A Quick and Dirty Irreducibility Test for Multivariate Polynomials over $\mathbb{F}_q$

H. -C. Graf v. Bothmer and F. -O. Schreyer

CONTENTS

2000 AMS Subject Classification: Primary 12E05

Keywords: Irreducibility test, multivariate polynomials, black box polynomials, finite fields

We provide some statistics about an irreducibility/reducibility test for multivariate polynomials over finite fields based on counting points. The test works best for polynomials in a large number of variables and can also be applied to black-box polynomials.

1. INTRODUCTION

Let $f \in \mathbb{F}_q[x_1, \dots, x_n]$ be a polynomial. Since $f(x)$ can take only q possible values for every point in $x \in \mathbb{A}^n(\mathbb{F}_q)$, we expect that $f(x) = 0$ for about $\frac{1}{q}$ of the points $\mathbb{A}^n(\mathbb{F}_q)$. If, on the other hand, $f = gh$ is a product of two polynomials $g, h \in \mathbb{F}_q[x_1, \dots, x_n]$, we have $f(x) = 0$ if $g(x) = 0$ or $h(x) = 0$. So, one might expect that products of polynomials satisfy $f(x) = g(x)h(x) = 0$ for approximately $\frac{2}{q} - \frac{1}{q^2}$ of the points $x \in \mathbb{A}^n(\mathbb{F}_q)$. This phenomenon is well explained by the Weil formulas [Milne 80, page 286], [Lang and Weil 54]. The number N_ν of $\mathbb{F}_{q^\nu}$-rational points on an absolutely irreducible variety of dimension r defined over $\mathbb{F}_q$ grows like

$$N_\nu = q^{r\nu} + O(q^{(r-1/2)\nu}).$$

However, in this paper, we follow a more naive approach. We propose the following irreducibility test for multivariate polynomials f over $\mathbb{F}_q$:

Evaluate f at N random points. We reject the hypothesis that f is reducible if the fraction of zeros $\gamma_q(f)$ found is significantly smaller than $\frac{2}{q} - \frac{1}{q^2}$. Note that 99.5% of all polynomial functions satisfy

$$\gamma_q(f) \leq \frac{1}{q} + 2.58\sqrt{\frac{\frac{1}{q}(1 - \frac{1}{q})}{q^n}}.$$

This irreducibility test is quick, since the number of evaluations needed to detect a given percentage $1 - \epsilon$ of all products of polynomial functions and of all general

1058-6458/2005 $0.50 per page

$$\begin{pmatrix} x_0+x_1-x_3-x_4 & x_0-x_1-x_2-x_4 & -x_0+x_3+x_4 \\ -x_0-x_2+x_3+x_4 & x_0-x_1-x_2-x_3+x_4 & -x_0+x_1-x_2+x_3+x_4 \\ -x_0-x_2-x_3-x_4 & -x_0-x_1-x_3-x_4 & -x_1+x_4 \\ -x_1-x_2-x_3+x_4 & -x_1-x_2 & -x_1+x_2 \\ -x_0+x_1-x_2-x_3-x_4 & -x_0+x_2-x_3+x_4 & x_0-x_1+x_2+x_3+x_4 \end{pmatrix}$$

FIGURE 1.

polynomial functions does not depend on the degree of the polynomials considered, i.e.,

$$N \sim O(-q \ln \epsilon).$$

On the other hand it is dirty, since it does not give a definite answer. Moreover, we cannot make ϵ arbitrarily small, because N is bounded by q^n, the number of $\mathbb{F}_q$ rational points in $\mathbb{A}^n(\mathbb{F}_q)$. There will always be a few polynomials that cannot be correctly classified by our method at all. For example, consider the product of an irreducible, absolutely reducible polynomial with a further absolutely irreducible polynomial or an irreducible polynomial that interpolates all rational points.

The test works for implicitly given (black-box) polynomials as well. We give examples of such polynomials below.

The expected fraction of zeros for special classes of polynomials can also be larger than $\frac{1}{q}$. For example, the expected fraction of zeros for $n \times n$ determinants is

$$E(\gamma_{q,\det}) = 1/q + 1/q^2 - 1/q^5 - 1/q^7 + O(1/q^{12}),$$

for $n \geq 12$.

We use the following notation:

$\mathbb{F}_q$	the finite field with q elements;
$X \subset \mathbb{A}^n$	an affine algebraic set;
$X(\mathbb{F}_q)$	the $\mathbb{F}_q$-rational points of X;
$\lvert X\rvert = \lvert X(\mathbb{F}_q)\rvert$	the number of $\mathbb{F}_q$-rational points of X;
$\gamma_q(X)$	the fraction of $\mathbb{F}_q$-rational points in $\mathbb{A}^n$ that are contained in X;
$\mathcal{B}(N,p,k) =$ $\binom{N}{k}p^k(1-p)^{N-k}$	the binomial distribution;
N	the number of trials;
p	the success probability;
k	the number of successes;
$\mathcal{N}(\mu,\sigma)$	the normal distribution with mean μ and variance σ^2.

$\mathcal{B}(N,p)$ can be approximated by $\mathcal{N}(p, \sqrt{p(1-p)/N})$.

2. FRACTIONS OF ZEROS

Example 2.1. (Random Polynomial.) We choose fixed polynomials f_1, f_2 of degree 5 and f_3 of degree 10 in $\mathbb{Z}[x_1, \ldots, x_4]$ with coefficients in $[-9, 9]$ using the random number generator of the computer algebra system Macaulay 2 [Grayson and Stillman 02] and consider $f = f_1 f_2 + 7 f_3$. Let X be the vanishing set $V(f)$.

A black-box polynomial is a polynomial for which it is easy, given x, to compute $f(x)$. For our method we need even less, namely that, given x, it is easy to check whether $f(x) = 0$ holds. Therefore, our method also applies to black-box hypersurfaces. Often these checks are possible even if the explicit formula for f in terms of the unknowns $x_1, \ldots, x_n$ is hard or impossible to write down.

Example 2.2. (Discriminant.) Let $S_d \subset H^0(\mathbb{P}^2, \mathcal{O}(d))$ be the hypersurface of singular homogeneous polynomials f of degree d in three variables. For each point $f \in H^0(\mathbb{P}^2, \mathcal{O}(d))$, it is easy to decide whether $f \in S_d$ via the Jacobi criterion [Eisenbud 95, Section 16.6]. On the other hand, the equation of S_d in $\binom{d+2}{2}$ variables is not obvious [Gel′fand et al. 94, page 38, Example 4.15].

Example 2.3. (Dual Variety.) Let $C \subset \mathbb{P}^4$ be the determinantal curve of degree 10 and genus 6 where the maximal minors of the 5×3 matrix in Figure 1 vanish.

Let $D = \{H \in \check{\mathbb{P}}^4 \mid H \cap C \text{ is singular}\}$ be the dual variety of C.

Definition 2.4. Let $X \subset \mathbb{A}^n$ an algebraic set. We denote by

$$\gamma_q(X) := \frac{|X(\mathbb{F}_q)|}{|\mathbb{A}^n(\mathbb{F}_q)|},$$

the *fraction of* $\mathbb{F}_q$*-rational points* on X. In particular, for a hypersurface $X = V(f)$, we have $\gamma_q(f) = \gamma_q(V(f))$. We call $\gamma_q(f)$ the *fraction of* $\mathbb{F}_q$*-rational zeros of* f.

Example 2.5. We estimate γ_q in three of our examples by evaluating $N = 1{,}000$ random points over all primes up to 17. Table 1 gives the 99% confidence interval for γ_q. In this article, we will explain these numbers.

q	X	S_8	D
2	$56.7\% \pm 4.0\%$	$68.4\% \pm 2.9\%$	$55.3\% \pm 4.1\%$
3	$33.8\% \pm 3.9\%$	$42.3\% \pm 3.1\%$	$49.2\% \pm 4.1\%$
5	$17.9\% \pm 3.1\%$	$24.0\% \pm 2.6\%$	$24.9\% \pm 3.5\%$
7	$26.2\% \pm 3.6\%$	$16.8\% \pm 2.3\%$	$35.3\% \pm 3.9\%$
11	$9.3\% \pm 2.4\%$	$8.9\% \pm 1.8\%$	$8.0\% \pm 2.2\%$
13	$8.6\% \pm 2.3\%$	$9.6\% \pm 1.8\%$	$8.4\% \pm 2.3\%$
17	$5.2\% \pm 1.8\%$	$8.1\% \pm 1.7\%$	$5.9\% \pm 1.9\%$

TABLE 1.

Remark 2.6. We can compute the true values $\gamma_2(X) = 56.3\%$, $\gamma_3(X) = 34.6\%$, and $\gamma_5(X) = 18.7\%$ with the same effort, since there are less than $1,000$ rational points in $\mathbb{A}^4(\mathbb{F}_q)$ for $q \leq 5$.

To study the map

$$\gamma_q \colon \mathbb{F}_q[x_1 \dots x_n] \to [0,1],\ f \mapsto \gamma_q(f),$$

we note that $\gamma_q(f)$ factors over the ring $R := \operatorname{map}(\mathbb{A}^n(\mathbb{F}_q), \mathbb{F}_q)$:

$$\begin{tikzcd}
\mathbb{F}_q[x_1 \dots x_n] \arrow[r, "\gamma_q"] \arrow[d, "\psi"] & {[0,1]} \\
R \arrow[ur] &
\end{tikzcd}$$

Lemma 2.7. *ψ is surjective.*

Proof: Since $|\mathbb{A}^n(\mathbb{F}_q)| = q^n < \infty$, we can find a polynomial with prescribed values at these points via interpolation. □

We study the distribution of γ_q on R by regarding it as a random variable on the finite probability space

$$(R, \Omega, P)$$

with Ω the sigma algebra of all subsets of R and P the constant probability measure.

Proposition 2.8. *The distribution of γ_q on R is binomial*

$$P\left(\gamma_q = \frac{k}{q^n}\right) = \mathcal{B}\left(q^n, \frac{1}{q}, k\right).$$

In particular, the expectation value of γ_q is $E(\gamma_q) = \frac{1}{q}$.

Proof: We have to count the maps $f \in R$ that map precisely k different points to 0. Since the values at different points are independent, this number is

$$\binom{q^n}{k} 1^k \cdot (q-1)^{q^n - k}.$$

The probability that $\gamma_q = \frac{k}{q^n}$ is, therefore,

$$\begin{aligned} P\left(\gamma_q = \frac{k}{q^n}\right) &= \binom{q^n}{k} \left(\frac{1}{q}\right)^k \cdot \left(\frac{q-1}{q}\right)^{q^n - k} \\ &= \mathcal{B}\left(q^n, \frac{1}{q}, k\right). \end{aligned}$$

□

Example 2.9. Consider maps

$$f \in R = \operatorname{map}(\mathbb{A}^4(\mathbb{F}_{11}), \mathbb{F}_{11}).$$

The distribution of fractions of zeros is

$$P\left(\gamma_{11} = k/11^4\right) = \mathcal{B}\left(11^4, 1/11, k\right).$$

From its approximation by the normal distribution $\mathcal{N}(0.0909, 0.0024)$, we obtain

$$P(0.0847 \leq \gamma_{11} \leq 0.0971) \geq 99\%.$$

We now consider products. The random variable

$$\begin{aligned} &\gamma_{q,\cup} \colon R \times R \to [0,1], \\ &\gamma_{q,\cup}(f,g) = \gamma_q(fg) = |V(f) \cup V(g))|/q^n \end{aligned}$$

assigns to each pair of functions the fraction of zeros of their product.

Proposition 2.10. *On $R \times R$, the distribution of $\gamma_{q,\cup}$ is*

$$P\left(\gamma_{q,\cup} = k/q^n\right) = \mathcal{B}\left(q^n, (2q-1)/q^2, k\right).$$

In particular, the expectation value of $\gamma_{q,\cup}$ is

$$E(\gamma_{q,\cup}) = \frac{2q-1}{q^2} = 1 - \left(\frac{q-1}{q}\right)^2.$$

Proof: The value of $f \cdot g$ at a point x depends on the values of f and g at x. There are q^2 ways of choosing these values, of which $(q-1)^2$ ways give $(f \cdot g)(x) \neq 0$. □

Example 2.11. Consider pairs (f, g) of functions in R as in Example 2.9. The distribution of $\gamma_{11,\cup}$ is now

$$P\left(\gamma_{11,\cup} = k/11^4\right) = \mathcal{B}\left(11^4, 21/11^2, k\right).$$

From its approximation by the normal distribution $\mathcal{N}(0.1736, 0.0031)$, we obtain

$$P(0.1655 \leq \gamma_{11,\cup} \leq 0.1816) \geq 99\%.$$

Note that this range does not intersect

$$P(0.0847 \leq \gamma_{11} \leq 0.0971) \geq 99\%.$$

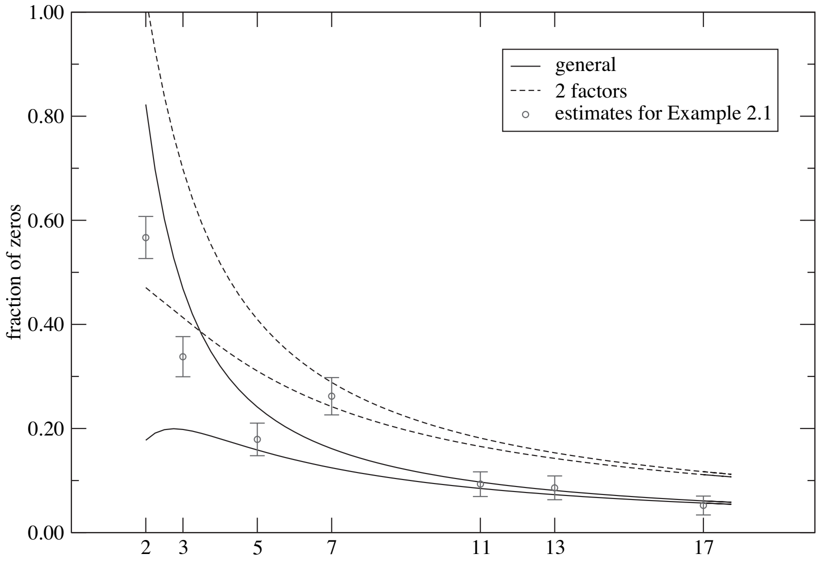

FIGURE 2. Points on a hypersurface of degree 10 in $\mathbb{A}^4$. 99% of polynomial functions on $\mathbb{A}^4$ have γ_q between the continuous lines. 99% of products have γ_q between the dashed lines.

Geometrically, products of functions correspond to the union of their zero sets. We now prove that γ_q also behaves well under other geometric operations.

Proposition 2.12. (Intersection.) *Let $X \subset \mathbb{A}^n$ be a subvariety. We consider the random variable*

$$\gamma_{q,\cap X} \colon R \to [0,1],\ \gamma_{q,\cap X}(f) = |V(f) \cap X|/q^n.$$

The distribution of $\gamma_{q,\cap X}$ is

$$P(\gamma_{q,\cap X} = k/q^n) = \mathcal{B}(|X|, 1/q, k).$$

In particular, the expectation value of $\gamma_{q,\cap X}$ is $E(\gamma_{q,\cap X}) = \gamma_q(X)/q$, where $\gamma_q(X) = |X|/q^n$ is the fraction of points of X in $\mathbb{A}^n(\mathbb{F}_q)$.

Proof: Clearly, $x \in X \cap V(f)$ if and only if $x \in X$ and $f(x) = 0$. Since the values of f can be chosen independently of the points on X, we have

$$P(x \in \ker f \cap X | x \in X) = \frac{1}{q}. \qquad \square$$

Corollary 2.13. *Consider the random variable*

$$\gamma_{q,\cap} \colon R^c \to [0,1],$$
$$\gamma_{q,\cap}(f_1, \dots, f_c) = |V(f_1) \cap \cdots \cap V(f_c)|/q^n.$$

Then, the expected fraction of points is $E(\gamma_{q,\cap}) = \frac{1}{q^c}$.

Proof: Use Proposition 2.12 inductively. □

Notice that for polynomials $f_1, \dots, f_c$, the expected codimension of $V(f_1, \dots, f_c) \subset \mathbb{A}^n$ is also c.

Proposition 2.14. (Substitution.) *Let*

$$R^m = \mathrm{map}(\mathbb{A}^n(\mathbb{F}_q), \mathbb{A}^m(\mathbb{F}_q))$$

and $X \subset \mathbb{A}^m(\mathbb{F}_q)$ be a subset. Consider the random variable

$$\gamma_{q,subst} \colon R^m \to [0,1],\ \gamma_{q,subst}(\phi) = |\phi^{-1}X|/q^n.$$

The distribution of $\gamma_{q,subst}$ is

$$P\left(\gamma_{q,subst} = k/q^n\right) = \mathcal{B}\left(q^n, \gamma_q(X), k\right).$$

In particular, the expectation value of $\gamma_{q,subst}$ is $E(\gamma_{q,subst}) = \gamma_q(X) = |X|/q^n$.

Proof: Choosing functions $f_1, \dots, f_n$ is equivalent to the independent choice of the image points. Therefore, the probability of $\phi^{-1}(X)$ containing exactly k points is the same as the probability of hitting k points of X when choosing q^n points in $\mathbb{F}_q^n$. This gives the desired binomial distribution. □

3. DETERMINANTAL VARIETIES

Even though we have shown that $E(\gamma_q) = \frac{1}{q}$ with a small variance on the set of all functions from A to $\mathbb{F}_q$, there are special classes of functions that have larger expected γ_q. It turns out that this behavior is common for determinants.

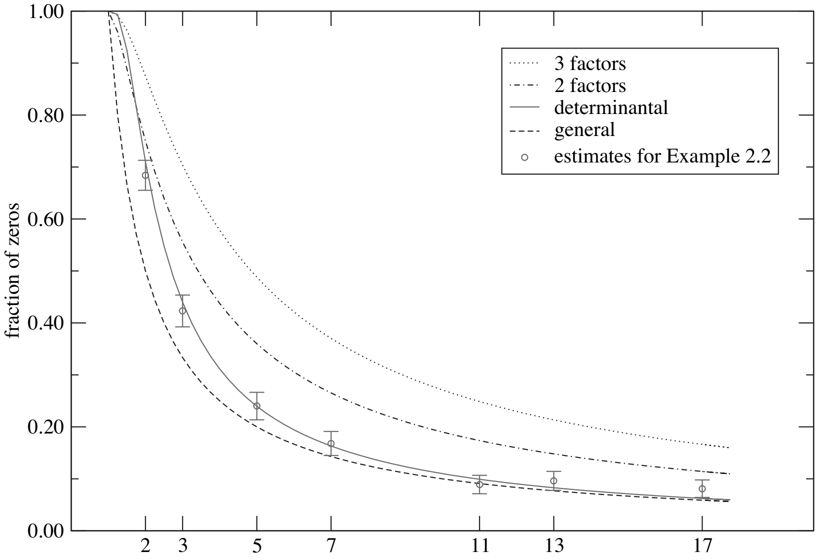

FIGURE 3. Singular curves in $\mathbb{P}^2$. The graph shows the expectation values for various classes of polynomials in a large number of variables and the measurement for S_8, the hypersurface of singular plane curves of degree 8. Note that the graph shows that about 70% of all plane curves over $\mathbb{F}_2$ are singular.

Proposition 3.1. *Let $X \subset \mathbb{A}^{nm}$ be the determinantal variety of $n \times m$ matrices with $n \leq m$ of rank less than n. Then, the fraction of rational points of X is*

$$\gamma_q(X) = 1 - \prod_{i=0}^{n-1} \left(1 - \frac{1}{q^{m-i}}\right),$$

i.e., X contains $\gamma_q(X) \cdot q^{nm}$ rational points.

Proof: We prove by induction that the number of matrices that have maximal rank is

$$\prod_{i=0}^{n-1} \left(q^m - q^i\right).$$

M is a matrix of full rank if and only if the first $n-1$ rows form a matrix of full rank and the last row is linearly independent of the first $n-1$ rows. Since there are q^{n-1} linear combinations of the first $n-1$ rows, we obtain another factor $(q^m - q^{n-1})$.

□

Corollary 3.2. *On the space of matrices R^{nm}, consider the random variable*

$$\gamma_{q,\det} \colon R^{nm} \to [0,1],$$
$$\gamma_{q,\det}(M) = |\{x \in \mathbb{A}^n \mid \operatorname{rank} M(x) < n\}|/q^n.$$

Then, the fraction of zeros has expectation value

$$E(\gamma_{q,\det}) = 1 - \prod_{i=0}^{n-1} \left(1 - \frac{1}{q^{m-i}}\right) = \frac{1}{q^{m-n+1}} + \dots .$$

The distribution of $\gamma_{q,det}$ is

$$P\left(\gamma_{q,\det} = k/q^n\right) = \mathcal{B}(q^n, E(\gamma_{q,\det}), k).$$

Proof: Substitute functions for the variables in the generic $n \times m$ matrix and use Proposition 2.14. □

In the special case of $n \times n$ square matrices we have

$$E(\gamma_{q,\det}) = 1/q + 1/q^2 - 1/q^5 - 1/q^7 + O(1/q^{12}),$$

for $n \geq 12$.

Example 3.3. (Example 2.2 continued.) For small primes the divisor S_d has more points than expected for irreducible polynomials, but not enough to seem reducible; see Figure 3. Our measurements are consistent with the well known fact that S_d is an irreducible determinantal hypersurface [Gel′fand et al. 94, Chapter 13, Propositions 1.6 and 1.7].

4. TESTING

To decide between two binomial distributions with success probabilities $p_1 < p_2$ and N experiments, we compute empirical probability $\bar{p} = \frac{k}{N}$ and decide for p_1 if

$$\bar{p} \leq p_{middle} := \sqrt{p_1 p_2}\frac{\sqrt{p_1(1-p_2)} + \sqrt{p_2(1-p_1)}}{\sqrt{p_1(1-p_1)} + \sqrt{p_2(1-p_2)}}$$
$$\approx \sqrt{p_1 p_2}.$$

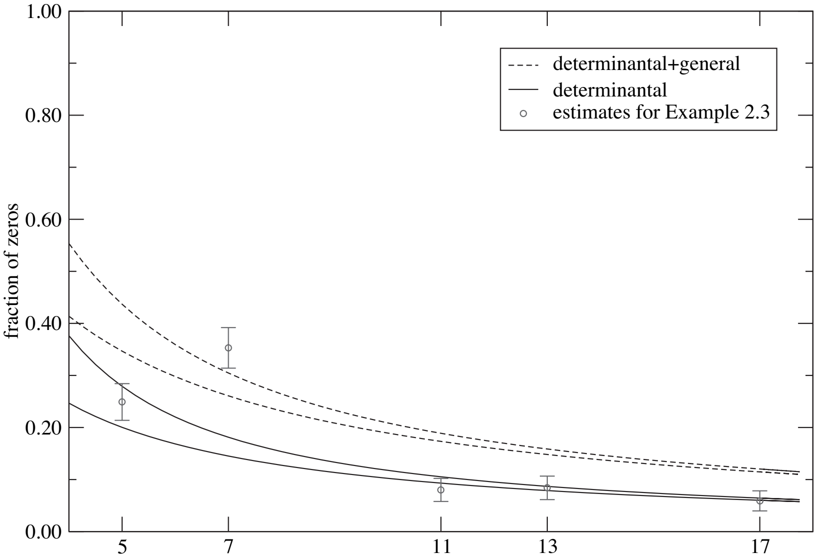

FIGURE 4. Points on the dual variety of a curve in $C \subset \mathbb{P}^4$. C has a simple node over $\mathbb{F}_7$ and is smooth over $\mathbb{F}_p$ for $p = 5, 11, 13, 17$.

To achieve a confidence level of $1 - \epsilon$ we choose $s = s(\epsilon)$ such that

$$\Phi(s) = \frac{1}{2} \operatorname{erfc} \frac{s}{\sqrt{2}} = \frac{1}{\sqrt{2\pi}} \int_s^\infty e^{-\frac{x^2}{2}} dx = \epsilon,$$

where erfc is the complementary error function and N such that

$$\sqrt{N} \geq s(\epsilon) \frac{\sqrt{p_1(1-p_1)} + \sqrt{p_2(1-p_2)}}{p_2 - p_1}. \tag{4–1}$$

This is certainly true if we choose

$$\sqrt{N} \geq s(\epsilon) \frac{\sqrt{p_1} + \sqrt{p_2}}{p_2 - p_1}.$$

We will now use this formula to estimate the number of evaluations needed in our irreducibility test. By Proposition 2.8, we know that $1 - \epsilon$ of all polynomials satisfy

$$\gamma_q \leq \frac{1}{q} + s(\epsilon) \sqrt{\frac{\frac{1}{q}(1 - \frac{1}{q})}{q^n}}.$$

In these cases, we will only overestimate N in Equation (4–1) if we set

$$p_1 = \frac{1}{q} + s(\epsilon) \sqrt{\frac{\frac{1}{q}(1 - \frac{1}{q})}{q^n}}.$$

Similarly, we know that $1 - \epsilon$ of all products of polynomials satisfy

$$\gamma_q \geq \frac{2q-1}{q^2} - s(\epsilon) \sqrt{\frac{\frac{2q-1}{q^2}(1 - \frac{2q-1}{q^2})}{q^n}}.$$

Again, we will only overestimate N in Equation (4–1) if we set

$$p_2 = \frac{2q-1}{q^2} - s(\epsilon) \sqrt{\frac{\frac{2q-1}{q^2}(1 - \frac{2q-1}{q^2})}{q^n}}$$

in these cases.

The decision based on the empirical probability $\bar{p} = \frac{k}{N}$ is then correct in $1 - \epsilon$ cases of the experiments. Note, however, that for fixed n and q we cannot make ϵ arbitrarily small, since we need $p_1 \leq p_2$.

We use

$$p_1 \leq p_2 \leq \frac{2}{q}$$

in the numerator and

$$\begin{aligned} p_2 - p_1 &\leq \left(\frac{2q-1}{q^2} - s(\epsilon) \sqrt{\frac{2}{q^{n+1}}} \right) - \left(\frac{1}{q} + s(\epsilon) \sqrt{\frac{1}{q^{n+1}}} \right) \\ &\leq \frac{q-1}{q^2} - s(\epsilon) \frac{\sqrt{2}+1}{q^{\frac{n+1}{2}}} \end{aligned}$$

in the denominator to see that

$$\sqrt{N} \geq s(\epsilon) \frac{(2q)^{\frac{3}{2}}}{q - 1 - s(\epsilon)(\sqrt{2}+1) q^{-\frac{n-1}{2}}} \ ,$$

which approaches $2s(\epsilon)\sqrt{2q}$ for large n or q. Since $s(\epsilon) = O(\sqrt{-\ln(\epsilon)})$, we conclude that N grows like $O(-q \ln \epsilon)$.

For $\epsilon = 0.5\%$ and $s = 2.575829304$, the number of trials needed is shown in Table 2. In Tables 2 and 3, ∞ indicates that there are not enough points in $\mathbb{A}^n(\mathbb{F}_q)$ to perform the test for the required $\epsilon = 0.5\%$. In the cases where we can perform the test, the deciding number of successes Np_{middle} is shown in Table 3.

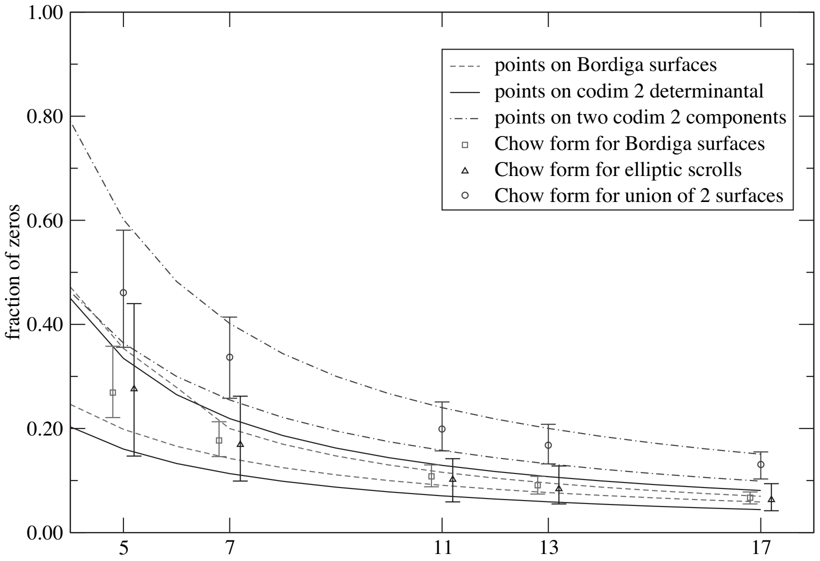

FIGURE 5. Surfaces in $\mathbb{P}^4$. The 5% and the 95% quantiles of γ_q for the Chow forms of 100 Bordiga surfaces, elliptic scrolls, and their unions compared with the error estimates for counting points on codimension 2 determinantal varieties rescaled. Using the geometry of Bordiga surfaces we obtain a better estimate.

	2	3	5	7	11	13	17
$n = 1$	∞	∞	∞	∞	∞	∞	∞
$n = 2$	∞	∞	∞	∞	∞	∞	∞
$n = 3$	∞	∞	∞	27473	2338	1897	1661
$n = 4$	∞	∞	1095	644	631	679	800
$n = 5$	∞	1685	366	367	481	549	693
$n = 6$	∞	382	258	307	446	520	670
$n = 7$	4361	223	224	288	436	512	665
$n = 8$	614	173	211	282	433	510	664
$n = 9$	293	151	205	279	432	509	663
$n = 10$	196	140	203	278	432	509	663

TABLE 2.

	2	3	5	7	11	13	17
$n = 1$	∞	∞	∞	∞	∞	∞	∞
$n = 2$	∞	∞	∞	∞	∞	∞	∞
$n = 3$	∞	∞	∞	5430	299	206	138
$n = 4$	∞	∞	301	128	80	73	66
$n = 5$	∞	745	100	73	61	59	57
$n = 6$	∞	169	71	61	56	56	55
$n = 7$	2760	99	61	57	55	55	55
$n = 8$	388	76	58	56	55	55	55
$n = 9$	185	67	56	55	55	55	55
$n = 10$	124	62	55	55	55	55	55

TABLE 3.

5. HIGHER CODIMENSION

In principle this method can be applied to algebraic sets of higher codimension.

Consider two surfaces in $\mathbb{P}^4$ and their union. We would like to distinguish their union from the irreducible examples. One possibility is to consider the Chow form, which is a determinantal hypersurface on $G(2, 5)$ in this case. In Figure 5, we indicate the 5% and the 95% quantiles of γ_q for the Chow forms of 100 Bordiga surfaces, elliptic scrolls, and their unions. A second possibility is to count points and apply Corollary 3.2. As Figure 5 shows, there is no difference between the two methods. The formula for the error term underestimates the number of points on a elliptic scroll, because the scroll is irregular.

The method of searching points at random in higher codimensional subsets of rational varieties helped us in proving the existence of several interesting components of Hilbert schemes [Schreyer 96, Schreyer and Tonoli 02, v. Bothmer et al. 04].

REFERENCES

[Eisenbud 95] D. Eisenbud. *Commutative Algebra With a View Toward Algebraic Geometry*, Graduate Texts in Mathematics, 150. New York: Springer, 1995.

[Gel′fand et al. 94] I. M. Gel′fand, M. M. Kapranov, and A. V. Zelevinsky. *Discriminants, Resultants, and Multidimensional Determinants*, Mathematics: Theory & Applications. Cambridge, MA: Birkhäuser Boston Inc., 1994.

[Grayson and Stillman 02] Daniel R. Grayson and Michael E. Stillman. "Macaulay 2, A Software System for Research in Algebraic Geometry." Available from World Wide Web (http://www.math.uiuc.edu/Macaulay2), 2002.

[Lang and Weil 54] S. Lang and A. Weil. "Number of Points of Varieties over Finite Fields." *Amer. J. Math.* 76 (1954), 819–827.

[Milne 80] James S. Milne. *Étale Cohomology*, Princeton Mathematical Series, 33. Princeton, NJ: Princeton University Press, 1980.

[Schreyer 96] Frank-Olaf Schreyer. "Small Fields in Constructive Algebraic Geometry." In *Moduli of Vector Bundles (Sanda, 1994; Kyoto, 1994)*, pp. 221–228, Lecture Notes in Pure and Appl. Math., 179. New York: Dekker, 1996.

[Schreyer and Tonoli 02] Frank-Olaf Schreyer and Fabio Tonoli. "Needles in a Haystack: Special Varieties via Small Fields." In *Computations in Algebraic Geometry with Macaulay 2*, pp. 251–279, Algorithms Comput. Math., 8. Berlin: Springer, 2002.

[v. Bothmer et al. 04] H. -Chr. Graf v. Bothmer, C. Erdenberger, and K. Ludwig. "A New Family of Rational Surfaces in $\mathbb{P}^4$." *Journal of Symbolic Computation* 29:1 (2005), 51–60.

H. -C. Graf v. Bothmer. Institut für Mathematik (C), Welfengarten 1, Universität Hannover, D-30167 Hannover, Germany (bothmer@math.uni-hannover.de)

F. -O. Schreyer, Mathematik und Informatik, Geb. 27, Universität des Saarlandes, D-66123 Saarbrücken, Germany (schreyer@math.uni-sb.de)

Received May 27, 2004; accepted March 22, 2005.