BULL. AUSTRAL. MATH. SOC. 11T06, 11G20, 68Q40
VOL. 43 (1991) [141–146]

VALUES OF POLYNOMIALS OVER FINITE FIELDS

JOACHIM VON ZUR GATHEN

Let q be a prime power, $\mathbf{F}_q$ a field with q elements, $f \in \mathbf{F}_q[x]$ a polynomial of degree $n \geqslant 1$, $V(f) = \#f(\mathbf{F}_q)$ the number of different values $f(a)$ of f, with $a \in \mathbf{F}_q$, 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 ρ 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 $\mathbf{F}_q$ (von zur Gathen [5]). There are rather few permutation polynomials: a random polynomial in $\mathbf{F}_q[x]$ 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 $\mathbf{F}_q$ 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, ρ 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 $p = \operatorname{char} \mathbf{F}_q$, then $a \mapsto a^p$ is a bijection of $\mathbf{F}_q$. If $f = g(x^p)$ for some $g \in \mathbf{F}_q[x]$, then $V(f) = V(g)$, and, in particular, f is a permutation polynomial if and only if g

Received 16 March 1990
This work was partly supported by Natural Sciences and Engineering Research Council of Canada, grant A-2514.

Copyright Clearance Centre, Inc. Serial-fee code: 0004-9729/91 \$A2.00+0.00.

https://doi.org/10.1017/S0004972700028860 Published online by Cambridge University Press

is. Replacing f by g (and repeating this process if necessary) we may therefore assume that f is not a pth power, that is, that $f' \neq 0$. Then f is called *separable*. We consider the difference polynomial

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

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

FACTS. *Let $f \in \mathbf{F}_q[x]$ 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 $f \in \mathbf{F}_q[x]$ of degree n we have: If $q \geqslant c_n$ and f is a permutation polynomial, then f is exceptional.*

(iii) (Williams [**15**]) *If q is a fixed prime, large compared with n, say $q \geqslant q_0(n)$, and $\rho = O(1)$ (that is, ρ 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 $\mathbf{F}_q$ 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 $n \geqslant 1$, $f \in \mathbf{F}_q[x]$ separable of degree n, $V(f)$ the number of values of f, $\rho = q - V(f)$, and $0 < \varepsilon \leqslant 8$.*

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

(ii) *If $q \geqslant \varepsilon^{-2} n^4$ and σ is the number of absolutely irreducible factors of f^* in $\mathbf{F}_q[x, y]$, 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 $n \geqslant 2$. For $1 \leqslant i \leqslant n$, let

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

be the set of points with exactly i preimages under f, and $r_i = \#R_i$. Then $\bigcup_{1 \leqslant i \leqslant n} R_i =$

https://doi.org/10.1017/S0004972700028860 Published online by Cambridge University Press

$f(\mathbf{F}_q)$ is a partition, and

$$\sum_{1\leqslant i\leqslant n} r_i = q-\rho, \tag{1}$$

$$\sum_{1\leqslant i\leqslant n} ir_i = q. \tag{2}$$

Subtracting (1) from (2), we find

$$\sum_{2\leqslant i\leqslant n} (i-1)r_i = \rho. \tag{3}$$

Let

$$S = \{(a, b) \in \mathbf{F}_q^2 : a \neq b,\ f(a) = f(b)\},$$

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

$$n\rho \geqslant \sum_{2\leqslant i\leqslant n} i(i-1)r_i = s. \tag{4}$$

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

Let K be an algebraic closure of $\mathbf{F}_q$, and for $1 \leqslant i \leqslant \tau$ let

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

be the curve defined by h_i, $X_i = \overline{X}_i \cap \mathbf{F}_q^2$ its rational points, $n_i = \deg h_i$, and $X = \bigcup_{1\leqslant i\leqslant \tau} X_i$. 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

$$n - 1 = \deg f^* \cdot \deg \Delta \geqslant \#(\overline{X} \cap \Delta) \geqslant \#(X \cap \Delta), \tag{5}$$

by Bezout's theorem. Similarly,

$$n_i n_j \geqslant \#(\overline{X}_i \cap \overline{X}_j) \geqslant \#(X_i \cap X_j)$$

https://doi.org/10.1017/S0004972700028860 Published online by Cambridge University Press

for $1 \leqslant i < j \leqslant \tau$. Furthermore, by Weil's Theorem (see Lidl and Niederreiter [**11**, p.331]) we have

$$\#X_i \geqslant q + 1 - \left((n_i - 1)(n_i - 2)q^{1/2} + n_i^2\right)$$

for $1 \leqslant i \leqslant \sigma$. Together, we obtain

$$\begin{aligned} \#X &\geqslant \# \bigcup_{1 \leqslant i \leqslant \sigma} X_i \geqslant \sum_{1 \leqslant i \leqslant \sigma} \#X_i - \sum_{1 \leqslant i < j \leqslant \sigma} \#(X_i \cap X_j) \\ &> \sigma q - \sum_{1 \leqslant i \leqslant \sigma} \left((n_i - 1)(n_i - 2)q^{1/2} + n_i^2\right) - \sum_{1 \leqslant i < j \leqslant \sigma} n_i n_j. \end{aligned} \tag{6}$$

The maximum value of $\sum_{1 \leqslant i \leqslant \sigma} (n_i - 1)(n_i - 2)$ with $\sum_{1 \leqslant i \leqslant \sigma} n_i \leqslant n - 1$ and $1 \leqslant n_1, \ldots, n_\sigma$ is achieved at $(n_1, \ldots, n_\sigma) = (n - \sigma, 1, \ldots, 1)$, where it equals $(n - \sigma - 1)(n - \sigma - 2) \leqslant (n - 2)(n - 3)$. Adding the terms n_i^2 into the last sum, we find again that $\sum_{1 \leqslant i \leqslant j \leqslant \sigma} n_i n_j$ 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)

$$\begin{aligned} n\rho &\geqslant s \geqslant \#X - (n - 1) \\ &> \sigma q - (n - 2)(n - 3)q^{1/2} - (n - 1)^2 - (n - 1). \end{aligned} \tag{7}$$

To prove (i), it is sufficient to have the right hand side of (7) nonnegative. This is clearly the case for $n \leqslant q^{1/4}$, since $\sigma \geqslant 1$. To prove (ii), we note that

$$0 \geqslant u(-5\sqrt{\varepsilon}u^2 + (6 + \varepsilon)u - \sqrt{\varepsilon}) \text{ for } u \geqslant \delta = \frac{6 + \varepsilon + \sqrt{36 - 8\varepsilon + \varepsilon^2}}{10\sqrt{\varepsilon}}.$$

Using this for $u = q^{1/4}$, assuming $q \geqslant \varepsilon^{-2}n^4$ (which implies $u \geqslant 2\varepsilon^{-1/2} \geqslant \delta$), and using (7), we have

$$\begin{aligned} n\rho &> \sigma q - \left((n - 2)(n - 3)q^{1/2} + n(n - 1)\right) \\ &\geqslant \sigma q - \left(\varepsilon q + \left(-5\sqrt{\varepsilon}q^{3/4} + 6q^{1/2} + \varepsilon q^{1/2} - \sqrt{\varepsilon}q^{1/4}\right)\right) \\ &\geqslant (\sigma - \varepsilon)q. \end{aligned}$$

∎

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

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

(ii) *If $\rho \leqslant q/2n$, then f is a permutation polynomial.*

https://doi.org/10.1017/S0004972700028860 Published online by Cambridge University Press

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

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 $q \geqslant c_n$" by "for all $q \geqslant n^4$"; we refer to their text for a complete bibliography.

COROLLARY 3. *Let $n \in \mathbb{N}$, $n \geqslant 1$, $\mathbf{F}_q$ a finite field with q elements, and assume $q \geqslant n^4$.*

(i) (Corollary 7.30) *Suppose that $f \in \mathbf{F}_q[x]$ 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 $\mathbf{F}_q$ contains an nth root of unity, different from 1. Then there is no permutation polynomial of $\mathbf{F}_q$ 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 $\mathbf{F}_q$ with degree n.*

(iv) (Corollary 7.33) *Suppose that* $\gcd(n, q) = 1$. *Then there exists a permutation polynomial of $\mathbf{F}_q$ 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 $f \in \mathbf{F}_q[x]$ of degree n is a permutation polynomial, as follows. We first note that any $u \in \mathbf{F}_q$ has exactly one preimage under f (that is, $\#f^{-1}(\{u\}) = 1$) if and only if $\gcd(x^q - x, f - u)$ is linear. Calculating $x^q - x \mod f - u$ by repeated squaring takes $O^\sim(n \log q)$ operations, and the gcd calculation then $O^\sim(n)$ operations in $\mathbf{F}_q$ (Aho, Hopcroft and Ullman [**1**, Section 8.9]). (The "soft O" notation $O^\sim(m)$ means $O\left(m \log^k m\right)$ for some fixed k, thus ignoring factors $\log m$.) If $q < 4n^4$, we test for each $u \in \mathbf{F}_q$ whether it has one (or at least one) preimage under f. This costs $O^\sim(nq)$ or $O^\sim\left(n^5\right)$ operations in $\mathbf{F}_q$.

If $q \geqslant 4n^4$, we have the following probabilistic algorithm, with a confidence parameter $\varepsilon > 0$ as further input. We choose $k = \lceil 2n \log_e \varepsilon^{-1} \rceil$ elements $u \in \mathbf{F}_q$ 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

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

by Corollary 2 (ii). The cost is k gcd's or $O^\sim\left(n \log \varepsilon^{-1} \cdot n \log q\right)$ operations in $\mathbf{F}_q$.

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

https://doi.org/10.1017/S0004972700028860 Published online by Cambridge University Press

References

[1] A.V. Aho, J.E. Hopcroft and J.D. Ullman, *The design and analysis of computer algorithms* (Addison-Wesley, Reading, MA, 1974).

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

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

[4] H. Davenport and D.J. Lewis, 'Notes on congruences (I)', *Quart. J. Math. Oxford* **14** (1963), 51–60.

[5] J. von zur Gathen, 'Tests for permutation polynomials', *SIAM J. Comput.* (to appear).

[6] J. von zur Gathen and E. Kaltofen, 'Factorization of multivariate polynomials over finite fields', *Math. Comp.* **45** (1985), 251–261.

[7] G. Gwehenberger, *Über die Darstellung von Permutationen durch Polynome und rationale Funktionen*, PhD thesis (TH Wien, 1970).

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

[9] E. Kaltofen, 'Fast parallel absolute irreducibility testing', *J Symbolic Comput.* **1** (1985), 57–67.

[10] 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.

[11] R. Lidl and H. Niederreiter, *Finite fields*: *Encyclopedia of Mathematics and its Applications* 20 (Addison–Wesley, Reading MA, 1983).

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

[13] A. Tietäväinen, 'On non-residues of a polynomial', *Ann. Univ. Turku Ser. A* **94** (1966).

[14] D. Wan, 'On a conjecture of Carlitz', *J. Austral. Math. Soc. (Series A)* **43** (1987), 375–384.

[15] K.S. Williams, 'On extremal polynomials', *Canad. Math. Bull.* **10** (1967), 585–594.

[16] K.S. Williams, 'On exceptional polynomials', *Canad. Math. Bull.* **11** (1968), 279–282.

Department of Computer Science
University of Toronto
Toronto, Ontario M5S 1A4
Canada

https://doi.org/10.1017/S0004972700028860 Published online by Cambridge University Press