Journal of Number Theory 133 (2013) 1409–1434

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

The number of reducible space curves over a finite field ☆

Eda Cesaratto [a,b,*], Joachim von zur Gathen [c], Guillermo Matera [a,b]

[a] Instituto del Desarrollo Humano, Universidad Nacional de General Sarmiento, J.M. Gutiérrez 1150 (B1613GSX), Los Polvorines, Buenos Aires, Argentina
[b] National Council of Science and Technology (CONICET), Argentina
[c] B-IT, Universität Bonn, D-53113 Bonn, Germany

ARTICLE INFO

Article history:
Received 19 July 2011
Accepted 31 August 2012
Available online xxxx
Communicated by D. Wan

Keywords:
Finite fields
Rational points
Algebraic curves
Asymptotic behavior
Chow variety
Irreducibility
Absolute irreducibility

ABSTRACT

"Most" hypersurfaces in projective space are irreducible, and rather precise estimates are known for the probability that a random hypersurface over a finite field is reducible. This paper considers the parametrization of space curves by the appropriate Chow variety, and provides bounds on the probability that a random curve over a finite field is reducible.

1. Introduction

The Prime Number Theorem and a well-known result of Gauß describe the density of primes and of irreducible univariate polynomials over a finite field, respectively. "Most" numbers are composite, and "most" polynomials reducible. The latter changes drastically for two are more variables, where "most" polynomials are irreducible.

Approximations to the number of reducible multivariate polynomials go back to Leonard Carlitz and Stephen Cohen in the 1960s. This question was recently taken up by Bodin [2] and Hou and

☆ Joachim von zur Gathen was supported by the B-IT Foundation and the Land Nordrhein–Westfalen. Eda Cesaratto and Guillermo Matera were partially supported by grant PIP 11220090100421 CONICET.

* Corresponding author at: Instituto del Desarrollo Humano, Universidad Nacional de General Sarmiento, J.M. Gutiérrez 1150 (B1613GSX), Los Polvorines, Buenos Aires, Argentina.

E-mail addresses: ecesarat@ungs.edu.ar (E. Cesaratto), gathen@bit.uni-bonn.de (J. von zur Gathen), gmatera@ungs.edu.ar (G. Matera).

0022-314X/$ – see front matter
http://dx.doi.org/10.1016/j.jnt.2012.08.027

Mullen [16]. The sharpest bounds are due to von zur Gathen [8] for bivariate and von zur Gathen et al. [9] for multivariate polynomials.

From a geometric perspective, these results say that almost all hypersurfaces are irreducible, and provide approximations to the number of reducible ones, over a finite field. Can we say something similar for other types of varieties?

This paper gives an affirmative answer for curves in $\mathbb{P}^r$ for arbitrary r. A first question is how to parametrize the curves. Moduli spaces only include irreducible curves, and systems of defining equations do not work except for complete intersections. The natural parametrization is by the Chow variety $\mathcal{C}_{d,r}$ of curves of degree d in $\mathbb{P}^r$, for some fixed d and r. The foundation of our work are the results by Eisenbud and Harris [6], who identified the irreducible components of $\mathcal{C}_{d,r}$ of maximal dimension. It turns out that there is a threshold $d_0(r) = 4r - 8$ so that for $d \geqslant d_0(r)$, most curves are irreducible, and for $d < d_0(r)$, most are reducible. This assumes $r \geqslant 3$; the planar case $r = 2$ is solved in the papers cited above, and single lines, with $d = 1$, are a natural exception.

Over a finite field, we obtain the following bounds for curves chosen uniformly at random from $\mathcal{C}_{d,r}$. For $d \geqslant d_0(r)$, Theorem 16 provides upper and lower bounds on the probability that the curve is reducible over $\mathbb{F}_q$. For $d \geqslant 6r - 12$, Corollary 19 does so for the probability that the curve is relatively irreducible over $\mathbb{F}_q$, that is, irreducible over $\mathbb{F}_q$ and absolutely reducible. For any d and r as above, both bounds tend to zero with growing q. In fact, the rate of convergence in terms of q is the same in the upper and lower bounds, with (different) coefficients depending only on d and r. Furthermore, we prove an "average-case Weil bound", estimating the absolute difference between $q + 1$ and the expected number of $\mathbb{F}_q$-points on a curve defined over $\mathbb{F}_q$.

All our estimates are explicit, without unspecified constants. The main technical tools are Bézout type estimates of the degrees of certain varieties, such as the incidence correspondence expressing that a curve in $\mathcal{C}_{d,r}$ is contained in the variety defined by a system of equations.

The structure of the paper is as follows. Section 2 introduces basic notations and facts, mainly concerning the Bézout inequality and Chow varieties. Section 3 determines the codimension of the set of reducible curves, for $d \geqslant d_0(r)$. This is mainly based on [6]. Section 4 bounds, in several steps, the degree of the Chow variety $\mathcal{C}_{d,r}$. These estimates form the technical core of this paper. Section 5 draws the conclusions for the probability of having a reducible curve, and Section 6 applies our technology to relatively irreducible curves. The final Section 7 yields an average Weil estimate.

2. Notions and notations

Let $\mathbb{F}_q$ be a finite field of $q = p^m$ elements, where p is a prime number, let $\overline{\mathbb{F}}_q$ be an algebraic closure, and let $\mathbb{P}^r = \mathbb{P}^r(\overline{\mathbb{F}}_q)$ denote the r-dimensional projective space over $\overline{\mathbb{F}}_q$. Let $\mathbb{P}^{r*}$ denote the dual projective space of $\mathbb{P}^r$, that is, $\mathbb{P}^{r*} = \mathbb{P}((\overline{\mathbb{F}}_q^{\,r+1})^*)$. Let $\mathbb{G}(k, r)$ denote the Grassmannian of k-dimensional linear spaces (k-planes for short) in $\mathbb{P}^r$. We shall also denote by $\mathbb{A}^{r+1} = \mathbb{A}^{r+1}(\overline{\mathbb{F}}_q)$ the affine $(r + 1)$-dimensional space over $\overline{\mathbb{F}}_q$.

Let $\mathbb{K}$ be a subfield of $\overline{\mathbb{F}}_q$ containing $\mathbb{F}_q$, and let $\mathbb{K}[X_0, \ldots, X_r]$ denote the ring of $(r + 1)$-variate polynomials in indeterminates $X_0, \ldots, X_r$ and coefficients in $\mathbb{K}$. Let V be a $\mathbb{K}$-definable projective subvariety of $\mathbb{P}^r$ (a $\mathbb{K}$-variety for short), namely the set of common zeros in $\mathbb{P}^r$ of a finite set of homogeneous polynomials of $\mathbb{K}[X_0, \ldots, X_r]$. For homogeneous polynomials $f_1, \ldots, f_s \in \mathbb{K}[X_0, \ldots, X_r]$, we shall use the notations $V(f_1, \ldots, f_s)$ or $\{f_1 = 0, \ldots, f_s = 0\}$ to denote the $\mathbb{K}$-variety V defined by $f_1, \ldots, f_s$. We shall denote by $I(V) \subset \mathbb{K}[X_0, \ldots, X_r]$ its defining ideal and by $\mathbb{K}[V]$ its coordinate ring, namely the quotient ring $\mathbb{K}[V] = \mathbb{K}[X_0, \ldots, X_r]/I(V)$. For any $d \geqslant 0$ we shall denote by $(\mathbb{K}[V])_d$ the dth graded homogeneous piece of the grading of the coordinate ring $\mathbb{K}[V]$ induced by the canonical grading of $\mathbb{K}[X_0, \ldots, X_r]$.

2.1. Degree and Bézout type inequalities

For an irreducible variety $V \subset \mathbb{P}^r$, we define its *degree* $\deg V$ as the maximum number of points lying in the intersection of V with a linear variety $L \subset \mathbb{P}^r$ of codimension $\dim V$ for which $\#(V \cap L)$ is finite. More generally, if $V = C_1 \cup \cdots \cup C_N$ is the decomposition of V into irreducible components, we define the degree of V as $\deg V = \sum_{i=1}^{N} \deg C_i$ (cf. [14]).

An important tool for our estimates is the *Bézout inequality* (see [14,7,21,5]): if V and W are subvarieties of $\mathbb{P}^r$, then the following inequality holds:

$$\deg(V \cap W) \leqslant \deg V \cdot \deg W. \tag{1}$$

The following inequality of Bézout type will also be useful (see [15, Proposition 2.3]): if $V_1, \ldots, V_s$ are subvarieties of $\mathbb{P}^r$, then

$$\deg(V_1 \cap \cdots \cap V_s) \leqslant \deg V_1 \Big(\max_{2 \leqslant i \leqslant s} \deg V_i \Big)^{\dim V_1}. \tag{2}$$

We mention another variant of (2) and [5, Lemma 1.28], adapted to our purposes.

Lemma 1. *Let U be an open subset of $\mathbb{P}^r$, let $V = V(f_1, \ldots, f_m)$ be a subvariety of $\mathbb{P}^r$ defined by homogeneous polynomials of degree d and let V_s denote the union of the irreducible components of V of codimension at most s, then*

$$\deg(U \cap V_s) \leqslant d^s. \tag{3}$$

Proof. Fix arbitrarily a point $\boldsymbol{x} \in \mathbb{P}^r \setminus V$. Then we may choose $a_{1,1}, \ldots, a_{1,m} \in \overline{\mathbb{F}}_q$ with $\sum_{j=1}^m a_{1,j} f_j(\boldsymbol{x}) \neq 0$. Setting $g_1 = \sum_{j=1}^m a_{1,j} f_j$, we have that $\{g_1 = 0\}$ is an equidimensional projective variety of dimension $r-1$ containing V.

Consider now the decomposition $\{g_1 = 0\} = \bigcup_{i=1}^n C_i$ of $\{g_1 = 0\}$ into irreducible components. Suppose that C_i is not contained in V for $1 \leqslant i \leqslant n_1$ and it is contained in V (and hence it is a component of V) for $n_1 + 1 \leqslant i \leqslant n$. Then there exist $\boldsymbol{x}^{(2,i)} \in C_i \setminus V$ for $1 \leqslant i \leqslant n_1$, and $a_{2,1}, \ldots, a_{2,m} \in \overline{\mathbb{F}}_q$ such that no point $\boldsymbol{x}^{(2,i)}$ is a zero of the polynomial $g_2 = \sum_{j=1}^m a_{2,j} f_j$. Observe that $\{g_1 = 0, g_2 = 0\}$ contains all the components of V of codimension at most 2 among its irreducible components.

Arguing inductively, we see that there exist homogeneous polynomials $g_1, \ldots, g_s \in \overline{\mathbb{F}}_q[X_0, \ldots, X_r]$ of degree d with the following property: all the irreducible components of V of codimension at most s are irreducible components of $\{g_1 = 0, \ldots, g_s = 0\}$. In particular, all the irreducible components of V_s are irreducible components of $\{g_1 = 0, \ldots, g_s = 0\}$. By the definition of degree and the Bézout inequality (1) it follows that $\deg(U \cap V_s) \leqslant d^s$, which finishes the proof of the lemma. □

Finally, we shall also use the following well-known inequality, which is proved here for lack of a suitable reference.

Lemma 2. *Let V be a projective subvariety of $\mathbb{P}^r$ and let $F = (f_0, \ldots, f_s) : V \to \mathbb{P}^s$ be a regular mapping defined by homogeneous polynomials of degree d. If m denotes the dimension of $F(V)$, then* $\deg F(V) \leqslant \deg V \cdot d^m$.

Proof. We may assume without loss of generality that V is irreducible. Then $F(V)$ is an irreducible variety of $\mathbb{P}^s$. Let $H_1, \ldots, H_m$ be hyperplanes of $\mathbb{P}^s$ such that $\#(F(V) \cap H_1 \cap \cdots \cap H_m) = \deg F(V)$ holds. Let $\mathcal{S} = F(V) \cap H_1 \cap \cdots \cap H_m$. Then

$$F^{-1}(\mathcal{S}) = V \cap F^{-1}(H_1) \cap \cdots \cap F^{-1}(H_m).$$

Observe that $F^{-1}(H_i) = V \cap \{g_i = 0\}$, where g_i is a linear combination of the polynomials $f_0, \ldots, f_s$ for $i = 1, \ldots, m$. Therefore, by the Bézout inequality (1) it follows that $\deg F^{-1}(\mathcal{S}) \leqslant \deg V \cdot d^m$ holds. Let $F^{-1}(\mathcal{S}) = \bigcup_{i=1}^N C_i$ be the decomposition of $F^{-1}(V)$ into irreducible components. Since $F(F^{-1}(\mathcal{S})) = \mathcal{S}$ and each irreducible component C_i of $F^{-1}(\mathcal{S})$ is mapped by F to a point of $\mathcal{S}$, we have

$$\deg F(V) = \#(\mathcal{S}) \leqslant N \leqslant \sum_{i=1}^{N} \deg C_i = \deg F^{-1}(\mathcal{S}) \leqslant \deg V \cdot d^m.$$

This finishes the proof of the lemma. □

2.2. $\mathbb{F}_q$-rational points

The set of $\mathbb{F}_q$-rational points of V, namely $V \cap \mathbb{P}^r(\mathbb{F}_q)$, is denoted by $V(\mathbb{F}_q)$. In some simple cases it is possible to determine the exact value of $\#V(\mathbb{F}_q)$. For instance, the number p_r of elements of $\mathbb{P}^r(\mathbb{F}_q)$ is given by $p_r = q^r + q^{r-1} + \cdots + q + 1$. In what follows we shall use repeatedly the following elementary upper bound on the number of $\mathbb{F}_q$-rational points of a projective variety V of dimension s and degree d (see, e.g., [11, Proposition 12.1] or [4, Proposition 3.1]):

$$\#V(\mathbb{F}_q) \leqslant dp_s \leqslant 2dq^s. \tag{4}$$

2.3. Chow varieties of curves

Suppose that $r \geqslant 2$ and fix $d > 0$. Consider the incidence variety

$$\Psi = \big\{(\boldsymbol{x}, H_1, H_2) \in \mathbb{P}^r \times \mathbb{P}^{r*} \times \mathbb{P}^{r*} \colon \boldsymbol{x} \in H_1 \cap H_2\big\}.$$

Let $\pi : \Psi \to \mathbb{P}^r$ and $\eta : \Psi \to \mathbb{P}^{r*} \times \mathbb{P}^{r*}$ denote the standard projections. Fix a curve $C \subset \mathbb{P}^r$ of degree d and consider the "restricted" incidence variety

$$\Psi_C = \pi^{-1}(C) = \big\{(\boldsymbol{x}, H_1, H_2) \in C \times \mathbb{P}^{r*} \times \mathbb{P}^{r*} \colon \boldsymbol{x} \in H_1 \cap H_2\big\}.$$

It turns out that $\eta(\Psi_C)$ is a bihomogeneous hypersurface of $\mathbb{P}^{r*} \times \mathbb{P}^{r*}$ of bidegree (d, d) (see, e.g., [13, Lecture 21]). This hypersurface is thus defined by a reduced bihomogeneous polynomial $F_C \in \overline{\mathbb{F}}_q[\boldsymbol{A}, \boldsymbol{B}] = \overline{\mathbb{F}}_q[A_0, \ldots, A_r, B_0, \ldots, B_r]$ of bidegree (d, d), unique up to scaling by nonzero elements of $\overline{\mathbb{F}}_q$. In this way, we see that $\eta(\Psi_C)$ can be represented by a point $[F_C]$ in the projective space $\mathbb{PV}_{d,r}$, where $\mathbb{V}_{d,r}$ denotes the vector subspace of $\overline{\mathbb{F}}_q[\boldsymbol{A}, \boldsymbol{B}]$ spanned by all the bihomogeneous polynomials of bidegree (d, d). The point $[F_C]$ is called the *Chow form* of C. The Zariski closure in $\mathbb{PV}_{d,r}$ of the set of points $[F_C]$, where C runs over the set of curves (equidimensional varieties of dimension 1) of degree d of $\mathbb{P}^r$, is called the *Chow variety* of curves of degree d in $\mathbb{P}^r$ and denoted by $\mathcal{C}_{d,r}$.

2.3.1. The correspondence between degree-d cycles in $\mathbb{P}^r$ and points in $\mathbb{PV}_{d,r}$

Each point of the Chow variety $\mathcal{C}_{d,r}$ actually corresponds to a unique *effective cycle* on $\mathbb{P}^r$ of dimension 1 and degree d, that is, to a formal linear combination $\sum a_i C_i$, where each C_i is an irreducible curve of $\mathbb{P}^r$, each a_i is a positive integer and $\sum a_i \deg(C_i) = d$. Such a correspondence is defined assigning to each cycle $\sum a_i C_i$ the point of $\mathbb{PV}_{d,r}$ determined by the polynomial $\prod_i F_{C_i}^{a_i}$, where F_{C_i} is a minimal-degree defining polynomial of the hypersurface $\eta(\Psi_{C_i})$ for each i.

Let $\sum a_i C_i$ be an effective cycle of dimension 1 and degree d and let $[F] \in \mathcal{C}_{d,r}$ be the corresponding Chow form. Let $\{f_\lambda \colon \lambda \in \Lambda\}$ be the set of all nonzero coefficients of F. Following, e.g., [18, Exercise I.1.18], we define the *smallest field of definition* of $[F]$ as the field extension $\mathbb{K}$ of $\mathbb{F}_p$ determined by the fractions of nonzero coefficients of F, namely $\mathbb{K} = \mathbb{F}_p(f_\lambda/f_\mu \colon \lambda, \mu \in \Lambda)$. It follows that there exists a scalar multiple of F with coefficients in $\mathbb{K}$, and there are no scalar multiples of F with coefficients in a proper subfield of $\mathbb{K}$. For an arbitrary subfield $\mathbb{K}$ of $\overline{\mathbb{F}}_q$, we say that an effective cycle $\sum a_i C_i$ is $\mathbb{K}$-definable (a $\mathbb{K}$-cycle for short) if the smallest field of definition of its Chow form $[\prod_i F_{C_i}^{a_i}]$ is a subfield of $\mathbb{K}$. We use the following result.

Theorem 3. *(See [18, Corollary I.3.24.5].) Let $\mathbb{K}$ be a subfield of $\overline{\mathbb{F}}_q$. There exists a one-to-one correspondence between the set of effective $\mathbb{K}$-cycles of dimension 1 and degree d and the set of $\mathbb{K}$-rational points in the Chow variety $\mathcal{C}_{d,r}$.*

The inverse of the correspondence of Theorem 3 can be explicitly described in the following terms. Let $[F]$ be a point of $\mathcal{C}_{d,r}$ with F reduced. We define the *support* of $[F]$ by

$$\operatorname{supp}(F) = \left\{ \boldsymbol{x} \in \mathbb{P}^r \colon \pi^{-1}(\boldsymbol{x}) \subset \eta^{-1}(V_F) \right\}, \tag{5}$$

where V_F is the hypersurface of $\mathbb{PV}_{d,r}$ defined by F. We have $\operatorname{supp}(F_C) = C$ for every curve $C \subset \mathbb{P}^r$ of degree d (see, e.g., [13, Lecture 21]). This identity is extended straightforwardly to cycles by taking into account the multiplicity of each factor of F.

2.3.2. Reducible and $\mathbb{K}$-reducible cycles

If $\mathbb{K}$ is a subfield of $\overline{\mathbb{F}}_q$, an effective $\mathbb{K}$-cycle C is called $\mathbb{K}$-*reducible* if there exist $s \geqslant 2$ and effective $\mathbb{K}$-cycles $C_1, \ldots, C_s$ such that $C = \sum_{i=1}^{s} C_i$ holds. When $\mathbb{K} = \overline{\mathbb{F}}_q$ we shall omit the reference to the field of definition and simply speak about (*absolutely*) *reducible* effective cycles.

The set $\mathcal{R}_{d,r}$ of reducible effective cycles of $\mathbb{P}^r$ of dimension 1 and degree d is a closed subset of the Chow variety $\mathcal{C}_{d,r}$. In order to prove this, fix $1 \leqslant k \leqslant d-1$ and consider the Chow varieties $\mathcal{C}_{k,r}$ and $\mathcal{C}_{d-k,r}$. We have a regular map

$$\mu_{k,d,r} : \mathcal{C}_{k,r} \times \mathcal{C}_{d-k,r} \to \mathcal{C}_{d,r},$$

which is induced by the multiplication mapping $\mathbb{PV}_{k,r} \times \mathbb{PV}_{d-k,r} \to \mathbb{PV}_{d,r}$. It is easy to see that the following identity holds:

$$\mathcal{R}_{d,r} = \bigcup_{1 \leqslant k \leqslant d/2} \operatorname{im}(\mu_{k,d,r}). \tag{6}$$

Since $\mathcal{C}_{k,r} \times \mathcal{C}_{d-k,r}$ is a projective variety and the image of a projective variety under a regular map is closed we conclude that $\mathcal{R}_{d,r}$ is a closed subset of $\mathcal{C}_{d,r}$.

3. The codimension of the variety of reducible curves

The irreducibility of a single polynomial over a finite field shows a qualitatively different behavior between one and at least two variables. In the former case, fairly few (a fraction of about $1/d$ at degree $d \geqslant 2$) are irreducible, while in the latter case almost all (a fraction of about $1 - q^{-d+1}$ over $\mathbb{F}_q$) are irreducible. One may wonder whether such a qualitative jump also occurs for systems of more than one polynomial. We consider this question in a special case, namely where the equations define a curve in $\mathbb{P}^r$. It turns out that there is a threshold $d_0(r) = 4r - 8$ for the degree where this jump occurs. At lower degrees, curves are generically reducible (with single lines, of degree 1, as a natural exception), while at degree $d \geqslant d_0(r)$ a generic curve is irreducible.

The qualitative result follows from the work of Eisenbud and Harris [6]. Our contribution are quantitative estimates for the fractions under consideration. Fairly precise bounds are available for single polynomials (that is, planar curves). Similarly, our lower and upper bounds for $d \geqslant d_0(r)$ are given by the same power of q, but with two different coefficients depending on d and r.

The foundation for our work are the following results from [6]. They consider two irreducible subvarieties of $\mathcal{C}_{d,r}$:

$$dG(1,r) = \left\{ \text{sums of } d \text{ lines in } \mathbb{P}^r \right\},$$
$$P(d,r) = \left\{ \text{plane curves of degree } d \text{ in } \mathbb{P}^r \right\}.$$

It is easy to see that, for $d \geqslant 2$,

$$\dim dG(1,r) = 2d(r-1),$$
$$\dim P(d,r) = 3(r-2) + d(d+3)/2.$$

Fact 4. *(See [6, Theorems 1 and 3].) Let $d \geqslant 2$ and $r \geqslant 3$. Then*

$$\dim \mathcal{C}_{d,r} = \max\bigl\{2d(r-1), 3(r-2) + d(d+3)/2\bigr\}. \tag{7}$$

For $r = 3$ and $d \geqslant 4$, and for $r \geqslant 4$, either $dG(1,r)$ or $P(d,r)$ is the unique irreducible component of maximal dimension.

We let $\mathcal{R}_{d,r} = \{C \in \mathcal{C}_{d,r}\colon\ C \text{ is reducible}\}$. In the case $(d,r) = (2,3)$, both $\mathcal{R}_{2,3} = 2G(1,3)$ and $P(2,3)$ have dimension 8, so that $\operatorname{codim}_{\mathcal{C}_{d,r}} \mathcal{R}_{d,r} = 0$. In the case $(d,r) = (3,3)$, we have $\mathcal{R}_{3,3} \supset 3G(1,3)$ and both $3G(1,3)$ and $P(3,3)$ have dimension 12, so that $\operatorname{codim}_{\mathcal{C}_{d,r}} \mathcal{R}_{d,r} = 0$. We have

$$2d(r-1) \leqslant 3(r-2) + \frac{d(d+3)}{2} \quad \Leftrightarrow \quad 4r - \frac{17}{2} - \frac{3}{2(2d-3)} \leqslant d,$$

and also equalities in the two conditions correspond to each other. Since $3/(2d-3)$ is not an integer for $d > 3$, $dG(1,r)$ and $P(d,r)$ never have the same dimension except for $d = 1$, where $P(1,r) = 1G(1,r) = G(1,r)$ has dimension $2(r-1)$, and for the exceptional cases from above, where

$$(d,r) \text{ is } (2,3) \text{ or } (3,3). \tag{8}$$

Furthermore, $3/2(2d-3) < 1/2$ for $d > 3$. We abbreviate $b_{d,r} = \dim \mathcal{C}_{d,r}$ and reword Fact 4 as follows.

Fact 5. *Let $d \geqslant 2$ and $r \geqslant 3$. Then*

$$b_{d,r} = \dim \mathcal{C}_{d,r} = \begin{cases} 3(r-2) + d(d+3)/2 & \text{if } d \geqslant 4r-8, \\ 2d(r-1) & \text{otherwise}. \end{cases}$$

$\mathcal{C}_{d,r}$ has exactly one component of maximal dimension, namely $P(d,r)$ and $dG(1,r)$ in the first and second case, respectively, except for (8).

When $d < 4r-8$ and excepting (8), then $dG(1,r)$ is the dominant component of $\mathcal{C}_{d,r}$ and a generic curve in $\mathcal{C}_{d,r}$ is reducible. On the other hand, for $d \geqslant 4r-8$ the generic curve is irreducible, and we now want to determine the codimension of the reducible ones. For planar curves and $d \geqslant 2$ this codimension is $d-1$, and the dominating component in the reducible ones consists of curves that are a union of a line and an irreducible (planar) curve of degree $d-1$ (see [8, Theorem 2.1]). For $r \geqslant 3$, the dimension of this set of curves is $2(r-1) + 3(r-2) + (d-1)(d+2)/2$ when $d \geqslant 4r-7$, and the codimension is $d - 2r + 3$.

Fix $1 \leqslant k \leqslant d-1$ and consider the Chow varieties $\mathcal{C}_{k,r}$ and $\mathcal{C}_{d-k,r}$. Recall the morphism

$$\mu_{k,d,r} : \mathcal{C}_{k,r} \times \mathcal{C}_{d-k,r} \to \mathcal{C}_{d,r},$$

induced by the multiplication mapping $\mathbb{PV}_{k,r} \times \mathbb{PV}_{d-k,r} \to \mathbb{PV}_{d,r}$. Our aim is to bound in (6) the dimension of the image $\operatorname{im}(\mu_{k,d,r})$ of $\mu_{k,d,r}$.

Theorem 6. *Let $r \geqslant 3$ and $d \geqslant 4r-8$. Then*

$$\operatorname{codim}_{\mathcal{C}_{d,r}} \mathcal{R}_{d,r} = \begin{cases} r-2 & \text{if } d = 4r-8, \\ d-2r+3 & \text{otherwise}, \end{cases}$$

$$\dim \mathcal{R}_{d,r} = \begin{cases} 8(r-1)(r-2) & \text{if } d = 4r-8, \\ 5r-9+d(d+1)/2 & \text{otherwise}. \end{cases}$$

Proof. We let $K = \{1, \ldots, \lfloor d/2 \rfloor\}$, $b_{d,r} = \dim \mathcal{C}_{d,r}$ for $d > 0$, and

$$u(k) = b_{d,r} - b_{k,r} - b_{d-k,r}$$

for $k \in K$, so that $\operatorname{codim}_{\mathcal{C}_{d,r}} \mathcal{R}_{d,r} \geqslant \min\{u(k)\colon\ k \in K\}$. We abbreviate the latter as m and first show that it equals the value claimed for the codimension.

We note that $d/2 \geqslant 2$ and $k \leqslant d-k$ for all $k \in K$ and define a partition of K into three subsets K_1, K_2, K_3 as follows:

$$K_1 = \{k \in K\colon\ k \geqslant 4r-8\},$$

$$K_2 = \{k \in K\colon\ k < 4r-8,\ d-k \geqslant 4r-8\},$$

$$K_3 = \{k \in K\colon\ d-k < 4r-8\}.$$

Furthermore, we let

$$m_i = \min\bigl\{u(k)\colon\ k \in K_i\bigr\}$$

for $1 \leqslant i \leqslant 3$, with $\min \emptyset = \infty$. Then $m = \min\{m_1, m_2, m_3\}$ and according to Fact 5,

$$u(k) = \begin{cases} k(d-k) - 3(r-2) & \text{if } k \in K_1, \\ (k/2)(2d-4r+7-k) & \text{if } k \in K_2, \\ 3(r-2) - 2dr + d(d+7)/2 & \text{if } k \in K_3. \end{cases}$$

In the last line, $u(k)$ does not depend on k.

If $d = 4r-8$, then $K = K_3$ and

$$u(k) = u(1) = r-2 = m_3$$

for all $k \in K$.

We may now assume that $d \geqslant 4r-7$. Then $1 \in K_2$ and $u(1) = d-2r+3$. For $k \in K_2$, $u(k)$ is a quadratic function of k with roots 0 and $2d-4r+7$ and takes its minimum in the range $1 \leqslant k \leqslant 2d-4r+6$ at $k = 1$. Since $k \leqslant d-4r+8 \leqslant 2d-4r+6$ for all $k \in K_2$, the range includes all of K_2. Thus $m_2 = d-2r+3$.

To determine m_1, we may assume that $d/2 \geqslant 4r-8$, since otherwise $K_1 = \emptyset$. The quadratic function $k(d-k)$ takes its minimum value in K_1 at $4r-8$. Now

$$m_1 = -16r^2 + 4dr + 61r - 8d - 58 = u(4r-8) \geqslant u(1) = m_2 \iff d \geqslant 4r - \frac{27}{4} + \frac{1}{4(4r-9)}.$$

The last inequality is strictly satisfied, since

$$d \geqslant 8r - 16 > 4r - \frac{27}{4} + \frac{1}{4(4r-9)}.$$

Thus $m_1 > m_2$. For $k \in K_3$, we have

$$m_3 = u(k) \geqslant u(1) = m_2 \quad \Leftrightarrow \quad 4r - \frac{15}{2} - \frac{3}{2(2d-5)} \leqslant d.$$

The last condition is strictly satisfied, and therefore $m_3 > m_2$ and $m = m_2$. In all cases, we have $m = u(1)$.

In order to prove a lower bound on $\dim \mathcal{R}_{d,r}$, it is sufficient to show that $\mu_{1,d,r}$ has some finite fiber, since then

$$\operatorname{codim}_{\mathcal{C}_{d,r}} (\operatorname{im} \mu_{1,d,r}) \leqslant m.$$

If $d \geqslant 4r-7$, then $1 \in K_2$, $d-1 \geqslant 4r-8$, $\operatorname{codim}_{\mathcal{C}_{d-1,r}} \mathcal{R}_{d-1,r} > 0$, and most curves in $\mathcal{C}_{d-1,r}$ are irreducible. Thus $\mu_{1,d,r}$ restricted to $\mathcal{C}_{1,r} \times (\mathcal{C}_{d-1,r} \setminus \mathcal{R}_{d-1,r})$ is injective, and in particular we have some finite fiber. If $d = 4r-8$, then $dG(1,r) \subseteq \mathcal{R}_{d,r}$ and $\operatorname{codim}_{\mathcal{C}_{d,r}} \mathcal{R}_{d,r} \leqslant \operatorname{codim}_{\mathcal{C}_{d,r}} dG(1,r) = r-2$. The claims about $\dim \mathcal{R}_{d,r}$ follow from Fact 5. □

4. The degree of the Chow variety of curves

Recall that an effective $\mathbb{F}_q$-cycle C of $\mathbb{P}^r$ of dimension 1 is $\mathbb{F}_q$-reducible if there exist $s \geqslant 2$ and effective $\mathbb{F}_q$-cycles $C_1, \ldots, C_s$ such that $C = \sum_{i=1}^{s} C_i$. According to Theorem 3, to each $\mathbb{F}_q$-cycle of degree d corresponds a unique $\mathbb{F}_q$-rational point of $\mathcal{C}_{d,r}$. Therefore, to each $\mathbb{F}_q$-cycle of degree d which is $\mathbb{F}_q$-reducible corresponds at least one point in the image of $\mathcal{C}_{k,r}(\mathbb{F}_q) \times \mathcal{C}_{d-k,r}(\mathbb{F}_q)$ under the mapping $\mu_{k,d,r}$ for a given $k \in K = \{1, \ldots, \lfloor d/2 \rfloor\}$. More precisely, we have

$$\mathcal{R}_{d,r}^{(q)}(\mathbb{F}_q) = \big\{C \in \mathcal{R}_{d,r}(\mathbb{F}_q) \colon C \text{ is } \mathbb{F}_q\text{-reducible}\big\} = \bigcup_{1 \leqslant k \leqslant d/2} \mu_{k,d,r}\big(\mathcal{C}_{k,r}(\mathbb{F}_q) \times \mathcal{C}_{d-k,r}(\mathbb{F}_q)\big).$$

From (4) we conclude that

$$\begin{aligned} \#\mathcal{R}_{d,r}^{(q)}(\mathbb{F}_q) &\leqslant \sum_{1 \leqslant k \leqslant d/2} \#\mathcal{C}_{k,r}(\mathbb{F}_q) \cdot \#\mathcal{C}_{d-k,r}(\mathbb{F}_q) \\ &\leqslant \sum_{1 \leqslant k \leqslant d/2} \deg \mathcal{C}_{k,r} \cdot 2q^{b_{k,r}} \cdot \deg \mathcal{C}_{d-k,r} \cdot 2q^{b_{d-k,r}}, \end{aligned}$$

with $b_{d,r} = \dim \mathcal{C}_{d,r}$. If $d \geqslant 4r-8 \geqslant 4$, then Theorem 6 implies that

$$\#\mathcal{R}_{d,r}^{(q)}(\mathbb{F}_q) \leqslant \begin{cases} 4 \sum_{1 \leqslant k \leqslant d/2} \deg \mathcal{C}_{k,r} \deg \mathcal{C}_{d-k,r} q^{b_{d,r}-r+2} & \text{if } d = 4r-8, \\ 4 \sum_{1 \leqslant k \leqslant d/2} \deg \mathcal{C}_{k,r} \deg \mathcal{C}_{d-k,r} q^{b_{d,r}-(d-2r+3)} & \text{otherwise.} \end{cases} \tag{9}$$

4.1. An upper bound on the degree of the restricted Chow variety $\widetilde{\mathcal{C}}_{d,r}$

The inequality (9) shows that an upper bound on the number of $\mathbb{F}_q$-reducible cycles in $\mathbb{P}^r$ of dimension 1 and degree d can be deduced from an upper bound on the degree of the Chow variety $\mathcal{C}_{d,r}$ of curves over $\overline{\mathbb{F}}_q$ of degree d in $\mathbb{P}^r$. In order to obtain an upper bound on the latter, we consider a suitable variant of the approach of Kollár [18, Exercise I.3.28] (see also [12]).

With the terminology of [6], we shall consider the *restricted Chow variety* $\widetilde{\mathcal{C}}_{d,r}$ of curves of degree d of $\mathbb{P}^r$, namely the union of the irreducible components of $\mathcal{C}_{d,r}$ whose generic point corresponds to a nondegenerate absolutely irreducible curve of $\mathbb{P}^r$.

Our purpose is to obtain an upper bound on the degree of $\widetilde{\mathcal{C}}_{d,r}$, from which an upper bound on the degree of $\mathcal{C}_{d,r}$ is readily obtained.

4.1.1. An incidence variety related to $\widetilde{\mathcal{C}}_{d,r}$

Let $\mathbb{P}^N$ denote the projective space of sequences $\boldsymbol{f} = (f_0, \dots, f_r)$ of homogeneous polynomials in $\overline{\mathbb{F}}_q[X_0, \dots, X_r]$ of degree d, and consider the incidence variety

$$\Gamma = \Gamma_{d,r} = \big\{(\boldsymbol{f}, [F]) \in \mathbb{P}^N \times \widetilde{\mathcal{C}}_{d,r} \colon V(\boldsymbol{f}) \supset \operatorname{supp}(F)\big\}. \tag{10}$$

In this section we obtain an upper bound on the degree of Γ.

Let $\theta : \Gamma \to \mathbb{P}^N$ and $\phi : \Gamma \to \widetilde{\mathcal{C}}_{d,r}$ denote the corresponding projections. The ϕ-fiber of a cycle $[F]$ corresponding to a curve C consists of the set of sequences $\boldsymbol{f} = (f_0, \dots, f_r)$ vanishing on C. On the other hand, it is clear that the image $\theta(\Gamma)$ is contained in the Zariski closed subset $\mathcal{U}$ of $\mathbb{P}^N$ defined by

$$\mathcal{U} = \big\{\boldsymbol{f} \in \mathbb{P}^N \colon \dim V(f) \geqslant 1\big\}.$$

According to [18, Exercise I.3.28], the following facts hold:

(1) $\mathcal{U}$ is a closed subset of $\mathbb{P}^N$,
(2) $\mathcal{U}$ can be defined by polynomials of degree $\binom{rd+d}{r}$.

Let $\mathcal{T}$ be an absolutely irreducible component of Γ. We have the following assertions (see [12, Proposition 2.4]):

(3) $\theta(\mathcal{T})$ is an absolutely irreducible component of $\mathcal{U}$,
(4) $\theta(\mathcal{T})$ has codimension at most $(r+1)(d^2+1)$ in $\mathbb{P}^N$,
(5) $\theta|_{\mathcal{T}} : \mathcal{T} \to \theta(\mathcal{T})$ is a birational map.

Lemma 7. *We have the estimate*

$$\deg \theta(\Gamma) \leqslant \binom{rd+d}{r}^{(r+1)(d^2+1)}.$$

Proof. Denote by $\mathcal{U}_{(r+1)(d^2+1)}$ the union of the absolutely irreducible components of $\mathcal{U}$ of codimension at most $(r+1)(d^2+1)$. According to (3)–(4), all the absolutely irreducible components of $\theta(\Gamma)$ are absolutely irreducible components of $\mathcal{U}_{(r+1)(d^2+1)}$. Thus, by definition of degree it follows that $\deg \theta(\Gamma) \leqslant \deg \mathcal{U}_{(r+1)(d^2+1)}$. By Lemma 1 we have

$$\deg \mathcal{U}_{(r+1)(d^2+1)} \leqslant \binom{rd+d}{r}^{(r+1)(d^2+1)},$$

from which the lemma follows. □

From the proof of [12, Proposition 2.4] one deduces that the points $\boldsymbol{f} \in \theta(\Gamma)$ for which $V(\boldsymbol{f})$ is an irreducible curve of $\mathbb{P}^r$ of degree d form a dense open subset of $\theta(\Gamma)$. Let $\mathcal{V}$ be the dense open subset of $\theta(\Gamma)$ where the inverse mapping θ^{-1} of θ is well-defined and $V(\boldsymbol{f})$ is an irreducible curve of degree d for every $\boldsymbol{f} \in \mathcal{V}$. By the definition of $\mathcal{V}$ it turns out that $\deg \theta(\Gamma) = \deg \mathcal{V}$ and $\theta^{-1}(\mathcal{V})$ is

a dense open subset of Γ, which in turn implies the equality $\deg\theta^{-1}(\mathcal{V}) = \deg\Gamma$. Furthermore, we have the identity

$$\theta^{-1}(\mathcal{V}) = \big\{\big(\boldsymbol{f}, [F]\big) \in \mathcal{V} \times \mathcal{I}_{d,r}\colon\ V(\boldsymbol{f}) \supset \operatorname{supp}(F)\big\}, \tag{11}$$

where $\mathcal{I}_{d,r}$ denotes the set of nondegenerate irreducible curves of $\mathbb{P}^r$ of degree d.

Denote by $(\overline{\mathbb{F}}_q[\mathbb{G}])_d = (\overline{\mathbb{F}}_q[\mathbb{G}(r-2,r)])_d$ the d-graded piece of the coordinate ring of the Grassmannian $\mathbb{G} = \mathbb{G}(r-2,r)$. Arguing as in Section 2.3.2 we see that the set $\mathcal{I}((\overline{\mathbb{F}}_q[\mathbb{G}])_d)$ of irreducible elements of $(\overline{\mathbb{F}}_q[\mathbb{G}])_d$ is an open subset of $(\overline{\mathbb{F}}_q[\mathbb{G}])_d$. If we denote by $\mathcal{I}_{\geqslant 1}((\overline{\mathbb{F}}_q[\mathbb{G}])_d)$ the set of irreducible cycles of dimension 1 and degree d, taking into account that each $\boldsymbol{f} \in \mathcal{V}$ defines an irreducible curve $V(\boldsymbol{f})$ of degree d, from (11) and [18, Corollary I.3.24.5] we deduce the identity:

$$\theta^{-1}(\mathcal{V}) = \big\{\big(\boldsymbol{f}, [F]\big) \in \mathcal{V} \times \mathcal{I}_{\geqslant 1}\big(\big(\overline{\mathbb{F}}_q[\mathbb{G}]\big)_d\big)\colon\ V(\boldsymbol{f}) \supset \operatorname{supp}(F)\big\}. \tag{12}$$

Proposition 8. *$\theta^{-1}(\mathcal{V})$ is defined in the product $\mathcal{V} \times \mathcal{I}_{\geqslant 1}((\overline{\mathbb{F}}_q[\mathbb{G}])_d)$ by bihomogeneous polynomials of bidegree at most (d, D_r), where $D_r = \binom{d^2+r}{r}$.*

Proof. Let $\boldsymbol{f} \in \mathcal{V}$, let $C = V(\boldsymbol{f})$ and let $[F]$ be an element of $\mathcal{I}((\overline{\mathbb{F}}_q[\mathbb{G}])_d)$. Then [18, Corollary I.3.24.5] shows that $\operatorname{supp}(F)$ is an irreducible curve of $\mathbb{P}^r$ of degree d. Assume without loss of generality that $\operatorname{supp}(F)$ has no components contained in the hyperplane $\{X_0 = 0\}$ at infinity. By (5) it follows that

$$\operatorname{supp}(F) = \big\{\boldsymbol{x} \in \mathbb{P}^r\colon\ \pi^{-1}(\boldsymbol{x}) \subset \eta^{-1}(V_F)\big\}.$$

Let $A_0, \ldots, A_r, B_0, \ldots, B_r$ be new indeterminates, let $\boldsymbol{A} = (A_0, \ldots, A_r)$, $\boldsymbol{B} = (B_0, \ldots, B_r)$ and $\boldsymbol{X} = (X_0, \ldots, X_r)$, and let $F = \sum_{|\boldsymbol{\alpha}|=|\boldsymbol{\beta}|=d} a_{\boldsymbol{\alpha},\boldsymbol{\beta}} \boldsymbol{A}^{\boldsymbol{\alpha}} \boldsymbol{B}^{\boldsymbol{\beta}}$. Then

$$\pi^{-1}(\boldsymbol{x}) = \big\{(\boldsymbol{x}, H_1, H_2)\colon\ A_0x_0 + \cdots + A_rx_r = B_0x_0 + \cdots + B_rx_r = 0\big\}.$$

Since $\operatorname{supp}(F)$ has no components at infinity, we see that the condition $\pi^{-1}(\boldsymbol{x}) \subset \eta^{-1}(V_F)$ is equivalent to the identity

$$F\left(-\sum_{i=1}^{r} A_iX_i, A_1X_0, \ldots, A_rX_0, -\sum_{i=1}^{r} B_iX_i, B_1X_0, \ldots, B_rX_0\right) = 0. \tag{13}$$

Denote by $\widehat{F}(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{X})$ the polynomial in the left-hand side of the previous expression and write

$$\widehat{F}(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{X}) = \sum_{\boldsymbol{\gamma},\boldsymbol{\delta}} c_{\boldsymbol{\gamma},\boldsymbol{\delta}}(\boldsymbol{a}, \boldsymbol{X}) \boldsymbol{A}^{\boldsymbol{\gamma}} \boldsymbol{B}^{\boldsymbol{\delta}},$$

where $\boldsymbol{a} = (a_{\boldsymbol{\alpha},\boldsymbol{\beta}})_{\boldsymbol{\alpha},\boldsymbol{\beta}}$ is the vector of coefficients of F and $\boldsymbol{\gamma}, \boldsymbol{\delta}$ run through the set of elements $\boldsymbol{\nu} \in (\mathbb{Z}_{\geqslant 0})^r$ with $|\boldsymbol{\nu}| = d$. Then (13) is equivalent to the following defining system of $\operatorname{supp}(F)$ in $\mathbb{P}^r$:

$$\big\{c_{\boldsymbol{\gamma},\boldsymbol{\delta}}(\boldsymbol{a}, \boldsymbol{X}) = 0\colon\ |\boldsymbol{\gamma}| = |\boldsymbol{\delta}| = d\big\}. \tag{14}$$

Observe that each polynomial $c_{\boldsymbol{\gamma},\boldsymbol{\delta}}(\boldsymbol{a}, \boldsymbol{X})$ is bihomogeneous of degree 1 in $\boldsymbol{a}$ and degree $2d$ in $\boldsymbol{X}$.

If the inclusion $V(\boldsymbol{f}) \supset \operatorname{supp}(F)$ is fulfilled then the ideal $(f_0, \ldots, f_r)$ generated by $f_0, \ldots, f_r$ is included in the ideal $I(C)$ of the curve $C = \operatorname{supp}(F)$. The latter condition implies the corresponding inclusion $(f_0, \ldots, f_r)^d \subset I(C)^d$ of dth powers of both ideals. According to [1] or [17], the inclusion of ideals $I(C)^d \subset (c_{\boldsymbol{\gamma},\boldsymbol{\delta}} : \boldsymbol{\gamma}, \boldsymbol{\delta})$ holds. We conclude that the inclusion $V(\boldsymbol{f}) \supset \operatorname{supp}(F)$ implies

$$(f_0,\dots,f_r)^d \subset (c_{\boldsymbol{\gamma},\boldsymbol{\delta}} : \boldsymbol{\gamma},\boldsymbol{\delta}). \tag{15}$$

On the other hand, the converse assertion is easily established by observing that (15) implies the corresponding inclusion of radical ideals, which in turn implies $V(\boldsymbol{f}) \supset \operatorname{supp}(F)$. As a consequence, for elements $[F] \in \mathcal{I}_{\geqslant 1}((\overline{\mathbb{F}}_q[\mathbb{G}])_d)$ we see that (15) is equivalent to the inclusion $V(\boldsymbol{f}) \supset \operatorname{supp}(F)$.

The inclusion (15) is equivalent to the membership of all products $f_0^{i_0}\cdots f_r^{i_r}$ with $i_0+\cdots+i_r = d$ in the ideal $(c_{\boldsymbol{\gamma},\boldsymbol{\delta}} : \boldsymbol{\gamma},\boldsymbol{\delta})$. Fix $(i_0,\dots,i_r) \in \mathbb{Z}_{\geqslant 0}^{r+1}$ with $i_0+\cdots+i_r = d$. Then $f_0^{i_0}\cdots f_r^{i_r} \in (c_{\boldsymbol{\gamma},\boldsymbol{\delta}} : \boldsymbol{\gamma},\boldsymbol{\delta})$ if and only if there exist homogeneous polynomials $h_{\boldsymbol{\gamma},\boldsymbol{\delta}} \in \overline{\mathbb{F}}_q[X_0,\dots,X_r]$ of degree d^2-2d for all $|\boldsymbol{\gamma}| = |\boldsymbol{\delta}| = d$ with

$$f_0^{i_0}\cdots f_r^{i_r} = \sum_{\boldsymbol{\gamma},\boldsymbol{\delta}} h_{\boldsymbol{\gamma},\boldsymbol{\delta}} c_{\boldsymbol{\gamma},\boldsymbol{\delta}}. \tag{16}$$

Equating the corresponding coefficients at both sides of (16) we can reexpress (16) as a linear system with the coefficients of the polynomials $h_{\boldsymbol{\gamma},\boldsymbol{\delta}}$ as indeterminates. The number of equations of this system equals the number of coefficients of the polynomials on both sides of (16). These are homogeneous polynomials of degree d^2 in r indeterminates, having thus at most $\binom{d^2+r}{r}$ nonzero coefficients. Then we have at most $\binom{d^2+r}{r}$ equations. On the other hand, the number of unknowns is equal to the number of coefficients of all the polynomials $h_{\boldsymbol{\gamma},\boldsymbol{\delta}}$, namely $\binom{d^2-2d+r}{r}\binom{d+r}{r}^2$. We also remark that the coefficients of the matrix of this system are linear combinations of the coefficients $\boldsymbol{a} = (a_{\boldsymbol{\alpha},\boldsymbol{\beta}})_{\boldsymbol{\alpha},\boldsymbol{\beta}}$ of F.

The existence of solutions of (16) is equivalent to the identity of the ranks of the coefficient matrix and the extended coefficient matrix of (16). Since these two matrices have rank at most $\binom{d^2+r}{r}$, the existence of solutions of (16) is equivalent to the vanishing of the determinant of certain minors of size at most $\binom{d^2+r}{r}+1 \times \binom{d^2+r}{r}+1$. The entries of such minors consist of linear combinations of the coefficients of the product $f_0^{i_0}\cdots f_r^{i_r}$ in their last column and linear combinations of the coefficients of the polynomials $c_{\boldsymbol{\gamma},\boldsymbol{\delta}}$ in the remaining columns. It follows that their determinants are bihomogeneous polynomials of degree $\binom{d^2+r}{r}$ in the vector $\boldsymbol{a} = (a_{\boldsymbol{\alpha},\boldsymbol{\beta}})_{\boldsymbol{\alpha},\boldsymbol{\beta}}$ of coefficients of F and degree d in the coefficients of the polynomials $f_0,\dots,f_r$. This finishes the proof of the proposition. □

Now we are in position to obtain an upper bound on the degree of the incidence variety Γ from (10).

Theorem 9. *The following upper bound holds for $d \geqslant r \geqslant 3$:*

$$\deg \Gamma \leqslant (ed)^{r(r+1)(d^2+1)+3rg_{d,r}},$$

where e denotes the basis of the natural logarithm and

$$g_{d,r} = \binom{r+d-2}{d}^2 \cdot \frac{r+d-1}{(r-1)(d+1)}. \tag{17}$$

Proof. By our previous remarks it turns out that the degree of the incidence variety Γ equals the degree of the open dense subset $\theta^{-1}(\mathcal{V})$ of Γ.

Let $\mathbb{G} = \mathbb{G}(r-2,2)$ and let $\mathcal{I}((\overline{\mathbb{F}}_q[\mathbb{G}])_d)$ be the open subset of $(\overline{\mathbb{F}}_q[\mathbb{G}])_d$ corresponding to irreducible cycles. According to [18, Exercise I.3.28.6], the set $\mathcal{I}_{\geqslant 1}((\overline{\mathbb{F}}_q[\mathbb{G}])_d)$ of cycles of $\mathcal{I}((\overline{\mathbb{F}}_q[\mathbb{G}])_d)$ of dimension 1 is a closed subset of $\mathcal{I}((\overline{\mathbb{F}}_q[\mathbb{G}])_d)$ which is described by equations in the coefficients $(a_{\boldsymbol{\alpha},\boldsymbol{\beta}})_{\boldsymbol{\alpha},\boldsymbol{\beta}}$ of the cycles of degree $\binom{2dr+d}{r}$. From Lemma 1 it follows that the union W_c of the irreducible components of $\mathcal{I}_{\geqslant 1}((\overline{\mathbb{F}}_q[\mathbb{G}])_d)$ of codimension at most c in $\mathcal{I}((\overline{\mathbb{F}}_q[\mathbb{G}])_d)$ has degree bounded by $\binom{2dr+d}{r}^c$.

Fix an integer $c \geqslant 0$ and consider the restriction $\theta|_{\Gamma_c}$ of θ to the (nonempty) incidence variety $\Gamma_c = \Gamma \cap (\mathcal{V} \times W_c) = \theta^{-1}(\mathcal{V}) \cap (\mathcal{V} \times W_c)$. To a generic cycle $[F]$ of an irreducible component of W_c corresponds a unique $\boldsymbol{f} \in \mathcal{V}$ such that $(\boldsymbol{f}, [F]) \in \Gamma_c$ holds. This shows that $\dim \Gamma_c = \dim W_c$.

Denote $g_{d,r} = \dim(\overline{\mathbb{F}}_q[\mathbb{G}])_d$ and observe that the following identity holds:

$$\dim\big(\overline{\mathbb{F}}_q[\mathbb{G}]\big)_d = \binom{r+d-2}{d}^2 - \binom{r+d-2}{d-1}\binom{r+d-2}{d+1} = g_{d,r}$$

(see, e.g., [10]). Then we have the following upper bound on $\operatorname{codim}_{\mathcal{V}\times W_c} \Gamma_c$:

$$\operatorname{codim}_{\mathcal{V}\times W_c} \Gamma_c = \dim \mathcal{V} + \dim W_c - \dim \Gamma_c = \dim \mathcal{V} \leqslant g_{d,r}.$$

Proposition 8 says that $\theta^{-1}(\mathcal{V})$ is defined in the product $\mathcal{V} \times \mathcal{I}_{\geqslant 1}(\overline{\mathbb{F}}_q[\mathbb{G}])_d$ by equations of bidegree at most (d, D_r), where $D_r = \binom{d^2+r}{r}$. Therefore, from Lemma 1 we conclude that

$$\deg \Gamma_c \leqslant \deg(\mathcal{V} \times W_c)(d + D_r)^{g_{d,r}} \leqslant \deg \mathcal{V} \deg W_c (d + D_r)^{g_{d,r}}.$$

By Lemma 7 we have $\deg \mathcal{V} = \deg \theta(\Gamma) \leqslant \binom{rd+d}{r}^{(r+1)(d^2+1)}$. As a consequence,

$$\deg \theta^{-1}(\mathcal{V}) = \deg \Gamma_{g_{d,r}} \leqslant \binom{rd+d}{r}^{(r+1)(d^2+1)} \binom{2dr+d}{r}^{g_{d,r}} (d + D_r)^{g_{d,r}}. \tag{18}$$

First we observe that the inequality $d + D_r \leqslant d + (e(d^2+r)/r)^r \leqslant d^{2r}$ holds for $d \geqslant r \geqslant 3$. On the other hand, from [20, Theorem 2.6] we easily deduce the following upper bounds:

$$\binom{rd+d}{r} \leqslant (ed)^r, \quad \binom{2dr+d}{r} \leqslant (2ed)^r.$$

Combining these inequalities with (18) and Remark 1 below, the bound of the statement of the theorem follows. □

Remark 1. The following identities hold:

$$\begin{aligned} g_{d,r} &= \binom{r+d-2}{d}^2 - \binom{r+d-2}{d-1}\binom{r+d-2}{d+1} \\ &= \frac{1}{d+1}\binom{d+r-2}{r-2}\binom{d+r-1}{r-1} = \prod_{i=1}^{r-2} \frac{d+r-i-1}{r-i-1}\frac{d+r-i}{r-i}. \end{aligned}$$

As a consequence of this result we obtain an upper bound on the degree of the union $\widetilde{\mathcal{C}}_{d,r}$ of the absolutely irreducible components of the Chow variety $\mathcal{C}_{d,r}$ containing an absolutely irreducible nondegenerate curve. Such a bound is deduced from the facts that $\widetilde{\mathcal{C}}_{d,r}$ is the image of the linear projection $\phi : \Gamma \to \widetilde{\mathcal{C}}_{d,r}$ and that the degree does not increase under linear mappings.

Corollary 10. *For $d \geqslant r \geqslant 3$, the following upper bound holds*:

$$\deg \widetilde{\mathcal{C}}_{d,r} \leqslant (ed)^{r(r+1)(d^2+1)+3rg_{d,r}},$$

with $g_{d,r}$ as in (17).

4.1.2. From an upper bound on the degree of $\widetilde{\mathcal{C}}_{d,r}$ to one for $\mathcal{C}_{d,r}$

Next we obtain an upper bound on the degree of the union $\widehat{\mathcal{C}}_{d,r}$ of the components of the Chow variety $\mathcal{C}_{d,r}$ for which the generic point corresponds to an absolutely irreducible curve. Since we have an upper bound on the degree of the restricted Chow variety $\widetilde{\mathcal{C}}_{d,r}$, namely the union of the components of $\mathcal{C}_{d,r}$ for which the generic point corresponds to a nondegenerate absolutely irreducible curve, there only remains to consider the degenerate cases.

Fix k with $2 \leqslant k < r$ and consider the union $\widehat{\mathcal{C}}^{(k)}_{d,r}$ of the absolutely irreducible components of $\widehat{\mathcal{C}}_{d,r}$ for which the generic point corresponds to an absolutely irreducible curve spanning a k-dimensional linear subspace of $\mathbb{P}^r$.

Lemma 11. *For $d \geqslant k \geqslant 2$ and $r \geqslant 3$, the following upper bound holds*:

$$\deg \widehat{\mathcal{C}}^{(k)}_{d,r} \leqslant \left(d^2+1\right)^{\dim \widehat{\mathcal{C}}^{(k)}_{d,r}} (k+1)(r-k) \deg \widetilde{\mathcal{C}}_{d,k}. \tag{19}$$

Proof. First we observe that it is easy to construct a set-theoretic bijection

$$\widetilde{\mathcal{C}}_{d,k} \times \mathbb{G}(k,r) \leftrightarrow \widehat{\mathcal{C}}^{(k)}_{d,r}.$$

Indeed, a curve in $\mathbb{P}^k$ can be embedded in $\mathbb{P}^r$ and moved to any subspace of dimension k using a suitable linear isomorphism. Fixing the embedding, a bijection as above is obtained. We claim that there exists a dense open subset U of $\mathbb{G}(k,r)$ such that the restriction of a set-theoretic bijection as above to $\widetilde{\mathcal{C}}_{d,k} \times U$ is given by a polynomial map $\phi : \mathbb{PV}_{d,k} \times U \to \mathbb{PV}_{d,r}$ such that $\phi(\widetilde{\mathcal{C}}_{d,k} \times U)$ contains a dense open subset of $\widehat{\mathcal{C}}^{(k)}_{d,r}$.

Fix a basis $\{e_0, \ldots, e_r\}$ of $\overline{\mathbb{F}}_q^{r+1}$, let $\mathbb{P}^k$ be embedded in $\mathbb{P}^r$ as the subspace spanned by the first $k+1$ basis vectors $e_0, \ldots, e_k$ in $\mathbb{P}^r$ and consider the corresponding embedding of $\mathbb{PV}_{d,k}$ in $\mathbb{PV}_{d,r}$. If $[F] \in \mathbb{PV}_{d,r}$ is the Chow form of a cycle $C \in \mathcal{C}_{d,r}$, then C is contained in $\mathbb{P}^k$ if and only if $[F]$ depends on $A_0, \ldots, A_k$ and $B_0, \ldots, B_k$ and not on $A_{k+1}, \ldots, A_r$ and $B_{k+1}, \ldots, B_r$. Let Φ be the linear space of $\mathbb{P}^r$ spanned by the last $r-k$ basis vectors $e_{k+1}, \ldots, e_r$ and let U_Φ be the affine open subset of $\mathbb{G}(k,r)$ consisting of the subspaces complementary to Φ. Then every $\Lambda \in U_\Phi$ is represented as the row space of a unique matrix of the form

$$\begin{pmatrix} 1 & 0 & \ldots & 0 & m_{0,1} & m_{0,2} & \ldots & m_{0,r-k} \\ 0 & 1 & \ldots & 0 & m_{1,1} & m_{1,2} & \ldots & m_{1,r-k} \\ \vdots & & & & & & \ldots & \\ 0 & 0 & \ldots & 1 & m_{k,1} & m_{k,2} & \ldots & m_{k,r-k} \end{pmatrix} \tag{20}$$

and viceversa. The entries $m_{i,j}$ of the last $r-k$ columns of this matrix yield a bijection of U_Φ with $\mathbb{A}^{(k+1)(r-k)}$, and are known as the Plücker coordinates of the Grassmannian $\mathbb{G}(k,r)$ (see, e.g., [13]).

For each $[F] \in \mathbb{PV}_{d,k}$ and $(m_{i,j}) \in \mathbb{A}^{(k+1)(r-k)}$, we define

$$\phi\big([F], (m_{i,j})\big)(\boldsymbol{A}, \boldsymbol{B}) = \big[F\big(\mathcal{M}^{-1}\boldsymbol{A}, \mathcal{M}^{-1}\boldsymbol{B}\big)\big],$$

where $\mathcal{M} \in \mathbb{A}^{(r+1)\times(r+1)}$ is the matrix

$$\mathcal{M} = \begin{pmatrix} \mathrm{Id}_{k+1} & (m_{i,j}) \\ \mathbf{0} & \mathrm{Id}_{r-k} \end{pmatrix}, \tag{21}$$

Id_j denotes the identity matrix of $\mathbb{A}^{j\times j}$ for every $j \in \mathbb{N}$ and $\mathbf{0}$ denotes the zero matrix of $\mathbb{A}^{(r-k)\times(k-1)}$. Since the identity

$$\mathcal{M}^{-1} = \begin{pmatrix} \mathrm{Id}_{k+1} & -(m_{i,j}) \\ \mathbf{0} & \mathrm{Id}_{r-k} \end{pmatrix}$$

holds, we easily conclude that the injection ϕ is a regular map defined by polynomials of degree at most d^2+1.

If $[F]$ is the Chow form of an irreducible nondegenerate curve C of $\mathbb{P}^k$, then we have that $\phi([F],(m_{i,j}))$ is the Chow form of the curve $C_{\mathcal{M}} = \{\mathcal{M}\boldsymbol{x}\colon\ \boldsymbol{x}\in C\}$. Clearly, $C_{\mathcal{M}}$ is an irreducible curve which is nondegenerate in the subspace spanned by the first $k+1$ rows of $\mathcal{M}$. This shows that $\phi(\widetilde{\mathcal{C}}_{d,k}\times\mathbb{A}^{(k+1)(r-k)})\subset\widehat{\mathcal{C}}^{(k)}_{d,r}$ holds.

Now, let V_Φ be the open dense subset of $\widehat{\mathcal{C}}^{(k)}_{d,r}$ consisting of the forms whose support spans a subspace complementary to Φ. For $[G]$ in V_Φ, consider the Plücker coordinates $(m_{i,j})\in\mathbb{A}^{(k+1)(r-k)}$ of the subspace spanned by $\operatorname{supp}(G)$ and the corresponding matrix $\mathcal{M}$ defined as in (21). By reversing the argument above, it turns out that the polynomial $F(\boldsymbol{A},\boldsymbol{B}) = G(\mathcal{M}\boldsymbol{A},\mathcal{M}\boldsymbol{B})$ depends only on the indeterminates $A_0,\dots,A_k$ and $B_0,\dots,B_k$, and hence its support is a nondegenerate curve in $\mathbb{P}^k$. We conclude that $[F]$ belongs to $\widetilde{\mathcal{C}}_{d,k}$ and the Chow form $[G]$ is the image under ϕ of the pair $([F],(m_{i,j}))$. It follows that $\phi(\widetilde{\mathcal{C}}_{d,k}\times\mathbb{A}^{(k+1)(r-k)})$ contains a dense open subset of $\widehat{\mathcal{C}}^{(k)}_{d,r}$, as claimed.

From our claim we deduce that

$$\deg\phi\big(\widetilde{\mathcal{C}}_{d,k}\times\mathbb{A}^{(k+1)(r-k)}\big) = \deg\widehat{\mathcal{C}}^{(k)}_{d,r}.$$

Applying Lemma 2, the estimate of the lemma follows. □

Proposition 12. *For $d\geqslant 1$ and $r\geqslant 3$, the following upper bound holds*:

$$\deg\widehat{\mathcal{C}}_{d,r}\leqslant 2(ed)^{r(r+1)(d^2+1)+3rg_{d,r}},$$

where $g_{d,r}$ is defined as in (17).

Proof. First suppose that $d\geqslant r$. From Fact 5, Corollary 10 and Lemma 11 we have

$$\sum_{k=2}^{r-1}\deg\widehat{\mathcal{C}}^{(k)}_{d,r}\leqslant\big(d^2+1\big)^{2d(r-1)+d(d+3)/2}\sum_{k=2}^{r-1}(k+1)(r-k)(ed)^{k(k+1)(d^2+1)+3kg_{d,k}}.$$

By Remark 1 we easily deduce that the numbers $g_{d,k}$ are increasing functions of k, which implies

$$(ed)^{(k+1)k(d^2+1)+3kg_{d,k}}\leqslant(ed)^{r(r-1)(d^2+1)+3rg_{d,r}}$$

for $2\leqslant k\leqslant r-1$. This shows that

$$\begin{aligned}\sum_{k=2}^{r-1}\deg\widehat{\mathcal{C}}^{(k)}_{d,r}&\leqslant(r-2)r^2\big(d^2+1\big)^{2d(r-1)+d(d+3)/2}(ed)^{r(r-1)(d^2+1)+3rg_{d,r}}\\&\leqslant(ed)^{r(r+1)(d^2+1)+3rg_{d,r}}.\end{aligned}$$

Since $\deg\widehat{\mathcal{C}}_{d,r}\leqslant\sum_{k=2}^{r-1}\deg\widehat{\mathcal{C}}^{(k)}_{d,r}+\deg\widetilde{\mathcal{C}}_{d,r}$, from the previous bound and Corollary 10 we deduce the statement of the proposition for $d\geqslant r$.

Next suppose that $2\leqslant d<r$. Since an irreducible nondegenerate curve in $\mathbb{P}^k$ has degree at least k (see, e.g., [13, Proposition 18.9]), we conclude that $\widehat{\mathcal{C}}^{(k)}_{d,r}$ is empty for $k>d$ and $\widetilde{\mathcal{C}}_{d,r}$ is also empty. This implies

$$\deg \widehat{\mathcal{C}}_{d,r} = \sum_{k=2}^{d} \deg \widehat{\mathcal{C}}_{d,r}^{(k)} \leqslant \sum_{k=2}^{d} (ed)^{(k+1)r(d^2+1)+3kg_{d,k}} \leqslant (d-2)(ed)^{(d+1)r(d^2+1)+3rg_{d,r}}$$

and proves the proposition in this case.

Finally, if $d = 1$, then $\widehat{\mathcal{C}}_{1,r} = \mathbb{G}(1,r)$. In this case we have an explicit expression for the degree of $\mathbb{G}(1,r)$, from which the estimate of the statement follows (see, e.g., [13, Example 19.14]):

$$\deg \widehat{\mathcal{C}}_{1,r} = \frac{(2r-2)!}{(r-1)!r!} = \frac{1}{r}\binom{2r-2}{r-1} \leqslant (2e)^{r-1} \leqslant 2e^{2r(r+1)+3rg_{1,r}}.$$

This finishes the proof of the proposition. □

Finally, we obtain an upper bound on the degree of the Chow variety $\mathcal{C}_{d,r}$ of curves of $\mathbb{P}^r$ of degree d. We recall the quantity $g_{d,r}$ from (17).

Theorem 13. *For $d \geqslant 1$ and $r \geqslant 3$, we set*

$$c_{d,r} = (2ed)^{r(r+1)(d^2+1)+4rg_{d,r}}. \tag{22}$$

Then $\deg \mathcal{C}_{d,r} \leqslant c_{d,r}$.

Proof. Let $(\boldsymbol{a}, \boldsymbol{d}) = (a_1, \ldots, a_s, d_1, \ldots, d_s)$ be a vector of positive integers with $d_1 \geqslant d_2 \geqslant \cdots \geqslant d_s$ and $a_1d_1 + \cdots + a_sd_s = d$, and consider the morphism

$$\begin{aligned} \mu_{(\boldsymbol{a},\boldsymbol{d})} : \widehat{\mathcal{C}}_{d_1,r} \times \cdots \times \widehat{\mathcal{C}}_{d_s,r} &\to \mathcal{C}_{d,r} \\ \big([F_1], \ldots, [F_s]\big) &\mapsto \left[\prod_{i=1}^{s} F_i^{a_i}\right]. \end{aligned}$$

For $(\boldsymbol{a}, \boldsymbol{d})$ as before, the numbers s and $d_1 + \cdots + d_s$ are called the length and the weight of $\boldsymbol{d}$ and are denoted by $\ell(\boldsymbol{d})$ and $w(\boldsymbol{d})$, respectively. If $\mathcal{D}$ denotes the set of all $(\boldsymbol{a}, \boldsymbol{d})$ with $d_1 \geqslant d_2 \geqslant \cdots \geqslant d_{\ell(\boldsymbol{d})}$ and $a_1d_1 + \cdots + a_sd_s = d$, then it is clear that

$$\mathcal{C}_{d,r} = \widehat{\mathcal{C}}_{d,r} \cup \mathcal{R}_{d,r} = \bigcup_{(\boldsymbol{a},\boldsymbol{d})\in\mathcal{D}} \operatorname{im} \mu_{(\boldsymbol{a},\boldsymbol{d})}.$$

Furthermore, since each image $\operatorname{im} \mu_{(\boldsymbol{a},\boldsymbol{d})}$ is a closed subset of $\mathcal{C}_{d,r}$, we have

$$\deg \mathcal{C}_{d,r} \leqslant \sum_{(\boldsymbol{a},\boldsymbol{d})\in\mathcal{D}} \deg \operatorname{im} \mu_{(\boldsymbol{a},\boldsymbol{d})}. \tag{23}$$

Applying Lemma 2 and Proposition 12, we obtain the following inequality:

$$\deg \operatorname{im} \mu_{(\boldsymbol{a},\boldsymbol{d})} \leqslant d^{g_{d,r}} \prod_{1\leqslant i\leqslant \ell(\boldsymbol{d})} \deg \widehat{\mathcal{C}}_{d_i,r} \leqslant d^{g_{d,r}} \prod_{1\leqslant i\leqslant \ell(\boldsymbol{d})} 2(ed_i)^{r(r+1)(d_i^2+1)+3rg_{d_i,r}}.$$

Claim 1. *Let $c_{\boldsymbol{d}} = \prod_{i=1}^{\ell(\boldsymbol{d})} 2(ed_i)^{r(r+1)(d_i^2+1)+3rg_{d_i,r}}$ for any $\boldsymbol{d} = (d_1, \ldots, d_s)$ with $w(\boldsymbol{d}) \leqslant d$. We have*

$$\sum_{(\boldsymbol{a},\boldsymbol{d})\in\mathcal{D}} c_{\boldsymbol{d}} \leqslant (2ed)^{r(r+1)(d^2+1)+3rg_{d,r}}.$$

Proof. Define $\widehat{c}_k = \exp(h(k))$, where $h : \mathbb{R}_{\geqslant 0} \to \mathbb{R}$ is the function defined by the identity $\exp(h(x)) = 2(ex)^{r(r+1)(x^2+1)+3rg_{x,r}}$. From Remark 1 we easily conclude that h is differentiable and its derivative is increasing. A straightforward argument shows the inequality $\widehat{c}_k\widehat{c}_m \leqslant \widehat{c}_{m+k}$ for arbitrary positive integers k, m and $r \geqslant 3$. Hence, for $\boldsymbol{d} = (d_1, \ldots, d_s)$ with $s \geqslant 2$,

$$c_{\boldsymbol{d}} = \widehat{c}_{d_1} \cdots \widehat{c}_{d_s} \leqslant \widehat{c}_{w(\boldsymbol{d})}.$$

This shows that

$$\sum_{\{(\boldsymbol{a},\boldsymbol{d}):\ w(\boldsymbol{d})=m\}} c_{(\boldsymbol{a},\boldsymbol{d})} \leqslant \#\big\{(\boldsymbol{a},\boldsymbol{d}):\ w(\boldsymbol{d}) = m\big\} \cdot \widehat{c}_m \leqslant 2^{m+d}\widehat{c}_m.$$

Taking into account that the expression $2^m\widehat{c}_m$ is increasing in m, we obtain

$$\sum_{(\boldsymbol{a},\boldsymbol{d})\in\mathcal{D}} c_{\boldsymbol{d}} = \sum_{m=1}^{d} \sum_{\{(\boldsymbol{a},\boldsymbol{d}):\ w(\boldsymbol{d})=m\}} c_{(\boldsymbol{a},\boldsymbol{d})} \leqslant \sum_{m=1}^{d} 2^{m+d}\widehat{c}_m \leqslant d2^{2d}\widehat{c}_d \leqslant (2ed)^{r(r+1)(d^2+1)+3rg_{d,r}}.$$

This proves the claim. □

Combining (23) with this claim proves the theorem. □

5. The number of $\mathbb{F}_q$-reducible curves

From Theorem 13 we derive an upper bound on the number of $\mathbb{F}_q$-reducible cycles of the Chow variety $\mathcal{C}_{d,r}$.

Theorem 14. *For $r \geqslant 3$ and $d \geqslant 4r - 8$, the following upper bound holds*:

$$\#\mathcal{R}_{d,r}^{(q)}(\mathbb{F}_q) \leqslant \begin{cases} c_{d,r}q^{b_{d,r}-r+2} & \text{if } d = 4r-8, \\ c_{d,r}q^{b_{d,r}-(d-2r+3)} & \text{otherwise}, \end{cases}$$

with $b_{d,r} = \dim \mathcal{C}_{d,r}$ and $c_{d,r}$ as in Fact 5 and (22), respectively.

Proof. Let $c_{k,r} = (2ek)^{r(r+1)(k^2+1)+4rg_{k,r}}$ for $k \in \mathbb{N}$. According to (9) and Theorem 13, we have the inequality

$$\#\mathcal{R}_{d,r}^{(q)}(\mathbb{F}_q) \leqslant \begin{cases} 4\sum_{1\leqslant k\leqslant d/2} c_{k,r}c_{d-k,r}q^{b_{d,r}-r+2} & \text{if } d = 4r-8, \\ 4\sum_{1\leqslant k\leqslant d/2} c_{k,r}c_{d-k,r}q^{b_{d,r}-d+2r-3} & \text{otherwise.} \end{cases} \tag{24}$$

Let $h : \mathbb{R}_{\geqslant 0} \to \mathbb{R}$ be the function defined by the identity $\exp(h(x)) = (2ex)^{r(r+1)(x^2+1)+4g_{x,r}}$. Arguing as in the proof of Theorem 13, we deduce that h is differentiable and its derivative is increasing. This implies that the function $f_y : [0, y/2] \to \mathbb{R}_{\geqslant 0}$ defined by $f_y(x) = \exp(h(x))\exp(h(y-x))$ is decreasing for any positive real number y. It follows that $c_{k,r}c_{d-k,r} \leqslant c_{1,r}c_{d-1,r}$ for $2 \leqslant k \leqslant d/2$, and hence

$$\sum_{1\leqslant k\leqslant d/2} c_{k,r}c_{d-k,r} \leqslant \frac{d}{2}c_{1,r}c_{d-1,r} \leqslant \frac{c_{d,r}}{4}. \tag{25}$$

Combining (24) and (25) we easily deduce the statement of the theorem. □

In order to obtain bounds on the probability that an $\mathbb{F}_q$-curve in $\mathbb{P}^r$ is $\mathbb{F}_q$-reducible, we take as a lower bound on the number of all $\mathbb{F}_q$-curves of $\mathbb{P}^r$ the number $\#P(d,r)(\mathbb{F}_q)$ of plane $\mathbb{F}_q$-curves in $\mathbb{P}^r$. Bounds on the number $\#R(d,r)(\mathbb{F}_q)$ of plane $\mathbb{F}_q$-reducible curves of $\mathbb{P}^r$ are provided by the estimates for irreducible bivariate and multivariate polynomials of [8] and [9]. For the homogeneous case, these estimates imply that the number $\#R(d,2)$ of $\mathbb{F}_q$-reducible curves in $P(d,2)$ is bounded as

$$\#P(d,2)\cdot(q-3)q^{-d} \leqslant \#R(d,2) \leqslant \#P(d,2)\cdot(q+2)q^{-d}. \tag{26}$$

Lemma 15. *Let $r \geqslant 3$ and $d \geqslant 4r-8$. Then*

$$q^{b_{d,r}} = q^{3(r-2)+d(d+3)/2} \leqslant \#P(d,r)(\mathbb{F}_q) \leqslant 7q^{b_{d,r}},$$
$$\#R(d,r)(\mathbb{F}_q) \leqslant 13q^{b_{d,r}-d+1},$$
$$q^{b_{d,r}} \leqslant \#C_{d,r}(\mathbb{F}_q) < 2c_{d,r}q^{b_{d,r}}.$$

Proof. We fix $\mathbb{F}_q$, drop it from the notation, and consider the incidence variety

$$I = \big\{(C,E) \in P(d,r)\times\mathbb{G}(2,r)\colon\ C\subseteq E\big\}. \tag{27}$$

The second projection $\pi_2 : I \to \mathbb{G}(2,r)$ is surjective, and all its fibers are isomorphic to the variety $P(d,2)$ of plane curves of degree d. The latter are parametrized by the nonzero homogeneous trivariate polynomials of degree d, and

$$\#P(d,2) = \frac{q^{(d+2)(d+1)/2}-1}{q-1},$$
$$\#I = \#P(d,2)\cdot\#G(2,r) = \#P(d,2)\cdot\frac{(q^{r+1}-1)(q^{r+1}-q)(q^{r+1}-q^2)}{(q^3-1)(q^3-q)(q^3-q^2)}.$$

The fibers of the first projection $\pi_1 : I \to P(d,r)$ usually are singletons. The only exceptions occur when $C = d\cdot L$ equals d times a line L. There are

$$\#\mathbb{G}(1,r) = \frac{(q^{r+1}-1)(q^{r+1}-q)}{(q^2-1)(q^2-q)}$$

such $d\cdot L$, and their fiber size is

$$\#\pi_1^{-1}(d\cdot L) = \frac{q^{r+1}-q^2}{q^3-q^2}.$$

It follows that

$$\begin{aligned}\#P(d,r) &= \#I - \#\mathbb{G}(1,r)\cdot\left(\frac{q^{r+1}-q^2}{q^3-q^2}-1\right)\\ &= \#\mathbb{G}(1,r)\cdot\left(\frac{\#P(d,2)\cdot(q^{r+1}-q^2)(q^2-1)(q^2-q)}{(q^3-1)(q^3-q)(q^3-q^2)} - \frac{q^{r+1}-q^3}{q^3-q^2}\right)\\ &= \#\mathbb{G}(1,r)\cdot\frac{(q^{(d+2)(d+1)/2}-1)(q^{r-1}-1)-(q^{r-1}-q)(q^3-1)}{(q^3-1)(q-1)}\end{aligned}$$

$$= q^{3(r-2)+d(d+3)/2}\frac{(1-q^{-r})(1-q^{-r-1})}{(1-q^{-1})^2(1-q^{-2})(1-q^{-3})} \cdot \big(\big(1-q^{-c}\big)\big(1-q^{-r+1}\big) - q^{3-c}\big(1-q^{-r+2}\big)\big(1-q^{-3}\big)\big), \tag{28}$$

where $c = (d+2)(d+1)/2$. Since q, $d \geqslant 2$, we have $c \geqslant 6$ and hence

$$2q \geqslant 1 + q^{5-c} + q^{2-c} + q^{3-r},$$
$$\big(1-q^{-c}\big)\big(1-q^{-r+1}\big) - q^{3-c} \geqslant \big(1-q^{-1}\big)^2.$$

Therefore, the last factor in (28) is at least $(1-q^{-1})^2$, which implies

$$\#P(d,r) \geqslant q^{3(r-2)+d(d+3)/2}.$$

On the other hand, from (28) we also deduce that

$$\#P(d,r) \leqslant q^{b_{d,r}}\frac{(1-q^{-c})(1-q^{-r-1})(1-q^{-r})(1-q^{-r+1})}{(1-q^{-1})^2(1-q^{-2})(1-q^{-3})} \leqslant q^{b_{d,r}}\frac{1}{(1-q^{-1})^2(1-q^{-2})(1-q^{-3})} \leqslant 7q^{b_{d,r}}.$$

This proves the bounds for $P(d,r)$. Concerning $R(d,r)$, we consider, instead of the incidence variety of (27), the "restricted" incidence variety

$$I_R = \big\{(C,E) \in R(d,r) \times \mathbb{G}(2,r)\colon\ C \subseteq E\big\}.$$

Arguing as before and applying (26), we obtain

$$\begin{aligned}\#R(d,r) &\leqslant \#I = \#R(d,2)\cdot\#G(2,r)\\ &\leqslant \#P(d,2)\cdot\frac{q+2}{q^d}\cdot\frac{(q^{r+1}-1)(q^{r+1}-q)(q^{r+1}-q^2)}{(q^3-1)(q^3-q)(q^3-q^2)}\\ &= q^{b_{d,r}-d+1}\frac{(1-q^{-(d+1)(d+2)/2})(1+2q^{-1})(1-q^{-r-1})(1-q^{-r})(1-q^{-r+1})}{(1-q^{-3})(1-q^{-2})(1-q^{-1})^2}\\ &< q^{b_{d,r}-d+1}\frac{1+2q^{-1}}{(1-q^{-3})(1-q^{-2})(1-q^{-1})^2} \leqslant 13q^{b_{d,r}-d+1}.\end{aligned}$$

The lower bound for $\mathcal{C}_{d,r}$ follows from the fact that $P(d,r) \subseteq \mathcal{C}_{d,r}$, and the upper bound from (4) and Theorem 13. □

We find the following bounds on the probability that a random curve in $\mathcal{C}_{d,r}(\mathbb{F}_q)$ is $\mathbb{F}_q$-reducible.

Theorem 16.

(1) *If $r \geqslant 3$ and $d \geqslant 4r-7$, then*

$$\frac{(1-13q^{2-d})}{2c_{d,r}}q^{-(d-2r+3)} \leqslant \frac{\#\mathcal{R}^{(q)}_{d,r}(\mathbb{F}_q)}{\#\mathcal{C}_{d,r}(\mathbb{F}_q)} \leqslant c_{d,r}q^{-(d-2r+3)},$$

with $c_{d,r}$ as in (22). If $d \geqslant 7$, then also

$$\frac{1}{4c_{d,r}} q^{-(d-2r+3)} \leqslant \frac{\#\mathcal{R}_{d,r}^{(q)}(\mathbb{F}_q)}{\#\mathcal{C}_{d,r}(\mathbb{F}_q)} \leqslant c_{d,r} q^{-(d-2r+3)}.$$

(2) *If $r \geqslant 3$ and $d = 4r - 8$, then*

$$\frac{1}{2d! c_{r,d}} q^{-r+2} \leqslant \frac{\#\mathcal{R}_{d,r}^{(q)}(\mathbb{F}_q)}{\#\mathcal{C}_{d,r}(\mathbb{F}_q)} \leqslant c_{d,r} q^{-r+2}.$$

Proof. Combining Lemma 15 with Theorem 14, the upper bounds follow immediately. It remains to prove the lower bounds.

(1) Recall the morphism $\mu_{1,d,r} : \mathcal{C}_{1,r} \times \mathcal{C}_{d-1,r} \to \mathcal{C}_{d,r}$ induced by the multiplication mapping. Theorem 6 asserts that $\operatorname{codim}_{\mathcal{R}_{d-1,r}} \mathcal{C}_{d-1,r} > 0$, which implies that $\mathcal{C}_{d-1,r} \setminus \mathcal{R}_{d-1,r}$ is a nonempty Zariski open subset of $\mathcal{C}_{d-1,r}$ of dimension $b_{d-1,r} = \dim \mathcal{C}_{d-1,r}$. Furthermore, the restriction of $\mu_{1,d,r}$ to $\mathcal{C}_{1,r} \times (\mathcal{C}_{d-1,r} \setminus \mathcal{R}_{d-1,r})$ is injective. Using Lemma 15, it follows that

$$\begin{aligned}
\#\mathcal{R}_{d,r}^{(q)}(\mathbb{F}_q) &\geqslant \#\mathcal{C}_{1,r}(\mathbb{F}_q) \cdot \#\big(\mathcal{C}_{d-1,r}(\mathbb{F}_q) \setminus \mathcal{R}_{d-1,r}^{(q)}(\mathbb{F}_q)\big) \\
&\geqslant \#\mathbb{G}(1,r)(\mathbb{F}_q) \cdot \#\big(P(d-1,r)(\mathbb{F}_q) \setminus R_{d-1,r}(\mathbb{F}_q)\big) \\
&> q^{2(r-1)} \cdot q^{3(r-2)+(d-1)(d+2)/2} \cdot \big(1 - 13q^{2-d}\big).
\end{aligned}$$

The bound $\#\mathcal{C}_{d,r}(\mathbb{F}_q) \leqslant 2c_{d,r} q^{b_{d,r}}$ implies the inequality

$$\frac{\#\mathcal{R}_{d,r}^{(q)}(\mathbb{F}_q)}{\#\mathcal{C}_{d,r}(\mathbb{F}_q)} \geqslant \frac{(1 - 13q^{2-d})}{2c_{d,r}} q^{-(d-2r+3)}.$$

The last claim follows since $1 - 13q^{2-d} \geqslant 1/2$ for $d \geqslant 7$.

(2) We consider $dG(1,r)(\mathbb{F}_q) \subseteq \mathcal{R}_{d,r}^{(q)}(\mathbb{F}_q)$ and the morphism from $G(1,r)^d$ to $dG(1,r)$ which takes a sequence of lines to their sum. Each fiber of this morphism has size at most $d!$. This implies that

$$\#\mathcal{R}_{d,r}^{(q)}(\mathbb{F}_q) \geqslant \#dG(1,r)(\mathbb{F}_q) > \frac{(\#G(1,r)(\mathbb{F}_q))^d}{d!} \geqslant \frac{q^{2d(r-1)}}{d!}.$$

Combined with Lemma 15, this yields

$$\frac{\#\mathcal{R}_{d,r}^{(q)}(\mathbb{F}_q)}{\#\mathcal{C}_{d,r}(\mathbb{F}_q)} \geqslant \frac{q^{2d(r-1)-b_{d,r}}}{2d! c_{d,r}}.$$

Furthermore,

$$2d(r-1) - b_{d,r} = 8(r-2)(r-1) - \big(3(r-2) + 2(r-2)(4r-5)\big) = -r + 2.$$

This finishes the proof of the theorem. □

An immediate consequence of this theorem is that the probability that an $\mathbb{F}_q$-curve in $\mathbb{P}^r$ of degree d is $\mathbb{F}_q$-reducible tends to zero as q grows for fixed $r \geqslant 3$ and $d \geqslant 4r - 8$. Furthermore, our bounds show that such a convergence has the same rate as $q^{-(d-2r+3)}$. In this sense, our bounds

are a suitable generalization of the corresponding bounds for $r = 2$, as stated in (26). We made no attempt to optimize the "constants" independent of q.

In [6] it is proved that for $d \geqslant 4r - 8$, the planar curves in $P(d, r)$ form the only component of $\mathcal{C}_{d,r}$ with maximal dimension. In this sense, "most" curves are planar. We can quantify this as follows.

Corollary 17. *For $r \geqslant 3$ and $d \geqslant 4r - 8$,*

$$\frac{\#(\mathcal{C}_{d,r} \setminus P(d,r))(\mathbb{F}_q)}{\#\mathcal{C}_{d,r}(\mathbb{F}_q)} \leqslant \frac{2c_{d,r}}{q}.$$

Proof. We denote as N the union of all components of $\mathcal{C}_{d,r}$ not contained in $P(d, r)$. Thus all non-planar curves are in N. By Fact 5, it follows that $\dim N < b_{d,r}$, and since each component of N is a component of $\mathcal{C}_{d,r}$, we have $\deg N \leqslant \deg \mathcal{C}_{d,r} = c_{d,r}$. Now (4) implies that $\#N(\mathbb{F}_q) \leqslant 2c_{d,r}q^{b_{d,r}-1}$, and using Lemma 15

$$\frac{\#((\mathcal{C}_{d,r} \setminus P(d,r))(\mathbb{F}_q))}{\#\mathcal{C}_{d,r}} \leqslant \frac{\#(N(\mathbb{F}_q))}{q^{b_{d,r}}} \leqslant \frac{2c_{d,r}}{q}.$$

This shows the corollary. □

In particular, for fixed $r \geqslant 3$ and $d \geqslant 4r - 8$, the probability for a random curve to be non-planar tends to 0 with growing q.

6. The probability that an $\mathbb{F}_q$-curve is absolutely reducible

An $\mathbb{F}_q$-curve can be absolutely reducible for two reasons: either it is $\mathbb{F}_q$-reducible, as treated above, or *relatively $\mathbb{F}_q$-irreducible*, that is, is $\mathbb{F}_q$-irreducible and $\overline{\mathbb{F}}_q$-reducible. The aim of this section is to obtain a bound on the probability for the latter to occur. The set of relatively $\mathbb{F}_q$-irreducible (or exceptional) $\mathbb{F}_q$-curves of degree d in $\mathbb{P}^r$ is denoted by $\mathcal{E}_{d,r}(\mathbb{F}_q)$ and the set of irreducible $\mathbb{F}_q$-curves of degree d in $\mathbb{P}^r$ is denoted by $\mathcal{I}_{d,r}(\mathbb{F}_q)$.

Theorem 18. *Let $r \geqslant 3$ and $d \geqslant 4r - 8$, and denote by ℓ the smallest prime divisor of d. We have the bounds*

$$q^{2d(r-1)}\left(1 - 4q^{2(1-d)(r-1)}\right) \leqslant \#\mathcal{E}_{d,r}(\mathbb{F}_q) \leqslant 2D_{\ell,d,r}q^{2d(r-1)} \quad \text{for } d/\ell \leqslant 4r - 7,$$
$$q^{\ell b_{d/\ell,r}}\left(1 - 16q^{\ell-d}\right) \leqslant \#\mathcal{E}_{d,r}(\mathbb{F}_q) \leqslant 3D_{\ell,d,r}q^{\ell b_{d/\ell,r}} \quad \text{for } d/\ell \geqslant 4r - 8,$$

with $D_{\ell,d,r} = (ed/\ell)^{r(r+1)(d^2/\ell^2+1)+4rg_{d/\ell,r}}$, $b_{d,r} = \dim \mathcal{C}_{d,r}$ and $g_{d/\ell,r}$ as in (17).

Proof. We follow the lines of the proof of [8, Theorem 5.1]. Let $A_0, \ldots, A_r, B_0, \ldots, B_r$ be new indeterminates, let $\boldsymbol{A} = (A_0, \ldots, A_r)$ and $\boldsymbol{B} = (B_0, \ldots, B_r)$. First we observe that, if a bihomogeneous polynomial $F \in \mathbb{F}_q[\boldsymbol{A}, \boldsymbol{B}]$ of bidegree (d, d) is relatively $\mathbb{F}_q$-irreducible, then it is reducible in $\mathbb{F}_{q^k}$ for k dividing d. Therefore, let k be a divisor of d and let $\mathcal{G}_k = \mathrm{Gal}(\mathbb{F}_{q^k} : \mathbb{F}_q)$ be the Galois group of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$. For σ in $\mathcal{G}_k$ and $[F]$ in $\mathcal{C}_{d/k,r}(\mathbb{F}_{q^k})$, the application of σ to the coordinates of $[F]$ yields a point $[F^\sigma]$ in $\mathbb{PV}_{d/k,r}$. Moreover, we have the following claim:

Claim 2. *$[F^\sigma]$ belongs to $\mathcal{C}_{d/k,r}(\mathbb{F}_{q^k})$, i.e., there is an $\mathbb{F}_{q^k}$-cycle of dimension 1 and degree d/k of $\mathbb{P}^r$ that corresponds to $[F^\sigma]$.*

Proof. Any morphism in $\mathcal{G}_k$ can be extended (not uniquely) to a morphism $\widetilde{\sigma}$ in $\mathrm{Gal}(\overline{\mathbb{F}}_q : \mathbb{F}_q)$. By Theorem 3 we see that the support $\mathrm{supp}(F) \subset \mathbb{P}^r$ of $[F]$ is an $\mathbb{F}_{q^k}$-curve. Applying $\widetilde{\sigma}$ to the

coordinates of the points of $\operatorname{supp}(F)$, by the $\mathbb{F}_{q^k}$-definability of $\operatorname{supp}(F)$ we deduce the equality $\operatorname{supp}(F^\sigma) = \sigma(\operatorname{supp}(F))$. This shows that $\operatorname{supp}(F^\sigma)$ is an $\mathbb{F}_{q^k}$-curve in $\mathbb{P}^r$, which in turn proves that $[F^\sigma] \in \mathcal{C}_{d/k,r}(\mathbb{F}_{q^k})$. □

The previous claim shows that the following mapping is well-defined:

$$\begin{aligned} \varphi_{k,d} : \mathcal{C}_{d/k,r}(\mathbb{F}_{q^k}) &\to \mathcal{C}_{d,r}(\mathbb{F}_q) \\ [F] &\mapsto \left[\prod_{\sigma \in \mathcal{G}_k} F^\sigma \right]. \end{aligned}$$

The image $\varphi_{k,d}([F])$ of the class of an $\mathbb{F}_{q^k}$-irreducible polynomial F is $\mathbb{F}_q$-reducible if and only if there exists a proper divisor l of k such that $[F]$ is $\mathbb{F}_{q^l}$-definable. Furthermore, if $[F]$ is relatively $\mathbb{F}_{q^l}$-irreducible, then $\varphi_{k,d}([F]) = \varphi_{j,d}([H])$ for an appropriate multiple j of k and $[H]$ in $\mathcal{I}_{d,r}(\mathbb{F}_{q^j})$. Thus, if we set for any integer m

$$\begin{aligned} \mathcal{I}^+_{m,r}(\mathbb{F}_{q^k} : \mathbb{F}_q) &= \mathcal{I}_{m,r}(\mathbb{F}_{q^k}) \setminus \left(\mathcal{E}_{m,r}(\mathbb{F}_{q^k}) \cup \bigcup_{s>1, s|k} \mathcal{I}_{m,r}(\mathbb{F}_{q^{k/s}}) \right), \\ \mathcal{E}_{k,d,r} &= \varphi_{k,d}\big(\mathcal{I}^+_{d/k,r}(\mathbb{F}_{q^k} : \mathbb{F}_q)\big), \end{aligned}$$

then we have the equality

$$\mathcal{E}_{d,r}(\mathbb{F}_q) = \bigcup_{k>1, k|d} \mathcal{E}_{k,d,r}.$$

In order to obtain bounds on the cardinality of $\mathcal{E}_{d,r}(\mathbb{F}_q)$, we observe that, for any divisor k of d with $k > 1$, we have

$$\#\mathcal{E}_{k,d,r} = \#\mathcal{I}^+_{d/k,r}(\mathbb{F}_{q^k} : \mathbb{F}_q).$$

Therefore,

$$\#\mathcal{I}^+_{d/l,r}(\mathbb{F}_{q^l}) \leqslant \#\mathcal{E}_{d,r}(\mathbb{F}_q) \leqslant \sum_{k>1, k|d} \#\mathcal{I}^+_{d/k,r}(\mathbb{F}_{q^k}) \leqslant \sum_{k>1, k|d} \#\widehat{\mathcal{C}}_{d/k,r}(\mathbb{F}_{q^k}) \tag{29}$$

for any divisor $l > 1$ of d.

The case d prime follows directly from this expression, since the sum in the right-hand side consists of only one term, namely $\#\mathcal{E}_{d,r}(\mathbb{F}_q) = \#\mathcal{I}^+_{1,r}(\mathbb{F}_{q^d})$. Furthermore,

$$\begin{aligned} \#\mathcal{I}^+_{1,r}(\mathbb{F}_{q^d} : \mathbb{F}_q) = \#\big(\mathcal{I}_{1,r}(\mathbb{F}_{q^d}) \setminus \mathcal{I}_{1,r}(\mathbb{F}_q)\big) &= \#\big(\mathbb{G}_{1,r}(\mathbb{F}_{q^d}) \setminus \mathbb{G}_{1,r}(\mathbb{F}_q)\big) \\ &= q^{2d(r-1)} - \frac{(q^{r+1}-1)(q^{r+1}-q)}{(q^2-1)(q^2-q)}. \end{aligned}$$

Hence, for d prime we have

$$q^{2d(r-1)}\big(1 - 4q^{2(1-d)(r-1)}\big) \leqslant \#\mathcal{E}_{d,r}(\mathbb{F}_q) \leqslant q^{2d(r-1)}. \tag{30}$$

Now, assume that d is not prime, and let ℓ denote the smallest prime divisor of d. Suppose that $d/\ell \leqslant 4r-7$. In this case, from Fact 5 we have $b_{d/k,r} = 2d(r-1)/k$ for every divisor k of d. As a consequence, if we denote

$$D_{k,d,r} = (ed/k)^{r(r+1)(d^2/k^2+1)+4rg_{d/k,r}},$$

from (29) and Proposition 12 we see that

$$\#\mathcal{E}_{d,r}(\mathbb{F}_q) \leqslant \sum_{k>1,k|d} 2D_{k,d,r}q^{kb_{d/k,r}} \leqslant D_{\ell,d,r}q^{2d(r-1)} \sum_{k>1,k|d} 2\frac{D_{k,d,r}}{D_{\ell,d,r}}.$$

For a nontrivial divisor $k > \ell$ of d, we have

$$\frac{D_{k,d,r}}{D_{\ell,d,r}} \leqslant \left(\frac{ed}{\ell}\right)^{(d^2/k^2-d^2/\ell^2)r(r+1)} \leqslant \left(\frac{ed}{\ell}\right)^{-2r(r+1)} \leqslant \frac{1}{2d}. \tag{31}$$

We conclude that, for $d/\ell \leqslant 4r-7$, the following upper bound holds:

$$\#\mathcal{E}_{d,r}(\mathbb{F}_q) \leqslant 2D_{\ell,d,r}q^{2d(r-1)}.$$

In order to determine a "matching" lower bound, arguing as above we obtain

$$\#\mathcal{E}_{d,r}(\mathbb{F}_q) \geqslant \#\mathcal{E}_{d,d,r} = \#\mathcal{I}^+_{1,r}(\mathbb{F}_{q^d} : \mathbb{F}_q) \geqslant q^{2d(r-1)} - 4q^{2(r-1)}.$$

Summarizing, we have

$$q^{2d(r-1)}\left(1 - 4q^{2(1-d)(r-1)}\right) \leqslant \#\mathcal{E}_{d,r}(\mathbb{F}_q) \leqslant 2D_{\ell,d,r}q^{2d(r-1)}. \tag{32}$$

Finally, assume that $d/\ell \geqslant 4r-8$. Then Fact 5 implies $b_{d/k,r} = 3(r-2) + d(d/k+3)/2k$ for $d/k \geqslant 4r-8$ and $b_{d/k,r} = 2d(r-1)/k$ for $d/k \leqslant 4r-7$.

Claim 3. *For any divisor $k > \ell$ of d, we have*

$$kb_{d/k,r} < \ell b_{d/\ell,r} = 3\ell(r-2) + d(d/\ell+3)/2. \tag{33}$$

Proof. First we consider the case $d/(4r-8) \geqslant k$. Then we have $kb_{d/k,r} = 3k(r-2) + d(d/k+3)/2$. Taking formal derivatives in this expression with respect to k, we conclude that $k \mapsto kb_{d/k,r}$ is a strictly decreasing function of k for $d/(4r-8) \geqslant k$. This implies the claim in this case.

Next assume that $d/k \leqslant 4r-7$. Then we have $kb_{d/k,r} = 2d(r-1)$. Up to a division by ℓ, we see that the claim is equivalent to the validity of the inequality

$$2(d/\ell)(r-1) < 3(r-2) + (d/\ell)(d/\ell+3)/2.$$

Then Fact 5 shows that the last inequality holds for $d/\ell \geqslant 4r-8 > 1$. This concludes the proof of our claim. □

From (29) and (33) it follows that

$$\#\mathcal{E}_{d,r}(\mathbb{F}_q) \leqslant \sum_{k>1,k|d} 2D_{k,d,r}q^{kb_{d/k,r}} \leqslant 2D_{\ell,d,r}q^{\ell b_{d/\ell,r}}\left(1 + q^{-1}\sum_{k>\ell,k|d}\frac{D_{k,d,r}}{D_{\ell,d,r}}\right).$$

Applying (31) we obtain, for $d/\ell \geqslant 4r-8$,

$$\#\mathcal{E}_{d,r}(\mathbb{F}_q) \leqslant 2D_{\ell,d,r}q^{\ell b_{d/\ell,r}}\big(1+(2q)^{-1}\big) \leqslant 3D_{\ell,d,r}q^{\ell b_{d/\ell,r}}. \tag{34}$$

Next we obtain a lower bound for this case. We have

$$\#\mathcal{E}_{d,r}(\mathbb{F}_q) \geqslant \#\mathcal{E}_{\ell,d,r} = \#\mathcal{I}^{+}_{d/\ell,r}(\mathbb{F}_{q^\ell}:\mathbb{F}_q) = \#\big(\mathcal{I}_{d/\ell,r}(\mathbb{F}_{q^\ell}) \setminus \mathcal{I}_{d/\ell,r}(\mathbb{F}_q)\big),$$

since ℓ is prime and there are no proper intermediate fields between $\mathbb{F}_q$ and $\mathbb{F}_{q^\ell}$. In order to find a lower bound for the right-hand side above, we observe that

$$\#\big(\mathcal{I}_{d/\ell,r}(\mathbb{F}_{q^\ell}) \setminus \mathcal{I}_{d/\ell,r}(\mathbb{F}_q)\big) \geqslant \#\big(\big(\mathcal{I}_{d/\ell,r}(\mathbb{F}_{q^\ell}) \setminus \mathcal{I}_{d/\ell,r}(\mathbb{F}_q)\big) \cap P(d/\ell,r)(\mathbb{F}_{q^\ell})\big).$$

According to Lemma 15, we have

$$\#\big(\mathcal{I}_{d/\ell,r}(\mathbb{F}_{q^\ell}) \cap P(d/\ell,r)(\mathbb{F}_{q^\ell})\big) = \#P(d/\ell,r)(\mathbb{F}_{q^\ell}) - \#R(d/\ell,r)(\mathbb{F}_{q^\ell}) \geqslant q^{\ell b_{d/\ell,r}}\big(1-15q^{\ell-d}\big).$$

On the other hand, Lemma 15 implies

$$\#\big(\mathcal{I}_{d/\ell,r}(\mathbb{F}_q) \cap P(d/\ell,r)(\mathbb{F}_{q^\ell})\big) \leqslant \#P(d/\ell,r)(\mathbb{F}_q) \leqslant 8q^{b_{d/\ell,r}}.$$

As a consequence, it follows that

$$\#\mathcal{E}_{d,r}(\mathbb{F}_q) \geqslant q^{\ell b_{d/\ell,r}}\big(1-15q^{\ell-d}-8q^{(1-\ell)b_{d/\ell,r}}\big) \geqslant q^{\ell b_{d/\ell,r}}\big(1-16q^{\ell-d}\big). \tag{35}$$

Combining (34) and (35), we obtain

$$q^{\ell b_{d/\ell,r}}\big(1-16q^{\ell-d}\big) \leqslant \#\mathcal{E}_{d,r}(\mathbb{F}_q) \leqslant 3D_{\ell,d,r}q^{\ell b_{d/\ell,r}}. \tag{36}$$

Putting together (30), (32), and (36) finishes the proof of the theorem. □

Arguing as in the proof of Corollary 16, we obtain the following consequence of Theorem 18, again with an exact rate of convergence in q.

Corollary 19. *With notations and assumptions as in Theorem 18, we have*

$$\frac{(1-4q^{2(1-d)(r-1)})}{2c_{d,r}}q^{(2d-3)(r-2)-\frac{d(d-1)}{2}} \leqslant \frac{\#\mathcal{E}_{d,r}(\mathbb{F}_q)}{\#\mathcal{C}_{d,r}(\mathbb{F}_q)} \leqslant 2D_{\ell,d,r}q^{(2d-3)(r-2)-\frac{d(d-1)}{2}} \quad \text{for } d/\ell \leqslant 4r-7,$$

$$\frac{(1-16q^{\ell-d})}{2c_{d,r}}q^{3(\ell-1)(r-2)-d^2(\ell-1)/2\ell} \leqslant \frac{\#\mathcal{E}_{d,r}(\mathbb{F}_q)}{\#\mathcal{C}_{d,r}(\mathbb{F}_q)} \leqslant 3D_{\ell,d,r}q^{3(\ell-1)(r-2)-d^2(\ell-1)/2\ell} \quad \text{for } d/\ell \geqslant 4r-8,$$

with $D_{\ell,d,r} = (ed/\ell)^{r(r+1)(d^2/\ell^2+1)+4rg_{d/\ell,r}}$, $c_{d,r} = (2ed)^{r(r+1)(d^2+1)+4rg_{d,r}}$ *and* $g_{d/\ell,r}$ *as in* (17).

7. The average number of $\mathbb{F}_q$-rational points on $\mathbb{F}_q$-curves

The present paper was partially motivated by the following question: how many rational points does a typical curve have? As a consequence of the seminal paper of A. Weil [22], for an absolutely irreducible $\mathbb{F}_q$-curve C of degree d of $\mathbb{P}^r$, we have the estimate (see, e.g., [19])

$$\left|\#C(\mathbb{F}_q) - (q+1)\right| \leqslant (d-1)(d-2)q^{1/2} + \lambda(d,r), \tag{37}$$

where $\lambda(d,r)$ is a constant independent of q. From [3] it follows that we can take $\lambda(d,r) = 6d^2$ if $q \geqslant 15d^{13/3}$. Combining these inequalities yields

$$\left|\#C(\mathbb{F}_q) - (q+1)\right| \leqslant d^2 q^{1/2} \tag{38}$$

for any absolutely irreducible $\mathbb{F}_q$-curve and $q \geqslant 15d^{13/3}$. Recall that Theorem 16 and Corollary 19 assert that "almost all" curves are absolutely irreducible for large values of q. The set of $\mathbb{F}_q$-curves C of $\mathbb{P}^r$ of degree d satisfying (38) contains the set of absolutely irreducible curves of $\mathcal{C}_{d,r}(\mathbb{F}_q)$. From these remarks we obtain the following result on the average number of $\mathbb{F}_q$-rational points of the curves in $\mathcal{C}_{d,r}(\mathbb{F}_q)$.

Theorem 20. *Let notation be as in Theorem 18 and assume that $q \geqslant 15d^{13/3}$, $r \geqslant 3$ and $d > 4r-7$. Then the expectation of $\#C(\mathbb{F}_q)$ for uniformly random C in $\mathcal{C}_{d,r}(\mathbb{F}_q)$ satisfies*

$$\left|\mathbb{E}\left[\#C(\mathbb{F}_q)\right] - (q+1)\right| \leqslant d^2 q^{1/2} + 3dc_{d,r}q^{-(d-2r+2)} \tag{39}$$

with $c_{d,r} = (2ed)^{r(r+1)(d^2+1)+4rg_{d,r}}$. Moreover, the probability distribution is concentrated around the expectation, namely

$$\Pr\left[\left|\#C(\mathbb{F}_q) - (q+1)\right| \leqslant d^2 q^{1/2}\right] \geqslant 1 - 2c_{d,r}q^{-(d-2r+3)}. \tag{40}$$

The latter bound tends to 1 *as q tends to infinity.*

Proof. First we prove (40). Let $\mathcal{A}_{d,r}(\mathbb{F}_q)$ denote the set of absolutely irreducible $\mathbb{F}_q$-curves. This set is the complement in $\mathcal{C}_{d,r}(\mathbb{F}_q)$ of the union of the set $\mathcal{R}^{(q)}_{d,r}(\mathbb{F}_q)$ of $\mathbb{F}_q$-reducible $\mathbb{F}_q$-curves plus the set $\mathcal{E}_{d,r}(\mathbb{F}_q)$ of relatively irreducible $\mathbb{F}_q$-curves. Hence we have

$$\Pr\left[\mathcal{A}_{d,r}(\mathbb{F}_q)\right] \geqslant 1 - 2\max\left\{\Pr\left[\mathcal{R}^{(q)}_{d,r}(\mathbb{F}_q)\right], \Pr\left[\mathcal{E}_{d,r}(\mathbb{F}_q)\right]\right\}.$$

The assumption on d implies

$$\min\left\{d(d-1)/2 - (2d-3)(r-2), d^2(\ell-1)/2\ell - 3(\ell-1)(r-2)\right\} \geqslant d - 2r + 3. \tag{41}$$

From Theorem 16, Corollary 19 and (41), it follows that

$$\max\left\{\Pr\left[\mathcal{R}^{(q)}_{d,r}(\mathbb{F}_q)\right], \Pr\left[\mathcal{E}_{d,r}(\mathbb{F}_q)\right]\right\} \leqslant c_{d,r}q^{-(d-2r+3)}. \tag{42}$$

Finally, (38) and (42) yield

$$\Pr\left[\left|\#C(\mathbb{F}_q) - (q+1)\right| \leqslant d^2 q^{1/2}\right] \geqslant \Pr\left[\mathcal{A}_{d,r}(\mathbb{F}_q)\right] \geqslant 1 - 2c_{d,r}q^{-(d-2r+3)}.$$

Now we estimate the expectation (39). For this purpose we observe that (4) implies $\#C(\mathbb{F}_q) \leqslant d(q+1)$ for any curve $C \in \mathcal{C}_{d,r}(\mathbb{F}_q)$. Combining this upper bound with (42) we obtain

$$\begin{aligned}\mathbb{E}\big[\#C(\mathbb{F}_q)\big] &\leqslant \big(q+1+d^2q^{1/2}\big)\Pr\big[\#C(\mathbb{F}_q) \leqslant q+1+d^2q^{1/2}\big] \\ &\quad + d(q+1)\Pr\big[\#C(\mathbb{F}_q) > q+1+d^2q^{1/2}\big] \\ &\leqslant q+1+d^2q^{1/2} + d(q+1)\Pr\big[\mathcal{E}_{d,r}(\mathbb{F}_q) \cup \mathcal{R}^{(q)}_{d,r}(\mathbb{F}_q)\big] \\ &\leqslant q+1+d^2q^{1/2} + 3dc_{d,r}q^{-(d-2r+2)}.\end{aligned}$$

On the other hand, we have

$$\begin{aligned}\mathbb{E}\big[\#C(\mathbb{F}_q)\big] &\geqslant \big(q+1-d^2q^{1/2}\big)\Pr\big[\#C(\mathbb{F}_q) \geqslant q+1-d^2q^{1/2}\big] \\ &\geqslant \big(q+1-d^2q^{1/2}\big)\Pr\big[\mathcal{A}_{d,r}(\mathbb{F}_q)\big] \\ &\geqslant q+1-d^2q^{1/2} - 2c_{d,r}q^{-(d-2r+2)}.\end{aligned}$$

Combining the upper and the lower bound on $\mathbb{E}[\#C(\mathbb{F}_q)]$, we deduce (39). □

Open question. Can one similarly determine the probabilities for other "rare" types of curves, say, the ones that are singular or not complete intersections?

References

[1] F. Amoroso, Multiplicité et formes éliminantes, Bull. Soc. Math. France 122 (2) (1994) 149–162.
[2] A. Bodin, Number of irreducible polynomials in several variables over finite fields, Amer. Math. Monthly 115 (7) (2008) 653–660.
[3] A. Cafure, G. Matera, Improved explicit estimates on the number of solutions of equations over a finite field, Finite Fields Appl. 12 (2) (2006) 155–185.
[4] A. Cafure, G. Matera, An effective Bertini theorem and the number of rational points of a normal complete intersection over a finite field, Acta Arith. 130 (1) (2007) 19–35.
[5] F. Catanese, Chow varieties, Hilbert schemes, and moduli spaces of surfaces of general type, J. Algebraic Geom. 1 (4) (1992) 561–595.
[6] D. Eisenbud, J. Harris, The dimension of the Chow variety of curves, Compos. Math. 83 (3) (1992) 291–310.
[7] W. Fulton, Intersection Theory, Springer, Berlin, Heidelberg, New York, 1984.
[8] J. von zur Gathen, Counting reducible and singular bivariate polynomials, Finite Fields Appl. 14 (4) (2008) 944–978.
[9] J. von zur Gathen, A. Viola, K. Ziegler, Counting reducible, powerful, and relatively irreducible multivariate polynomials over finite fields, in: A. López-Ortiz (Ed.), LATIN 2010: Theoretical Informatics, Proceedings of the 9th Latin American Symposium, Oaxaca, Mexico, April 19–23, 2010, in: Lecture Notes in Comput. Sci., vol. 6034, Springer, Berlin, Heidelberg, 2010, pp. 243–254 (Extended Abstract). Final version to appear in SIAM J. Discrete Math.
[10] S. Ghorpade, C. Krattenthaler, The Hilbert series of Pfaffian rings, in: C. Christensen, et al. (Eds.), Algebra, Arithmetic and Geometry with Applications. Papers from Shreeram S. Ahhyankar's 70th Birthday Conference, Purdue University, West Lafayette, IN, USA, July 19–26, 2000, Springer, Berlin, 2004, pp. 337–356.
[11] S. Ghorpade, G. Lachaud, Étale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields, Mosc. Math. J. 2 (3) (2002) 589–631.
[12] L. Guerra, Complexity of Chow varieties and number of morphisms on surfaces of general type, Manuscripta Math. 98 (1) (1999) 1–8.
[13] J. Harris, Algebraic Geometry: A First Course, Grad. Texts in Math., vol. 133, Springer, New York, Berlin, Heidelberg, 1992.
[14] J. Heintz, Definability and fast quantifier elimination in algebraically closed fields, Theoret. Comput. Sci. 24 (3) (1983) 239–277.
[15] J. Heintz, C.P. Schnorr, Testing polynomials which are easy to compute, in: International Symposium on Logic and Algorithmic, Zurich, 1980, in: Monogr. Enseign. Math., vol. 30, 1982, pp. 237–254.
[16] X.-D. Hou, G. Mullen, Number of irreducible polynomials and pairs of relatively prime polynomials in several variables over finite fields, Finite Fields Appl. 15 (3) (2009) 304–331.
[17] J. Kollár, Effective Nullstellensatz for arbitrary ideals, J. Eur. Math. Soc. (JEMS) 1 (3) (1999) 313–337.
[18] J. Kollár, Rational Curves on Algebraic Varieties, Springer, 1999.

[19] W. Schmidt, Equations Over Finite Fields. An Elementary Approach, Lecture Notes in Math., vol. 536, Springer, New York, 1976.
[20] P. Stanica, Good lower and upper bounds on binomial coefficients, JIPAM. J. Inequal. Pure Appl. Math. 2 (3) (2001), Article 30.
[21] W. Vogel, Results on Bézout's Theorem, Tata Inst. Fund. Res. Lect. Math., vol. 74, Tata Inst. Fund. Res, Bombay, 1984.
[22] A. Weil, Sur les courbes algébriques et les varietés qui s'en déduisent, Hermann, Paris, 1948.