)}$. As the zero matrix 0 belongs to M_s, if $0 + u = u$ is in M_s, then $t = \operatorname{rank} u \leq s$. Let $C \in \mathbb{F}_q^{m\times m}$ be an invertible matrix such that the last $m - t$ rows of $C \cdot u$ are equal to zero. Let $A \in \mathbb{F}_q^{m\times n}$ be a matrix whose first t rows and last $m - s - 1$ rows are zero, and the remaining $m - t - (m - s - 1) = s - t + 1$ rows, together with the first t rows of $C \cdot u$, are linearly independent. Such an A exists, since $t + s - t + 1 = s + 1 \leq \min\{m, n\}$. Then

$$\begin{aligned} \operatorname{rank} A &= s - t + 1 \leq s, \\ \operatorname{rank}(C \cdot u + A) &= t + s - t + 1 = s + 1. \end{aligned}$$

It follows that $C^{-1}A \in M_s$ and $C^{-1}(C \cdot u + A) = u + C^{-1}A \notin M_s$, so that $M_s \neq M_s^{(u)}$, and thus M_s is $\mathbb{F}_q^{m\times n}$-shift-free. Applying Theorem 3.3 we obtain for $U \subseteq \mathbb{F}_q^{m\times n}$

$$\Delta \leq \#U\#(U-U)d^2q^{r-1}. \tag{3.5}$$

$\Diamond$

As a further example, we consider the variety of decomposable univariate polynomials. For a univariate polynomial $f = a_d x^d + \cdots + a_1 x + a_0$ in a polynomial ring $R[x]$ over a ring R and $k \in \mathbb{N}$, its *kth Hasse derivative* $\mathcal{D}^{(k)} f$ is

$$\mathcal{D}^{(k)} f = \sum_{k\leq i\leq d} \binom{i}{k} a_i x^{i-k}. \tag{3.6}$$

Since $\binom{i}{k}\binom{i-k}{\ell} = \binom{k+\ell}{\ell}\binom{i}{k+\ell}$ in the usual ranges for binomial coefficients, we have $\mathcal{D}^{(k)} \circ \mathcal{D}^{(\ell)} = \binom{k+\ell}{\ell}\mathcal{D}^{(k+\ell)}$.

Example 3.8. A univariate polynomial $f = f_n x^n + \cdots + f_0 \in F[x]$ of degree n over a field F is *decomposable* if there exist $g, h \in F[x]$ of degrees $\ell, m \geq 2$, respectively, with $f = g \circ h$. Then $n = \ell m$, and denoting their coefficients by g_i and h_j, respectively, we also have for the monic (leading coefficient 1) and original (constant coefficient 0, graph containing the origin) polynomial $h' = h_m^{-1}(h - h_0)$:

$$f = g \circ h = g \circ ((h_m x + h_0) \circ h') = (g \circ (h_m x + h_0)) \circ h'.$$

We may thus assume that h is monic original. Then $g_\ell = f_n$.

All such polynomials f, g, and h are parametrized by their coefficients in $\mathbb{A}^{n+1}$, $\mathbb{A}^{\ell+1}$, and $\mathbb{A}^{m-1}$, respectively. The Zariski closure of the image of the *composition map* $\gamma\colon \mathbb{A}^{\ell+m} \to \mathbb{A}^{n+1}$ with $(g,h) \mapsto g \circ h$ is the set of decomposable polynomials. This is an absolutely irreducible closed affine subvariety $C_{n,\ell}$ of $\mathbb{A}^{n+1}$, of dimension $\ell+m$ and with degree $d \leq \ell^{\ell+m-2}$; see von zur Gathen and Matera (2017).

In the remainder of this example, we assume that F is a finite field $\mathbb{F}_q$ of characteristic greater than n and that q is sufficiently large (compared to n).

We want to show that $C_{n,\ell}$ is $\mathbb{F}_q^{n+1}$-shift-free. It is sufficient to exhibit for every nonzero $u \in \mathbb{F}_q^{n+1}$ some $f \in C_{n,\ell}(\mathbb{F}_q)$ so that $u + f \notin C_{n,\ell}(\mathbb{F}_q)$. Addition here is the standard coefficient-wise addition of polynomials.

We consider a nonzero $u \in \mathbb{F}_q^{n+1}$, supposing first that $\deg u = n$ and $\mathcal{D}u(0) = \mathcal{D}^{(1)}u(0) \neq 0$, where $\mathcal{D}u$ denotes the Hasse derivative $\mathcal{D}u = \mathcal{D}^{(1)}u$. Any $f = \sum_{0 \leq i \leq \ell} \lambda_i x^{im}$ with $\lambda_0, \ldots, \lambda_\ell \in \mathbb{F}_q$ belongs to $C_{n,\ell}(\mathbb{F}_q)$ and it suffices to prove that there exists such an f with $u + f \notin C_{n,\ell}(\mathbb{F}_q)$. When $\lambda_0, \ldots, \lambda_\ell$ vary over $\mathbb{F}_q$, the set of polynomials

$$\mathcal{F} := \big\{\mathcal{D}u + \sum_{1 \leq i \leq \ell} im\lambda_i x^{im-1} : \lambda_1, \ldots, \lambda_\ell \in \mathbb{F}_q\big\}$$

constitutes a linear family with prescribed coefficients in the sense of, e.g., Mullen and Panario (2013), §3.5. If $\mathcal{F} \subseteq \mathbb{F}_q[x^k]$ for some $k \geq 1$, then k divides the exponents $m-1$ and $2m-1$ of variable terms in $\mathcal{F}$, and hence $k = 1$.

Thus we may apply Cohen (1972), Theorem 1, which shows that for sufficiently large q there exists a polynomial f so that $\deg(u+f) = n$ and $\mathcal{D}(u+f) \in \mathcal{F}$ is irreducible in $\mathbb{F}_q[x]$. Furthermore, there exists such an f with $\deg \mathcal{D}(u+f) = n-1$, since there are only $q^{\ell-1}$ elements in $\mathcal{F}$ of degree less than $n-1$.

For such an f, $u+f$ is not in $C_{n,\ell}(\mathbb{F}_q)$, since a decomposition $u + f = g \circ h$ with $\deg g = \ell$ and $\deg h = m$ yields, by the chain rule, a factor $\mathcal{D}h$ of $\mathcal{D}(u+f)$ with degree $m-1$. This proves our assertion.

For the remaining case, where $\deg u < n$, we add a fixed term $\lambda_n x^n$ with $\lambda_n \neq 0$ and let the remaining terms vary, while if $\mathcal{D}u(0) = 0$, we make a similar argument considering the Taylor expansion of $\mathcal{D}u$ in powers of $x - \alpha$ and the set of elements $f = \sum_{0 \leq i \leq \ell} \lambda_i (x-\alpha)^{im}$ with $\lambda_0, \ldots, \lambda_\ell \in \mathbb{F}_q$, for a suitable $\alpha \in \mathbb{F}_q \setminus \{0\}$.

Thus $C_{n,\ell}$ is $\mathbb{F}_q^{n+1}$-shift-free and the estimate of Theorem 3.3 (ii) applies. ◊

4. Shift-invariant varieties

In order to apply Theorem 3.3 (ii) to an $\mathbb{F}_p$-variety $X \subseteq \mathbb{A}^n$, the critical point is to check whether X is $(U-U)$-shift-free. We say for some $u \in \mathbb{F}_q^n \setminus \{0\}$ that X is *u-shift-invariant* if $X = X^{(u)}$. Furthermore, X is *shift-invariant* if it is u-shift-invariant for some nonzero $u \in \mathbb{F}_q^n$. We call X a *cylinder in the direction of u* if $a + tu \in X$ for any $a \in X$ and $t \in \overline{\mathbb{F}}_q$. We have the following characterization of shift-invariance.

Proposition 4.1. *Let $p > d$, q a power of p, let $X \subset \mathbb{A}^n$ be an $\mathbb{F}_q$-variety of degree d and $u \in \mathbb{F}_q^n \setminus \{0\}$. Then X is u-shift-invariant if and only if X is a cylinder in the direction of u.*

Proof. Suppose that X is invariant under a shift $u \in \mathbb{F}_q^n \setminus \{0\}$. Let a be an arbitrary point of X and consider the line $\ell_a = \{a + tu : t \in \overline{\mathbb{F}}_q\}$. Since X is invariant under the shift u, it is also invariant under $2u, 3u, \ldots, (p-1)u$. Thus

$$\#(X \cap \ell_a) \geq \#\{a + tu : t \in \mathbb{F}_p\} = p > d.$$

If $\dim(X \cap \ell_a) = 0$, then by the Bézout inequality (2.1) we would have

$$\#(X \cap \ell_a) = \deg(X \cap \ell_a) \leq \deg X = d,$$

which contradicts the previous inequality. It follows that

$$0 < \dim(X \cap \ell_a) \leq \dim \ell_a = 1,$$

so that $\dim(X \cap \ell_a) = 1$. The fact that the variety $X \cap \ell_a$ of dimension 1 is contained in the absolutely irreducible variety ℓ_a of dimension 1 shows that $X \cap \ell_a = \ell_a$, that is, $\ell_a \subseteq X$. Since this holds for any $a \in X$, we conclude that X is a cylinder in the direction of u.

The converse assertion is clear. □

The following example shows that the condition "$p > d$" is required. We pick a prime p, a linear subspace $V \subset \mathbb{A}^{n-1}$ of some dimension m, the variety $X = \mathbb{F}_p \times V \subset \mathbb{A}^n$, and $u = (1, 0, \ldots, 0) \in \mathbb{A}^n$. Then X is u-shift-invariant. For $a = (0, \ldots, 0) \in X$ and $t \in \overline{\mathbb{F}}_p \setminus \mathbb{F}_p$, the value $a + tu$ is not in X. Thus X is not a cylinder in the direction of u.

We can reformulate the condition of shift-invariance as follows.

Corollary 4.2. *With hypotheses as in Proposition 4.1, X is shift-invariant if and only if there exists an invertible map $L\colon \mathbb{A}^n \to \mathbb{A}^n$ of linear forms in $\mathbb{F}_q[x_1, \ldots, x_n]$ such that $L(X) = Y \times \mathbb{A}^1$ for some $\mathbb{F}_q$-variety $Y \subseteq \mathbb{A}^{n-1}$. If this is the case and $I(Y) \subset \overline{\mathbb{F}}_q[y_1, \ldots, y_{n-1}]$ is the ideal of Y, then $I(Y \times \mathbb{A}^1) = I(Y)\,\overline{\mathbb{F}}_q[y_1, \ldots, y_n]$.*

Proof. We assume that $X = X^{(w)}$ with some nonzero $w \in \mathbb{F}_q^n$. For ease of presentation, we apply a coordinate permutation C so that $(Cw)_n \neq 0$, and now assume $w_n \neq 0$. We define the vector of linear forms

$$L = \big(x_1 - \frac{w_1 x_n}{w_n}, \ldots, x_{n-1} - \frac{w_{n-1} x_n}{w_n}, \frac{x_n}{w_n}\big) \in (\mathbb{F}_q[x_1, \ldots, x_n])^n \tag{4.1}$$

and also denote the induced mapping as

$$L \colon \mathbb{A}^n \to \mathbb{A}^n.$$

The linear forms in L are linearly independent. Let N be L followed by the projection to the first $n-1$ coordinates, and $Y = N(X)$. Thus $N(w) = 0$. We claim that $L(X) = Y \times \mathbb{A}^1$.

The inclusion "$\subseteq$" is clear. So let $b \in Y$ and $c \in \mathbb{A}^1$, and $b = N(a)$ for some $a \in X$. As in the proof of Proposition 4.1, the line $\{a+tw \colon t \in \mathbb{A}^1\}$ is contained in X. Then

$$\begin{aligned} L\big(a + (c - \frac{a_n}{w_n})w\big) &= \big(N(a + (c - \frac{a_n}{w_n})w), (a_n + (c - \frac{a_n}{w_n})w_n)/w_n\big) \\ &= \big(N(a), \frac{a_n}{w_n} + c - \frac{a_n}{w_n})\big) = (b, c), \end{aligned}$$

which shows the claim. The invertible map in the proposition is $L \circ C$.

Finally, the identity $I(Y \times \mathbb{A}^1) = I(Y)\,\overline{\mathbb{F}}_q[y_1, \ldots, y_n]$ is a standard fact on ideals of varieties. □

Are the upper bounds on Δ in Theorem 3.3 "small" in relation to the two arguments of Δ, which are defined in terms of $\#X(\mathbb{F}_q)$? This is not always the case, as shown in Corollary 4.5 below. Furthermore, if $\sigma = 0$ in (3.2), the asymptotic behavior of $\#X(\mathbb{F}_q)$ does not have a simple description suitable for our purposes. For a partial positive answer, we now rule out this case and substitute the Weil bounds in Fact 2.1 to obtain a numerical approximation for $\#X(\mathbb{F}_q)$ depending only on the dimension and degree of X. Then the upper bound in Theorem 3.3 (ii) indeed turns out to be small.

Corollary 4.3. *With hypotheses and notations as in Theorem 3.3 (ii), assume further that $\sigma > 0$ and denote $D = \sum_{1 \leq i \leq \sigma} \deg X_i$. Then*

$$|\#(X(\mathbb{F}_q){+}U) - \#U \cdot \sigma q^r| \leq \#U\big(D^2 q^{r-1/2} + (5D^{13/3} + \#(U-U)d^2)q^{r-1}\big).$$

Proof. By Fact 2.1 (ii) we have

$$|\#X(\mathbb{F}_q) \cdot \#U{-}\#U \cdot \sigma q^r| \leq \#U\big(D^2 q^{r-1/2} + (5D^{13/3} + d^2)q^{r-1}\big).$$

Theorem 3.3 (ii) and the triangle inequality imply the claim. □

In the next result, a subset $U \subset \mathbb{F}_q^n$ is called *closed under shifts to zero* if for any $u \in U$, replacing any set of coordinates of u by all zeroes yields an element of U. We remark that the standard neighborhood $U_h \subset \mathbb{F}_p^n$ is closed under shifts to zero. Finally, we recall Δ from (3.1).

Theorem 4.4. *Let p be a prime, $p > d \geq 1$, $U \subseteq \mathbb{F}_p^n$ closed under shifts to zero, and X be an absolutely irreducible $\mathbb{F}_p$-variety of dimension r and degree d which is not $(U - U)$-shift-free. Furthermore, let*

$$\alpha = d^2 + (5d^{13/3} + d^2\#(U-U))p^{-1/2} \tag{4.2}$$

and assume that $p \geq 4\alpha^2$. Then

$$\Delta \geq p^r/2. \tag{4.3}$$

Proof. The mapping given by $X \mapsto X^{(u)}$ for an $\mathbb{F}_p$-variety X constitutes an action of the additive group $\mathbb{F}_p^n$ on the set of $\mathbb{F}_p$-varieties, since $(X^{(u)})^{(u')} = X^{(u+u')}$. We let $B \subseteq U - U$ be a basis of the subgroup generated by the $u \in U - U$ with $X = X^{(u)}$. This subgroup is an $\mathbb{F}_p$-vector space of some dimension m and we write $B = \{b_1, \ldots, b_m\}$. We take the invertible linear map $L_1 \colon \mathbb{A}^n \to \mathbb{A}^{n-1} \times \mathbb{A}^1$ from (4.1) with $w = b_1$, ignoring (for ease of presentation) the possibly required coordinate permutation. Thus $L_1(X) = Y_1 \times \mathbb{A}^1$ and $L_1(b_1) = (0, \ldots, 0, 1)$, for some subvariety Y_1 of $\mathbb{A}^{n-1}$. Also, N_1 is L_1 followed by the projection to the first $n-1$ coordinates.

We claim that $V_1 = N_1(U)$ is closed under shifts to zero. So let $u = (u_1, u_2, \ldots, u_n) \in U$, $v = (v_1, v_2, \ldots, v_{n-1}) = N_1(u)$ be an arbitrary element of V_1, and consider annihilating its first coordinate. Since U is closed under shifts to zero, also $u' = (0, u_2, \ldots, u_{n-1}, 0) \in U$ and $(0, v_2, \ldots, v_{n-1}) = N_1(u') \in V_1$.

If $m \geq 2$, we claim that $Y_1^{(N_1(b_2))} = Y_1$. Writing $L_1(b_2) = (b_2', b_2'')$ with $b_2' = N_1(b_2) \in \mathbb{A}^{n-1}$ and $b_2'' \in \mathbb{A}^1$, we have

$$\begin{aligned} Y_1 \times \mathbb{A}^1 = L_1(X) &= L_1(X^{(b_2)}) = (L_1(X))^{(L_1(b_2))} \\ &= (Y_1 \times \mathbb{A}^1)^{(b_2', b_2'')} = Y_1^{(b_2')} \times \mathbb{A}^1. \end{aligned}$$

Thus $Y_1 = Y_1^{(b_2')}$, and we can again apply Corollary 4.2 to find $L_2 \colon \mathbb{A}^{n-1} \to \mathbb{A}^{n-1}$ and $Y_2 \subseteq \mathbb{A}^{n-2}$ with $L_2(Y_1) = Y_2 \times \mathbb{A}^1$ and $L_2(b_2') = (0, \ldots, 0, 1)$. This yields an invertible linear map $M_2 = L_2 \times \mathrm{id} \colon \mathbb{A}^n \to \mathbb{A}^n$ with $(M_2 \circ L_1)(X) = Y_2 \times \mathbb{A}^2$. The last two entries of $((M_2 \circ L_1)(b_1), (M_2 \circ L_1)(b_2))$ have the lower antitriangular form

$$\begin{pmatrix} 0 & 1 \\ 1 & * \end{pmatrix}, \tag{4.4}$$

with some value $*$ below the antidiagonal.

Continuing in this way for a total of m steps, we obtain an invertible linear map $M = M_m \circ M_{m-1} \circ \cdots \circ L_1 \colon \mathbb{A}^n \to \mathbb{A}^n$, where $M_j = L_j \times \mathrm{id}_{j-1}$ and $\mathrm{id}_k \colon \mathbb{A}^k \to \mathbb{A}^k$ is the identity map, with $M(X) = Y \times \mathbb{A}^m$ for some variety Y in $\mathbb{A}^{n-m}$. Furthermore, Y is absolutely irreducible of dimension $r - m$ and degree d. The last m columns of $(M(b_1), \ldots, M(b_m))$ have a shape as in (4.4), namely lower antitriangular with 1 on the antidiagonal, zeroes above it, and arbitrary values below it. We let $V \subseteq \mathbb{F}_p^{n-m}$ be the projection of $M(U)$ to the first $n - m$ coordinates.

Applying inductively the argument for V_1 from above, it follows that also V is closed under shifts to zero.

We claim that Y is $(V-V)$-shift-free. So let $v \in V-V$ with $Y = Y^{(v)}$ and $z = M^{-1}(v, 0)$. Then

$$M(X) = Y \times \mathbb{A}^m = Y^{(v)} \times \mathbb{A}^m = (Y \times \mathbb{A}^m)^{(v,0)} = M(X)^{(M(z))} = M(X^{(z)}),$$

and hence $X = X^{(z)}$. For the last equation in the above, we have for any $a \in \mathbb{A}^n$:

$$\begin{aligned} a \in M(X)^{(M(z))} &\iff a - M(z) \in M(X) \iff M^{-1}(a) - z \in X \\ &\iff M^{-1}(a) \in X^{(z)} \iff a \in M(X^{(z)}). \end{aligned}$$

Furthermore, we claim that $z \in U - U$ and $z_{n-m+1} = \cdots = z_n = 0$, and use induction on m to show this. We first consider the situation $m = 1$ in Corollary 4.2, so that $V = N(U)$, and write $v = v_1 - v_2$ with $v_1, v_2 \in V \subseteq \mathbb{F}_p^{n-1}$. Since V is closed under shifts to zero, also $(v_i, 0) \in V$ and $z_i = L^{-1}(v_i, 0) \in U$ for $i \in \{1, 2\}$. Now L is a linear map and therefore $z = z_1 - z_2 \in U - U$. Thus the claim follows in this situation, and in general by induction.

Thus z is a linear combination, say $z = \sum_{1 \leq i \leq m} \lambda_i b_i$ with all $\lambda_i \in \mathbb{F}_p$, of the basis vectors b_i, and also $M(z) = \sum_{1 \leq i \leq m} \lambda_i M(b_i)$. The last m coordinates of $M(z)$ are zero by the above claim and those of the $M(b_i)$ have antitriangular shape, with 1 on the diagonal, so that all λ_i are zero. It follows that $z = 0$ and $v = 0$, and therefore Y is $(V - V)$-shift-free.

We now follow the reasoning in Example 3.6. Thus we write $\Delta' = \#Y(\mathbb{F}_p)\#V - \#(Y(\mathbb{F}_p) + V)$ and $k = \#U/\#V$. Then $\#X(\mathbb{F}_p) = p^m \#Y(\mathbb{F}_p)$ and

$$M(X+U) = M(X)+M(U) = (Y \times \mathbb{A}^m)+M(U) = (Y+V)\times \mathbb{A}^m. \tag{4.5}$$

For the last equation, we first take some $b \in Y$, $c \in \mathbb{A}^m$, and $u = (u_1, \ldots, u_n) \in M(U)$. Then $v = (u_1, \ldots, u_{n-m}) \in V$ and

$$(b, c) + u = ((b + v, c + (u_{n-m+1}, \ldots, u_n)) \in (Y + V) \times \mathbb{A}^m.$$

For the reverse inclusion, we take $b \in Y$, $v \in V$, and any $u = (u_1, \ldots, u_n) \in M(U)$ with $(u_1, \ldots, u_{n-m}) = (v_1, \ldots, v_{n-m})$. Then

$$(b + v, c) = (b, c - (u_{n-m+1}, \ldots, u_n)) + (v, u) \in (Y \times \mathbb{A}^m) + M(U).$$

In particular, we have $\#(X(\mathbb{F}_p) + U) = p^m \#(Y(\mathbb{F}_p) + V)$.

Since $b_1 \in U-U$, we also have $-b_1 \in U-U$ and $N_1(-b_1) = N_1(b_1) = 0$. Thus $\#V < \#U$ and $\#(V - V) < \#(U - U)$.

Since Y is $(V-V)$-shift-free and absolutely irreducible of dimension $r - m$ and degree d, Corollary 4.3 implies that

$$\#(Y(\mathbb{F}_p) + V) > p^{r-m}\#V(1 - \alpha p^{-1/2}).$$

In fact, α is defined so that this inequality holds. Now $\Delta' \geq 0$ and we have

$$\begin{aligned}\Delta &= \#X(\mathbb{F}_p)\#U - \#(X(\mathbb{F}_p) + U)\\ &= p^m\#Y(\mathbb{F}_p)\#U - p^m\#(Y(\mathbb{F}_p) + V)\\ &= p^m\big(k\Delta' + (k-1)\#(Y(\mathbb{F}_p) + V)\big) \qquad (4.6)\\ &\geq p^m(k-1)\#(Y(\mathbb{F}_p) + V)\\ &> (\#U - \#V)(p^r - \alpha p^{r-1/2}) \geq p^r - \alpha p^{r-1/2} \geq p^r/2.\end{aligned}$$

□

The condition $p \geq 4\alpha^2$ has a wide range of solutions, for example $d \geq 13$, $\#U \leq d^\gamma$ for some real $\gamma \geq 1.5$, and $p \geq 9d^{2+2\gamma}$. Then $\#(U - U) \leq d^{2\gamma}$, $5d^{13/3} \leq d^5 \leq d^{2+2\gamma}$, $d^2 \leq 56d^{1+\gamma}$,

$$\begin{aligned}4\alpha^2 &\leq 4(d^2 + 2d^{2+2\gamma}p^{-1/2})^2 \leq 4(d^2 + 2d^{2+2\gamma}d^{-1-\gamma}/3)^2\\ &= 4(d^2 + 2d^{1+\gamma}/3)^2 \leq 4(3d^{1+\gamma}/2)^2 = 9d^{2+2\gamma} \leq p.\end{aligned}$$

The bound in Theorem 3.3 (ii) is roughly $(\#U)^3d^2p^{r-1}$, if $\#(U - U)$ is about $(\#U)^2$. For this to be less than the first argument $\#X(\mathbb{F}_p)\#U \approx p^r\#U$ of Δ, we certainly need $p > (\#U)^2$, which explains the requirement $p > d^{2\gamma}$ above.

We now come to a characterization of the absolutely irreducible varieties for which the answer to Question (Q) is "yes". The bounds on Δ in this paper depend on q and r, and also on the parameters n, U, and various degrees. For such a function g and $s \geq 0$, we write $g \in O(q^s)$ and $g \in \Omega(q^s)$, respectively, if $g \leq cq^s$ and $g \geq cq^s$ hold with functions c of the parameters, but independent of q and s, and which are positive for a large range of the parameters.

Corollary 4.5. *Let p be a prime, $p > d \geq 1$, and $U \subseteq \mathbb{F}_p^n$ closed under shifts to zero. Furthermore, we assume $p \geq 4\alpha^2$ for α from (4.2). Then for absolutely irreducible $\mathbb{F}_p$-varieties X of dimension r and degree d, we have:*

$$\begin{aligned}X \textit{ is } (U-U)\textit{-shift-free} &\Longrightarrow \Delta \in O(p^{r-1}),\\ X \textit{ is not } (U-U)\textit{-shift-free} &\Longrightarrow \Delta \in \Omega(p^r).\end{aligned}$$

Proof. The claim in the first line is in Theorem 3.3 (ii). The second line follows from Theorem 4.4. □

5. Standard neighborhoods and hypersurfaces

The paper's introduction explains our original motivation of dealing with standard neighborhoods $U_h = \{a \in \mathbb{F}_p^n : ||a|| \leq h\}$ over $\mathbb{F}_p$. We spell out the consequences of our more general results for this special case. Furthermore, we discuss the particular case of hypersurfaces in more detail.

5.1. **Standard neighborhoods.** Throughout this subsection, we have a prime p, an $\mathbb{F}_p$-variety $X \subseteq \mathbb{A}^n$ of dimension r, degree $d < p$, and with decomposition (3.2), $D = \sum_{1 \leq i \leq \sigma} \deg X_i$, an integer h with $p > 2h \geq 2$, and the standard neighborhood $U_h = \{u \in \mathbb{F}_p^n \colon ||u|| \leq h\}$. Then

$$\#U_h = (2h+1)^n, \quad \#(U_h - U_h) = \#U_{2h} = (4h+1)^n.$$

Now $\Delta = \#X(\mathbb{F}_p) \cdot \#U_h - \#(X(\mathbb{F}_p) + U_h)$ as in (1.2). If X is essentially U_{2h}-shift-free, then the following bounds are consequences of Theorem 3.3 (ii) and Corollary 4.3.

Corollary 5.1. (i) $\Delta \leq ((2h+1)(4h+1))^n d^2 p^{r-1}$,

(ii)

$$\begin{aligned}&|\#(X(\mathbb{F}_p) + U_h) - (2h+1)^n \sigma p^r| \\ &\leq (2h+1)^n \big(D^2 p^{r-1/2} + (5D^{13/3} + (4h+1)^n d^2) p^{r-1}\big).\end{aligned}$$

(iii) *If furthermore X is absolutely irreducible, then $D = d$ in (ii).*

Next we specialize to some of our examples. For the determinantal variety M_s of $m \times n$ matrices with rank at most s from Example 3.7, we have

$$\begin{aligned}&\Delta \leq ((2h+1)(4h+1))^{mn} d^2 p^{r-1}, \\ &|\#(M_s(\mathbb{F}_p) + U_h) - (2h+1)^{mn} p^r| \\ &\quad \leq (2h+1)^{mn} d^2 \big(p^{r-1/2} + (5d^{7/3} + (4h+1)^{mn}) p^{r-1}\big).\end{aligned}$$

The variety $C_{n,\ell}$ of decomposable polynomials from Example 3.8 has degree $d \leq \ell^{\ell+m-2}$ and satisfies:

$$\begin{aligned}&\Delta \leq ((2h+1)(4h+1))^{n+1} d^2 p^{\ell+m-1}, \\ &|\#(C_{n,\ell}(\mathbb{F}_p) + U_h) - (2h+1)^{n+1} p^r| \\ &\quad \leq (2h+1)^{n+1} d^2 \big(p^{r-1/2} + (5d^{7/3} + (4h+1)^{n+1}) p^{r-1}\big).\end{aligned}$$

5.2. **Hypersurfaces.** For a hypersurface $X = \{f = 0\} \subset \mathbb{A}^n$, where $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ is squarefree, the decomposition (3.2) of X corresponds to the factorization of f into irreducible polynomials of $\mathbb{F}_q[x_1, \ldots, x_n]$, the first $\sigma = \rho$ many being absolutely irreducible. We assume that $d = \deg X = \deg f < q$ and that X is essentially $(U-U)$-shift-free. With the usual notation in this section, we have the following bounds.

Corollary 5.2. (i) $\Delta \leq \#U \#(U-U) d^2 q^{n-2}$,

(ii)

$$\begin{aligned}&|\#(X(\mathbb{F}_q) + U) - \#U \cdot \sigma q^{n-1}| \\ &\qquad \leq \#U \big(D^2 q^{n-3/2} + (5D^{13/3} + \#(U-U) d^2) q^{n-2}\big).\end{aligned}$$

For $q = p$ prime and $U = U_h$, we have

(iii) $\Delta \leq ((2h+1)(4h+1))^n d^2 p^{n-2}$,

(iv)

$$\begin{aligned}&|\#(X(\mathbb{F}_p)+U_h)-(2h+1)^n\sigma p^{n-1}|\\&\qquad\le(2h+1)^n\bigl(D^2p^{n-3/2}+(5D^{13/3}+(4h+1)^nd^2)p^{n-2}\bigr).\end{aligned}$$

6. Shift-invariant polynomials

This section derives some properties of shift-invariant polynomials and studies algorithmic aspects.

We use the Taylor expansion of multivariate polynomials, employing the Hasse derivatives from (3.6). For $f\in\mathbb{F}_q[x_1,\ldots,x_n]$, its *kth partial (Hasse) derivative $\mathcal{D}^{(k)}_{x_i}f$ with respect to x_i* is $\mathcal{D}^{(k)}f$ for f considered as an element of $R[x_i]$ with $R=\mathbb{F}_q[x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n]$. Derivatives with respect to different variables commute: $\mathcal{D}^{(k)}_{x_i}\circ\mathcal{D}^{(\ell)}_{x_j}=\mathcal{D}^{(\ell)}_{x_j}\circ\mathcal{D}^{(k)}_{x_i}$ for $i\neq j$. For a multi-index $s=(s_1,\ldots,s_n)\in\mathbb{Z}^n$, we write $\mathcal{D}^{(s)}f=\mathcal{D}^{(s_1)}_{x_1}\circ\cdots\circ\mathcal{D}^{(s_n)}_{x_n}$ if $s_1,\ldots,s_n\ge 0$, and $\mathcal{D}^{(s)}f=0$ otherwise. For $s,t\in\mathbb{N}^n$, we have

$$\mathcal{D}^{(s)}\circ\mathcal{D}^{(t)}=\binom{s+t}{s}\mathcal{D}^{(s+t)},\text{ where }\binom{s+t}{s}=\prod_{1\le i\le n}\binom{s_i+t_i}{s_i}. \tag{6.1}$$

Furthermore, we let $\mathbb{N}^n_{\le d}\subset\mathbb{N}^n$ be the set of indices $s=(s_1,\ldots,s_n)$ with $|s|=s_1+\cdots+s_n\le d$. For $s\in\mathbb{N}^n$ and $w=(w_1,\ldots,w_n)\in W^n$ for some ring W, we set

$$w^s=\prod_{1\le i\le n}w_i^{s_i}. \tag{6.2}$$

With this terminology, we have the following version of the Taylor formula: if $f\in\mathbb{F}_q[x_1,\ldots,x_n]$ and $y=(y_1,\ldots,y_n)$ are new indeterminates, then

$$f=\sum_{s\in\mathbb{N}^n_{\le d}}\bigl((\mathcal{D}^{(s)}f)(y)\bigr)\cdot(x-y)^s, \tag{6.3}$$

The gradient of $f\in\mathbb{F}_q[x_1,\ldots,x_n]$ is $\nabla f=(\mathcal{D}^{(1)}_{x_1}(f),\ldots,\mathcal{D}^{(1)}_{x_n}(f))\in\mathbb{F}_q[x_1,\ldots,x_n]^n$. We have the following consequence of shift invariance in terms of derivatives.

Corollary 6.1. *With hypotheses as in Proposition 4.1, if X is u-shift-invariant for some $u\in\mathbb{F}_q^n\setminus\{0\}$, then for any $f\in I(X)$ and $a\in X$ we have $(\nabla f)(a)\cdot u=0$.*

Proof. Let $a\in X$ and $f\in I(X)$. Proposition 4.1 shows that the line $\{a+tu : u\in\overline{\mathbb{F}}_q\}$ is contained in X. As a consequence, $f(a+tu)=0$ for any $t\in\mathbb{A}^1$. Then the corollary follows by the chain rule. □

In order to study the shift-invariance of $f \in \mathbb{F}_p[x_1, \ldots, x_n]$ of degree d, let $y_1, \ldots, y_n$ be new indeterminates. By the Taylor formula (6.3),

$$\begin{aligned} f(x+y) &= \sum_{s \in \mathbb{N}^n_{\leq d}} (\mathcal{D}^{(s)} f)(x) y^s \\ &= f(x) + \sum_{1 \leq i \leq n} (\mathcal{D}_{x_i} f)(x) y_i + \cdots + \sum_{|s|=d} (\mathcal{D}^{(s)} f)(x) y^s, \end{aligned}$$

with y^s as in (6.2).

We write $f = \sum_{1 \leq i \leq d} f_i$, where each $f_i \in \mathbb{F}_q[x_1, \ldots, x_n]$ is zero or homogeneous of degree i, and similarly $f(x+y) = \sum_{i=1}^d f_i^*$, where each $f_i^* \in (\mathbb{F}_q[y_1, \ldots, y_n])[x_1, \ldots, x_n]$ is zero or homogeneous of degree i in the x_j. The Taylor formula for each $f_j(x+y)$ implies that

$$\begin{aligned} f_d^* &= f_d, \\ f_{d-1}^* &= f_{d-1} + \sum_{1 \leq i \leq n} (\mathcal{D}_{x_i} f_d)(x) y_i, \\ &\vdots \\ f_0^* &= f_0 + \sum_{1 \leq i \leq n} (\mathcal{D}_{x_i} f_1)(x) y_i + \cdots + \sum_{|s|=d} (\mathcal{D}^{(s)} f_d)(x) y^s. \end{aligned}$$

Now for $u = (u_1, \ldots, u_n) \in \mathbb{F}_q^n$ and replacing each y_i by $-u_i$ in the above, we conclude that $f = f^{(u)}$ if and only if

$$f_j = f_j - \sum_{1 \leq i \leq n} (\mathcal{D}_{x_i} f_{j+1})(x) u_i + \cdots + (-1)^{d-j} \sum_{|s|=d-j} (\mathcal{D}^{(s)} f_d)(x) u^s \tag{6.4}$$

for $0 \leq j \leq d$.

Lemma 6.2. *For $u = (u_1, \ldots, u_n) \in \mathbb{F}_q^n$ and $j > 0$, we have*

$$\Big(\sum_{1 \leq i \leq n} u_i \mathcal{D}_{x_i} \Big) \circ \Big(\sum_{|t|=j-1} u^t \mathcal{D}^{(t)} \Big) = j \sum_{|s|=j} u^s \mathcal{D}^{(s)}. \tag{6.5}$$

Proof. Equation (6.1) shows that for $t \in \mathbb{N}^n$ we have

$$u_i \mathcal{D}_{x_i} \circ u^t \mathcal{D}^{(t)} = u_i u^t (t_i + 1) \mathcal{D}^{(\mathrm{e}_i + t)} = (t_i + 1) u^{\mathrm{e}_i + t} \mathcal{D}^{(\mathrm{e}_i + t)},$$

where $e_i \in \mathbb{N}^n$ is the ith unit vector. We consider some $s = (s_1, \ldots, s_n) \in \mathbb{N}^n$ with $|s| = j$. Then $\mathcal{D}^{(s)}$ arises in the following sum on the left hand side of (6.5):

$$\sum_{1 \leq i \leq n} u_i \mathcal{D}_{x_i} \circ u^{s - \mathrm{e}_i} \mathcal{D}^{(s - \mathrm{e}_i)} = \sum_{1 \leq i \leq n} s_i u^s \mathcal{D}^{(s)} = j u^s \mathcal{D}^{(s)}.$$

This shows the claim. □

The following characterizes the shift-invariant polynomials.

Proposition 6.3. *Let $p > d$, q a power of p, and $f \in \mathbb{F}_q[x_1, \ldots, x_n] \backslash \{0\}$ of degree d. Then f is shift-invariant under $u = (u_1, \ldots, u_n) \in \mathbb{F}_q^n \backslash \{0\}$ if and only if*

$$\sum_{1 \le i \le n} u_i \mathcal{D}_{x_i} f = 0. \tag{6.6}$$

Proof. According to (6.4), $f = f^{(u)}$ holds if and only if

$$-\sum_{1 \le i \le n} (\mathcal{D}_{x_i} f_{j+1})(x) u_i \pm \cdots + (-1)^{d-j} \sum_{|s|=d-j} (\mathcal{D}^{(s)} f_d)(x) u^s = 0$$

for $0 \le j < d$. For $1 \le k \le j$, (6.5) implies inductively that

$$\sum_{|s|=j+k} u^s \mathcal{D}^{(s)} f_{j+k} = \frac{1}{(j+k)!} \big(\sum_{1 \le i \le n} u_i \mathcal{D}_{x_i} \big)^{(j+k)} (f_{j+k}),$$

where on the right hand side, the operator given by the sum is iterated $j + k$ times. We deduce that, for $0 \le j < d$,

$$\big(-\sum_{1 \le i \le n} u_i \mathcal{D}_{x_i} \big)(f_{j+1}) \pm \cdots + \frac{(-1)^{d-j}}{(d-j)!} \big(\sum_{i=1}^{n} u_i \mathcal{D}_{x_i} \big)^{(d-j)} (f_d) = 0. \tag{6.7}$$

In the particular case $j = d - 1$, the sum consists of only one summand:

$$\sum_{1 \le i \le n} u_i \mathcal{D}_{x_i} f_d = 0. \tag{6.8}$$

We claim that, for $1 \le j \le d$,

$$\sum_{1 \le i \le n} u_i \mathcal{D}_{x_i} f_j = 0.$$

Arguing by backward induction, the case $j = d$ is (6.8). Now suppose that the assertion holds for any k with $k > j \ge 1$. By (6.7) we have

$$\begin{aligned} 0 &= \big(-\sum_{1 \le i \le n} u_i \mathcal{D}_{x_i} \big)(f_j) \pm \cdots + \frac{(-1)^{d-j+1}}{(d-j+1)!} \big(\sum_{1 \le i \le n} u_i \mathcal{D}_{x_i} \big)^{(d-j+1)} (f_d) \\ &= \big(-\sum_{1 \le i \le n} u_i \mathcal{D}_{x_i} \big)(f_j), \end{aligned}$$

where the second identity is due to the inductive hypothesis. This proves the claim. Thus we have

$$\sum_{1 \le i \le n} u_i \mathcal{D}_{x_i} f = \sum_{1 \le i \le n} u_i \mathcal{D}_{x_i} \big(\sum_{1 \le j \le d} f_j \big) = \sum_{1 \le j \le d} \big(\sum_{1 \le i \le n} u_i \mathcal{D}_{x_i} f_j \big) = 0.$$

This finishes the proof of (6.6).

On the other hand, if (6.6) holds, then by homogeneity it follows that

$$\sum_{1 \le i \le n} u_i \mathcal{D}_{x_i} f_j = 0$$

for $1 \leq j \leq d$. This implies (6.7), from which the u-shift-invariance of f is readily deduced. □

This statement strengthens the corresponding one for varieties (Corollary 6.1) by providing a necessary and sufficient condition. It also yields a polynomial-time algorithm for testing a polynomial for (nontrivial) $\mathbb{F}_q^n$-shift-invariance. Namely, (6.6) corresponds to a system of linear equations in $u_1, \ldots, u_n$ with coefficients in $\mathbb{F}_q[x_1, \ldots, x_n]$. Its size is polynomial in the input size of f, given either in dense or sparse representation. Its kernel consists of all u under which f is shift-invariant, and its triviality can be checked efficiently.

However, the problem of deciding U_h-shift-freeness turns out to be computationally hard, namely coNP-complete under randomized reductions; see Theorem 7.1 below. Thus under standard complexity assumptions, no efficient algorithm for it exists.

We now provide an alternative statement and proof of Corollary 4.2 in the special case where $X = \{f = 0\}$ is a hypersurface.

Proposition 6.4. *With hypotheses as in Proposition 6.3, f is shift-invariant if and only if there exist linearly independent linear forms $\ell_1, \ldots, \ell_{n-1} \in \mathbb{F}_p[x_1, \ldots, x_n]$ and a polynomial $g \in \mathbb{F}_p[y_1, \ldots, y_{n-1}]$ with new variables $y_1, \ldots, y_{n-1}$ such that $f = g(\ell_1, \ldots, \ell_{n-1})$.*

Proof. First suppose that f is invariant under a nonzero shift $u \in \mathbb{F}_p^n$. We assume without loss of generality that $u_n \neq 0$ and consider the linear invertible change of variables

$$x_1 = y_1 + u_1 y_n, \; x_2 = y_2 + u_2 y_n, \ldots, x_n = u_n y_n,$$

similar to (4.1). By the Chain rule we see that $\mathcal{D}_{y_i} f = \mathcal{D}_{x_i} f$ for $1 \leq i < n$, and

$$\mathcal{D}_{y_n} f = u_1 \mathcal{D}_{x_1} f + u_2 \mathcal{D}_{x_2} f + \cdots + u_n \mathcal{D}_{x_n} f,$$

which equals 0 by Proposition 6.3. Since $\deg f = d < p$, $f(y_1 + u_1 y_n, y_2 + u_2 y_n, \ldots, u_n y_n)$ is separable in y_n, that is, no exponent of y_n is divisible by p. As a consequence, $f(x_1, \ldots, x_n) = f(y_1 + u_1 y_n, y_2 + u_2 y_n, \ldots, u_n y_n)$ does not depend on y_n, and is actually a polynomial $g \in \mathbb{F}_p[y_1, \ldots, y_{n-1}]$. Thus $f = g(\ell_1, \ldots, \ell_{n-1})$ with $\ell_i = x_i - u_i x_n / u_n$ for $i < n$.

On the other hand, suppose that $f = g(\ell_1, \ldots, \ell_{n-1})$ with $g \in \mathbb{F}_p[y_1, \ldots, y_{n-1}]$ and linear forms $\ell_1, \ldots, \ell_{n-1} \in \mathbb{F}_p[x_1, \ldots, x_n]$. Then we can write $y = Ax$ with $A \in \mathbb{F}_p^{(n-1)\times n}$ and let $u \in \mathbb{F}_p^n \setminus \{0\}$ be any vector in the kernel of A. Then f is invariant under the shift u. □

We illustrate the application of Propositions 6.3 and 6.4 with examples of hypersurfaces satisfying the hypotheses of Theorem 3.3 (ii).

Example 6.5. Consider the graph $G = \{x_n = g(x_1, \ldots, x_{n-1})\} \subset \mathbb{F}_q^n$ of $g \in \mathbb{F}_p[x_1, \ldots, x_{n-1}]$ with $p > d = \deg g \geq 2$. Let $f = x_n -$

$g(x_1, \ldots, x_{n-1})$. Then $\#G(\mathbb{F}_p) = p^{n-1}$ and $f \in \mathbb{F}_p[x_1, \ldots, x_n]$ is absolutely irreducible with

$$\mathcal{D}_{x_i} f = -\mathcal{D}_{x_i} g \text{ for } 1 \leq i \leq n-1 \text{ and } \mathcal{D}_{x_n} f = 1.$$

We now show that f is not shift-invariant. According to Proposition 6.3, we should check if there exists $(u_1, \ldots, u_n) \in \mathbb{F}_p^n \setminus \{0\}$ such that

$$u_n = u_1 \mathcal{D}_{x_1} g + \cdots + u_{n-1} \mathcal{D}_{x_{n-1}} g.$$

As $\deg g \geq 2$ and g is separable, this condition is not satisfied for any $(u_1, \ldots, u_n) \in \mathbb{F}_p^n \setminus \{0\}$. Thus Theorem 3.3 (ii) implies

$$\Delta \leq \#U \#(U-U) \cdot d^2 q^{r-1},$$

and for $U = U_h$

$$\begin{aligned} &|\#(G(\mathbb{F}_p) + U_h) - (2h+1)^n p^{n-1}| \\ &\quad \leq (2h+1)^n d^2 \big(p^{n-3/2} + (5d^{7/3} + (4h+1)^n) p^{n-2}\big). \diamondsuit \end{aligned}$$

Example 6.6. For $p > n \geq 2$ and q a power of p, consider the variety $\mathcal{S}_n$ of univariate polynomials $f = \sum_{0 \leq i \leq n} a_i x^i \in \overline{\mathbb{F}}_q[x]$ of degree at most n that are not squarefree. Then $\mathcal{S}_n \subset \mathbb{A}^{n+1}$ is the hypersurface defined by the generic discriminant $\mathrm{disc}_n \in \mathbb{F}_q[a_0, \ldots, a_n]$. As disc_n is absolutely irreducible (see, e.g., Benoist (2012), Théorème 1.7), we check that it is not shift-invariant.

If $f \in \mathbb{F}_q[x]$ has a unique double root $\alpha \in \overline{\mathbb{F}}_p$, then by Gelfand et al. (1994), Chapter 12, Equation (1.28)[1] (compare with Shparlinski (2015)), the following two projective points are equal:

$$[1 : \alpha : \cdots : \alpha^n] = [(\mathcal{D}_{a_0} \mathrm{disc}_n)(f) : (\mathcal{D}_{a_1} \mathrm{disc}_n)(f) : \cdots : (\mathcal{D}_{a_n} \mathrm{disc}_n)(f)].$$

Now, if $u = (u_0, \ldots, u_n) \in \mathbb{F}_p^{n+1}$ is such that

$$\nabla \mathrm{disc}_n \cdot u = 0,$$

where $\nabla \mathrm{disc}_n$ is the gradient of disc_n, then in particular

$$(1, \alpha, \ldots, \alpha^n) \cdot u = 0 \tag{6.9}$$

for any $\alpha \in \mathbb{F}_p$, since there exists some polynomial with α as its unique double root. As $p > n$, there exist pairwise distinct elements $\alpha_0, \ldots, \alpha_n \in \mathbb{F}_p$ for which (6.9) is satisfied. We conclude that u is in the kernel of the $(n+1) \times (n+1)$ Vandermonde matrix defined by $\alpha_0, \ldots, \alpha_n$, which is nonsingular. It follows that $u = 0$, and Proposition 6.3 implies that disc_n is not shift-invariant.

Since $\deg \mathrm{disc}_n = 2n - 1 < 2n$, we obtain

$$\Delta \leq \#U \#(U-U) \cdot (2n)^2 q^{n-1},$$

[1] Although the identity is stated in Gelfand et al. (1994) for the case of characteristic zero, it holds for $p > 2$.

and for $U = U_h \subseteq \mathbb{F}_p$:

$$\begin{aligned}&|\#(\mathcal{S}_n(\mathbb{F}_p) + U_h) - (2h+1)^{n+1}p^n| \\ &\qquad \leq 4n^2(2h+1)^{n+1}\big(p^{n-1/2} + (5(2n)^{7/3} + (4h+1)^{n+1})p^{n-1}\big). \diamondsuit\end{aligned}$$

Example 6.7. Generalizing Example 6.6, for $p > n+m+2$ and q a power of p, we consider the variety $\mathcal{S}_{n,m}$ of pairs of univariate polynomials $f = \sum_{0\leq i\leq n} a_i x^i \in \overline{\mathbb{F}}_q[x]$ and $g = \sum_{0 \leq i \leq m} b_i x^i \in \overline{\mathbb{F}}_q[x]$ of degrees at most n and m that are not coprime. It is well-known that $\mathcal{S}_{n,m} \subset \mathbb{A}^{n+m+2}$ is the hypersurface defined by the generic resultant $\mathrm{res}_{n,m} \in \mathbb{F}_q[a_0, \ldots, a_n, b_0, \ldots, b_m]$. As $\mathrm{res}_{n,m}$ is absolutely irreducible (see, e.g., Mora (2003), Corollary 6.7.2), we check that it is not shift-invariant, using the approach of the previous example.

If $f, g \in \mathbb{F}_q[x]$ have a unique common root $\alpha \in \overline{\mathbb{F}}_q$, then by Gelfand et al. (1994), Chapter 12, Equation (1.11)[2], we have the following identities of projective points:

$$\begin{aligned}[1 : \alpha : \cdots : \alpha^n] &= [(\mathcal{D}_{a_0}\mathrm{res}_{n,m})(f,g) : \cdots : (\mathcal{D}_{a_n}\mathrm{res}_{n,m})(f,g)]\,, \\ [1 : \alpha : \cdots : \alpha^m] &= [(\mathcal{D}_{b_0}\mathrm{res}_{n,m})(f,g) : \cdots : (\mathcal{D}_{b_m}\mathrm{res}_{n,m})(f,g)]\,.\end{aligned}$$

In particular, considering suitable scalar multiples λf and μg of f and g, with nonzero $\lambda, \mu \in \overline{\mathbb{F}}_p$, we have

$$(1, \alpha, \ldots, \alpha^{n+m+1}) = \nabla \mathrm{res}_{n,m}(\lambda f, \mu g) = \lambda^m \mu^n \, \nabla \mathrm{res}_{n,m}(f, g),$$

where $\nabla \mathrm{res}_{n,m}$ is the gradient of $\mathrm{res}_{n,m}$.

Now, if $u = (u_0, \ldots, u_{n+m+1}) \in \mathbb{F}_p^{n+m+2}$ is such that

$$\nabla \mathrm{res}_{n,m} \cdot u = 0,$$

then in particular,

$$(1, \alpha, \ldots, \alpha^{n+m+1}) \cdot u = 0 \tag{6.10}$$

for any $\alpha \in \mathbb{F}_p$, since there exist pairs of polynomials with α as its unique common root. As $p > n+m+2$, there exist pairwise distinct elements $\alpha_1, \ldots, \alpha_{n+m+2} \in \mathbb{F}_p$ for which (6.10) is satisfied. We conclude that u is in the kernel of the $(n+m+2) \times (n+m+2)$ Vandermonde matrix defined by $\alpha_1, \ldots, \alpha_{n+m+2}$, which is nonsingular. It follows that $u = 0$, and Proposition 6.3 implies that $\mathrm{res}_{n,m}$ is not shift-invariant.

Since $\deg \mathrm{res}_{n,m} = n+m$, we obtain

$$\Delta \leq \#U \#(U-U) \cdot (n+m)^2 q^{n+m},$$

and for $U = U_h \subseteq \mathbb{F}_p$:

$$\begin{aligned}&|\#(\mathcal{S}_{n,m}(\mathbb{F}_p) + U_h) - (2h+1)^{n+m+2}p^{n+m+1}| \\ &\leq (n+m)^2(2h+1)^{n+m+2}p^{n+m}\big(p^{1/2} + 5(n+m)^{7/3} + (4h+1)^{n+m+2}\big). \diamondsuit\end{aligned}$$

[2] Although the identity is stated in Gelfand et al. (1994) for the case of characteristic zero, it holds for $p > 2$.

7. Computational hardness of detecting shift-freeness

A natural question concerns the algorithmic aspect of shift-freeness: can we determine efficiently whether a variety is U-shift-free? Single polynomials can be tested for $\mathbb{F}_q^n$-shift-freeness in polynomial time, using (6.6). However, the neighborhood given by $U = \mathbb{F}_q^n$ is not relevant in our context, since then $X + U = \mathbb{F}_q^n$ for any X.

For more interesting neighborhoods U, the answer to the above question is negative: the problem of determining U_h-shift-freeness turns out to be coNP-complete under randomized reductions. This means that under standard complexity assumptions, no efficient algorithm exists for this task. This holds even for the special case where the variety X is a hyperplane $\{f = 0\}$ with a linear f and $U = U_h$ is a standard neighborhood, already for $h = 1$.

For a fixed $u \in \mathbb{F}_q^n$ and hypersurfaces $X = \{f = 0\}$ and $Y = \{g = 0\}$ with squarefree polynomials f and g and leading coefficients (in some term order) a and b, respectively, we have $X = Y^{(u)}$ if and only if $bf(x) - ag(x - u) = 0$. This can be tested in random polynomial time (with one-sided error) by evaluating that difference at $x = c$ for uniformly random points c in a large enough finite subset of $\overline{\mathbb{F}}_p^n$. This works even in a very concise presentation by a "black box" which produces the values of polynomials in unit time.

Our starting point is the decision problem Equal subset sum, whose input is a sequence $(a_1, \ldots, a_n)$ of nonnegative integers presented in binary. The task is to decide whether there exist two disjoint nonempty sets $S, T \subseteq \{1, \ldots, n\}$ with $\sum_{i \in S} a_i = \sum_{i \in T} a_i$. Woeginger and Yu (1992) show that it is NP-complete. It is a variant of Partition, one of the "original" NP-complete problems.

The variant Equal subset sum modulo prime has $(a_1, \ldots, a_n)$ as above and a prime p (in binary) as input, and the question is again whether subsets S and T as above exists, now with $\sum_{i \in S} a_i \equiv \sum_{i \in T} a_i \bmod p$.

Our interest is in the decision problem Non-shiftfreeness. We only consider the simple version with a standard neighborhood U_h and a single polynomial $f \in \mathbb{F}_p[x_1, \ldots, x_n]$ of total degree at most d. The input is presented by the prime p and an integer h with $p > 2h > 2$ in binary, n and d in unary, and f in dense representation. That is, for each exponent vector $(e_1, \ldots, e_n)$ with $\sum_{1 \leq i \leq n} e_i \leq d$, the coefficient of x^e in f is given in binary. The task is to decide whether there exists a nonzero $u \in U_h$ with $f = f^{(u)}$.

For two decision problems A and B, we write $A \leq_p B$ if there exists a deterministic polynomial-time reduction from A to B, and $A \leq_r B$ if there is some randomized polynomial-time reduction from A to B. The notion here is "Las Vegas", that is, the reduction returns either the correct answer or "fail"; the latter with probability at most $1/2$. The corresponding complexity class is called ZPP (zero error probabilistic polynomial time).

Theorem 7.1. *We have*

$$\begin{aligned}\textsc{Equal subset sum} &\leq_r \textsc{Equal subset sum modulo prime}\\ &\leq_p \textsc{Non-shiftfreeness} \in \mathit{NP}.\end{aligned}$$

Proof. For the first reduction, on input of nonnegative integers $(a_1, \ldots, a_n)$, we randomly choose a prime $p > \sum_{1 \leq i \leq n} a_i$ and consider Equal subset sum modulo prime with input $((a_1, \ldots, a_n), p)$. The random choice is done by choosing integers larger than $b = \sum_{1 \leq i \leq n} a_i$, testing them deterministically for primality and accepting the first one that is certified to be prime. Since the length of b is polynomial in the input size, all this can be done error-free in polynomial expected time. It is the only step where randomization intervenes. If prime gaps were of polynomial size, this could even be done deterministically.

If (S, T) is a solution for the Equal subset sum instance, then it is also one for this instance of Equal subset sum modulo prime. On the other hand, suppose that (S, T) is a solution for this Equal subset sum modulo prime instance, so that $\sum_{i \in S} a_i \equiv \sum_{i \in T} a_i \bmod p$. We denote the two sums, taken as integers, as b_S and b_T, respectively. Then there exists an integer k with $b_S - b_T = kp$ in $\mathbb{Z}$. But $|b_S - b_T| \leq b < p$, so that $k = 0$ and (S, T) is also a solution for Equal subset sum.

For Equal subset sum modulo prime $\leq_p$ Non-shiftfreeness, on input $((a_1, \ldots, a_n), p)$ with all $a_i \in \mathbb{F}_p$, we take the linear form $f = \sum_{1 \leq i \leq n} a_i x_i \in \mathbb{F}_p[x_1, \ldots, x_n]$ and $U_1 = \{0, 1, -1\}^n \subseteq \mathbb{F}_p^n$. Then $\mathcal{D}_{x_i}(f) = a_i$ for all i. By Proposition 6.3, f is shift-invariant under some $u \in U_1$ if and only if $\sum_{1 \leq i \leq n} a_i u_i = 0$. We set up a bijection between U_1 and pairs of disjoint nonempty subsets $S, T \subseteq \{1, \ldots, n\}$ by requiring for each $i \in \{1, \ldots, n\}$:

$$i \in S \Longleftrightarrow u_i = 1; \quad i \in T \Longleftrightarrow u_i = -1.$$

This bijection maps solutions u of Non-shiftfreeness to solutions (S, T) of Equal subset sum modulo prime, and vice versa. Furthermore, the reduction can be executed in deterministic polynomial time.

For Non-shiftfreeness $\in$ NP, we have some u with $f = f^{(u)} = f(x - u)$. Since the input f is given in dense representation, we can compute the dense representation of $f(x - u)$ in polynomial time, and then compare it to that of f. □

It follows that Non-shiftfreeness is NP-complete under randomized reductions, and the natural complementary problem Shiftfreeness is similarly coNP-complete. Under standard complexity assumptions, no efficient algorithm for it exists.

Open questions

When $u \in \mathbb{F}_q$ and two varieties X and Y are given, can we test efficiently whether $X = Y^{(u)}$? When $X = Y$? For hypersurfaces, this is feasible; see above.

When Y is absolutely irreducible, $u \in U$ nonzero, and $X = Y \cup Y^{(u)}$, what can we say about question (Q)?

Acknowledgements

Many thanks go to Igor Shparlinski who mentioned this problem to us, on a visit by JvzG to Sydney. We are grateful to Heiko Röglin for pointing the reference Woeginger and Yu (1992) out to us, and to anonymous referees for their comments and valuable suggestions.

References

C. Beltrán, L. M. Pardo, Estimates on the distribution of the condition number of singular matrices, Foundations of Computational Mathematics 7 (2007) 87–134.

O. Benoist, Degrés d'homogénéité de l'ensemble des intersections complètes singulières, Ann. Inst. Fourier (Grenoble) 62 (2012) 1189–1214.

W. Bruns, U. Vetter, Determinantal rings, volume 1327 of *Lecture Notes in Math.*, Springer, Berlin Heidelberg New York, 1988.

A. Cafure, G. Matera, Improved explicit estimates on the number of solutions of equations over a finite field, Finite Fields Appl. 12 (2006) 155–185.

S. Cohen, Uniform distribution of polynomials over finite fields, J. Lond. Math. Soc. (2) 6 (1972) 93–102.

J. W. Demmel, The probability that a numerical analysis problem is difficult, Mathematics of Computation 50 (1988) 449–480.

A. Edelman, Eigenvalues and condition numbers of random matrices, SIAM Journal on Matrix Analysis and Applications 9 (1988) 543–560.

A. Edelman, On the distribution of a scaled condition number, Mathematics of Computation 58 (1992) 185–190.

W. Fulton, Intersection Theory, Springer, Berlin Heidelberg New York, 1984.

J. von zur Gathen, G. Matera, Density of real and complex decomposable univariate polynomials, Quart. J. Math. 68 (2017) 1227–1246.

I. Gelfand, M. Kapranov, A. Zelevinsky, Discriminants, Resultants, and Multidimensional Determinants, Birkhäuser, Boston, 1994.

J. Harris, Algebraic Geometry: a first course, volume 133 of *Grad. Texts in Math.*, Springer, New York Berlin Heidelberg, 1992.

J. Heintz, Definability and fast quantifier elimination in algebraically closed fields, Theoret. Comput. Sci. 24 (1983) 239–277.

H. Hotelling, Tubes and spheres in n-spaces, and a class of statistical problems, American Journal of Mathematics 61 (1939) 440–460.

V. Hribernig, H. J. Stetter, Detection and Validation of Clusters of Polynomial Zeros, Journal of Symbolic Computation 24 (1997) 667–682.

T. Mora, Solving polynomial equation systems. Vol. I. The Kronecker-Duval philosophy, volume 88 of *Encyclopedia Math. Appl.*, Cambridge Univ. Press, Cambridge, 2003.

G. Mullen, D. Panario, Handbook of finite fields, CRC Press, Boca Raton, FL, 2013.

J. Renegar, On the efficiency of Newton's method in approximating all zeros of a system of complex polynomials, Mathematics of Operations Research 12 (1987) 121–148.

A. Schönhage, Quasi-GCD Computations, Journal of Complexity 1 (1985) 118–137.

I. Shparlinski, Distribution of polynomial discriminants modulo a prime, Arch. Math. 105 (2015) 251–259.

S. Smale, The fundamental theorem of algebra and complexity theory, Bulletin of the American Mathematical Society 4 (1981) 1–36.

W. Vogel, Results on Bézout's theorem, volume 74 of *Tata Inst. Fundam. Res. Lect. Math.*, Tata Inst. Fund. Res., Bombay, 1984.

H. Weyl, On the volume of tubes, American Journal of Mathematics 61 (1939) 461–472.

G. J. Woeginger, Z. Yu, On the equal-subset-sum problem, Inform. Process. Lett. 42 (1992) 299–301.

[1]B-IT, Universität Bonn, D-53113 Bonn
E-mail address: gathen@bit.uni-bonn.de

[2]Instituto del Desarrollo Humano, Universidad Nacional de General Sarmiento, J.M. Gutiérrez 1150 (B1613GSX) Los Polvorines, Buenos Aires, Argentina

[3]National Council of Science and Technology (CONICET), Argentina

[4]Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Ciudad Universitaria, Pabellón I (1428) Buenos Aires, Argentina
E-mail address: gmatera@dm.uba.ar