WAN'S THEOREM

TREVOR HYDE

If R is an integral domain, $V \subseteq R$ is a finite multiset, and $f(x) \in R[x]$ is a polynomial, let $f(V)$ denote the image of f with multiplicity and V_f denote the number of distinct $v \in V$ such that $f(v) \in V$. Wan proved the following theorem in [11].

Theorem 1. *Let $V = \mathbb{F}_q$ be the field with q elements. Suppose $f(x) \in \mathbb{F}_q[x]$ is a polynomial of degree d. If f is not surjective, then*

$$V_f \leq q - \frac{q-1}{d}.$$

If the degree of $f(x)$ is larger than q, then Theorem 1 tells us nothing. However, if the degree of $f(x)$ is small with respect to q, then Theorem 1 says that either $f(x)$ is a permutation polynomial or it misses at least $\frac{q-1}{d}$ elements of $\mathbb{F}_q$. An arbitrary function $g : \mathbb{F}_q \to \mathbb{F}_q$ may be interpolated by a polynomial of degree at most $q-1$, which explains the vacuous conclusion in that case.

Surprisingly, the mechanism underlying Theorem 1 has nothing to do with finite fields. We illustrate this claim with the following generalization.

Theorem 2. *Let R be an integral domain and $g(x) = x^m + h(x) \in R[x]$ where $\deg h(x) = m - k$ for some $k \geq 1$. Let V be the multiset of roots of $g(x)$ in an algebraic closure $\overline{R}$. If $f(x) \in R[x]$ is a polynomial of degree d such that $f(0) = 0$, then either $f(V) = V$ or*

$$V_f \leq m - \frac{k}{d}.$$

To see how Theorem 2 generalizes Theorem 1, let $R = \mathbb{F}_q$ and $g(x) = x^q - x$. Hence $m = q$ and $k = q - 1$. Then $V = \mathbb{F}_q$ is the set of roots of $g(x)$. We may compose any $f(x) \in \mathbb{F}_q[x]$ with a linear function to achieve $f(0) = 0$ since linear polynomials induce permutations of $V = \mathbb{F}_q$. The conclusion of Theorem 2 asserts that either f is a bijection or f misses at least $\frac{k}{d} = \frac{q-1}{d}$ points. Thus, Theorem 1 is a special case of Theorem 2. The hypotheses of Theorem 2 depend awkwardly on the form of the polynomial $g(x)$. A more natural statement uses the language of symmetric functions. For any $n \geq 1$ let e_n be the *nth elementary symmetric function*, a formal power series in countably many variables $x_1, x_2, \ldots$ defined by

$$e_n = \sum_{i_1 < i_2 < \ldots < i_n} x_{i_1} x_{i_2} \cdots x_{i_n}.$$

Date: March 11th, 2016.

If R is a commutative ring and $V \subseteq R$ is any finite multiset, then $e_n(V) \in R$ is well-defined. The following is equivalent to Theorem 2.

Theorem 3. *Let R be an integral domain and $V \subseteq R$ be a finite multiset. Let k be the smallest positive integer so that $e_k(V) \neq 0$. If $f(x) \in R[x]$ is a polynomial of degree d such that $f(0) = 0$, then either $f(V) = V$ or*

$$V_f \leq \#V - \frac{k}{d}.$$

To see the equivalence between Theorem 2 and Theorem 3, let

$$g(x) = \prod_{a \in V} (x - a). \tag{1}$$

Then the assumption that k is minimal such that $e_k(V) \neq 0$ is the same as $g(x) = x^m + h(x)$ where $m = \#V$ and $\deg h(x) = m - k$. Theorem 3 highlights the importance of k as the subscript of the first non-vanishing elementary symmetric function $e_k(V)$.

All three theorems are special cases of a more general fact regarding the images of polynomials on highly symmetric sets.

Theorem 4. *Let R be an integral domain. Suppose $V, W \subseteq R$ are finite multisets with the same cardinality m and $f(x), g(x) \in R[x]$ have degree at most d such that $f(0) = g(0) = 0$. Let $I_{f,g}$ be the number of distinct elements in $f(V) \cap g(W)$. Suppose k is the smallest integer so that $e_k(V)e_k(W) \neq 0$. Then either $f(V) = g(W)$ or*

$$I_{f,g} \leq m - \frac{k}{d}.$$

Theorem 3 follows from Theorem 4 by setting $V = W$ and $g(x) = x$. These generalizations of Theorem 1 are due to my advisor Mike Zieve, and to the best of my knowledge do not appear elsewhere in print.

There are two steps to proving these results: the first is to determine the relationship between $e_n(V)$ and $e_n(f(V))$ for a polynomial $f(x)$ which we do in Lemma 5 below; the second is to write down a clever choice of polynomial which vanishes precisely on the set we are trying to count and use Lemma 5 to bound its degree.

Lemma 5. *Suppose R is a commutative ring and $V \subseteq R$ is a finite multiset. Let $f(x) \in R(x)$ be a degree at most d polynomial such that $f(0) = 0$. If $e_n(V) = 0$ for $n < k$, then $e_n(f(V)) = 0$ for $n < \frac{k}{d}$*

Proof. Suppose

$$F(x) = \sum_{i \geq 1} a_i x^i \in \mathbb{Z}[a_1, a_2, a_3, \ldots][[x]]$$

is a formal power series with indeterminate coefficients and no constant term. We compute

$$e_n\bigl(F(x_1), F(x_2), F(x_3), \dots\bigr) = \sum_{i_1<i_2<\dots<i_n} \prod_{j=1}^{n} F(x_{i_j}) = \sum_{\ell(\lambda)=n} a_\lambda m_\lambda,$$

where $\ell(\lambda)$ denotes the length of a partition, m_λ is the λth monomial symmetric function [9, Sec. 7.3] in $\{x_i : i \geq 1\}$, and $a_\lambda = \prod_{i=1}^{k} a_{\lambda_i}$. Note that we require $F(0) = 0$ for this formal composition to be well-defined. Given a partition μ of length $\ell(\mu) = n$, the symmetric function e_μ is defined by

$$e_\mu = \prod_{i=1}^{n} e_{\mu_i}.$$

The elementary symmetric functions $\{e_\mu\}$ form a homogeneous $\mathbb{Z}$-basis for the graded ring of symmetric functions [9, Thm. 7.4.4], so there exist integers $E_{\lambda\mu}$ such that

$$m_\lambda = \sum_{|\mu|=|\lambda|} E_{\lambda\mu} e_\mu.$$

Therefore we may write

$$e_n\bigl(F(x)\bigr) = \sum_{\ell(\lambda)=n} \sum_{|\mu|=|\lambda|} a_\lambda E_{\lambda\mu} e_\mu. \tag{2}$$

We specialize (2) by setting $F(x) = f(x)$ and substituting the elements of V for the symmetric variables x_i. Our assumption that $e_n(V) = 0$ for $n < k$ implies $e_\mu(V) = 0$ if μ has any part smaller than k, hence $e_\mu(V) \neq 0$ implies $|\mu| \geq k$. Our assumption that $f(x)$ has degree at most d implies $a_\lambda = 0$ if λ has any part larger than d, hence $a_\lambda \neq 0$ implies $|\lambda| \leq dn$. Together these give a necessary condition for $e_n\bigl(f(V)\bigr) \neq 0$:

$$dn \geq |\lambda| = |\mu| \geq k \implies n \geq \frac{k}{d}.$$

Therefore $n < \frac{k}{d}$ implies $e_n(f(V)) = 0$, as desired. □

We now prove Theorem 4.

Proof. Consider the polynomial

$$\Delta(x) = \prod_{v\in V} \bigl(x - f(v)\bigr) - \prod_{w \in W} \bigl(x - g(w)\bigr).$$

If $u \in f(V) \cap g(W)$, then $\Delta(u) = 0$. If $f(V) = g(W)$, then $\Delta(x) \equiv 0$. Otherwise, R being an integral domain implies $\deg \Delta(x)$ is an upper bound on the number of distinct roots, hence on $I_{f,g}$. Since $\#V = \#W = m$, we have $\deg \Delta(x) < m$. The coefficient of x^{m-n} in $\Delta(x)$ is $(-1)^n\bigl(e_n(f(V)) - e_n(g(W))\bigr)$. By Lemma 5, we conclude that $e_n(f(V)) = e_n(g(W)) = 0$ for $n < \frac{k}{d}$, hence the degree of $\Delta(x)$ is at most $m - \frac{k}{d}$. We conclude that $I_{f,g} \leq m - \frac{k}{d}$. □

The story behind Wan's theorem begins with a conjecture of Davenport and Lewis [3]. Let $f(x) \in \mathbb{F}_q[x]$ be a polynomial, then $f(x)$ is called *exceptional* if the only absolutely irreducible factors of $f(x) - f(y)$ in $\mathbb{F}_q[x, y]$ are associates of $(x - y)$. Davenport and Lewis observe that all permutation polynomials are exceptional for sufficiently large degree and conjecture the converse. Cohen [2] proved their conjecture using algebraic number theory. Williams [12] gives an elementary proof of Cohen's theorem when the characteristic of $\mathbb{F}_q$ is sufficiently large with respect to the degree d of $f(x)$. His proof proceeds by relating the power symmetric functions of the image $f(\mathbb{F}_q)$ to those of $\mathbb{F}_q$. The power symmetric functions do not form an integral basis for the ring of symmetric functions, hence his conditions are to avoid dividing by the characteristic. Decades later, Wan [11] circumvents this issue by p-adically lifting Williams argument to characteristic zero, proving Theorem 1 on the way to a complete proof of Cohen's theorem. If $s_n = \sum_i x_i^n$ is the nth power symmetric function, then both Williams and Wan focus on the fact that for $1 \leq n \leq q$,

$$s_n(\mathbb{F}_q) = \begin{cases} 0 & \text{if } n \neq q-1, \text{ and} \\ q-1 & \text{if } n = q-1, \end{cases} \tag{3}$$

Wan calls (3) the *orthogonality relations.* Newton's identities relating the elementary and power symmetric functions show that (3) follows immediately from the elements of $\mathbb{F}_q$ satisfying $x^q - x = 0$. Turnwald [10] uses elementary symmetric functions to prove Wan's theorem directly over a finite field without any characteristic zero lifts. Our proof of Theorem 3 is essentially his. Aitken [1] generalized Turnwald's results in another direction, considering sets V with other types of symmetry, but also proving a result similar to our Theorem 4 over finite fields.

Higher dimensional generalizations of Wan's theorem have recently been found [4–8, 13] for polynomial mappings of finite dimensional vector spaces over $\mathbb{F}_q$. It seems likely that they too will hold in greater generality for polynomial mappings of "sufficiently symmetric" sets.

References

[1] Wayne Aitken. On value sets of polynomials over a finite field. *Finite Fields Appl.*, 4(4):441–449, 1998.

[2] Stephen D. Cohen. The distribution of polynomials over finite fields. *Acta Arith.*, 17:255–271, 1970.

[3] H. Davenport and D. J. Lewis. Notes on congruences. I. *Quart. J. Math. Oxford Ser. (2)*, 14:51–60, 1963.

[4] Zhicheng Gao and Qiang Wang. A probabilistic approach to value sets of polynomials over finite fields. *Finite Fields and Their Applications*, 33:160 – 174, 2015.

[5] Michiel Kosters. Polynomial maps on vector spaces over a finite field. *Finite Fields and Their Applications*, 31:1 – 7, 2015.

[6] Gary L. Mullen, Daqing Wan, and Qiang Wang. Value sets of polynomial maps over finite fields. *Q. J. Math.*, 64(4):1191–1196, 2013.

[7] Gary L. Mullen, Daqing Wan, and Qiang Wang. Index bounds for value sets of polynomials over finite fields. In *Applied algebra and number theory*, pages 280–296. Cambridge Univ. Press, Cambridge, 2014.

[8] Luke Smith. Polytope bounds on multivariate value sets. *Finite Fields Appl.*, 28:132–139, 2014.

[9] R.P. Stanley. *Enumerative Combinatorics: Volume 2*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2001.

[10] Gerhard Turnwald. A new criterion for permutation polynomials. *Finite Fields Appl.*, 1(1):64–82, 1995.

[11] Daqing Wan. A p-adic lifting lemma and its application to permutation polynomials. *Recall*, 1:1, 1993.

[12] Kenneth S. Williams. On exceptional polynomials. *Canad. Math. Bull.*, 11:279–282, 1968.

[13] Haixia Zan and Wei Cao. Powers of polynomials and bounds of value sets. *J. Number Theory*, 143:286–292, 2014.

Dept. of Mathematics, University of Michigan, Ann Arbor, MI 48109-1043,
E-mail address: `tghyde@umich.edu`