VALUES OF POLYNOMIALS
OVER FINITE FIELDS
JOACHIM VON ZUR GATHEN

Let \( q \) be a prime power, \( F_q \) a field with \( q \) elements, \( f \in F_q[z] \) a polynomial of degree \( n \geq 1 \), \( V(f) = \# f(F_q) \) the number of different values \( f(a) \) of \( f \), with \( a \in F_q \), and \( \rho = q - V(f) \). It is shown that either \( \rho = 0 \) or \( 4n^4 > q \) or \( 2\rho n > q \). Hence, if \( q \) is “large” and \( f \) is not a permutation polynomial, then either \( n \) or \( \rho \) is “large”.

Possible cryptographic applications have recently rekindled interest in permutation polynomials, for which \( \rho = 0 \) in the notation of the abstract (see Lidl and Mullen [10]). There is a probabilistic test for permutation polynomials using an essentially linear (in the input size \( n \log q \)) number of operations in \( F_q \) (von zur Gathen [5]). There are rather few permutation polynomials: a random polynomial in \( F_q[z] \) of degree less than \( q \) is a permutation polynomial with probability \( q! / q^q \), or about \( e^{-q} \). For cryptographic applications, we think of \( q \) as being exponential, about \( 2^N \), in some input size parameter \( N \); then this probability is doubly exponentially small: \( e^{-2^N} \).

In the hope of enlarging the pool of suitable polynomials, one can relax the notion of “permutation polynomial” by allowing a few, say polynomially many in \( N \), values of \( F_q \) not to be images of \( f: \rho = N^{O(1)} \). There is a probabilistic test for this property, whose expected number of operations is essentially linear in \( n\rho \log q \) (von zur Gathen [5]). The purpose of this note is to show that this relaxation does not include new examples with \( q \) large and \( n, \rho \) small: if \( \rho \neq 0 \), then either \( +4n^4 > q \) or \( 2\rho n > q \) (Corollary 2 (ii)).

The theorem below provides quantitative versions of results of Williams [15], Wan [14], and others, which we now first state. As an application, we will show that a naïve probabilistic polynomial-time test for permutation polynomials has a good chance of success; this could not be concluded from the previous less quantitative versions.

If \( p = \text{char} F_q \), then \( a \mapsto a^p \) is a bijection of \( F_q \). If \( f = g(x^p) \) for some \( g \in F_q[z] \), then \( V(f) = V(g) \), and, in particular, \( f \) is a permutation polynomial if and only if \( g \)
is. Replacing $f$ by $g$ (and repeating this process if necessary) we may therefore assume that $f$ is not a $p$th power, that is, that $f' \neq 0$. Then $f$ is called separable. We consider the difference polynomial

$$f^* = \frac{f(x) - f(y)}{x - y} \in \mathbb{F}_q[z, y],$$

and the number $\sigma$ of absolutely irreducible (that is, irreducible over an algebraic closure of $\mathbb{F}_q$) factors in a complete factorisation of $f^*$ into irreducible factors in $\mathbb{F}_q[x, y]$. We call $f$ exceptional if $\sigma = 0$. Any linear $f$ is exceptional.

**Facts.** Let $f \in \mathbb{F}_q[z]$ be separable of degree $n$.

(i) (MacCluer [12], Williams [16], Gwehenberger [7], Cohen [3]). If $f$ is exceptional, then $f$ is a permutation polynomial.

(ii) (Davenport and Lewis [4], Bombieri and Davenport [2], Tietäväinen [13], Hayes [8], Wan [14]). There exist $c_1, c_2, \ldots$ such that for any separable $f \in \mathbb{F}_q[z]$ of degree $n$ we have: If $q \geq c_n$ and $f$ is a permutation polynomial, then $f$ is exceptional.

(iii) (Williams [15]) If $q$ is a fixed prime, large compared with $n$, say $q \geq q_0(n)$, and $\rho = O(1)$ (that is, $\rho$ depends only on $n$, but not on $q$), then $f$ is exceptional (hence, by (i), a permutation polynomial).

(iv) (von zur Gathen and Kaltofen [6], and Kaltofen [9]) There is a probabilistic test whether $f$ is exceptional using a number of operations in $\mathbb{F}_q$ that is polynomial in $n \log q$.

We will establish quantitative versions of Facts (ii) and (iii). The proof follows the lines of Williams’ argument; a central ingredient is, as in Williams’ and Wan’s work, Weil’s theorem on the number of rational points of an algebraic curve over a finite field.

**Theorem 1.** Let $n \geq 1$, $f \in \mathbb{F}_q[z]$ separable of degree $n$, $V(f)$ the number of values of $f$, $\rho = q - V(f)$, and $0 < \varepsilon \leq 8$.

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

(ii) If $q \geq \varepsilon^{-2}n^4$ and $\sigma$ is the number of absolutely irreducible factors of $f^*$ in $\mathbb{F}_q[z, y]$, then $\rho > (\sigma - \varepsilon)q/n$.

**Proof:** Since any linear polynomial is a permutation polynomial and exceptional (that is, $\sigma = 0$), we may assume that $n \geq 2$. For $1 \leq i \leq n$, let

$$R_i = \{a \in \mathbb{F}_q : \#(f^{-1}(\{a\})) = i\}$$

be the set of points with exactly $i$ preimages under $f$, and $r_i = \#R_i$. Then $\bigcup_{1 \leq i \leq n} R_i = \{a \in \mathbb{F}_q : f^{-1}(a) \neq \emptyset\}$.

Downloaded from https://www.cambridge.org/core. IP address: 54.70.40.11, on 06 Mar 2019 at 21:52:29, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0004972700028860
$f(F_q)$ is a partition, and

\begin{align*}
(1) \quad \sum_{1 \leq i \leq n} r_i &= q - \rho, \\
(2) \quad \sum_{1 \leq i \leq n} ir_i &= q.
\end{align*}

Subtracting (1) from (2), we find

\begin{equation}
(3) \quad \sum_{2 \leq i \leq n} (i - 1)r_i = \rho.
\end{equation}

Let

\[ S = \{(a, b) \in F_q^2 : a \neq b, f(a) = f(b)\}, \]

and \( s = \#S \). We map every \((a, b) \in S\) to \( c = f(a) \in \bigcup_{2 \leq i \leq n} R_i \); every \( c \in R_i \) with \( i \geq 2 \) has exactly \( i(i-1) \) preimages under this map. Together with (3), this shows that

\begin{equation}
(4) \quad np \geq \sum_{2 \leq i \leq n} i(i-1)r_i = s.
\end{equation}

We may assume that \( f \) is not exceptional, and it is sufficient to prove \( \rho > 0 \) if \( q \geq n^4 \) for (i), and \( \rho n > (\sigma - \varepsilon)q \) if \( q \geq \varepsilon^{-2}n^4 \) for (ii). We write \( f^* = h_1 \cdots h_\sigma h_{\sigma+1} \cdots h_\tau \), with \( h_1, \ldots, h_\tau \in F_q[x, y] \) irreducible, and \( h_i \) absolutely irreducible if and only if \( i \leq \sigma \). We have \( \sigma \geq 1 \).

Let \( K \) be an algebraic closure of \( F_q \), and for \( 1 \leq i \leq \tau \) let

\[ \overline{X}_i = \{(a, b) \in K^2 : h_i(a, b) = 0\} \]

be the curve defined by \( h_i \), \( X_i = \overline{X}_i \cap F_q^2 \) its rational points, \( n_i = \deg h_i \), and \( X = \bigcup_{1 \leq i \leq \tau} X_i \). We observe that \( f(x) - f(y) \) is squarefree, since for a factor \( h^2 \) one finds, by differentiating, that \( h \) divides \( \gcd(f'(x), f'(y)) = 1 \). In particular, \( x - y \) does not divide \( f^* \), and if \( \Delta \subseteq K^2 \) is the diagonal, then \( \overline{X}_i \neq \Delta \) for all \( i \). Then

\begin{equation}
(5) \quad n - 1 = \deg f^* \cdot \deg \Delta \geq \#(\overline{X} \cap \Delta) \geq \#(X \cap \Delta),
\end{equation}

by Bezout's theorem. Similarly,

\[ n_i n_j \geq \#(\overline{X}_i \cap \overline{X}_j) \geq \#(X_i \cap X_j) \]
for $1 \leq i < j \leq \tau$. Furthermore, by Weil's Theorem (see Lidl and Niederreiter [11, p.331]) we have
\[
\#X_i \geq q + 1 - \left( (n_i - 1)(n_i - 2)q^{1/2} + n_i^2 \right)
\]
for $1 \leq i \leq \sigma$. Together, we obtain
\[
(6) \quad \#X \geq \# \bigcup_{1 \leq i \leq \sigma} X_i \geq \sum_{1 \leq i \leq \sigma} \#X_i - \sum_{1 \leq i < j \leq \sigma} \#(X_i \cap X_j)
\]
\[
> \sigma q - \sum_{1 \leq i \leq \sigma} \left( (n_i - 1)(n_i - 2)q^{1/2} + n_i^2 \right) - \sum_{1 \leq i < j \leq \sigma} n_i n_j.
\]

The maximum value of $\sum_{1 \leq i \leq \sigma} (n_i - 1)(n_i - 2)$ with $\sum_{1 \leq i \leq \sigma} n_i \leq n - 1$ and $1 \leq n_1, \ldots, n_{\sigma}$ is achieved at $(n_1, \ldots, n_{\sigma}) = (n - \sigma, 1, \ldots, 1)$, where it equals $(n - \sigma - 1)(n - \sigma - 2) \leq (n - 2)(n - 3)$. Adding the terms $n_i^2$ into the last sum, we find again that $\sum_{1 \leq i < j \leq \sigma} n_i n_j$ reaches, under the given conditions, its maximum at the same $(n_1, \ldots, n_{\sigma})$. Its value there is $(n - \sigma)^2 + (\sigma - 1)(n - \sigma) + (\sigma - 1)\sigma/2$. This function achieves its maximum $(n - 1)^2$ at $\sigma = 1$.

Since $X \setminus (X \cap \Delta) \subseteq S$, we have from these estimates and (4), (5), and (6)
\[
(7) \quad n \rho \geq s \geq \#X - (n - 1)
\]
\[
> \sigma q - (n - 2)(n - 3)q^{1/2} - (n - 1)^2 - (n - 1).
\]

To prove (i), it is sufficient to have the right hand side of (7) nonnegative. This is clearly the case for $n \leq q^{1/4}$, since $\sigma \geq 1$. To prove (ii), we note that
\[
0 \geq u\left(-5\sqrt{\varepsilon} u^2 + (6 + \varepsilon) u - \sqrt{\varepsilon}\right) \text{ for } u \geq \delta = \frac{6 + \varepsilon + \sqrt{36 - 8\varepsilon + \varepsilon^2}}{10\sqrt{\varepsilon}}.
\]
Using this for $u = q^{1/4}$, assuming $q \geq \varepsilon^{-2} n^4$ (which implies $u \geq 2\varepsilon^{-1/2} \geq \delta$), and using (7), we have
\[
n \rho > \sigma q - ((n - 2)(n - 3)q^{1/2} + n(n - 1))
\]
\[
> \sigma q - (\varepsilon q + (\varepsilon q^{3/4} + 6q^{1/2} + \varepsilon^{1/2} - \sqrt{\varepsilon} q^{1/4}))
\]
\[
> (\sigma - \varepsilon) q.
\]

**COROLLARY 2.** Let $n \geq 1$, $f \in \mathbb{F}_q[x]$ separable of degree $n$, $V(f)$ the number of values of $f$, $\rho = q - V(f)$, and assume that $q \geq 4n^4$.

(i) If $\sigma$ is the number of absolutely irreducible factors of $f^*$ in $\mathbb{F}_q[x, y]$, then
\[
\rho > (\sigma - 1/2)q/n.
\]

(ii) If $\rho \leq q/2n$, then $f$ is a permutation polynomial.
PROOF: (i) Set $\epsilon = 1/2$ in (ii) of the Theorem. (ii) If $f$ is not a permutation polynomial, then it is not exceptional (Fact (i)); hence $\sigma \geq 1$ and $\rho > q/2n$ by (i).

In various statements (the numbering of which is indicated below) of Lidl and Niederreiter [11], we can replace "there exist $c_1, c_2, \ldots$ such that for all $q \geq c_n$" by "for all $q \geq n^4$"; we refer to their text for a complete bibliography.

**Corollary 3.** Let $n \in \mathbb{N}$, $n \geq 1$, $F_q$ a finite field with $q$ elements, and assume $q \geq n^4$.

(i) (Corollary 7.30) Suppose that $f \in F_q[x]$ is separable of degree $n$. Then $f$ is a permutation polynomial if and only if $f$ is exceptional.

(ii) (Theorem 7.31) Suppose that $\gcd(n, q) = 1$ and $F_q$ contains an $n$th root of unity, different from 1. Then there is no permutation polynomial of $F_q$ with degree $n$.

(iii) (Corollary 7.32) Suppose that $n$ is positive and even, and $\gcd(n, q) = 1$. Then there is no permutation polynomial of $F_q$ with degree $n$.

(iv) (Corollary 7.33) Suppose that $\gcd(n, q) = 1$. Then there exists a permutation polynomial of $F_q$ with degree $n$ if and only if $\gcd(n, q - 1) = 1$.

We obtain a probabilistic polynomial-time algorithm to test whether a given polynomial $f \in F_q[x]$ of degree $n$ is a permutation polynomial, as follows. We first note that any $u \in F_q$ has exactly one preimage under $f$ (that is, $\#f^{-1}(\{u\}) = 1$) if and only if $\gcd(x^n - x, f - u)$ is linear. Calculating $x^n - x \mod f - u$ by repeated squaring takes $O^*(n \log q)$ operations, and the gcd calculation then $O^*(n)$ operations in $F_q$ (Aho, Hopcroft and Ullman [1, Section 8.9]). (The "soft $O$" notation $O^*(m)$ means $O(m \log^k m)$ for some fixed $k$, thus ignoring factors $\log m$.) If $q < 4n^4$, we test for each $u \in F_q$ whether it has one (or at least one) preimage under $f$. This costs $O^*(nq)$ or $O^*(n^5)$ operations in $F_q$.

If $q \geq 4n^4$, we have the following probabilistic algorithm, with a confidence parameter $\epsilon > 0$ as further input. We choose $k = \lceil 2n \log_q^{-1} \rceil$ elements $u \in F_q$ independently at random, and test whether $u$ has exactly one preimage under $f$. If this is not the case for some $u$, then $f$ is not a permutation polynomial. If it is true for all $u$ tested, then we declare $f$ to be a permutation polynomial. It may of course happen that $f$ is not a permutation polynomial and this test answers incorrectly; the probability of this event is at most

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

by Corollary 2 (ii). The cost is $k \gcd$'s or $O^*(n \log e^{-1} \cdot n \log q)$ operations in $F_q$.

This test is conceptually much simpler than the one in von zur Gathen [5]; however, that test is more efficient, using only $O^*(n \log e^{-1})$ operations (if $\epsilon \leq q^{-1}$).
REFERENCES