JOACHIM VON ZUR GATHEN & IGOR E. SHPARLINSKI (1998). Computing components and projections of curves over finite fields. *SIAM Journal on Computing* **28**(3), 822–840. URL http://dx.doi.org/10.1137/S0097539794277741X.

COMPUTING COMPONENTS AND PROJECTIONS OF CURVES OVER FINITE FIELDS

JOACHIM VON ZUR GATHEN
Fachbereich Mathematik-Informatik
Universität-GH Paderborn
D-33098 Paderborn, Germany
gathen@uni-paderborn.de

IGOR SHPARLINSKI
School of MPCE, Macquarie University
Sydney, NSW 2109, Australia
igor@mpce.mq.edu.au

February 26, 1997

Abstract. This paper provides an algorithmic approach to some basic algebraic and combinatorial properties of algebraic curves over finite fields: the number of points on a curve or a projection, its number of absolutely irreducible components, and the property of being "exceptional".

1. Introduction

Let $\mathbb{F}_q$ be a finite field with q elements, $f \in \mathbb{F}_q[x,y]$ a bivariate polynomial of total degree n over $\mathbb{F}_q$, and $\mathcal{C} = \{f = 0\} = \{(u,v) \in \mathbb{F}_q^2 \colon f(u,v) = 0\} \subseteq \mathbb{F}_q^2$ the plane curve defined by f over $\mathbb{F}_q$. In this paper we present some algorithms to compute approximations to the curve size $\#\mathcal{C}$ and to the number r_i^* of points with exactly i preimages under the projection to a coordinate axis. Since this task generalizes Weil's estimate of $\#\mathcal{C}$, it might be called a "computational Weil estimate".

In von zur Gathen *et al.* (1996), a "strip-counting" method was introduced. It is based on the general principle that the behaviour of a curve can be deduced from its behaviour over a wide enough vertical strip.

To be specific, let $S \subseteq \mathbb{F}_q$, $i \in \mathbb{N}$ and $\mathcal{C}(S)$ be the set of $(u,v) \in S \times \mathbb{F}_q$ with $f(u,v) = 0$. Furthermore, $R_i(S)$ is the set of $u \in S$ for which there are exactly i values $v \in \mathbb{F}_q$ with $f(u,v) = 0$, $r_i(S) = \#R_i(S)$, $M(S)$ is the number

of $(u, v, w) \in S^2 \times \mathbb{F}_q$ with $f(u - v, w) = 0$, and $t_i(S)$ is the number of pairs $(u, v) \in S^2$ for which there are exactly i values $w \in \mathbb{F}_q$ satisfying $f(u-v, w) = 0$.

The basic idea now is that for some properties of curves, we can find reasonably small sets S such that the above parameters are not too hard to compute, and give information about some of the global parameters we are interested in.

A completely different approach, pioneered by Schoof (1985), leads to deterministic algorithms for computing the size of $\mathcal{C} \subseteq \mathbb{F}_p^2$ with time polynomial in $\log p$ (and exponential in the degree); see Pila (1990), Huang & Ierardi (1993).

If the set S is given in some reasonable sense, e.g., if we have an efficient way to enumerate all elements of S, then one can compute $\#\mathcal{C}(S)$ and all $r_i(S)$, for $0 \le i \le n$ in time $O^{\sim}(|S| n \log q)$ (see Lemma 2.5 below). Thus $\#\mathcal{C}$ and r_i^* may be computed in exponential time of order $O^{\sim}(nq)$ by this 'brute force' algorithm. Here, we use the 'soft-Oh' notation: $A = O^{\sim}(B)$ if and only if $A = B(\log B + 2)^{O(1)}$.

Continuing the work in von zur Gathen *et al.* (1996), we show that for certain sets S, the numbers $q\#\mathcal{C}(S)/\#S$ or $qM(S)/\#S^2$, and $qr_i(S)/\#S$ or $qt_i(S)/\#S^2$ are rather good approximations to the curve size $\#\mathcal{C}$ and the projection statistics r_i^*, respectively. (The quality of these approximations is described in detail below.) In particular, to estimate $\#\mathcal{C}$, this is true for random sets of cardinality of order n^3, for any set of size of order $n^2 q^{1/2}$, and for a random shift of any set of size of order n^4. The latter is a positive answer on Question 7.2 of von zur Gathen *et al.* (1996) and is an example of reducing the number of random choices required in probabilistic algorithms. These results motivate the "strip counting" terminology, in that it is sufficient to count points in the "strip" $S \times \mathbb{F}_q$ over S.

We consider mainly the case of finite prime fields, but we also show how some results can be generalized to the case of general finite fields, and outline some difficulties that do not allow us to generalize all results.

From $r_i(S)$ and $t_i(S)$, for $0 \le i \le n$ (or their approximations) we can compute (or estimate) the numbers $\#\mathcal{C}(S)$ and $M(S)$, respectively, as

$$\#\mathcal{C}(S) = \sum_{1 \le i \le n} r_i(S) i, \quad M(S) = \sum_{1 \le i \le n} t_i(S) i.$$

A connection in the opposite direction is given in Lemma 2.2 below.

The more general problem about the number of $u \in \mathbb{F}_q$ for which the polynomial $f(u, y) \in \mathbb{F}_q[y]$ has a given 'factorization pattern' can be reduced to calculating analogues of r_i^* in extensions of the ground field $\mathbb{F}_q$.

For a curve of the form $f(x, y) = x - h(y)$, with $h(y) \in \mathbb{F}_q[y]$, $r_0^* = 0$ is equivalent to h being a permutation polynomial over $\mathbb{F}_q$.

Throughout the paper, we use the following terminology. Let K be an algebraic closure of $\mathbb{F}_q$, and $\mathcal{X} \subseteq K^{m+1}$ an algebraic curve over K, defined over $\mathbb{F}_q$, and $\mathcal{C} = \mathcal{X} \cap \mathbb{F}_q^{m+1}$ the $\mathbb{F}_q$–rational points on $\mathcal{X}$. Since we are only interested in set–theoretic (counting) properties of $\mathcal{C}$ (and not sheaf–theoretic ones), we assume that $\mathcal{X}$ is reduced and without embedded points; $\mathcal{X}$ may be reducible and have singular points. Most of our results deal with the case $m = 1$, where we assume that $\mathcal{C}$ (and $\mathcal{X}$) are given by some polynomial $f \in \mathbb{F}_q[x, y]$, as $\mathcal{C} = \{f = 0\}$. Since the curve is reduced, f is squarefree. In the proofs, certain fibre products of $\mathcal{C}$ occur. A further assumption, without loss of generality, is that $\mathcal{C} \subseteq \mathbb{F}_q^2$ contain no vertical lines; this is defined in Section 2. We denote by σ the number of absolutely irreducible components, i.e., the number of irreducible components of $\mathcal{C}$ over K that are defined over $\mathbb{F}_q$, and we use parameters λ_i defined in (2.3), via the fibre power of the curve. Lemmas 2.1 and 2.3 show that we automatically get approximations of order $O(q^{1/2})$ (for n fixed) to $\#\mathcal{C}$ and r_i^*, respectively, from approximations to σ and λ_i. So we shall mainly concentrate on algorithms to compute the latter parameters. Moreover, it also follows from those lemmas that in order to determine σ and r_i^*, it is enough to get approximations to $\#\mathcal{C}$ and to r_i^* with absolute errors less than $q/2$ and $q/2n!$, respectively. We consider the following three important special cases: $\sigma = 0$ ('exceptional curves'), $\sigma = 1$ ('almost absolutely irreducible curves') and $\lambda_0 = 0$ ('almost permutation curves').

Our algorithms address a fairly difficult problem, and have the following properties:

- they are easy to state and implement,
- their proofs of correctness rely on deep results from arithmetical algebraic geometry.

Table 1 below summarizes our algorithmic results.

2. Some general results

We start by collecting some facts about curves over finite fields. The following inequality is a consequence of the famous Weil result and Lemma 2.2 of von zur Gathen *et al.* (1996), which gives a bound for the number of points on intersections of absolutely irreducible curves and for the number of points on irreducible but not absolutely irreducible curves.

parameter	time	random	$q \geq$	cond	Alg
comp	$n^4 \log \delta^{-1} \log q$	$n^3 \log \delta^{-1}$	n^4		3.2
comp	$n^5 \delta^{-2} \log q$	1	n^4		4.9
comp	$n^3 q^{1/2}$	0	n^4	A	4.7
λ_i	$(n!)^2 \log \delta^{-1} \log q$	$n!^2 \log \delta^{-1}$	$(n!)^2 n^{4n}$		3.8
λ_i	$(n!)^2 n^{4n} \delta^{-1} \log p$	1	$(n!)^2 n^{4n}$	p	4.13
λ_i	$n! n^{2n} p^{1/2}$	0	$(n!)^2 n^{4n}$	p	4.11
except	$n^3 \log \delta^{-1} \log q$	$n^2 \log \delta^{-1}$	n^4		3.4
one comp	$n^3 \log \delta^{-1} \log q$	$n^2 \log \delta^{-1}$	n^4		3.6
$\lambda_0 = 0$	$n! \log \delta^{-1} \log q$	$n! \log \delta^{-1}$	$(n!)^2 n^{4n}$		3.10

Table 1: Computing various parameters for a curve in $\mathbb{F}_q^2$ of degree n: absolutely irreducible *comp*onents, λ_i (see (2.3)), *except*ional, *one comp*onent, and $\lambda_0 = 0$. The *time* is the number of operations in $\mathbb{F}_q$, and *random* the number of random elements; both in the $O^\sim$-sense. If random is 0, we have a deterministic algorithm. For all probabilistic algorithms, the error probability is at most δ, and $q \geq$ indicates the lower bound on q, in the $O^\sim$-sense. The *cond*ition is either Condition A from Section 4, or that the field size be a prime p.

LEMMA 2.1. *Let $\mathcal{C} \subseteq \mathbb{F}_q^{m+1}$ be a curve of degree n over $\mathbb{F}_q$ with σ absolutely irreducible components defined over $\mathbb{F}_q$. Then*

$$|\#\mathcal{C} - \sigma q| \leq n^2 q^{1/2}.$$

PROOF. Let $\mathcal{C}_1, \ldots, \mathcal{C}_\tau$ be the irreducible components of $\mathcal{C}$ over $\mathbb{F}_q$, with $\mathcal{C}_i$ absolutely irreducible if and only if $i \leq \sigma$. From the proof of Lemma 2.2 in von zur Gathen *et al.* (1996), we find

$$\begin{aligned} |\#\mathcal{C} - \sigma q| &\leq \Big|\#\mathcal{C} - \sum_{1 \leq i \leq \sigma} \#\mathcal{C}_i\Big| + \sum_{1 \leq i \leq \sigma} \Big|\#\mathcal{C}_i - q\Big| \\ &< \sum_{1 \leq i < j \leq \sigma} n_i n_j + \sum_{\sigma < i \leq \tau} n_i^2/4 + q^{1/2} + \sum_{1 \leq i \leq \sigma} n_i^2 \\ &\leq \Big(\sum_{1 \leq i \leq \tau} n_i\Big)^2 q^{1/2} \leq n^2 q^{1/2}. \qquad \square \end{aligned}$$

Let $\mathcal{C} \subset \mathbb{F}_q^{m+1}$ be a curve. Throughout this paper, we assume that $\mathcal{C}$ is *without vertical components*, i.e., no absolutely irreducible component of $\mathcal{C}$

is contained in a hyperplane $\{a\} \times \mathbb{F}_q^m$, for some $a \in \mathbb{F}_q$. For a plane curve $\mathcal{C} = \{f = 0\}$, with $f = \sum_i f_i y^i \in \mathbb{F}_q[x,y]$ and all $f_i \in \mathbb{F}_q[x]$, this is the case if and only if $\gcd(f_0, f_1, \ldots) = 1$. In that case, we also say that $\mathcal{C}$ is *without vertical lines*. For the computational problems we consider, the general case is easily reduced to this (slightly) restricted one.

Let furthermore $i \in \mathbb{N}$, and $S \subseteq \mathbb{F}_q$. We consider the difference map $\delta\colon S^2 \to \mathbb{F}_q$ with $\delta(u_1, u_2) = u_1 - u_2$, and denote by id the identity on $\mathbb{F}_q^m$. We define the following.

$$\begin{aligned}
\mathcal{C}(S) &= \mathcal{C} \cap (S \times \mathbb{F}_q^m) = \{(u,v)\colon (u,v) \in \mathcal{C},\ u \in S\} \subseteq \mathbb{F}_q^{m+1},\\
R_i(S) &= \{u \in S\colon \#\mathcal{C}(\{u\}) = i\},\\
r_i(S) &= \#R_i(S),\\
\mathcal{C}^\delta(S) &= (\delta \times \mathrm{id})^{-1}(\mathcal{C}) = \{(u_1,u_2,v)\colon (u_1-u_2,v) \in \mathcal{C},\ u_1,u_2 \in S\},\\
M(S) &= \#\mathcal{C}^\delta(S),\\
t_i(S) &= \#\delta^{-1}(R_i(S)).
\end{aligned}$$

We also set $r_i^* = r_i(\mathbb{F}_q)$ and $t_i^* = t_i(\mathbb{F}_q)$. All these definitions coincide with the ones in the Introduction if $\mathcal{C}$ is plane. For a plane curve $\mathcal{C}$ given by $f \in \mathbb{F}_q[x,y]$ and $1 \le k \le n$, we define the curve $\mathcal{C}_k \subseteq \mathbb{F}_q^{k+1}$ as the closure of

$$\begin{aligned}
S_k = \{&(u, v_1, \ldots, v_k) \in \mathbb{F}_q^{k+1} :\\
&f(u,v_1) = \cdots = f(u,v_k) = 0,\ v_i \neq v_j \text{ for } 1 \le i < j \le k\}.
\end{aligned} \tag{2.1}$$

To define this closure of S_k, we take the set X of all points in K^{k+1} satisfying the equations and inequalities in (2.1), its (Zariski–)closure $\overline{X}$ (i.e., all points satisfying all polynomials over K that vanish on X), and then $\mathcal{C}_k = \overline{X} \cap \mathbb{F}_q^{k+1}$. The geometry of $\mathcal{C}_2$ and the equations defining it as a complete intersection are described in detail in von zur Gathen & Shparlinski (1995a) and an example is given below. $\mathcal{C}_k$ is the k-fold fibre power of $\mathcal{C}$ along the first projection; it may be empty. Applying Bézout's Theorem to the equations in (2.1), we find $\deg \mathcal{C}_k \le n^k$; in fact, $\deg \mathcal{C}_k \le n(n-1)\cdots(n-k+1)$. It can, of course, also be defined for curves in $\mathbb{F}_q^{m+1}$ with $m > 1$. The following statement is essentially Lemma 3.2 of von zur Gathen *et al.* (1996).

LEMMA 2.2. *For a plane curve $\mathcal{C} \subseteq \mathbb{F}_q^2$ without vertical lines and of degree n, $S \subseteq \mathbb{F}_q$ and $0 \le i \le n$, we have*

$$\begin{aligned} r_i(S) &= \frac{1}{i!} \sum_{i \le k \le n} \frac{(-1)^{i+k}\, \#\mathcal{C}_k(S)}{(k-i)!}, \\ t_i(S) &= \frac{1}{i!} \sum_{i \le k \le n} \frac{(-1)^{i+k}\, \#\mathcal{C}_k^{\delta}(S)}{(k-i)!}. \end{aligned} \tag{2.2}$$

In view of these expressions, we consider the number σ_k of absolutely irreducible components defined over $\mathbb{F}_q$ of $\mathcal{C}_k$, with $\sigma_0 = 1$, and for $0 \le i \le n$ set

$$\lambda_i = \frac{1}{i!} \sum_{i \le k \le n} \frac{(-1)^{i+k} \sigma_k}{(k-i)!} \in \mathbb{Q}. \tag{2.3}$$

LEMMA 2.3. *Let $\mathcal{C} \subseteq \mathbb{F}_q^2$ be a curve without vertical lines given by $f \in \mathbb{F}_q[x,y]$ of degree n, and $\lambda_0, \ldots, \lambda_n$ as above. Then for $0 \le i \le n$, we have $n!\lambda_i \in \mathbb{Z}$, and*

$$|r_i^* - \lambda_i q| \le 2n^{2n} q^{1/2}. \tag{2.4}$$

PROOF. Noting that $\mathcal{C}_k$ is of degree at most n^k and using σ_k as above, we find from Lemmas 2.1 and 2.2 that

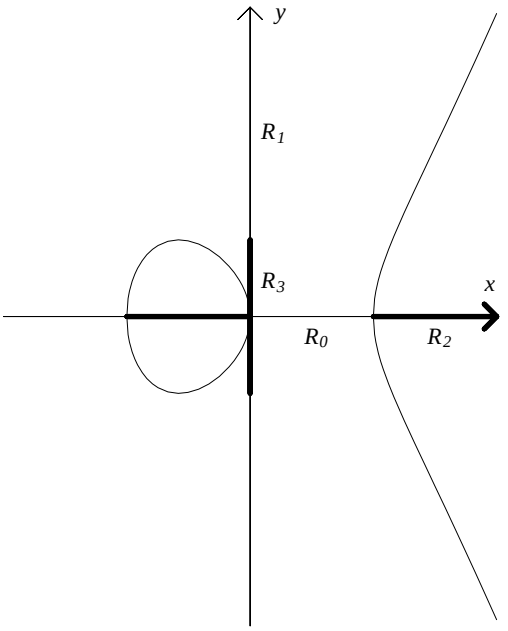
$$\begin{aligned} \left| r_i^* - q\lambda_i \right| &= \frac{1}{i!} \Big| \sum_{i \le k \le n} \frac{(-1)^{i+k} (\#\mathcal{C}_k - \sigma_k q)}{(k-i)!} \Big| \\ &\le \frac{q^{1/2}}{i!} \sum_{i \le k \le n} \frac{n^{2k}}{(k-i)!} \le \frac{q^{1/2}(n^2)^{n+1} - 1}{n^2 - 1} \le 2n^{2n} q^{1/2} \end{aligned}$$

for $n \ge 2$; the case $n = 1$ is trivial. Furthermore $i!(k-i)!$ divides $n!$ for all $0 \le i \le k \le n$. □

EXAMPLE 2.4. *We take the (irreducible) elliptic curve $\mathcal{C} = \{f = 0\}$ of degree $n = 3$ given by $f = y^2 - x^3 + x \in \mathbb{F}_q[x,y]$, where $q = 1019$ is prime. Figure 1 gives the picture over $\mathbb{R}$. Then $\mathcal{C}_2$ is given by the equations*

$$-u^3 + u = v_1^2, v_1 + v_2 = 0;$$

Figure 2.1: The elliptic curve $y^2 = x^3 - x$ over $\mathbb{R}$, the sets R_0 and R_2 for the first projection, and the sets R_1 and R_3 for the second projection.



the latter equation comes from eliminating u *and dividing the result* $v_1^2 - v_2^2$ *by* $v_1 - v_2$. *Thus* $\mathcal{C}_2$ *is isomorphic to* $\mathcal{C}$ *and irreducible, and* $\sigma_2 = 1$. *Furthermore,* $\mathcal{C}_3 = \emptyset$ *and* $\sigma_3 = 0$, *so that*

$$\lambda_0 = \frac{1}{2}, \lambda_1 = 0, \lambda_2 = \frac{1}{2}, \lambda_3 = 0.$$

For the two sets $S_1 = \mathbb{F}_q$ *and* $S_2 = \{0, 1, 2, \ldots, 49\}$ *we find*

i	$r_i(S_1) = r_i^*$	$\#\mathcal{C}_i(S_1)$	$r_i^* - \lambda_i q$	$r_i(S_2)$	$\#\mathcal{C}_i(S_2)$
0	*508*	*1019*	*-1.5*	*26*	*50*
1	*3*	*1019*	*3*	*2*	*2*
2	*508*	*1016*	*-1.5*	*22*	*22*
3	*0*	*0*	*0*	*0*	*0*

Of course, (2.2) could have been used to predict the r_i^* *approximately. The pessimistic bound (2.4) actually holds with the error term* $3 < 46541.95 \approx 2n^{2n}q^{1/2}$. *As expected from the picture of the curve* $\{y^2 = x^3 - x\}$ *over* $\mathbb{R}$, *there are (almost) no points with* 1 *or* 3 *preimages under the first projection. The other two possibilities, of* 0 *or* 2 *preimages, occur equally often. The three points with one preimage are* $0, 1, -1$.

It is instructive to also look at the projection of $\mathcal{C}$ *onto the* y*–axis. To preserve terminology, we thus take* $f = x^2 - y^3 + y$. *Then* $\mathcal{C}_2$ *is*

$$\mathcal{C}_2 = \{(u, v_1, v_2) \in \mathbb{F}_q^3 : f(u, v_1) = 0, v_1^2 + v_1 v_2 + v_2^2 - 1 = 0\}. \qquad (2.5)$$

$\mathcal{C}_2$ *is irreducible, as witnessed by its projection onto the plane ?, which is given by the irreducible polynomial* $\operatorname{res}(f(x, y), y^2 + yz + z^2 - 1) \in \mathbb{F}_q[x, y]$ *of degree* 6. *Thus* $\sigma_2 = 1$.

For $\mathcal{C}_3$, *we have to add the equation*

$$v_1 + v_2 + v_3 = 0$$

to those in (2.5); thus $\mathcal{C}_3 \cong \mathcal{C}_2$ *and* $\sigma_3 = 1$. *We find*

$$\lambda_0 = \frac{1}{3}, \lambda_1 = \frac{1}{2}, \lambda_2 = 0, \lambda_3 = \frac{1}{6},$$

and with S_1 and S_2 as above, we have

i	$r_i(S_1) = r_i^*$	$\#\mathcal{C}_i(S_1)$	$r_i^* - \lambda_i q$	$r_i(S_2)$	$\#\mathcal{C}_i(S_2)$
0	*340*	*1019*	*0.33*	*14*	*50*
1	*508*	*1019*	*-1.5*	*24*	*60*
2	*2*	*1020*	*2*	*0*	*72*
3	*169*	*1020*	*-0.83*	*12*	*72*

Again, (2.4) holds with the bound $2 < 46541.95$. This example shows how the λ_i's comprise in a concise way reasonably good information about the projection statistics of the curve. Note that in the picture over $\mathbb{R}$ the set corresponding to R_0 is empty.

We denote by $\mathsf{M}(n)$ the Boolean complexity of multiplication of two n-bit numbers. The currently best estimate (Schönhage & Strassen 1971) of this function is

$$\mathsf{M}(n) = O(n \log n \log\log n).$$

As in the proof of Lemma 2.5 of von zur Gathen *et al.* (1996), we find the following result.

LEMMA 2.5. *Let $\mathcal{C} \subseteq \mathbb{F}_q^2$ be without vertical lines and given by $f \in \mathbb{F}_q[x, y]$ of degree n, and $u \in \mathbb{F}_q$. Then $\#\mathcal{C}(\{u\})$ can be computed with $O(\mathsf{M}(n)\log(nq))$ arithmetic operations in $\mathbb{F}_q$.*

3. Counting with random elements

Throughout this section, $\mathcal{C}$ is a plane curve without vertical lines. We extend our notions $\mathcal{C}(S)$, $R_i(S)$, $r_i(S)$ to a sequence $S = (s_1, \ldots, s_h)$ of elements of $\mathbb{F}_q$ in the obvious way; e.g., we set $\#\mathcal{C}(S) = \sum_{1 \le i \le h} \#\mathcal{C}(\{s_i\})$. In particular, when S is a sequence of random elements of $\mathbb{F}_q$, $\#\mathcal{C}(S)$ and $r_i(S)$ are random variables. We state our algorithms in this Section for a sequence of h random elements, because for a computer implementation such a sequence is slightly more natural than a random subset of size h; the results also hold for such a random subset.

The following bound on the difference between a sample mean and the true expected value is a direct consequence of the general result of Karp *et al.* (1989) (see also Theorem 7.2 of von zur Gathen *et al.* 1996), and the trivial bounds $\#\mathcal{C} \le nq$ and $r_i^* \le q$.

LEMMA 3.1. *Let S be a sequence of h independently and uniformly distributed random elements of $\mathbb{F}_q$, $0 \le i \le n$, and $\delta > 0$. Then the following hold with probability at least $1 - \delta$:*

$$\begin{aligned} |\#\mathcal{C} - q\#\mathcal{C}(S)h^{-1}| &\le \left(2n(n+1)q\#\mathcal{C}\log(2n/\delta)h^{-1}\right)^{1/2} \\ &\le nq\left(2(n+1)\log(2n/\delta)h^{-1}\right)^{1/2}, \end{aligned}$$

$$|r_i^* - qr_i(S)h^{-1}| \le 2\left(qr_i^*\log(2/\delta)h^{-1}\right)^{1/2} \le 2q\left(\log(2/\delta)h^{-1}\right)^{1/2}.$$

ALGORITHM 3.2. *Components.*
Input: *$f \in \mathbb{F}_q[x,y]$ of degree n, and $\delta > 0$.*
Output: *An estimate of the number of absolutely irreducible components of $\mathcal{C} = \{f = 0\}$ defined over $\mathbb{F}_q$.*

1. *Set $h = \lceil 72n^2(n+1)\log(2n/\delta)\rceil$.*
2. *Choose a sequence S of h random independently uniformly distributed elements of $\mathbb{F}_q$.*
3. *Compute $\#\mathcal{C}(S)$.*
4. *Return the nearest integer to $\#\mathcal{C}(S)/h$.*

THEOREM 3.3. *Assume that $q \ge 36n^4$. Then the probabilistic algorithm above outputs the number σ of absolutely irreducible components correctly with probability at least $1 - \delta$. It uses $O(n^3\log(n/\delta))$ random elements and $O(n^3\mathsf{M}(n)\log(n/\delta)\log(nq))$ arithmetic operations in $\mathbb{F}_q$.*

PROOF. The cost bound follows from Lemma 2.5, and Lemmas 2.1 and 3.1 show that

$$|\sigma - \#\mathcal{C}(S)h^{-1}| \le n^2q^{-1/2} + n\Big(2(n+1)\log(2n/\delta)h^{-1}\Big)^{1/2} \le 1/6 + 1/6 = 1/3$$

with probability at least $1 - \delta$. 2

We call a curve $\mathcal{C}$ over $\mathbb{F}_q$ *exceptional* (over $\mathbb{F}_q$) if and only if none of the irreducible components of $\mathcal{C}$ defined over $\mathbb{F}_q$ is absolutely irreducible. In particular, a plane curve $\mathcal{C} = \{f = 0\}$ with $f \in \mathbb{F}_q[x,y]$ is *exceptional* if and only if none of the irreducible factors of f over $\mathbb{F}_q$ is absolutely irreducible. This notion plays a central role in the study of permutation polynomials: $g \in \mathbb{F}_q[x]$ is a permutation polynomial if and only if $(g(x) - g(y))/(x - y)$ is exceptional provided that $q \ge 16(\deg g)^4$ (Cohen 1970, von zur Gathen 1991).

ALGORITHM 3.4. *Exceptional test.*
Input: $f \in \mathbb{F}_q[x,y]$ *of degree* n, *and* $\delta > 0$.
Output: *YES if* f *is exceptional, and NO otherwise.*

1. *Set* $h = \lceil 16n(n+1)\log(2n/\delta)\rceil$.
2. *Choose a sequence* S *of* h *random independently uniformly distributed elements of* $\mathbb{F}_q$.
3. *Compute* $\#\mathcal{C}(S)$.
4. *If* $\#\mathcal{C}(S) \le n^2/4$ *then return YES else return NO.*

THEOREM 3.5. *Assume that* $q \ge 4n^4$. *If* f *is exceptional, the algorithm answers correctly. If* f *is not exceptional, the algorithm answers correctly with probability at least* $1-\delta$. *It uses* $O(n^2\log(n/\delta))$ *random elements and* $O(n^2\mathsf{M}(n)\log(n/\delta)\log(nq))$ *arithmetic operations in* $\mathbb{F}_q$.

PROOF. Let σ be the required number of components. If $\sigma = 0$, then $\#\mathcal{C} \le d^2/4$; see Lemma 5.2 (ii) of von zur Gathen *et al.* (1996) for example. Thus the algorithm answers correctly in this case. It is sufficient to estimate the probability that $\#\mathcal{C}(S) \le n^2$ when $\sigma \ge 1$. From Lemma 2.1 we get

$$\#\mathcal{C} \ge q - n^2 q^{1/2} \ge q/2.$$

Assuming that $\delta \le 1$, Lemma 3.1 implies that with probability at least $1-\delta$ we have

$$\begin{aligned}\#\mathcal{C}(S) &\ge \frac{h\#\mathcal{C}}{q} - \frac{h}{q}\left(2n(n+1)q\#\mathcal{C}\log(2n/\delta)h^{-1}\right)^{1/2}\\ &\ge \frac{h\#\mathcal{C}}{q}\left(1-(\frac{q}{\#\mathcal{C}}\cdot\frac{1}{8})^{1/2}\right) \ge \frac{h}{2}\left(1-(\frac{1}{4})^{1/2}\right) = \frac{h}{4} > n^2. \qquad \square\end{aligned}$$

ALGORITHM 3.6.
Input: $f \in \mathbb{F}_q[x,y]$ *of degree* n, *and* $\delta > 0$.
Output: *YES if* $\mathcal{C} = \{f = 0\}$ *has exactly one absolutely irreducible component defined over* $\mathbb{F}_q$, *and NO otherwise.*

1. *Return NO if* f *is exceptional, using Exceptional Test with input* $(f, \delta/2)$.

2. *Set* $h = \lceil 90n(n+1)\log(4n/\delta)\rceil$.

3. *Choose a sequence* S *of* h *random independent uniformly distributed elements of* $\mathbb{F}_q$.

4. *Compute* $\#\mathcal{C}(S)$.

5. *If* $\#\mathcal{C}(S) \le 17h/12$ *then return YES else return NO.*

THEOREM 3.7. *Let* $q \ge 16n^4$. *With probability at least* $1-\delta$, *the algorithm decides correctly whether* $\mathcal{C}$ *has exactly one absolutely irreducible component defined over* $\mathbb{F}_q$. *It uses* $O(n^2\log(n/\delta))$ *random elements and* $O(n^2\mathsf{M}(n)\log(n/\delta)\log(nq))$ *arithmetic operations in* $\mathbb{F}_q$.

PROOF. Let σ be the number of components. The cost estimate follows from Lemma 2.5. We may assume that $\sigma \ge 1$, and have to bound the error probability. If $\sigma = 1$, then we get from Lemma 2.1 that

$$\#\mathcal{C} \le q + n^2 q^{1/2} \le 5q/4,$$

and from Lemma 3.1 that

$$\begin{aligned} \#\mathcal{C}(S) &\le h\#\mathcal{C}/q + \frac{h}{q}\Big(2n(n+1)q\#\mathcal{C}\log(4n/\delta)h^{-1}\Big)^{1/2} \\ &\le \frac{5h}{4} + h\Big(\frac{5}{4\cdot 45}\Big)^{1/2} = \frac{17h}{12} \end{aligned}$$

with probability at least $1-\delta/2$. Otherwise,

$$7q/4 \le 2q - n^2q^{1/2} \le \#\mathcal{C} \le 2q + n^2q^{1/2} \le 9q/4,$$

and with probability at least $1-\delta/2$

$$\begin{aligned} \#\mathcal{C}(S) &\ge \frac{h\#\mathcal{C}}{q} - \frac{h}{q}\Big(2n(n+1)q\#\mathcal{C}\cdot\log(4n/\delta)h^{-1}\Big)^{1/2} \\ &\ge \frac{7h}{4} - h\cdot\Big(\frac{9}{4\cdot 45}\Big)^{1/2} = \frac{(35-2\sqrt{5})h}{20} > \frac{17h}{12}. \end{aligned}$$

2

Our next algorithm computes the rational numbers $\lambda_0,\ldots,\lambda_n$. In view of (2.3), this is equivalent to calculating $\sigma_0,\ldots,\sigma_n$, up to a triangular system of linear equations; we do not know a direct easy way to compute these σ_i's.

ALGORITHM 3.8.
Input: $f \in \mathbb{F}_q[x,y]$ *of degree* n, *and* $\delta > 0$.
Output: *The parameters* $\lambda_0, \ldots, \lambda_n$ *of* $\mathcal{C} = \{f = 0\}$ *as defined in (2.3).*

1. *Set* $h = \lceil 144(n!)^2 \log(2/\delta) \rceil$.
2. *Choose a sequence* S *of* h *random independently uniformly distributed elements of* $\mathbb{F}_q$.
3. *For* $i = 1, \ldots, n$ *do steps 4, 5, 6.*
4. *Compute* $r_i(S)$.
5. *Compute the nearest integer* Λ_i *to* $n! r_i(S)/h$.
6. *Return* $\Lambda_i/n!$.

THEOREM 3.9. *If* $q \geq 144 n^{4n} (n!)^2$, *then the above algorithm computes the parameters* $\lambda_0, \ldots, \lambda_n$ *of* $\mathcal{C} = \{f = 0\}$ *correctly with probability at least* $1 - \delta$. *It uses* $O((n!)^2 \log(\delta^{-1}))$ *random elements, and* $O((n!)^2 \mathsf{M}(n) \log(\delta^{-1}) \log(nq))$ *arithmetic operations in* $\mathbb{F}_q$.

PROOF. From Lemmas 2.3 and 3.1, we find that with probability at least $1 - \delta$

$$|\lambda_i - r_i(S) h^{-1}| \leq 2n^{2n} q^{-1/2} + 2(\log(2/\delta) h^{-1})^{1/2} < 1/6n! + 1/6n! < 1/3n!,$$

and in this case the output is correct. The cost estimate follows from Lemma 2.5. 2

Let us now consider the special case of testing if $\lambda_0 = 0$. For a curve of the form $f = y - g(x)$ with $g \in \mathbb{F}_q[x]$, the condition $\lambda_0 = 0$ implies $r_0 = 0$ (at least for q large enough), i.e., that h is a permutation polynomial (see von zur Gathen 1991 for details).

ALGORITHM 3.10.
Input: $f \in \mathbb{F}_q[x,y]$ *of degree* n, *and* $\delta > 0$.
Output: *YES if* $\lambda_0 = 0$ *for* $\mathcal{C} = \{f = 0\}$, *else NO.*

1. *Set* $h = \lceil 256(n!)^2 \log(2/\delta) \rceil$.

2. *Choose a sequence S of h random independently uniformly distributed elements of $\mathbb{F}_q$.*
3. *Compute $\#\mathcal{C}(S)$.*
4. *Return YES if $\#\mathcal{C}(S) \le h/4n!$, else NO.*

THEOREM 3.11. *If $q \ge 256n^{4n}(n!)^2$, then the output of the above algorithm is correct with probability at least $1-\delta$. It uses $O(n!\log(\delta^{-1}))$ random elements and $O(n!\mathsf{M}(n)\log(\delta^{-1})\log(nq))$ arithmetic operations in $\mathbb{F}_q$.*

PROOF. The cost estimate follows from Lemma 2.5. To bound the error probability, we have from Lemma 2.3 that

$$\lambda_0 q - q/8n! \le \lambda_0 q - 2n^{2n}q^{1/2} \le r_0^* \le \lambda_0 q + 2n^{2n}q^{1/2} \le \lambda_0 q + q/8n!.$$

If $\lambda_0 = 0$, then we find from Lemma 3.1 that with probability at least $1-\delta$

$$r_0(S) \le hr_0^*/q + 2(h\log(2/\delta))^{1/2} \le h/8n! + h/8n! = h/4n!.$$

Now suppose that $\lambda_0 \ne 0$. Then $|\lambda_0| \ge 1/n!$. Furthermore, $\lambda_0 < 0$ would imply that $0 \le r_0^* \le -q/n! + q/8n! < 0$. Thus $\lambda_0 \ge 1/n!$, and with probability at least $1-\delta$

$$r_0(S) \ge hr_0^*/q - 2(h\log(2/\delta))^{1/2} \ge 7h/8n! - h/8n! = 3h/4n!. \qquad 2$$

4. Counting in additive strips

In this section, we continue to study properties of curves in 'additive strips'. Our main tool is Bombieri's (1966) bound on exponential sums along a curve.

For integers a and h, we denote by $A(a,h)$ the interval

$$A(a,h) = \{(a+j) \bmod p : 0 \le j < h\} \subseteq \mathbb{F}_q,$$

where $p = \operatorname{char}\mathbb{F}_q$, and for a curve $\mathcal{C} \subseteq \mathbb{F}_q^{m+1}$, we write

$$\mathcal{C}(a,h) = \mathcal{C}(A(a,h)), \qquad r_i(a,h) = r_i(A(a,h)),$$
$$M(a,h) = M(A(a,h)), \qquad t_i(a,h) = t_i(A(a,h)).$$

It follows from Lemma 2.1 of von zur Gathen *et al.* (1996) that if x is not a constant along any absolutely irreducible component of $\mathcal{C}$ and $n = \deg\mathcal{C}$, then for any integers a and $h \le p$

$$|\#\mathcal{C}(a,h) - h\#\mathcal{C}/p| \le 2n^2 p^{1/2}\log p. \tag{4.1}$$

Let K be an algebraic closure of $\mathbb{F}_q$. We will repeatedly use the following assumption on a curve $\mathcal{C} \subseteq \mathbb{F}_q^{m+1}$, which arises in Bombieri's work:

HYPOTHESIS A. *For every absolutely irreducible component $\mathcal{D}$ of $\mathcal{C}$ and every rational function g on K^{m+1}, x is different from $g^p - g$ on $\mathcal{D}$, where $p = \operatorname{char} \mathbb{F}_q$.*

In general, given the equations for $\mathcal{C}$, it seems not easy to check whether $\mathcal{C}$ satisfies hypothesis A or not. If $x = g^p - g = \prod_{u \in \mathbb{F}_p}(g - u)$, then each $g - u$ has the same poles as x, and in particular the degree of the pole divisor of x is divisible by p. Thus

$$\deg \mathcal{C} < p \quad \Longrightarrow \quad \mathcal{C} \text{ satisfies hypothesis A;} \tag{4.2}$$

see also Lemma 4 of Bombieri & Davenport (1966).

Below we show that for the parameter $\#\mathcal{C}^\delta(S)$ a slightly stronger result than (4.1) holds for an arbitrary set $S \subseteq \mathbb{F}_q$.

LEMMA 4.1. *Let $\mathcal{C} = \mathbb{F}_q^{m+1}$ be a curve without vertical components and of degree n satisfying hypothesis A, $S \subseteq \mathbb{F}_q$, and $h = \#S$. Then*

$$|\#\mathcal{C}^\delta(S) - h^2 \#\mathcal{C}/q| < 2n^2 h q^{1/2}.$$

PROOF. Let χ be a nontrivial additive character of $\mathbb{F}_q$. Then

$$|\#\mathcal{C}^\delta(S)| = \frac{1}{q} \sum_{(a,b)\in\mathcal{C}} \sum_{u,v\in S} \sum_{\lambda\in\mathbb{F}_q} \chi(\lambda(a - u + v)) = h^2 \#\mathcal{C}/q + t/q,$$

where $a \in \mathbb{F}_q$ and $b \in \mathbb{F}_q^m$ in the sum, and

$$t = \sum_{\lambda\in\mathbb{F}_q^\times} \sum_{(a,b)\in\mathcal{C}} \chi(\lambda a) \sum_{u,v\in S} \chi(\lambda(u - v)).$$

The bound of Bombieri (1966), Theorem 6, implies that for $\lambda \in \mathbb{F}_q^\times$,

$$\Big| \sum_{(a,b)\in\mathcal{C}} \chi(\lambda a) \Big| \le (n^2 - n) q^{1/2} + n^2 < 2n^2 q^{1/2}.$$

Therefore

$$\begin{aligned} t &< 2n^2 q^{1/2} \Big| \sum_{\lambda\in\mathbb{F}_q^\times} \sum_{u,v\in S} \chi(\lambda(u - v)) \Big| \\ &= 2n^2 q^{1/2} \Big| \sum_{u,v\in S} \sum_{\lambda\in\mathbb{F}_q} \chi(\lambda(u - v)) - h^2 \Big|. \end{aligned}$$

Since the inner sum equals 0 when $u \neq v$ and q otherwise, we get

$$t < 2n^2 h q^{3/2}. \qquad 2$$

Note that this lemma is non-trivial for sets of cardinality $h \geq 2n^2 q^{1/2}$, while the above mentioned result from von zur Gathen *et al.* (1996) works only in case of a prime field $\mathbb{F}_q = \mathbb{F}_p$ and needs $h \geq 2n^2 p^{1/2} \log p$.

For $w \in \mathbb{F}_q$ and $S \subseteq \mathbb{F}_q$, we denote by S_w the w-shift of S:

$$S_w = \{w + u : u \in S\}.$$

The following lemma shows that $q\#\mathcal{C}(S_w)/h$ is a good approximation to $\#\mathcal{C}$ for almost all w-shifts of any set $S \subseteq \mathbb{F}_q$ with $\#S \gg n^3$.

LEMMA 4.2. *Let $\mathcal{C} \subseteq \mathbb{F}_q^{m+1}$ be a curve without vertical components and of degree n satisfying hypothesis A, $w \in \mathbb{F}_q$, $S \subseteq \mathbb{F}_q$, $h = \#S$, and*

$$s = \frac{1}{q} \sum_{w \in \mathbb{F}_q} (\#\mathcal{C}(S_w) - h\#\mathcal{C}/q)^2.$$

Then $s \leq 4n^4 h$, and if $q \geq n^2$, then $s \leq n^4 h$.

PROOF. Let χ be a nontrivial additive character on $\mathbb{F}_q$. We have, as in the proof of the previous lemma,

$$\#\mathcal{C}(S_w) - h\#\mathcal{C}/q = \frac{1}{q} \sum_{\lambda \in \mathbb{F}_q^\times} \sum_{(a,b) \in \mathcal{C}} \chi(\lambda a) \sum_{u \in S} \chi(-\lambda(w+u)),$$

where $a \in \mathbb{F}_q$ and $b \in \mathbb{F}_q^m$. Hence

$$\sum_{w \in \mathbb{F}_q} |\#\mathcal{C}(S_w) - h\#\mathcal{C}/q|^2 = tq^{-2},$$

where

$$\begin{aligned} t &= \sum_{w \in \mathbb{F}_q} \left| \sum_{\lambda \in \mathbb{F}_q^\times} \sum_{(a,b) \in \mathcal{C}} \chi(\lambda a) \sum_{u \in S} \chi(-\lambda(w+u)) \right|^2 \\ &= \sum_{\lambda_1, \lambda_2 \in \mathbb{F}_q^\times} \sum_{(a_1,b_1),(a_2,b_2) \in \mathcal{C}} \chi(\lambda_1 a_1 - \lambda_2 a_2) \sum_{u_1, u_2 \in S} \chi(-\lambda_1 u_1 + \lambda_2 u_2) \\ &\quad \cdot \sum_{w \in \mathbb{F}_q} \chi(w(-\lambda_1 + \lambda_2)). \end{aligned}$$

Since the last sum equals 0 when $\lambda_1 \neq \lambda_2$ and q otherwise, we find from Theorem 6 of Bombieri (1966) that

$$\begin{aligned} t &= q \sum_{\lambda \in \mathbb{F}_q^\times} \sum_{(a_1,b_1),(a_2,b_2) \in \mathcal{C}} \chi(\lambda(a_1 - a_2)) \sum_{u_1,u_2 \in S} \chi(\lambda(-u_1 + u_2)) \\ &= q \sum_{\lambda \in \mathbb{F}_q^\times} \Big| \sum_{(a,b) \in \mathcal{C}} \chi(\lambda a) \Big|^2 \sum_{u_1,u_2 \in S} \chi(\lambda(-u_1 + u_2)) \\ &\leq q((n^2 - n)q^{1/2} + n^2)^2 \sum_{\lambda \in \mathbb{F}_q^\times} \sum_{u_1,u_2 \in S} \chi(\lambda(u_1 - u_2)) \\ &\leq 4n^4 q^2 \Big| \sum_{\lambda \in \mathbb{F}_q} \sum_{u_1,u_2 \in S} \chi(\lambda(u_1 - u_2)) - h^2 \Big|. \end{aligned}$$

We can replace 4 by 1 if $n^2 \leq q$. The sum is zero when $u_1 \neq u_2$ and q otherwise, so that

$$t \leq 4n^4 q^2 (qh - h^2) \leq 4n^4 h q^3. \qquad 2$$

COROLLARY 4.3. *Let $\mathcal{C} \subseteq \mathbb{F}_q^{m+1}$ be a curve without vertical components and of degree n satisfying hypothesis A, $\delta > 0$, $S \subseteq \mathbb{F}_q$, and $h = \#S$. Then*

$$|\#\mathcal{C}(S_a) - h\#\mathcal{C}/q| \leq 2\delta^{-1/2} n^2 h^{1/2}$$

holds with probability at least $1 - \delta$ for random $a \in \mathbb{F}_q$.

LEMMA 4.4. *Let p be a prime, $\mathcal{C} \subseteq \mathbb{F}_p^2$ be a plane curve without vertical lines of degree n satisfying hypothesis A, $0 \leq i \leq n$, $p > n^n$, and $a, h \in \mathbb{N}$ with $h \leq p$. Then*

$$\begin{aligned} |t_i(a,h) - h^2 r_i^*/p| &\leq 3n^{2n} h p^{1/2}, \\ |r_i(a,h) - h r_i^*/p| &\leq 3n^{2n} p^{1/2} \log p. \end{aligned}$$

PROOF. For $1 \leq k \leq n$, we have $\deg \mathcal{C}_k \leq n^k < p$, and thus $\mathcal{C}_k$ satisfies hypothesis A, by (4.2). Lemma 4.1 implies that

$$|\#\mathcal{C}_k^\delta(a,h) - h^2 \#\mathcal{C}_k/p| \leq 2n^{2k} h p^{1/2}.$$

Let $0 \leq i \leq n$. From Lemma 2.2, we have

$$\begin{aligned} |t_i(a,h) - h^2 t_i^*/p| &\leq \frac{1}{i!} \sum_{i \leq k \leq n} \frac{|\#\mathcal{C}_k^\delta(a,h) - h^2 \#\mathcal{C}_k/p|}{(k-i)!} \\ \leq \frac{1}{i!} \sum_{i \leq k \leq n} \frac{2n^{2k} h p^{1/2}}{(k-i)!} &\leq 2n^{2n} h p^{1/2} \frac{n^2}{n^2 - 1} \leq 3n^{2n} h p^{1/2}. \end{aligned}$$

Using (4.1), the second bound follows in a similar way. 2

We next show that for "almost all" a a much stronger bound than the second estimate in Lemma 4.4 holds.

LEMMA 4.5. *Let $p > n^n$ be a prime, $\mathcal{C} \subseteq \mathbb{F}_p^2$ a plane curve without vertical lines and of degree n, $0 \le i \le n$, and $h \le p$. Then*

$$\frac{1}{p} \sum_{0 \le a < p} (r_i(a,h) - h r_i^*/p)^2 \le 8n^{4n}h.$$

PROOF. For $0 \le k \le n$, we have $\deg \mathcal{C}_k \le n^k < p$, and $\mathcal{C}_k$ satisfies hypothesis A by (4.2). Using Lemma 4.2, we find

$$\begin{aligned}
\sum_{0 \le a < p} (r_i(a,h) - h r_i^*/p)^2 &\le \frac{1}{i!^2} \sum_{0 \le a < p} \Big(\sum_{i \le k \le n} \frac{(\#\mathcal{C}_k(a,h) - h\#\mathcal{C}_k/p)}{(k-i)!} \Big)^2 \\
&\le \sum_{i \le k \le n} \sum_{0 \le a < p} (\#\mathcal{C}_k(a,h) - h\#\mathcal{C}_k/p)^2 \\
&\le 4ph \sum_{i \le k \le n} n^{4k} \le 8n^{4n}ph. \qquad 2
\end{aligned}$$

COROLLARY 4.6. *Let $p > n^n$ be a prime, $\mathcal{C} \subseteq \mathbb{F}_p^2$ a plane curve without vertical lines and of degree n, $0 < \delta < 1$, and $h \le p$. Then*

$$|r_i(a,h) - h r_i^*/p| \le n^{2n}(8h\delta^{-1})^{1/2}$$

holds with probability at least $1 - \delta$ for a random element $a \in \mathbb{F}_p$.

It was proved in von zur Gathen *et al.* (1996) that for a plane curve $\mathcal{C} \subseteq \mathbb{F}_p^2$ of degree n, one can find the number of absolute irreducible components with $O(n^2 \mathsf{M}(n) p^{1/2} \log^2 p)$ arithmetic operations in $\mathbb{F}_p$. A similar result is true for r_i, namely, one can find the parameters λ_i as in (2.3) with $O(n! n^{2n} \mathsf{M}(n) p^{1/2} \log^2 p)$ arithmetic operations in $\mathbb{F}_p$. Indeed, choose

$$h = \lceil 18 n! n^{2n} p^{1/2} \log p \rceil.$$

Setting $\Lambda_i = \lambda_i n! \in \mathbb{Z}$, we find from Lemmas 4.4 and 2.3

$$\begin{aligned}
|n!\, r_i(0,h) h^{-1} - \Lambda_i| &\le n! h^{-1} |r_i(0,h) - h r_i^* p^{-1}| + n! p^{-1} |r_i^* - \lambda_i p| \\
&\le n! h^{-1} \cdot 3 n^{2n} p^{1/2} \log p + n! p^{-1} \cdot 2 n^{2n} p^{1/2} \\
&\le 1/6 + 1/6 = 1/3,
\end{aligned}$$

if $p \geq 144n^{4n}(n!)^2$. Thus we may determine Λ_i as the nearest integer to $n!r_i(0,h)h^{-1}$.

Below we show how to improve this method and partially generalize it to the case of arbitrary finite fields.

ALGORITHM 4.7. *Deterministic Components.*
Input: $f \in \mathbb{F}_q[x,y]$ *of degree* $n \leq q^{1/4}/4$, *and a basis* $\omega_1, \ldots, \omega_k$ *of* $\mathbb{F}_q$ *over* $\mathbb{F}_p$, *where* $p = \mathrm{char}\ \mathbb{F}_q$ *and* $q = p^k$.
Output: *The number of absolutely irreducible components of* $\mathcal{C} = \{f = 0\}$ *defined over* $\mathbb{F}_q$.

1. *Set* $H = \lceil 12n^2q^{1/2} \rceil$.
2. *Compute integers* l, h_0, *and* h *such that*
$$p^{l-1} \leq H < p^l, \quad (h_0 - 1)p^{l-1} \leq H < h_0 p^{l-1}, \quad h = \min\{(p-1)/2, h_0\}.$$
3. *Set*
$$S = \{a_1\omega_1 + \ldots + a_l\omega_l \colon a_1, \ldots, a_{l-1} \in \mathbb{F}_p,\ a_l \in A(0,h)\}.$$
4. *Compute* $M(S)$.
5. *Return the nearest integer to* $M(S)/\#S^2$.

THEOREM 4.8. *Let* $q > 256n^4$, *and* $\mathcal{C} \subseteq \mathbb{F}_q^2$ *be a plane curve without vertical lines and of degree* n *satisfying Hypothesis A. The above deterministic algorithm correctly computes the number of absolutely irreducible components of* $\mathcal{C}$. *It uses* $O(n^2\mathsf{M}(n)q^{1/2}\log q)$ *arithmetic operations in* $\mathbb{F}_q$.

PROOF. Since $H \leq 8n^2q^{1/2} + 1 < 16n^2q^{1/2} \leq q$, we have $l \leq k$. Using $\delta \colon S^2 \to \mathbb{F}_q$, and that $l \geq 1$, $h_0 \geq 2$, we find
$$H/2 \leq \#S \leq \#\delta(S^2) \leq 2\#S \leq 4H,$$
and for any $a = a_1\omega_1 + \ldots + a_l\omega_l \in \delta(S^2)$, with $-h < a_l < h$, the number $\#\delta^{-1}(\{a\})$ of $(u_1, u_2) \in S^2$ with $a = u_1 - u_2$ is equal to $p^{l-1}(h - |c_l|)$. Using Lemma 2.5, one can compute $M(S)$ in $O(\mathsf{M}(n)\#S \cdot \log q)$ or $O(n^2\mathsf{M}(n)q^{1/2}\log q)$ arithmetic operations in $\mathbb{F}_q$. From Lemmas 2.1, and 4.1, we get
$$\begin{aligned} |\sigma - M(S)/\#S^2| &\leq |\sigma - \#\mathcal{C}/q| + |\#\mathcal{C}/q - M(S)/\#S^2| \\ < n^2q^{-1/2} + 2n^2q^{1/2}/\#S &\leq 1/16 + 1/3 = 19/48. \end{aligned}$$
□

ALGORITHM 4.9. *Components.*
Input: *A curve* $\mathcal{C} \subseteq \mathbb{F}_q^2$ *without vertical lines, given by* $f \in \mathbb{F}_q[x,y]$ *of degree* n *satisfying hypothesis A, and* $\delta > 0$.
Output: *An estimate of the number of absolutely irreducible components of* $\mathcal{C}$ *defined over* $\mathbb{F}_q$.

1. *Set* $H = \lceil 288\,\delta^{-2} n^4 \rceil$.
2. *Determine the set* $S \subseteq \mathbb{F}_q$ *as in Algorithm 4.7.*
3. *Choose* $a \in \mathbb{F}_q$ *at random.*
4. *Compute* $\#\mathcal{C}(S_a)$.
5. *Return the nearest integer to* $\#\mathcal{C}(S_a)/\#S^2$.

THEOREM 4.10. *If* $q > 36n^4$, *then the above probabilistic algorithm computes the number of absolutely irreducible components of* $\mathcal{C}$ *correctly with probability at least* $1 - \delta$. *It uses one random element and* $O(n^4 \mathsf{M}(n) \delta^{-2} \log q)$ *arithmetic operations in* $\mathbb{F}_q$.

PROOF. The cost estimate follows from the fact that $\#\mathcal{C}(S_a)$ can be computed in $O(\mathsf{M}(n)\#S \cdot \log q)$ or $O(\delta^{-2} n^4 \mathsf{M}(n) \log q)$ arithmetic operations in $\mathbb{F}_q$. Corollary 4.3 implies that

$$|\#\mathcal{C}(S_a) - \#S \cdot \#\mathcal{C}/q| \le 2\delta^{-1} n^2 (\#S)^{1/2}$$

with probability at least $1 - \delta$. From Lemma 2.1 we obtain

$$\begin{aligned} |\sigma - \#\mathcal{C}(S_a)/\#S| &\le |\sigma - \#\mathcal{C}/q| + |\#\mathcal{C}/q - \#\mathcal{C}(S_a)/\#S| \\ \le\ n^2 q^{-1/2} + 2\delta^{-1} n^2 (\#S)^{-1/2} &\le 1/6 + 1/6 \ =\ 1/3. \end{aligned}$$

with probability at least $1 - \delta$. 2

ALGORITHM 4.11. *Parameters* λ_i.
Input: *A curve* $\mathcal{C} \subseteq \mathbb{F}_q^2$ *without vertical lines and given by* $f \in \mathbb{F}_p[x,y]$ *of degree* n, *and* $\delta > 0$.
Output: *The parameters* λ_i *for* $0 \le i \le n$.

1. *Set* $h = \lceil 12! n^{2n} p^{1/2} \rceil$.

2. *For $0 \le i \le n$, compute $t_i(0,h)$.*

3. *For $0 \le i \le n$, let Λ_i be the nearest integer to $t_i(0,h)n!/h^2$, and return $\lambda_i = \Lambda_i/n!$.*

THEOREM 4.12. *Let $p > 576(n!)^2 n^{4n}$ be a prime. Then the above deterministic algorithm computes λ_i for $0 \le i \le n$. It uses $O(n! n^{2n} \mathsf{M}(n) p^{1/2} \log p)$ arithmetic operations in $\mathbb{F}_p$.*

PROOF. Set $S = A(0,h)$, and let $0 \le i \le n$. It follows from Lemmas 2.3 and 4.4 that

$$\begin{aligned} |\lambda_i - t_i(0,h)/h^2| &\le |\lambda_i - r_i^*/p| + |r_i^*/p - t_i(0,h)/h^2| \\ &\le 2n^{2n}p^{-1/2} + 3n^{2n}p^{1/2}h^{-1} \\ &< 1/24n! + 1/4n! = 7/(24n!). \end{aligned}$$

Thus the algorithm works correctly. Since $12n!n^{2n}p^{1/2} < p/2$, we have $h \le (p+1)/2$, and for $-h < a < h$ the number of $u_1, u_2 \in \mathbb{N}$ with $a = u_1 - u_2$ and $0 \le u_1, u_2 < h$ is equal to $h - |a|$. Using this fact and Lemma 2.5, one can compute $t_i(0,h)$ in $O(\mathsf{M}(n) h \log p)$ or $O(n! n^{2n} \mathsf{M}(n) p^{1/2} \log q)$ arithmetic operations in $\mathbb{F}_p$. 2

ALGORITHM 4.13. *Parameters λ_i.*
Input: *A curve $\mathcal{C} \subset \mathbb{F}_q^2$ without vertical lines and given by $f \in \mathbb{F}_q[x,y]$ of degree n, and $\delta > 0$.*
Output: *An estimate of the parameters λ_i for $0 \le i \le n$.*

1. *Set $h = \lceil 288(n!)^2 n^{4n} \delta^{-1} \rceil$.*

2. *Choose $a \in \mathbb{F}_p$ at random.*

3. *For $0 \le i \le n$, compute $r_i(a,h)$, determine the nearest integer Λ_i to $n! r_i(a,h)/h$, and return $\lambda_i = \Lambda_i/n!$.*

THEOREM 4.14. *Let $p > 144(n!)^2 n^{4n}$ be a prime, $\mathcal{C} \subseteq \mathbb{F}_p^2$ a plane curve of degree n without vertical lines, and $\delta > 0$. The above probabilistic algorithm computes λ_i for $0 \le i \le n$ correctly with probability at least $1 - \delta$. It uses one random element and $O((n!)^2 n^{4n} \mathsf{M}(n) \delta^{-1} \log p)$ arithmetic operations in $\mathbb{F}_p$.*

PROOF. The algorithm uses $O(\mathsf{M}(n)h \log p)$ or $O((n!)^2 n^{4n} \mathsf{M}(n)\delta^{-1} \log p)$ arithmetic operations in $\mathbb{F}_p$. Let $0 \le i \le n$. It follows from Corollary 4.6 that

$$|r_i(a,h) - hr_i^*/p| \le n^{2n}(8h\delta^{-1})^{1/2}$$

with probability at least $1 - \delta$. If this inequality holds, we find from Lemma 2.3 that

$$\begin{aligned} |\lambda_i - r_i(a,h)/h| &\le |\lambda_i - r_i^*/p| + |r_i^*/p - r_i(a,h)/h| \\ &\le 2n^{2n}p^{-1/2} + n^{2n}(8/h\delta)^{1/2} \\ &\le 1/6n! + 1/6n! = 1/3n!. \end{aligned}$$

Then $\lambda_i = \Lambda_i/n!$ is the correct answer. 2

5. Distribution of points in multiplicative strips

In the previous sections we did not succeed in computing the projection distribution parameters r_i in an arbitrary finite field, as we have to know the behavior of x along absolutely irreducible components of the fibre product curves $\mathcal{C}_k$. Instead of 'additive strips', we consider in this section 'multiplicative strips' that may help us in some cases.

Our main tool is Perel'muter's (1969) bound on multiplicative character sums along an algebraic curve, rather than Bombieri's (1966) bound used before.

For $\lambda \in \mathbb{F}_q^\times$ and integers a and h, we denote by $M(\lambda, a, h)$ the 'multiplicative interval'

$$M(\lambda, a, h) = \{\lambda^{a+t} : 1 \le t \le h\} \subseteq \mathbb{F}_q^\times,$$

and given a curve $\mathcal{C} \subseteq \mathbb{F}_q^{m+1}$, we let

$$\mathcal{C}(\lambda, a, h) = \mathcal{C}(M(\lambda, a, h)).$$

We prove some analogues of Lemma 2.1 of von zur Gathen *et al.* (1996) and Lemma 4.2 of this paper.

The following condition on a curve $\mathcal{C} \subseteq \mathbb{F}_q^{m+1}$ is used in Perel'muter's Theorem.

HYPOTHESIS B. *The first coordinate function x is not a power g^e of a rational function g on any absolutely irreducible component of $\mathcal{C}$, where g is defined over an algebraic closure of $\mathbb{F}_q$, and $e \geq 2$ is an integer.*

THEOREM 5.1. *Let $\mathcal{C} \subseteq \mathbb{F}_q^m$ be a curve of degree n without vertical components and satisfying hypothesis B, $\lambda \in \mathbb{F}_q^\times$ be of order τ, and a and $h \leq \tau$ be integers. Then*

$$|\#\mathcal{C}(\lambda, a, h) - h\#\mathcal{C}/q| \leq 2n^2 q^{1/2} \log q.$$

PROOF. Let $\theta \in \mathbb{F}_q$ be a primitive element such that $\lambda = \theta^{(q-1)/\tau}$.

Denote by $\mathrm{ind}u$ the index of $u \in \mathbb{F}_q^\times$ in base θ, i.e., the smallest nonnegative integer t with $u = \theta^t$, so that

$$\mathrm{ind}(\lambda^{a+t}) \equiv (q-1)(a+t)\tau^{-1} \bmod (q-1).$$

Then

$$\begin{aligned}\#\mathcal{C}(\lambda, a, h) &= \frac{1}{q-1} \sum_{(u,v)\in\mathcal{C}} \sum_{1\leq t\leq h} \sum_{0\leq s\leq q-2} \exp\Big(\frac{2\pi i s(\mathrm{ind}u - (q-1)(a+t)\tau^{-1})}{q-1}\Big) \\ &= \frac{1}{q-1} \sum_{0\leq s\leq q-2} \sum_{(u,v)\in\mathcal{C}} \chi_s(u) \sum_{1\leq t\leq h} \exp(-2\pi i s(a+t)/\tau),\end{aligned}$$

where $u \in \mathbb{F}_q$ and $v \in \mathbb{F}_q^m$ in the sums. For $0 \leq s \leq q-2$, define a multiplicative character χ_s on $\mathbb{F}_q$ by

$$\chi_s(u) = \exp[2\pi i s\, \mathrm{ind}u/(q-1)],$$

for $u \in \mathbb{F}_q^\times$, and set $\chi_s(0) = 0$. Separating the term corresponding to $s = 0$ we get

$$\begin{aligned}\#\mathcal{C}(\lambda, a, h) &= \frac{h}{q-1}(\#\mathcal{C} - E) \\ &\quad + \frac{1}{q-1} \sum_{1\leq s\leq q-2} \sum_{(u,v)\in\mathcal{C}} \chi_s(u) \sum_{1\leq t\leq h} \exp(-2\pi i s(a+t)/\tau),\end{aligned} \tag{5.1}$$

where

$$E = \sum_{(0,v)\in\mathcal{C}} 1 = \#(\mathcal{C} \cap \{x = 0\}) \leq n,$$

by Bézout's Theorem. Theorem 2 of Perel'muter (1969) implies that for any s

$$\Big|\sum_{(u,v)\in\mathcal{C}} \chi_s(x)\Big| \leq (n^2 - 3n)q^{1/2} + n^2.$$

Since $h \le q-1$, we have

$$\begin{aligned}
&|\#\mathcal{C}(\lambda,a,h) - h\#\mathcal{C}/(q-1)| \\
&\quad\le \frac{hn}{q-1} + \frac{(n^2-3n)q^{1/2}+n^2}{q-1} \sum_{1\le s\le q-2} \Big| \sum_{1\le t\le h} \exp(2\pi i s(a+t)/\tau)\Big| \\
&\quad\le n + \frac{(n^2-3n)q^{1/2}+n^2}{\tau} \sum_{1\le s<\tau} \Big| \sum_{1\le t\le h} \exp(-2\pi i s t/\tau)\Big|.
\end{aligned}$$

Using the following well-known inequality

$$\sum_{1\le s<\tau} \Big| \sum_{1\le t\le h} \exp(2\pi i s t/\tau)\Big| \le \tau \log \tau,$$

we get

$$|\#C(\lambda,a,h) - h\#\mathcal{C}/(q-1)| \le n + ((n^2-3n)q^{1/2}+n^2)\log\tau.$$

Taking into account that $\#\mathcal{C} \le nq$ and thus

$$\Big|\frac{h\#C}{q-1} - \frac{h\#C}{q}\Big| = \frac{h\#C}{q(q-1)} \le n, \tag{5.2}$$

finally we obtain

$$\begin{aligned}
|\#\mathcal{C}(\lambda,a,h) - h\#\mathcal{C}/q| &\le n + n + ((n^2-3n)q^{1/2}+n^2)\log\tau \\
&\le 2n + ((n^2-3n)q^{1/2}+n^2)\log\tau \\
&\le 2n^2 q^{1/2}\log q. \qquad 2
\end{aligned}$$

THEOREM 5.2. *Let $\mathcal{C} \subseteq \mathbb{F}_q^m$ be a curve without vertical components and of degree $n \ge 2$ satisfying hypothesis B, $\lambda \in \mathbb{F}_q^\times$ be of order τ, and $h \le \tau$. Then*

$$\sum_{0\le a\le q-2} (\#\mathcal{C}(\lambda,a,h) - h\#\mathcal{C}/q)^2 \le 8n^4 qh.$$

PROOF. Using the notation of the previous proof, we have

$$(q-1)\Big|\frac{\#\mathcal{C}}{q} - \frac{\#\mathcal{C}-E}{q-1}\Big| = \Big|\frac{-\#\mathcal{C}}{q} + E\Big| \le n,$$

$$\sum_{0\le a\le q-2} (\#\mathcal{C}(\lambda,a,h) - h\#\mathcal{C}/q)^2$$
$$\le\ 2\sum_{0\le a\le q-2}\Big[\#\mathcal{C}(\lambda,a,h) - \frac{h(\#\mathcal{C}-E)}{q-1}\Big]^2 + 2\sum_{0\le a\le q-2}\Big[\frac{h\#\mathcal{C}}{q} - \frac{h(\#\mathcal{C}-E)}{q-1}\Big)\Big]^2$$
$$\le\ 2W + 2n^2h^2/(q-1),$$

where

$$W = \sum_{0\le a\le q-2}\Big[\#\mathcal{C}(\lambda,a,h) - \frac{h(\#\mathcal{C}-E)}{q-1}\Big]^2$$
$$= (q-1)^{-2}\sum_{0\le a\le q-2}\Big|\sum_{1\le s\le q-2}\sum_{(u,v)\in\mathcal{C}}\chi_s(u)\sum_{1\le t\le h}\exp(2\pi is(a+t)/\tau)\Big|^2,$$

by (5.1). Using $|\alpha|^2 = \alpha\bar{\alpha}$ for $\alpha\in\mathbb{C}$, we have

$$W = (q-1)^{-2}\sum_{1\le s_1,s_2\le q-2}\sum_{(u_1,v_1),(u_2,v_2)\in\mathcal{C}}\chi_{s_1}(u_1)\chi_{s_2}(u_2^{-1})$$
$$\cdot\sum_{1\le t_1,t_2\le h}\exp(2\pi i(s_1t_1-s_2t_2)/\tau)\sum_{0\le a\le q-2}\exp(2\pi ia(s_1-s_2)/\tau).$$

Noting that the inner sum equals 0 when $s_1\ne s_2$ and $q-1$ otherwise, we get

$$W = (q-1)^{-1}\sum_{1\le s\le q-2}\sum_{(u_1,v_1),(u_2,v_2)\in\mathcal{C}}\chi_s(u_1u_2^{-1})\sum_{1\le t_1,t_2\le h}\exp(2\pi is(t_1-t_2)/\tau)$$
$$= (q-1)^{-1}\sum_{1\le s\le q-2}\Big|\sum_{(u,v)\in\mathcal{C}}\chi_s(u)\Big|^2\Big|\sum_{1\le t\le h}\exp(2\pi ist/\tau)\Big|^2.$$

Theorem 2 of Perel'muter (1969) yields

$$W\le\frac{((n^2-3n)q^{1/2}+n^2)^2}{q-1}\sum_{1\le s\le q-2}\Big|\sum_{1\le t\le h}\exp(2\pi ist/\tau)\Big|^2.$$

Taking into account the equality

$$\sum_{0\le s\le q-2}\Big|\sum_{1\le t\le h}\exp(2\pi ist/\tau)\Big|^2 = \sum_{1\le t_1,t_2\le h}\sum_{0\le s\le q-2}\exp(2\pi is(t_1-t_2)/\tau) = h(q-1),$$

we obtain

$$W\le\frac{((n^2-3n)q^{1/2}+n^2)^2}{q-1}\cdot(h(q-1)-h^2),$$

$$\sum_{0 \le a \le q-2} (\#\mathcal{C}(\lambda, a, h) - h\#\mathcal{C}/q)^2 \le 2n^2h^2/(q-1) + 2((n^2-3n)q^{1/2} + n^2)^2 h$$
$$\le 2n^2h(1 + ((n-3)q^{1/2} + n)^2) \le 2n^2h(nq^{1/2} + n)^2 \ \le \ 8n^4hq. \qquad 2$$

We now show that hypothesis B is not a severe restriction, in that it is satisfied after a generic linear transformation. This is most naturally shown for a projective curve over an algebraically closed field $\mathbb{K}$.

So let $\mathcal{X} \subseteq \mathbb{P}_{\mathbb{K}}^{m+1}$ be a reduced curve of degree n, possibly reducible or singular, $\mathbb{H} \cong \mathbb{P}_{\mathbb{K}}^{m+1}$ the space of hyperplanes in $\mathbb{P}_{\mathbb{K}}^{m+1}$, and for $\mathcal{H} \in \mathbb{H}$, let $l_{\mathcal{H}}$ be the rational linear function whose zero set is $\mathcal{H}$. We say that $\mathcal{H} \in \mathbb{H}$ *intersects $\mathcal{X}$ transversally* if and only if $\#(\mathcal{X} \cap \mathcal{H}) = n$. The following facts are well known.

FACT 5.3. *Let $\mathcal{X}$ be as above, and $\mathcal{H} \in \mathbb{H}$.*

(i) If no component of $\mathcal{X}$ is contained in $\mathcal{H}$, then $\#(\mathcal{X} \cap \mathcal{H}) \le n$.

(ii) If $\mathcal{H}$ does not contain a tangent line to $\mathcal{X}$ or a singular point of $\mathcal{X}$, then $\mathcal{H}$ intersects $\mathcal{X}$ transversally.

(iii) There is a proper closed subvariety $E \subseteq \mathbb{H}$ of degree at most $n(n-1)$ such that $\mathcal{H}$ intersects $\mathcal{X}$ transversally if $\mathcal{H} \in \mathbb{H} \setminus E$.

(iv) if $\mathcal{H}$ intersects $\mathcal{X}$ transversally, then $l_{\mathcal{H}}$ is not a power g^e of a rational function g on any absolutely irreducible component of $\mathcal{X}$, with $e \ge 2$.

For a plane curve, (iii) follows from, e.g., Proposition 5.2.2 of Brieskorn & Knörrer (1986).

For a curve $\mathcal{C} \subseteq \mathbb{F}_q^{m+1}$, Fact 5.3 implies that almost all linear transformations of $\mathcal{C}$ satisfy hypothesis B. We only make this explicit for $m = 1$. We need the fact that there exist a line (over $\mathbb{K}$) through the origin which is not a tangent to $\mathcal{C}$; this is true for all curves except the "strange" conic in characteristic two (see Hartshorne 1977, Theorem IV.3.9).

PROPOSITION 5.4. *Let $f \in \mathbb{F}_q[x, y]$ be squarefree of degree n, with either $n \ne 2$ or $\operatorname{char} \mathbb{F}_q \ne 2$, and for $\alpha \in \mathbb{F}_q$, let*

$$\mathcal{C}_\alpha = \{f(x, y + \alpha x) = 0\} = \{(a, b) \in \mathbb{F}_q^2 : f(a, b + \alpha a) = 0\}.$$

Then there exists $E \subseteq \mathbb{F}_q$ with $\#E \le n(n-1)$ and such that $\mathcal{C}_\alpha$ satisfies hypothesis B for all $\alpha \in \mathbb{F}_q \setminus E$.

In order to design algorithms from the above results, we have to construct wide enough multiplicative strips or, equivalently, to find elements $\lambda \in \mathbb{F}_q^*$ of sufficiently large order (von zur Gathen & Shparlinski 1995b); certainly a primitive root is sufficient. Results about the construction, distribution and density of primitive roots can be found in Lidl & Niederreiter (1983); see Shparlinski (1992b) for a survey and also von zur Gathen & Giesbrecht (1990), Perel'muter & Shparlinski (1990), Shoup (1992), Shparlinski (1992a) for the currently best results in this area.

Acknowledgements

Parts of the first author's work was done on a visit to Macquarie University and during a sabbatical visit to the Institute for Scientific Computation at ETH Zürich, whose hospitality is gratefully acknowledged. The research was also supported by the Information Technology Research Centre and the Natural Sciences and Engineering Research Council of Canada. Part of the second author's work was done during a sabbatical visit to Universität Paderborn, which was supported by Deutsche Forschungsgemeinschaft.

An Extended Abstract of this paper has appeared in Proc. ISAAC '94, ed. Ding-Zhu Du, Xiang-Sun Zhang, Beijing P. R. China, Springer-Verlag, LNCS **834** (1994), 297-305.

We thank Gerhard Frey and Henning Stichtenoth for pointing out (4.2).

References

E. Bombieri, On exponential sums in finite fields. *Amer. J. Math.* **88** (1966), 71–105.

E. Bombieri and H. Davenport, On two problems of Mordell. *Amer. J. Math.* **88** (1966), 61–70.

E. Brieskorn and H. Knörrer, *Plane Algebraic Curves.* Birkhäuser, Basel, 1986.

S. D. Cohen, The distribution of polynomials over finite fields. *Acta Arith.* **17** (1970), 255–271.

J. von zur Gathen, Values of polynomials over finite fields. *Bull. Austral. Math. Soc.* **43** (1991), 141–146.

J. von zur Gathen and M. Giesbrecht, Constructing normal bases in finite fields. *J. Symb. Comp.* **10** (1990), 547–570.

J. VON ZUR GATHEN AND I. E. SHPARLINSKI, Finding points on curves over finite fields. In *Proc. 36th Ann. IEEE Symp. on Foundations of Computer Science*, 1995a, 284–292.

J. VON ZUR GATHEN AND I. E. SHPARLINSKI, Orders of gauss periods in finite fields. In *Proc. ISAAC '95, Cairns, Australia*, 1995b, 209–215. to appear.

J. VON ZUR GATHEN, M. KARPINSKI, AND I. E. SHPARLINSKI, Counting curves and their projections. *Computational complexity* **6** (1996). To appear.

R. HARTSHORNE, *Algebraic Geometry*. Springer-Verlag, 1977.

M.-D. HUANG AND D. IERARDI, Counting rational points on curves over finite fields. In *Proc. 34th Ann. IEEE Symp. on Foundations of Computer Science*, Palo Alto CA, 1993, 616–625.

R. M. KARP, M. LUBY, AND N. MADRAS, Monte-Carlo approximation algorithms for enumeration problems. *J. Algorithms* **10**(3) (1989), 429–448.

R. LIDL AND H. NIEDERREITER, *Finite Fields*, vol. 20 of *Encyclopedia of Mathematics and its Applications*. Addison-Wesley, Reading MA, 1983.

G. I. PEREL'MUTER, Оценка суммы вдоль алгебраическои кривои (Bounds on sums along algebraic curves). *Mat. Zametki* **5** (1969), 373–380.

G. I. PEREL'MUTER AND I.E. SHPARLINSKI, О распределении нервообразных корнеи в конечных полях (On the distribution of primitive roots in finite fields). *Uspekhi Matem. Nauk* **45**(1) (1990), 185–186.

R. PILA, Frobenius maps of Abelian varieties and finding roots of unity in finite fields. *Math. Comp.* **55** (1990), 745–763.

A. SCHÖNHAGE AND V. STRASSEN, Schnelle Multiplikation großer Zahlen. *Computing* **7** (1971), 281–292.

R. J. SCHOOF, Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.* **44**(170) (1985), 483–494.

V. SHOUP, Searching for primitive roots in finite fields. *Math. Comp.* **58**(197) (1992), 369–380.

I. E. SHPARLINSKI, On primitive elements in finite fields and on elliptic curves. *Math. USSR Sbornik* **71**(1) (1992a), 41–50.

I. E. SHPARLINSKI, *Computational and algorithmic problems in finite fields*, vol. 88 of *Mathematics and its applications*. Kluwer Academic Publishers, 1992b.