Turnwald's proof of Wan's value set bound

Peter Müller

November 23, 2017

Theorem 1 (Wan [Wan93]). *Let $f \in \mathbb{F}_q[X]$ be a non-constant polynomial which is not bijective on $\mathbb{F}_q$. Then $|f(\mathbb{F}_q)| \leq q - \frac{q-1}{\deg f}$.*

In [Tur95] Turnwald gave an elementary proof of Wan's theorem which avoided his use of p-adic lifting techniques. The following is an even further simplification which grew out from a discussion with Mike Zieve.

Lemma 2. *Let $F(X_1, \dots, X_q)$ be a homogeneous and symmetric polynomial of degree r where $1 \leq r \leq q-2$. Then $F(a_1, \dots, a_q) = 0$, where the a_i are distinct elements from $\mathbb{F}_q$.*

Proof. Pick $0 \neq b \in \mathbb{F}_q$. Then $ba_1, \dots, ba_q$ is a permutation of $a_1, \dots, a_q$, so $F(a_1, \dots, a_q) = F(ba_1, \dots, ba_q)$ by the symmetry of F. Furthermore, $F(ba_1, \dots, ba_q) = b^r F(a_1, \dots, a_q)$, as F is homogeneous of degree r. Thus $(1 - b^r)F(a_1, \dots, a_q) = 0$. The polynomial $X^r - 1$ has at most $r \leq q-2$ roots in $\mathbb{F}_q$, therefore there is a nonzero $b \in \mathbb{F}_q$ such that $1 - b^r \neq 0$. Then $F(a_1, \dots, a_q) = 0$. □

Lemma 3. *Let $F(X_1, \dots, X_q)$ be a symmetric polynomial of degree $\leq q-2$. Then $F(a_1, \dots, a_q) = F(0, \dots, 0)$, where the a_i are distinct elements from $\mathbb{F}_q$.*

Proof. Write F as a sum of its homogeneous components (which are symmetric too), and apply the previous lemma. □

Upon replacing $f(X)$ with $f(X) - f(0)$ we may and do assume that $f(0) = 0$.

Let T be another variable, and set

$$G(T, X_1, \dots, X_q) = \prod_{i=1}^{q}(T - f(X_i)) - \prod_{i=1}^{q}(T - X_i).$$

Note that the T-degree of G is at most $q-1$. For $0 \le j \le q-1$ let F_j be the coefficient of T^j in $G(T, X_1, \dots, X_q)$. Then $F_j \in \mathbb{F}_q[X_1, \dots, X_q]$ is symmetric in $X_1, \dots, X_q$ and has degree at most $(q-j)\deg f$. Thus $\deg F_j < q-1$ for $j > q - \frac{q-1}{\deg f}$. Note that $G(T, 0, \dots, 0) = T^q - T^q = 0$, so $F_j(0, \dots, 0) = 0$ for all j. Again let $a_1, \dots, a_q$ be the elements from $\mathbb{F}_q$. The previous lemma then shows that $F_j(a_1, \dots, a_q) = 0$ for all $j > q - \frac{q-1}{\deg f}$. Thus $G(T, a_1, \dots, a_q)$ hat degree at most $q - \frac{q-1}{\deg f}$.

By construction, every element in $f(\mathbb{F}_q)$ is a root of $G(T, a_1, \dots, a_q)$. The assertion follows unless $G(T, a_1, \dots, a_q) = 0$. But then $\prod_{a\in\mathbb{F}_q}(T - f(a)) = \prod_{a\in\mathbb{F}_q}(T - a)$, so f is bijective on $\mathbb{F}_q$.

References

[Tur95] G. Turnwald, *A new criterion for permutation polynomials*, Finite Fields Appl. (1995), **1**(1), 64–82.

[Wan93] D. Q. Wan, *A p-adic lifting lemma and its applications to permutation polynomials*, in *Finite fields, coding theory, and advances in communications and computing (Las Vegas, NV, 1991)*, vol. 141 of *Lecture Notes in Pure and Appl. Math.*, Dekker, New York, 1993 pp. 209–216.

E-mail: peter.mueller@mathematik.uni-wuerzburg.de