comput complexity 5 (1995), 76–97 1016-3328/95/010076-22 $1.50+0.20

THE COMPUTATIONAL COMPLEXITY OF RECOGNIZING PERMUTATION FUNCTIONS

KEJU MA AND JOACHIM VON ZUR GATHEN

Abstract. Let $\mathbb{F}_q$ be a finite field with q elements and $f \in \mathbb{F}_q(x)$ a rational function over $\mathbb{F}_q$. No polynomial-time deterministic algorithm is known for the problem of deciding whether f induces a permutation on $\mathbb{F}_q$. The problem has been shown to be in co-$\mathcal{R} \subseteq$ co-$\mathcal{NP}$, and in this paper we prove that it is in $\mathcal{R} \subseteq \mathcal{NP}$ and hence in $\mathcal{ZPP}$, and it is deterministic polynomial-time reducible to the problem of factoring univariate polynomials over $\mathbb{F}_q$. Besides the problem of recognizing prime numbers, it seems to be the only natural decision problem in $\mathcal{ZPP}$ unknown to be in $\mathcal{P}$. A deterministic test and a simple probabilistic test for permutation functions are also presented.

Subject classifications. 68Q15, 68Q25; 11Y16, 12Y05.

1. Introduction

Let q be a power of a prime, $\mathbb{F}_q$ a finite field with q elements, $f = g/h \in \mathbb{F}_q(x)$ an arbitrary rational function with $g, h \in \mathbb{F}_q[x]$ and $\gcd(g, h) = 1$. Then f induces a partial mapping $\mathbb{F}_q \to \mathbb{F}_q$ via $a \mapsto f(a)$ for all $a \in \mathbb{F}_q$ with $h(a) \neq 0$. If f is total (i.e., $h(a) \neq 0$ for all $a \in \mathbb{F}_q$) and bijective, then f is called a *permutation function* over $\mathbb{F}_q$. In the special case $h = 1$, so that $f = g \in \mathbb{F}_q[x]$, it is called a *permutation polynomial* over $\mathbb{F}_q$.

Permutation functions have been studied since the last century. In recent years considerable attention has been given to their potential applications in public-key cryptography. Further references can be found in the survey articles Lidl & Mullen (1988, 1993) and Mullen (1993).

The importance of permutation functions lies in the fact that they connect two essential components of the theory of finite fields: combinatorics and algebra. The permutation property and the applications in cryptography are of a combinatorial nature, and the use of polynomials or rational functions for representing these combinatorial objects allows powerful algebraic methods to be employed. It is the same type of synthesis that has worked very successfully in the theory of error-correcting codes.

The efficient representation of permutations on $\mathbb{F}_q$ is a nontrivial computational task: a general representation via enumeration requires exponential size (in $\log q$). Algebra presents a partial solution by representing permutations as polynomials or rational functions over $\mathbb{F}_q$. Such permutation functions always exist, since any total function over $\mathbb{F}_q$ can be represented by a unique polynomial of degree less than q, computable by interpolation over $\mathbb{F}_q$. This introduces the degree of the representing polynomial or rational function as an interesting measure. A fundamental problem for manipulating these objects is to determine when an arbitrary rational function represents a permutation on $\mathbb{F}_q$. We denote by PermFunction this decision problem, and it includes, of course, the special problem of testing whether an arbitrary polynomial is a permutation polynomial. For a random polynomial $f \in \mathbb{F}_q[x]$ of degree $< q$, the probability that f is a permutation polynomial is $q!/q^q \approx e^{-q}$.

If f has degree $n = \max\{\deg g, \deg h\}$, then its input size is $O(n \log q)$ bits under the dense representation of polynomials; we may always assume that $n \leq q$, since $a^q = a$ for all $a \in \mathbb{F}_q$. No polynomial-time (in $n \log q$) deterministic decision procedure is known for PermFunction.

Based on the subresultant approach introduced in von zur Gathen (1991a), Ma & von zur Gathen (1993) recently designed a fast random polynomial-time test for PermFunction, using $O^{\sim}(n \log q)$ operations in $\mathbb{F}_q$ (i.e., essentially linear in the input size), or $O^{\sim}(n \log^2 q)$ bit operations. Here we use the "soft O" notation to ignore logarithmic factors:

$$s = O^{\sim}(t) \iff s = O(t \log^k t) \text{ for some constant } k.$$

The resulting test has one-sided error for the complement ("No-biased"), so that if the input f is a permutation function, it returns Yes; if f is not, it returns Yes with exponentially small probability. This demonstrates that PermFunction is in co-$\mathcal{RP}$.

Since $f = g/h$ is not a permutation function if and only if f is either not total or not injective, it is trivial that PermFunction $\in$ co-$\mathcal{NP}$: any $a \in \mathbb{F}_q$ with $h(a) = 0$ or $(a, b) \in \mathbb{F}_q^2$ with $a \neq b$ and $f(a) = f(b)$ is a certificate. On the other

hand, it is not clear whether PermFunction is in $\mathcal{NP}$. What would constitute a "succinct certificate" that all q elements in $\mathbb{F}_q$ are images of f?

Among the very few natural decision problems in $\mathcal{NP} \cap$ co-$\mathcal{NP}$ unknown to be in $\mathcal{P}$, the most celebrated one is the problem Prime of recognizing prime numbers (Pratt 1975). Solovay & Strassen (1977), and later Miller (1976) and Rabin (1980), designed random polynomial-time tests for Prime that are No-biased, and thus proved that Prime $\in$ co-$\mathcal{R}$. Building on results of Goldwasser & Kilian (1986), Adleman & Huang (1992) established that Prime is in $\mathcal{ZPP} = \mathcal{R} \cap$ co-$\mathcal{R}$ by giving a complementary "Yes-biased" probabilistic polynomial-time test, albeit a rather impractical one. Assuming the Extended Riemann Hypothesis (ERH), Miller (1976) showed that Prime $\in \mathcal{P}$.

In this paper, we prove that PermFunction $\in \mathcal{ZPP}$; it seems to be the second natural decision problem in $\mathcal{ZPP}$ unknown to be in $\mathcal{P}$, and the only one under the ERH.

We start with an introduction to *exceptional functions* in Section 2. We prove a quantitative version of the well-known result that over a sufficiently large finite field, permutation functions are essentially exceptional functions. Since exceptional functions have polynomial-time verifiable certificates, it thus follows that PermFunction $\in \mathcal{NP}$.

In Section 3, we reduce PermFunction in deterministic polynomial time to the problem of factoring bivariate polynomials over $\mathbb{F}_q$, which is in turn deterministic polynomial-time reducible to the problem PolyFactor of factoring univariate polynomials over $\mathbb{F}_q$. This yields a Yes-biased random polynomial-time test for permutation functions (it can be made error-free running in expected polynomial time), and thus proves that PermFunction is in $\mathcal{R}$ and hence in $\mathcal{ZPP}$. We also give a decision-problem version of PolyFactor; it is debatable whether this is a "natural decision problem".

We design a deterministic test for permutation functions in Section 4. The deterministic test is based on Bombieri's estimate on exponential sums along a curve and uses $\tilde{O}(n^3 q^{1/2})$ field operations for $f \in \mathbb{F}_q(x)$ of degree $n \leq \operatorname{char} \mathbb{F}_q$ if q is sufficiently large, and it extends a previous deterministic test for permutation polynomials in Shparlinski (1992b).

We return to probabilistically testing permutation functions in Section 5. We develop a No-biased random polynomial-time test for PermFunction using $\tilde{O}(n^2 \log^2 q)$ operations in $\mathbb{F}_q$, which is about the square of the cost of the test in Ma & von zur Gathen (1993). The appeal of the new test is its simplicity of statement and ease of implementation; the proof of its correctness, however, relies on an application of Weil's famous theorem on the number of points on algebraic curves over finite fields.

2. Certificates for permutation functions

A rational function $f = g/h \in \mathbb{F}_q(x)$ is called *separable* if and only if $\partial f/\partial x \neq 0$.

NOTATION 2.1. *We use the following conventions throughout the paper.*

$f = g/h \in \mathbb{F}_q(x)$ *is separable with* $g, h \in \mathbb{F}_q[x]$ *and* $\gcd(g,h) = 1$,
$n = \deg f = \max\{\deg g, \deg h\} \leq q$, *and* $n \geq 1$,
$\rho = q - \#\{f(a) : a \in \mathbb{F}_q,\ h(a) \neq 0\}$ *is the number of non-images of* f,
$f^* = [g(x)\,h(y) - g(y)\,h(x)]/(x-y)$ *is the* difference polynomial *of* f,
n^* *is the (total) degree of* f^*,
K *is an algebraic closure of* $\mathbb{F}_q$,
$\mathcal{C} = \{(a,b) \in K^2 : f^*(a,b) = 0\}$ *is the plane curve defined by* f^*,
$\mathcal{C}^* = \{(a,b) \in \mathcal{C} : (a,b) \in \mathbb{F}_q^2,\ a \neq b\} = \{(a,b) \in \mathbb{F}_q^2 : f(a) = f(b),\ a \neq b\}$,
$\gamma = \#\mathcal{C}^*$ *is the number of rational points on* $\mathcal{C}$ *off the diagonal.*

Let $\mathsf{M} : \mathbb{N} \to \mathbb{R}$ be a "universal" cost of multiplication, so that the multiplication st takes $O(\mathsf{M}(n))$ arithmetic operations or bit operations, respectively, for two polynomials $s, t \in F[x]$ of degree at most n, or two n-bit integers $s, t \in \mathbb{Z}$. Similarly, the division with remainder $s \operatorname{rem} t$ (if $t \neq 0$), and the gcd computation $\gcd(s,t)$ can be performed in $O(\mathsf{M}(n))$, and $O(\mathsf{M}(n)\log n)$ operations, respectively (Aho *et al.* 1974, Section 7.5). We can choose $\mathsf{M}(n) = n \log n \operatorname{loglog} n$ with "fast arithmetic" (Schönhage & Strassen 1971, Cantor & Kaltofen 1991), and $\mathsf{M}(n) = n^2$ with "classical arithmetic".

The following proposition shows that we can always preprocess the input $f \in \mathbb{F}_q(x)$ for PermFunction and make it separable.

PROPOSITION 2.2. *For any* $f \in \mathbb{F}_q(x)$, *one can find a separable* $\bar{f} \in \mathbb{F}_q(x)$ *in* $O(n \log q \log n)$ *operations in* $\mathbb{F}_q$, *so that* f *is a permutation function if and only if* $\bar{f}$ *is.*

PROOF. Let $f = g/h \in \mathbb{F}_q(x)$ with $\gcd(g,h) = 1$, and $p = \operatorname{char} \mathbb{F}_q$ be the characteristic of $\mathbb{F}_q$. Since $\gcd(g,h) = 1$, we have $f' = 0$ (and thus $g'h - g\,h' = 0$) if and only if $g' = h' = 0$, i.e., if and only if $f \in \mathbb{F}_q(x^p)$ with $g = \sum a_{ip}\,x^{ip}$ and $h = \sum b_{ip}\,x^{ip}$. In that case, we can write $f(x) = [\bar{f}(x)]^p$ with $\bar{f} = \bar{g}/\bar{h} \in \mathbb{F}_q(x)$, $\gcd(\bar{g},\bar{h}) = 1$, $\bar{g} = \sum a_{ip}^{q/p}\,x^i$ and $\bar{h} = \sum b_{ip}^{q/p}\,x^i$, computable via repeated squaring in $O(n/p \cdot \log(q/p))$ multiplications in $\mathbb{F}_q$.

Since $a \mapsto a^p$ is a bijection of $\mathbb{F}_q$, it follows that f is a permutation function if and only if $\bar{f}$ is. In fact, they both have the same image size.

Replacing f by $\bar{f}$ and repeating this process until $\bar{f}' \neq 0$, we obtain a separable $\bar{f} = \bar{g}/\bar{h} \in \mathbb{F}_q(x)$ with $\gcd(\bar{g}, \bar{h}) = 1$ such that f is a permutation function if and only if $\bar{f}$ is. The total cost is $O(n/p \cdot \log(q/p) \cdot \log_p n)$ or $O(n \log n \log q)$ operations in $\mathbb{F}_q$. □

The following proposition gives a simple geometric characterization of permutation functions.

PROPOSITION 2.3. *Let $f \in \mathbb{F}_q(x)$ be total, and γ as in Notation 2.1. Then f is a permutation function if and only if $\gamma = 0$.*

While it seems in general hard to compute γ, i.e., to count the rational points of $\mathcal{C}$ off the diagonal, it is easy to count the rational points on the diagonal.

PROPOSITION 2.4. *Let $f = g/h \in \mathbb{F}_q(x)$, $\tilde{f} = g'h - gh' \in \mathbb{F}_q[x]$, n and $\mathcal{C}$ be as in Notation 2.1, and $\Delta \subseteq \mathbb{F}_q^2$ be the diagonal. Then we have $\mathcal{C} \cap \Delta = \{(a, a) \in \mathbb{F}_q^2 : \tilde{f}(a) = 0\}$, and $\#(\mathcal{C} \cap \Delta) = \deg \gcd(x^q - x, \tilde{f})$ can be computed with $O(\mathsf{M}(n) \log(qn))$ operations in $\mathbb{F}_q$.*

PROOF. We recall from Notation 2.1 that

$$\begin{aligned} f^*(x, y) &= \frac{g(x)\,h(y) - g(y)\,h(x)}{x - y} \\ &= \frac{[g(x) - g(y)]\,h(y) - g(y)\,[h(x) - h(y)]}{x - y} \\ &= \frac{g(x) - g(y)}{x - y}\,h(y) - g(y)\,\frac{h(x) - h(y)}{x - y}. \end{aligned}$$

Therefore, $f^*(x, x) = \tilde{f} = g'h - gh' \in \mathbb{F}_q[x]$, and hence

$$\mathcal{C} \cap \Delta = \{(a, a) \in \mathbb{F}_q^2 : f^*(a, a) = 0\} = \{(a, a) \in \mathbb{F}_q^2 : \tilde{f}(a) = 0\}.$$

From Fermat's little theorem $\prod_{a \in \mathbb{F}_q}(x - a) = x^q - x$, we have $\#(\mathcal{C} \cap \Delta) = \deg \gcd(x^q - x, \tilde{f})$. Using repeated squaring and polynomial gcd computations, we can thus count the rational points of $\mathcal{C}$ on the diagonal with $O(\mathsf{M}(n) \log(qn))$ operations in $\mathbb{F}_q$. □

Combining Propositions 2.3 and 2.4, we obtain the following equivalent characterization of permutation functions.

COROLLARY 2.5. *Let $f = g/h \in \mathbb{F}_q(x)$ be total, and $\mathcal{C}$ as in Notation 2.1. Then f is a permutation function if and only if $\mathcal{C}$ has exactly* $\deg \gcd(x^q - x, g'h - gh')$ *rational points over $\mathbb{F}_q$.*

LEMMA 2.6. *Let $f \in \mathbb{F}_q(x)$ be total, and n, ρ, γ as in Notation 2.1. Then $n\rho \geq \gamma$.*

PROOF. For $i \in \mathbb{N}$, let $R_i = \{a \in \mathbb{F}_q : \#f^{-1}(\{a\}) = i\}$ be the set of field elements with exactly i preimages under f, and $r_i = \#R_i$. Clearly, $R_i = \emptyset$ for $i > n$, since for any $a \in \mathbb{F}_q$, $g - a\,h \in \mathbb{F}_q[x]$ has at most n roots in $\mathbb{F}_q$. Since

$$\bigcup_{0 \leq i \leq n} R_i = \mathbb{F}_q \text{ and } \bigcup_{1 \leq i \leq n} R_i = f(\mathbb{F}_q)$$

are partitions of $\mathbb{F}_q$ and $f(\mathbb{F}_q)$, respectively, we have

$$\sum_{1 \leq i \leq n} r_i = q - \rho, \quad \sum_{1 \leq i \leq n} i r_i = q, \quad \sum_{2 \leq i \leq n} (i-1)\, r_i = \rho. \tag{2.1}$$

Consider the mapping from $\mathcal{C}^*$ onto $\bigcup_{2 \leq i \leq n} R_i$ given by $(a, b) \mapsto f(a)$. Clearly, every $c \in R_i$ has exactly $i(i-1)$ preimages under this mapping. It thus follows from (2.1) that

$$n\rho = \sum_{2 \leq i \leq n} n(i-1)\, r_i \geq \sum_{2 \leq i \leq n} i(i-1)\, r_i = \gamma. \qquad \square$$

PROPOSITION 2.7. *Let $f \in \mathbb{F}_q(x)$, and n, f^*, n^* be as in Notation 2.1. Then $n - 1 \leq n^* \leq 2(n-1)$ and $x - y \nmid f^*$.*

PROOF. Let $f = g/h$ with $g = \sum_{0 \leq i \leq n} a_i x^i$ and $h = \sum_{0 \leq i \leq n} b_i x^i$ with $a_i, b_i \in \mathbb{F}_q$. Then we can write

$$\begin{aligned} f^* &= \frac{g(x)\,h(y) - g(y)\,h(x)}{x - y} \\ &= \sum_{0 \leq i \leq n} \sum_{0 \leq j \leq n} a_i b_j \frac{x^i y^j - x^j y^i}{x - y} = \sum_{0 \leq i,j < n} z_{ij}\, x^i y^j, \end{aligned}$$

with the symmetric *Bézoutian matrix* $Z = (z_{ij})_{0 \leq i,j < n} \in \mathbb{F}_q^{n \times n}$. It is well-known that the resultant of g and h satisfies $\operatorname{res}(g, h) = (-1)^{n(n-1)/2} \det Z$ (see, e.g., Barnett 1983, Section 1.5).

Clearly, $z_{n-1,j} = z_{j,n-1} \neq 0$ for some $0 \leq j \leq n-1$, since otherwise the last row of Z would comprise all zeroes, resulting in $\det Z = \operatorname{res}(g, h) = 0$ and hence $\gcd(g, h) \neq 1$, which is a contradiction, since f is separable. $\square$

REMARK 2.8. The difference polynomial f^* can be computed with $O(n^3)$ operations in $\mathbb{F}_q$, and the degree bounds on f^* are tight. The lower bound $n-1$ is achieved for $f = (x^n + a)/x^n$ and the upper bound $2(n-1)$ is achieved for $f = (x^{n-1} + a)/x^n$, for any $a \in \mathbb{F}_q \setminus \{0\}$.

Since $\mathbb{F}_q[x, y]$ is a unique factorization domain, every non-constant polynomial in $\mathbb{F}_q[x, y]$ has a complete factorization into irreducible factors over $\mathbb{F}_q$. An irreducible polynomial in $\mathbb{F}_q[x, y]$ is *absolutely irreducible* if it is irreducible over any algebraic extension of $\mathbb{F}_q$, or equivalently, irreducible over an algebraic closure of $\mathbb{F}_q$.

Kaltofen (1985, 1987) shows that for polynomials in $\mathbb{F}_q[x, y]$ of degree n, both irreducibility over $\mathbb{F}_q$ and absolute irreducibility can be tested deterministically in polynomial time (seemingly, in $\tilde{O}(n^8 \log q)$ operations in $\mathbb{F}_q$).

DEFINITION 2.9. A non-constant rational function $f \in \mathbb{F}_q(x)$ is *exceptional* if and only if its difference polynomial $f^* \in \mathbb{F}_q[x, y]$ has no absolutely irreducible factors over $\mathbb{F}_q$.

For example, any linear rational function $(ax + b)/(cx + d) \in \mathbb{F}_q(x)$ with $ad - bc \neq 0$ is exceptional.

REMARK 2.10. Every exceptional function (or non-exceptional function) of degree n can be certified in time polynomial in the input size $n \log q$, via Kaltofen's two deterministic irreducibility tests. This shows that exceptional functions are in $\mathcal{NP} \cap \text{co-}\mathcal{NP}$.

Perhaps the most important development in the contemporary study of permutation functions is the fundamental result stating that exceptional functions are essentially equivalent to permutation functions.

Special and weaker versions of the following facts for polynomials over $\mathbb{F}_q$ were proved by MacCluer (1967) and Williams (1968) for part (i), and by Davenport & Lewis (1963), Bombieri & Davenport (1966) and Hayes (1967) for part (ii). The general and stronger version for rational functions over $\mathbb{F}_q$ was established in its entirety by Cohen (1970) using deep methods in algebraic number theory.

FACT 2.11. (Cohen) *Let $f \in \mathbb{F}_q(x)$ be total and separable of degree n.*

(i) *If f is exceptional, then f is a permutation function.*

(ii) *There exists a function c_n of n such that if $q \geq c_n$ and f is a permutation function, then f is exceptional.*

Our aim in the remainder of this section is to find an explicit value for c_n and then demonstrate that every permutation function has a polynomial-time verifiable certificate.

LEMMA 2.12. *Let $\varphi \in \mathbb{F}_q[x,y]$ have degree $m \geq 1$, and suppose that $x - y \nmid \varphi$. Let $\gamma = \#\{(a,b) \in \mathbb{F}_q^2 : \varphi(a,b) = 0,\ a \neq b\}$, and σ be the number of non-associate absolutely irreducible factors of φ over $\mathbb{F}_q$.*

(i) *If $q \geq (m+1)^4$ and $\sigma \geq 1$, then $\gamma > 0$.*

(ii) *If $0 < \epsilon \leq 1$ and $q \geq \epsilon^{-2}(m+1)^4$, then $\gamma > (\sigma - \epsilon)q$.*

PROOF. Without loss of generality, we assume that φ is squarefree, and write $\varphi = \varphi_1 \cdots \varphi_\sigma \varphi_{\sigma+1} \cdots \varphi_\tau$, with $\varphi_i \in \mathbb{F}_q[x,y]$ irreducible and pairwise non-associated for $1 \leq i \leq \tau$, and φ_i absolutely irreducible if and only if $i \leq \sigma$. We may further assume that $\sigma \geq 1$.

Let K be an algebraic closure of $\mathbb{F}_q$, and for $1 \leq i \leq \tau$, let $\mathcal{C}_i = \{(a,b) \in K^2 : \varphi_i(a,b) = 0\}$ be the curve defined by φ_i, $\mathcal{X}_i = \mathcal{C}_i \cap \mathbb{F}_q^2$ its rational points, and $n_i = \deg \varphi_i \geq 1$. By Bézout's theorem, for $1 \leq i < j \leq \tau$, we have

$$n_i n_j \geq \#(\mathcal{C}_i \cap \mathcal{C}_j) \geq \#(\mathcal{X}_i \cap \mathcal{X}_j). \tag{2.2}$$

Furthermore, for $1 \leq i \leq \sigma$, Weil's bound (Fried & Jarden 1986, Theorem 4.9; Bach) on the number of points on a plane curve over a finite field yields that

$$\#\mathcal{X}_i \geq q + 1 - (n_i - 1)(n_i - 2)q^{1/2} - n_i \geq q - n_i^2 q^{1/2}. \tag{2.3}$$

Since $x - y$ does not divide φ, $\varphi(x,x) \in \mathbb{F}_q[x]$ is a non-zero polynomial of degree at most m, and hence by (2.2) and (2.3)

$$\begin{aligned} \gamma &\geq \# \bigcup_{1 \leq i \leq \tau} \mathcal{X}_i - m \geq \# \bigcup_{1 \leq i \leq \sigma} \mathcal{X}_i - m \\ &\geq \sum_{1 \leq i \leq \sigma} \#\mathcal{X}_i - \sum_{1 \leq i < j \leq \sigma} \#(\mathcal{X}_i \cap \mathcal{X}_j) - m \\ &\geq \sigma q - q^{1/2} \sum_{1 \leq i \leq \sigma} n_i^2 - \sum_{1 \leq i < j \leq \sigma} n_i n_j - m \\ &\geq \sigma q - m^2 q^{1/2} - m^2 - m, \end{aligned} \tag{2.4}$$

because $n_1 + \cdots + n_\sigma \leq m$.

A simple calculation shows that if $q \geq (m+1)^4$ and $\sigma \geq 1$, then $\sigma q - m^2 q^{1/2} - m^2 - m > 0$, and hence (i) follows from (2.4).

To prove (ii), we use (2.4) and write

$$\begin{aligned}\gamma &\geq \sigma q - m^2 q^{1/2} - m^2 - m \\ &= (\sigma - \epsilon)\, q + \epsilon q - m^2 q^{1/2} - m^2 - m \;>\; (\sigma - \epsilon)\, q,\end{aligned}$$

since $0 < \epsilon \leq 1$ and $q \geq \epsilon^{-2}(m+1)^4$ imply that $\epsilon q - m^2 q^{1/2} - m^2 - m > 0$. □

THEOREM 2.13. *Let $f \in \mathbb{F}_q(x)$ be total, and n, ρ, f^* as in Notation 2.1, and furthermore $0 < \epsilon \leq 1$.*

(i) *If $q \geq 16\, n^4$ and f is a permutation function, then f is exceptional.*

(ii) *If $q \geq 16\, \epsilon^{-2}\, n^4$ and σ is the number of non-associate absolutely irreducible factors of f^* over $\mathbb{F}_q$, then $\rho > (\sigma - \epsilon)\, q/n$.*

(iii) *If $q \geq 64\, n^4$ and f is not a permutation function, then $\rho > q/2n$.*

PROOF. We may assume that $n \geq 2$, since any total linear rational function is a polynomial.

We recall γ, n^* from Notation 2.1. Proposition 2.7 shows that $n - 1 \leq n^* \leq 2\,(n-1)$ and $x - y \nmid f^*$. Using $16\, n^4 > (2\, n - 1)^4 \geq (n^* + 1)^4$, Lemma 2.12 (i) proves (i), since f is a permutation function if and only if $\gamma = 0$.

Similarly, since $16\, \epsilon^{-2} n^4 > \epsilon^{-2}(2\, n - 1)^4 \geq \epsilon^{-2}\,(n^* + 1)^4$, (ii) follows from Lemma 2.6 and Lemma 2.12 (ii).

(iii) follows from (ii) with $\epsilon = 1/2$, using Fact 2.11 (i). □

Combining Fact 2.11 (i) with Theorem 2.13 (i), we have the following result.

COROLLARY 2.14. *Let $q \geq 16\, n^4$ and $f = g/h \in \mathbb{F}_q(x)$ be total and separable of degree n. Then f is a permutation function if and only if f is exceptional.*

If $h = 1$, then $f = g \in \mathbb{F}_q[x]$ and the difference polynomial $f^* = [f(x) - f(y)]/(x - y)$ has degree $n^* = n - 1$, and hence Corollary 2.14 holds for $q \geq n^4$ (see also von zur Gathen 1991b). In this special case, Wan (1993) proves a stronger version for Theorem 2.13 (iii): if $f \in \mathbb{F}_q[x]$ of degree n is not a permutation polynomial, then the number ρ of non-images of f in $\mathbb{F}_q$ satisfies $\rho \geq (q-1)/n$, for any n and q.

REMARK 2.15. Fermat's little theorem states that $x^q - x = \prod_{a \in \mathbb{F}_q}(x - a)$, and hence $f = g/h \in \mathbb{F}_q(x)$ is total if and only if $\gcd(x^q - x, h) = 1$. This can be verified with $O(\mathsf{M}(n)\log(qn))$ operations in $\mathbb{F}_q$ via repeated squaring and the Knuth-Schönhage gcd algorithm for polynomials (Aho *et al.* 1974, Section 7.5).

Corollary 2.14 implies that PermFunction $\in \mathcal{NP}$ when $q \geq 16\,n^4$, since every exceptional function can be certified deterministically in time polynomial in $n \log q$. When $q < 16\,n^4$, PermFunction $\in \mathcal{P} \subseteq \mathcal{NP}$, since for each $a \in \mathbb{F}_q$, we can check if it has a unique preimage under f, i.e., if $\deg \gcd(x^q - x, g - a\,h) = 1$, using the same method as mentioned above. The total cost of this deterministic procedure is $O(q\mathsf{M}(n)\log(qn))$ or $O(q\mathsf{M}(n)\log n)$ operations in $\mathbb{F}_q$.

For a permutation function $f = g/h \in \mathbb{F}_q(x)$ of degree n and $a \in \mathbb{F}_q$, $f^{-1}(a)$ can be calculated with $O(\mathsf{M}(n)\log(qn))$ operations in $\mathbb{F}_q$, using that $x - b = \gcd(x^q - x, g - a\,h)$ if and only if $a = f(b)$.

3. Reduction to polynomial factorization

We have seen that every permutation function $f \in \mathbb{F}_q(x)$ of degree n has a certificate that is deterministically verifiable in time polynomial in $n \log q$. To find such a certificate when q is large, say, $q \geq 16\,n^4$, we need to factor the difference polynomial $f^* \in \mathbb{F}_q[x, y]$ of degree n^* for $n - 1 \leq n^* \leq 2\,(n-1)$, and check that each irreducible factor of f^* over $\mathbb{F}_q$ is not absolutely irreducible.

Although no polynomial-time deterministic algorithm is known for the bivariate polynomial factoring problem over $\mathbb{F}_q$, there are some efficient probabilistic algorithms in the literature. Chistov & Grigoryev (1982), Lenstra (1985), and von zur Gathen & Kaltofen (1985) design polynomial-time "Las Vegas" algorithms that either produce a correct complete factorization or report failure.

The latter paper presents an algorithm for factoring polynomials in $\mathbb{F}_q[x, y]$ of degree n, which uses $(n \log q)^{O(1)}$ operations in $\mathbb{F}_q$ and fails with probability at most 2^{-n}, and also shows that factoring bivariate polynomials over $\mathbb{F}_q$ of degree n is deterministic polynomial-time reducible to factoring univariate polynomials over $\mathbb{F}_q$ of degree at most n. Shparlinski (1993) gives a deterministic factoring algorithm using $O(n^{3.7} \log q)$ field operations for almost all bivariate polynomials over $\mathbb{F}_q$ of degree n.

The following theorem is immediate from the above discussion.

THEOREM 3.1. PermFunction *is deterministic polynomial-time reducible to the problem* PolyFactor *of factoring univariate polynomials over finite fields.*

REMARK 3.2. Although PolyFactor is usually considered to be a search problem, it can be formulated as a decision problem; it is debatable whether this is

a "natural decision problem". Here we only state this for a prime field $\mathbb{F}_p$, but the method can be easily generalized for any finite field.

Let $F_n = \{f \in \mathbb{F}_p[x] : \deg f \leq n\}$ and $Z_{p^{n+1}} = \{0, 1, \ldots, p^{n+1} - 1\}$. Then the p-adic representation of numbers yields a natural bijection τ between F_n and $Z_{p^{n+1}}$, given by

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \mapsto a_n p^n + a_{n-1} p^{n-1} + \cdots + a_1 p + a_0.$$

For $f, g \in F_n$, we say $f \leq g$ if and only if $\tau(f) \leq \tau(g)$, and define the decision problem

PolyFactor (f, g): Does f have a factor $\leq g$ over $\mathbb{F}_p$?

Clearly, PolyFactor $\in \mathcal{ZPP}$. Furthermore, PolyFactor is self-reducible: using PolyFactor as an oracle, we can completely factor a polynomial in $\mathbb{F}_p[x]$ via binary search in deterministic polynomial time.

Assuming the ERH, Evdokimov (1993) shows that PolyFactor can be solved deterministically in quasi-polynomial time, i.e., in $(n^{\log n} \log q)^{O(1)}$ field operations, for polynomials in $\mathbb{F}_q[x]$ of degree n. We thus obtain the following corollary.

COROLLARY 3.3. *Under the ERH, one can decide deterministically whether an arbitrary rational function in $\mathbb{F}_q(x)$ of degree n is a permutation function in time $(n^{\log n} \log q)^{O(1)}$.*

THEOREM 3.4. PermFunction *is in* $\mathcal{R}$.

PROOF. Given $f = g/h \in \mathbb{F}_q(x)$ with degree n as in Notation 2.1, we have the following probabilistic algorithm to test whether f is a permutation function.

1. If f is not total, then return No; otherwise, return Yes if f is a linear polynomial.
2. If $q < 16\,n^4$, then return Yes if and only if every $a \in \mathbb{F}_q$ has a unique preimage under f.
3. If $q \geq 16\,n^4$, then construct the difference polynomial of f and call von zur Gathen & Kaltofen's algorithm BivariateFactor with the input f^*.
4. If BivariateFactor reports failure, then return No; otherwise, let $f^* = f_1 f_2 \cdots f_k$ be the produced complete factorization, where $1 \leq k \leq 2(n-1)$ and $f_i \in \mathbb{F}_q[x, y]$ is irreducible over $\mathbb{F}_q$ for $1 \leq i \leq k$.

5. Check each f_i for absolute irreducibility using Kaltofen's deterministic test. Return Yes if each f_i is not absolutely irreducible, and No otherwise.

For the error analysis, we note that if f is not a permutation function, then the test returns No. This follows from Corollary 2.14 when $q \geq 16n^4$, or the fact that some $a \in \mathbb{F}_q$ does not have a unique preimage under f when $q < 16n^4$.

If f is a permutation function, then the test gives a wrong answer No only when BivariateFactor fails, which happens with probability at most $\epsilon = 2^{-\deg f^*} \leq 1/2$, since $\deg f^* \geq n - 1 \geq 1$. This shows that the test has a Yes-biased error probability at most ϵ.

As analyzed in Remark 2.15, Step 1 takes $O^{\sim}(n \log q)$ operations in $\mathbb{F}_q$; Step 2 takes place when $q < 16n^4$, using $O^{\sim}(n^5)$ operations in $\mathbb{F}_q$.

Steps 3, 4 and 5 take place when $q \geq 16n^4$. Constructing f^* uses $O(n^3)$ operations in $\mathbb{F}_q$. Factoring f^* by von zur Gathen & Kaltofen's algorithm takes $O^{\sim}(n^{13} \log^2 q)$ operations in $\mathbb{F}_q$. Testing each f_i for absolute irreducibility by the deterministic algorithm in Kaltofen (1985) seems to take $O^{\sim}(n^8 \log q)$ operations in $\mathbb{F}_q$.

The total cost of this test is clearly polynomial in the input size $n \log q$. □

Combining Theorem 3.4 with the co-$\mathcal{R}$ test for PermFunction in Ma & von zur Gathen (1993), we have the following result.

COROLLARY 3.5. PermFunction *is in* $\mathcal{ZPP}$.

We can design an error-free test for PermFunction running in expected polynomial time as follows: one alternates the $\mathcal{R}$ and co-$\mathcal{R}$ tests repeatedly until both tests report the same answer, which then must be the desired correct answer. The expected cost will be dominated by the running time of the much slower $\mathcal{R}$ test.

Alternatively, we can use the $\mathcal{R}$ test alone and reformulate it as follows: one repeats calling von zur Gathen & Kaltofen's BivariateFactor algorithm in Step 4 until a complete factorization of f^* is produced, and then takes whatever answer returned in Step 5. The resulting test will be error-free running in expected polynomial time.

COROLLARY 3.6. *For any rational function in* $\mathbb{F}_q(x)$ *of degree* n, *one can decide if it is a permutation function in expected time* $(n \log q)^{O(1)}$.

4. A deterministic test

Let $\mathbb{F}_q$ be a finite field with characteristic p. If p is small, e.g., $p = n^{O(1)}$, then it is well-known that any polynomial in $\mathbb{F}_q[x]$ of degree n can be factored in deterministic polynomial time. In that case, we obtain a polynomial-time deterministic test for PermFunction by Theorem 3.1.

In this section, we develop a deterministic test in time sublinear in q for permutation functions of degree $n \leq p$ if q is sufficiently large, without resorting to polynomial factorizations over $\mathbb{F}_q$.

The basic technique used in our design of this test is the so-called "strip counting" method, which has been used in Shparlinski (1992b) for recognizing permutation polynomials, and in von zur Gathen *et al.* (1993) for counting points on a curve. It relies on the general principle that the behavior of an algebraic curve in a wide enough strip reflects that of the entire curve.

If $f \in \mathbb{F}_q(x)$ is total, then by Proposition 2.3, f is a permutation function if and only if the curve $\mathcal{C}$ as in Notation 2.1 has no rational points off the diagonal, i.e., if $\mathcal{C}^* = \emptyset$. However, if $\mathcal{C}^* \neq \emptyset$, then the strip counting method implies that $\mathcal{C}$ has a rational point off the diagonal in some wide enough strip.

More formally, let

$$\mathcal{C}^*(D) = \mathcal{C}^* \cap (D \times \mathbb{F}_q) \tag{4.1}$$

denote the set of rational points of $\mathcal{C}$ off the diagonal in the strip over $D \subseteq \mathbb{F}_q$. Clearly, $\mathcal{C}^*(\mathbb{F}_q) = \mathcal{C}^*$, but we are interested in finding a $D \subseteq \mathbb{F}_q$ of size $o(q)$, so that $\mathcal{C}^* = \emptyset$ if and only if $\mathcal{C}^*(D) = \emptyset$.

Suppose that $p = \operatorname{char} \mathbb{F}_q$, $q = p^l$, and that

$$\mathbb{F}_q = \mathbb{F}_p[x]/(\omega) = \left\{ \sum_{0 \leq i < l} a_i x^i \bmod \omega : a_i \in \mathbb{F}_p \right\}$$

is represented by some monic irreducible polynomial $\omega \in \mathbb{F}_p[x]$ of degree l. For any $N \in \mathbb{N}$ with $2 \leq N \leq q$, the following inequalities uniquely determine $k, h \in \mathbb{N}$ with $1 \leq k \leq l$ and $2 \leq h \leq p$:

$$p^{k-1} < N \leq p^k, \quad (h-1)p^{k-1} < N \leq h p^{k-1}.$$

Now define a subset $B \subseteq \mathbb{F}_q$, called the *box of order* N, as follows:

$$B = \left\{ \sum_{0 \leq i < k} a_i x^i \bmod \omega : a_1, \ldots, a_{k-1} \in \mathbb{F}_p,\ 0 \leq a_0 < h \right\}. \tag{4.2}$$

Clearly, we have $N \le \#B = h\,p^{k-1} < 2N$, and $\mathbb{F}_q$ is the box of order q. Furthermore, let $D = \{a - b : a, b \in B\}$ denote the *difference set* of the box B. It is evident that $\#B \le \#D \le 2\#B$.

LEMMA 4.1. *Let $p = \operatorname{char} \mathbb{F}_q$, $\varphi \in \mathbb{F}_q[x, y]$ be absolutely irreducible with degree m, $\mathcal{V} = \{(a, b) \in \mathbb{F}_q^2 : \varphi(a, b) = 0,\ a \ne b\}$, and assume that $0 < \deg_y \varphi < p$ and $x - y \nmid \varphi$. If $q \ge 4(m+1)^4$, $N \in \mathbb{N}$ with $N \ge 2m^2 q^{1/2} + 2m$, and D is the difference set of the box B of order N as in (4.2), then $\mathcal{V}(D) \ne \emptyset$.*

PROOF. Let K be an algebraic closure of $\mathbb{F}_q$, $\mathcal{C} = \{(a, b) \in K^2 : \varphi(a, b) = 0\}$ the plane curve defined by φ, $\mathcal{X} = \mathcal{C} \cap \mathbb{F}_q^2$ its rational points, $r = \#\mathcal{X}$, and $v = \#\mathcal{X}(D)$ be the number of rational points of $\mathcal{C}$ in the strip over D. Since $x - y$ does not divide φ, $\varphi(x, x) \in \mathbb{F}_q[x]$ is a non-zero polynomial of degree at most m, and hence $\#\mathcal{V}(D) \ge v - m$.

Let $s = \#B$, $T : \mathbb{F}_q \to \mathbb{F}_p$ be the absolute trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$, and $\chi(\lambda) = \exp(2\pi i T(\lambda)/p)$ the canonical additive character on $\mathbb{F}_q$. Using the well-known identity

$$\frac{1}{q} \sum_{\lambda \in \mathbb{F}_q} \chi(\lambda a) = \begin{cases} 1 & \text{if } a = 0, \\ 0 & \text{if } a \in \mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\} \end{cases}$$

(see, e.g., Shparlinski 1992a, Theorem G, p. 5), and noting that for each $d \in D$, there are at most s different ways to write $d = a - b$ with $a, b \in B$, we have

$$s\,v \ge t = \frac{1}{q} \sum_{\lambda \in \mathbb{F}_q} \sum_{(x,y) \in \mathcal{X}} \sum_{a,b \in B} \chi(\lambda[x - (a - b)]). \tag{4.3}$$

Separating the terms corresponding to $\lambda = 0$ and rearranging the sum in (4.3), we get

$$t - rs^2/q = \frac{1}{q} \sum_{\lambda \in \mathbb{F}_q^\times} \sum_{(x,y) \in \mathcal{X}} \chi(\lambda x) \sum_{a,b \in B} \chi(\lambda(b - a)).$$

Since $0 < \deg_y \varphi < p$, Lemma 4 from Bombieri & Davenport (1966) says that we can apply Bombieri's (1966, Theorem 6) bound on exponential sums along a curve:

$$\left| \sum_{(x,y) \in \mathcal{X}} \chi(\lambda x) \right| \le (m^2 - m) q^{1/2} + m^2.$$

Since $q \ge m^2$, we have $(m^2 - m)q^{1/2} + m^2 \le m^2 q^{1/2}$, and the following bound

$$
\begin{aligned}
|t - rs^2/q| &\le m^2 q^{-1/2} \sum_{\lambda \in \mathbb{F}_q^\times} \left| \sum_{a,b \in B} \chi(\lambda(b-a)) \right| \le m^2 q^{-1/2} \sum_{\lambda \in \mathbb{F}_q} \left| \sum_{a,b \in B} \chi(\lambda(b-a)) \right| \\
&= m^2 q^{-1/2} \sum_{\lambda \in \mathbb{F}_q} \left| \sum_{b \in B} \chi(\lambda b) \right| \left| \sum_{b \in B} \chi(-\lambda b) \right| = m^2 q^{-1/2} \sum_{\lambda \in \mathbb{F}_q} \left| \sum_{b \in B} \chi(\lambda b) \right|^2 \\
&= m^2 q^{-1/2} \sum_{\lambda \in \mathbb{F}_q} \sum_{b \in B} \chi(\lambda b) \sum_{b \in B} \chi(-\lambda b) = m^2 q^{-1/2} \sum_{\lambda \in \mathbb{F}_q} \sum_{a,b \in B} \chi(\lambda(a-b)) \\
&= m^2 q^{-1/2} \sum_{\lambda \in \mathbb{F}_q} \sum_{b \in B} 1 = m^2 q^{1/2} s.
\end{aligned}
$$

This shows that $t \ge rs^2/q - m^2 q^{1/2} s$, and $v \ge rs/q - m^2 q^{1/2}$ by (4.3). Applying Weil's bound $r \ge q - m^2 q^{1/2}$ (Fried & Jarden 1986, Theorem 4.9; Bach), we obtain $v \ge (1 - m^2 q^{-1/2})\, s - m^2 q^{1/2}$.

Since $q \ge 4\,(m+1)^4$, we have $1 - m^2 q^{-1/2} > 1/2$, and $s \ge N \ge 2\,m^2\, q^{1/2} + 2\,m$ implies that

$$
\#\mathcal{V}(D) \ge v - m \ge (1 - m^2 q^{-1/2})\, s - m^2 q^{1/2} - m > 0. \quad \square
$$

THEOREM 4.2. *Let $q \ge 64\,n^4$, $N \in \mathbb{N}$ with $N \ge 8\,(n-1)^2\, q^{1/2} + 4\,n$, $f \in \mathbb{F}_q(x)$ be total, $\mathcal{C}^*$ and $n \le \operatorname{char} \mathbb{F}_q$ as in Notation 2.1, and D be the difference set of the box of order N as in (4.2). Then f is a permutation function if and only if $\mathcal{C}^*(D) = \emptyset$.*

PROOF. If $f = g/h$ is a permutation function, then $\mathcal{C}^* = \emptyset$ by Proposition 2.3, and hence $\mathcal{C}^*(D) = \emptyset$ by (4.1).

By Proposition 2.7, we have $x - y \nmid f^*$, $\deg_y f^* \le n - 1$, and $\deg f^* \le 2\,(n-1)$. If f is not a permutation function, then f is not exceptional by Fact 2.11 (i). Therefore, f^* has an absolutely irreducible factor $\varphi \in \mathbb{F}_q[x, y]$ such that $x - y \nmid \varphi$, $\deg_y \varphi \le n - 1 < \operatorname{char} \mathbb{F}_q$, and $m = \deg \varphi \le 2\,(n-1)$.

We claim that $\deg_y \varphi > 0$, since otherwise φ has the form $\varphi = ax + b \in \mathbb{F}_q[x]$ with $a, b \in \mathbb{F}_q$ and $a \ne 0$. For $c = -b/a \in \mathbb{F}_q$, this implies that

$$
f^*(c, y) = g(c)h(y) - h(c)g(y) = 0;
$$

this is impossible because $\gcd(g, h) = 1$.

Since $q \ge 64\,n^4 > 4\,(m+1)^4$ and $N \ge 8\,(n-1)^2\, q^{1/2} + 4\,n > 2\,m^2\, q^{1/2} + 2\,m$, Lemma 4.1 implies that $\mathcal{V}(D) \ne \emptyset$, and hence $\mathcal{C}^*(D) \ne \emptyset$. $\square$

A DETERMINISTIC TEST FOR PERMUTATION FUNCTIONS.
Input: $f = g/h \in \mathbb{F}_q(x)$ as in Notation 2.1 and $n \le \operatorname{char} \mathbb{F}_q$.

Answer: Yes or No.

1. If f is not total, then return No; otherwise, return Yes if f is a linear polynomial.
2. If $q < 64\,n^4$, then return Yes if and only if every $a \in \mathbb{F}_q$ has a unique preimage under f.
3. If $q \geq 64\,n^4$, then let $D \subseteq \mathbb{F}_q$ be the difference set of the box of order $N = \lceil 8\,(n-1)^2\,q^{1/2} \rceil + 4\,n$ as in (4.2).
4. Return Yes if and only if for every $d \in D$, we have

$$\gcd(x^q - x, g - f(d)\,h) = x - d.$$

THEOREM 4.3. *The algorithm tests deterministically if $f \in \mathbb{F}_q(x)$ of degree $n \leq \operatorname{char} \mathbb{F}_q$ is a permutation function. It uses $O(q\mathsf{M}(n)\log n)$ operations in $\mathbb{F}_q$ if $q < 64\,n^4$, and $O(q^{1/2}n^2\mathsf{M}(n)\log q)$ operations if $q \geq 64\,n^4$.*

PROOF. The correctness of the test follows from Theorem 4.2.

As analyzed in Remark 2.15, Step 1 takes $O(\mathsf{M}(n)\log(qn))$ operations in $\mathbb{F}_q$; Step 2 takes place when $q < 64\,n^4$, using $O(q\mathsf{M}(n)\log n)$ operations in $\mathbb{F}_q$.

Steps 3 and 4 take place when $q \geq 64\,n^4$. For each $d \in D$, evaluating f at d takes $O(n)$ operations in $\mathbb{F}_q$ and calculating $\gcd(x^q - x, g - f(d)\,h)$ uses $O(\mathsf{M}(n)\log q)$ operations.

The total cost is thus $O(q\mathsf{M}(n)\log n)$ or $O\tilde{}(n^5)$ operations in $\mathbb{F}_q$ if $q < 64\,n^4$, and $O(q^{1/2}n^2\mathsf{M}(n)\log q)$ or $O\tilde{}(n^3\,q^{1/2})$ operations if $q \geq 64\,n^4$. □

5. A simple probabilistic test

In this section we design a new co-$\mathcal{R}$ test for permutation functions. Although the technical details of this test differ from the previous test in Ma & von zur Gathen (1993), both tests rely on the following principle: if $f \in \mathbb{F}_q(x)$ is not a permutation function, then there are plenty of "witnesses" to this non-bijectivity; using random choices, one can quickly find such a witness and thus prove that f is not a permutation function. What essentially distinguishes the two tests, however, is their choice of witnesses.

The new test uses the following criterion for permutation functions: f is a permutation function if and only if every element in $\mathbb{F}_q$ has a unique preimage under f. Therefore the witnesses to a non-permutation function f are those

field elements that are either non-images of f, or that have multiple preimages under f. By Theorem 2.13 (iii), if f has degree n and $q \geq 64\,n^4$, then the number of such witnesses in $\mathbb{F}_q$ is greater than $q/2n$. The probability that a randomly chosen element in $\mathbb{F}_q$ is a witness is thus greater than $1/2n$.

In Ma & von zur Gathen (1993), a novel criterion for permutation functions is designed, so that a significantly larger number of witnesses can testify the non-bijectivity. More specifically, a field extension $\mathbb{F}_{q^m} \supset \mathbb{F}_q$ with $m \geq 2$ is used in that test, and witnesses to a non-permutation function of degree n come from a subset of $\mathbb{F}_{q^m}$ with at least $q^m - q$ elements, for any n and q. Consequently, the probability that a randomly chosen element in $\mathbb{F}_{q^m}$ is a witness is at least $1 - q^{1-m} \geq 1/2$, and it is almost one when q or m is large enough.

A SIMPLE TEST FOR PERMUTATION FUNCTIONS.
Input: $f = g/h \in \mathbb{F}_q(x)$ with n as in Notation 2.1, and $\epsilon > 0$.

Answer: Yes or No.

1. If f is not total, then return No; otherwise, return Yes if f is a linear polynomial.

2. If $q < 64\,n^4$, then return Yes if and only if every $a \in \mathbb{F}_q$ has a unique preimage under f.

3. If $q \geq 64\,n^4$, then repeat $k = \lceil 2n \ln \epsilon^{-1} \rceil$ times:

   Randomly and uniformly choose $a \in \mathbb{F}_q$, and compute $u = \gcd(x^q - x, g - a\,h)$. If $\deg u \neq 1$, then stop and return No.

4. Return Yes.

THEOREM 5.1. *If $q < 64\,n^4$, the test is deterministic and uses $O(q\mathsf{M}(n) \log n)$ operations in $\mathbb{F}_q$. If $q \geq 64\,n^4$, the test is probabilistic with a* No*-biased error probability at most ϵ, so that if f is a permutation function, the answer is* Yes*; if f is not, the answer is* No *with probability at least $1 - \epsilon$. The probabilistic test is performed with $k = \lceil 2n \ln \epsilon^{-1} \rceil$ random choices and $O(n\mathsf{M}(n) \log q \log \epsilon^{-1})$ operations in $\mathbb{F}_q$.*

PROOF. If f is a permutation function, then the test returns Yes, since every element in $\mathbb{F}_q$ has a unique preimage under f.

If f is not a permutation function, however, the test may give a wrong answer Yes in Step 4, after having failed to find a single witness (to the non-bijectivity) among the k randomly chosen field elements. By Theorem 2.13

(iii), this happens with probability at most

$$\left(1-\frac{1}{2n}\right)^k = \left(\left(1-\frac{1}{2n}\right)^{2n}\right)^{k/2n} < (e^{-1})^{k/2n} \leq \epsilon.$$

As analyzed in Remark 2.15, Step 1 takes $O(\mathsf{M}(n)\log(qn))$ operations in $\mathbb{F}_q$; Step 2 takes place when $q < 64\,n^4$, using $O(q\mathsf{M}(n)\log n)$ operations in $\mathbb{F}_q$. Step 3 takes place when $q \geq 64\,n^4$ and uses $O(k\mathsf{M}(n)\log q)$ operations.

The total cost is thus $O(q\mathsf{M}(n)\log n)$ or $O^{\sim}(n^5)$ operations if $q < 64\,n^4$, and $O(n\mathsf{M}(n)\log q \log \epsilon^{-1})$ or $O^{\sim}(n^2 \log q \log \epsilon^{-1})$ operations if $q \geq 64\,n^4$. □

REMARK 5.2. This test extends the "naive" test for permutation polynomials in von zur Gathen (1991b).

For the special case of polynomials, Wan (1993) shows that if $f \in \mathbb{F}_q[x]$ has degree n and is not a permutation polynomial, then the number of non-images of f in $\mathbb{F}_q$ is at least $(q-1)/n$, for any n and q. This implies that the probability that a randomly chosen element in $\mathbb{F}_q$ is a witness (to a non-permutation polynomial) is at least $(1-1/q)/n \geq 1/2n$, for any n and q.

In view of this result, we can remove Steps 1 and 2 and also the restriction $q \geq 64\,n^4$ in Step 3 from the above test. The resulting test for permutation polynomials then works probabilistically with a No-biased error probability at most ϵ and uses $O^{\sim}(n^2 \log q \log \epsilon^{-1})$ operations in $\mathbb{F}_q$, for any n and q.

6. Conclusion

We have demonstrated that PermFunction $\in \mathcal{ZPP}$, and reduced it in deterministic polynomial time to the problem PolyFactor of factoring univariate polynomials over finite fields. Besides the problem Prime of recognizing prime numbers, it seems to be the only natural decision problem in $\mathcal{ZPP}$ unknown to be in $\mathcal{P}$.

For all of these three problems, the assumption of the ERH reduces the known upper bounds on their complexity: Prime $\in \mathcal{P}$ (Miller 1976), PolyFactor is solvable in deterministic quasi-polynomial time (Evdokimov 1993), and so is PermFunction (Corollary 3.3).

In view of these developments, it would be interesting to know whether under the ERH we can find a polynomial-time deterministic algorithm for PermFunction (or even for PolyFactor).

It is expected that our method would also work for partial permutation functions and bijective functions, namely, rational functions that need not be total and are a permutation and injective, respectively, on their domains of definition (Ma & von zur Gathen 1993). The central ingredient missing is an analogue of Cohen's theorem relating exceptional functions to permutation functions.

Acknowledgements

This research was supported by the Information Technology Research Centre and the Natural Sciences and Engineering Research Council of Canada. Parts of the second author's work were done during a sabbatical visit to the Institute for Scientific Computation at ETH Zürich, whose hospitality is gratefully acknowledged.

An Extended Abstract appeared in Proc. 26th Ann. ACM Symp. Theory of Computing, Montréal, Québec, 1994, 392-401.

References

LEONARD M. ADLEMAN AND MING-DEH HUANG, *Primality Testing and Abelian Varieties Over Finite Fields*, vol. 1512 of *Lecture Notes in Mathematics*. Springer-Verlag, 1992.

A. V. AHO, J. E. HOPCROFT, AND J. D. ULLMAN, *The Design and Analysis of Computer Algorithms*. Addison-Wesley, Reading MA, 1974.

E. BACH, Weil bounds for singular curves. *AAECC*, to appear.

S. BARNETT, *Polynomials and Linear Control Systems*, vol. 77 of *Monographs and Textbooks in Pure and Applied Mathematics*. Marcel Dekker, New York NY, 1983.

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.

D. G. CANTOR AND E. KALTOFEN, On fast multiplication of polynomials over arbitrary algebras. *Acta. Inform.* **28** (1991), 693–701.

A. L. CHISTOV AND D. YU. GRIGORYEV, Polynomial-time factoring of the multivariable polynomials over a global field. LOMI preprint E-5-82, Leningrad, USSR, 1982.

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

H. DAVENPORT AND D. J. LEWIS, Notes on congruences (I). *Quart. J. Math. Oxford* **14** (1963), 51–60.

S. A. EVDOKIMOV, Efficient factorization of polynomials over finite fields and the generalized Riemann hypothesis. Technical Report, Universität Bonn, 1993.

M. D. FRIED AND M. JARDEN, *Field Arithmetic.* Springer-Verlag, 1986.

J. VON ZUR GATHEN, Tests for permutation polynomials. *SIAM J. Comput.* **20** (1991a), 591–602.

J. VON ZUR GATHEN, Values of polynomials over finite fields. *Bull. Austral. Math. Soc.* **43** (1991b), 141–146.

J. VON ZUR GATHEN AND E. KALTOFEN, Factorization of multivariate polynomials over finite fields. *Math. Comp.* **45** (1985), 251–261.

J. VON ZUR GATHEN, M. KARPINSKI, AND I. E. SHPARLINSKI, Counting curves and their projections. In *Proc. 25th ACM Symp. Theory of Computing*, 1993, 805–812.

S. GOLDWASSER AND J. KILIAN, Almost all primes can be quickly certified. In *Proc. 18th Ann. ACM Symp. Theory of Computing*, Berkeley, CA, 1986, 316–329. See also: J. Kilian, *Uses of randomness in algorithms and protocols*, ACM Distinguished Doctoral Dissertation Series, MIT Press, Cambridge MA, 1990.

D. R. HAYES, A geometric approach to permutation polynomials over a finite field. *Duke Math. J.* **34** (1967), 293–305.

E. KALTOFEN, Fast parallel absolute irreducibility testing. *J. Symb. Computation* **1** (1985), 57–67.

E. KALTOFEN, Deterministic irreducibility testing of polynomials over large finite fields. *J. Symb. Comp.* **4** (1987), 77–82.

A. K. LENSTRA, Factoring multivariate polynomials over finite fields. *J. Comput. System Sci.* **30** (1985), 235–248.

R. LIDL AND G.L. MULLEN, When does a polynomial over a finite field permute the elements of the field? *Amer. Math. Monthly* **95** (1988), 243–246.

R. LIDL AND G.L. MULLEN, When does a polynomial over a finite field permute the elements of the field?, II. *Amer. Math. Monthly* **100** (1993), 71–74.

K. MA AND J. VON ZUR GATHEN, Counting value sets of functions and testing permutation functions. In *Abstracts of Int. Conf. Number Theoretic and Algebraic Methods in Computer Science*, Moscow, 1993, 62–65. Finite Fields and Their Applications **1** (1995), to appear.

C. R. MACCLUER, On a conjecture of Davenport and Lewis concerning exceptional polynomials. *Acta Arith.* **12** (1967), 289–299.

G. L. MILLER, Riemann's hypothesis and tests for primality. *J. Comput. System Sci.* **13** (1976), 300–317.

G. L. MULLEN, Permutation polynomials over finite fields. In *Proc. 1992 Conf. Finite Fields, Coding Theory, and Advances in Communications and Computing*, ed. G. L. MULLEN AND P. J.-S. SHIUE, vol. 141 of *Lecture Notes in Pure and Applied Mathematics*. Marcel Dekker, 1993, 131–151.

V. PRATT, Every prime has a succinct certificate. *SIAM J. of Comput.* (1975), 214–220.

M. O. RABIN, Probabilistic algorithms for testing primality. *J. of Number Theory* **12** (1980), 128–138.

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

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

I. E. SHPARLINSKI, A deterministic test for permutation polynomials. *Comput complexity* **2** (1992b), 129–132.

I. E. SHPARLINSKI, On bivariate polynomial factorization over finite fields. *Math. Comp.* **60** (1993), 787–791.

R. SOLOVAY AND V. STRASSEN, A fast Monte-Carlo test for primality. *SIAM J. Comput.* **6** (1977), 84–85. Erratum, in **7** (1978), 118.

D. WAN, A p-adic lifting lemma and its applications to permutation polynomials. In *Proc. 1992 Conf. Finite Fields, Coding Theory, and Advances in Communications and Computing*, ed. G. L. MULLEN AND P. J.-S. SHIUE, vol. 141 of *Lecture Notes in Pure and Applied Mathematics*. Marcel Dekker, 1993, 209–216.

K. S. WILLIAMS, On exceptional polynomials. *Canad. Math. Bull.* **11** (1968), 279–282.

Manuscript received 27 March 1994

KEJU MA
JOACHIM VON ZUR GATHEN
Department of Computer Science
University of Toronto
Toronto, Ontario M5S 1A4, Canada
{keju,gathen}@cs.toronto.edu

Second author's current address:
Fachbereich Mathematik-Informatik
Universität-GH Paderborn
D-33098 Paderborn, Germany
gathen@uni-paderborn.de