Hokkaido Mathematical Journal Vol. 9 (1980) p. 135-137

Note on intersections of translates of powers in finite fields

By Ronald J. EVANS

(Received July 18, 1979)

Let F be a finite field of odd order q. Fix integers t, $n\geq 2$ with $n|(q-1)$. Let R denote the set of $(q-1)/n$ nonzero n-th powers in F. For $a\in F$, let R_a denote the translate $R+a$, and for $A\subset F$, define $R_A=\bigcap_{a\in A} R_a$. In this note, we consider the following problem suggested by N. Ito. Find the fields F for which

(1) $\quad R_A\neq R_B$ whenever $A\neq B$ and $\min(|A|, |B|)=t$.

We will give a number theoretical proof of the following theorem.

THEOREM: *Let* $Q(n, t)=2X^2+Y+2X\sqrt{X^2+Y}$, *where*

$$X=tn^t-\frac{(n+1)(n^t-1)}{2(n-1)}-\frac{n(t^2-t)}{4}-\frac{(t^2+t)}{4}$$

and

$$Y=\frac{tn^t}{n-1}+\frac{n(t^2-t)}{2}-\frac{(t^2+t)}{2}.$$

Then (1) *holds whenever* $q>Q(t, n)$.

An easily proved consequence is:

COROLLARY: *If* $q>(2t+1)^2n^{2t}$, *then* (1) *holds.*

If we were to let $t=1$, then (1) would in fact hold for all fields F. Equivalently, R is distinct from each of its translates $R+a$ $(a\neq 0)$. To see this, assume that $R=R+a$ for some $a\neq 0$. Then R is the disjoint union of sets of the form $\{x+a, x+2a, \cdots, x+pa\}$, where p is the characteristic of F. Thus p divides $|R|=(q-1)/n$, a contradiction.

In studying Hadamard matrices and block design, Ito [1, Lemma 5] showed in the case $n=t=2$, $q\equiv -1 \pmod 4$ that (1) holds for $q>7$. No better lower bound for q exists, since $R_{\{0,1\}}=R_{\{0,2\}}$ when $q=7$. Now, the only odd prime powers between 7 and $Q(2, 2)\cong 14.56$ are 9, 11, 13, and inspection easily shows that (1) holds for these values of q when $n=t=2$. Thus our theorem proves Ito's result in the more general setting $q\equiv\pm 1 \pmod 4$.

For large values of n or t, $Q(n, t)$ is undoubtedly far from the best lower bound for q. This is because, in applying the Weil estimate, we ignored possibly large amounts of cancellation between character sums.

PROOF of THEOREM.

Let $q>Q(n, t)$. Assume that $A\neq B$ and $|B|\geq|A|=t$. Since $R_{A\cup B}=R_A\cap R_B$, it suffices to show that $|R_{A\cup B}|<|R_A|$. Since $|A\cup B|>|A|$, it suffices to show that $|R_C|<|R_A|$ for any set $C=A\cup\{w\}$ with $w\notin A$.

Let χ be a character on F of order n. For $u\in F$, $D\subset F$, write

$$P_D(u)=\prod_{a\in D}\left(1+\chi(u-a)+\cdots+\chi^{n-1}(u-a)\right).$$

Then

$$n^t|R_A|=\sum_{u\in F-A}P_A(u)=\sum_{u\in F}P_A(u)-\sum_{u\in A}P_A(u).$$

Since

$$0\leq\sum_{u\in A}P_A(u)\leq\sum_{u\in A}n^{t-1}=tn^{t-1},$$

$$n^t|R_A|\geq\sum_{u\in F}P_A(u)-tn^{t-1}, \tag{2}$$

and similarly,

$$n^{t+1}|R_C|\leq\sum_{u\in F}P_C(u). \tag{3}$$

Expanding the product $P_A(u)$ and summing over $u\in F$, we see that $\sum_{u\in F}P_A(u)$ equals q plus a sum of character sums of the form

$$\sum_{u\in F}\chi^{i_1}(u-a_1)\cdots\chi^{i_r}(u-a_r), \tag{4}$$

where $2\leq r\leq n-1$, $1\leq i_1, \cdots, i_r\leq n-1$, and where $a_1, \cdots, a_r$ are distinct elements of A. We isolate out $(n-1)\binom{t}{2}$ of the sums in (4) which equal -1, namely the sums

$$\sum_{u\in F}\chi^i(u-a)\,\chi^{n-i}(u-b)$$

with $1\leq i\leq n-1$, a, $b\in A$, $a\neq b$.

Then we use Weil's estimate [2, Theorem 2 C′, p. 43] on each of the remaining sums in (4), as follows:

$$\left|\sum_{u\in F}\chi^{i_1}(u-a_1)\cdots\chi^{i_r}(u-a_r)\right|\leq(r-1)\sqrt{q}.$$

Thus,

$$\begin{aligned}&\sum_{u\in F} P_A(u)-q+(n-1)\binom{t}{2}\\&\quad\geq -\sqrt{q}\left(-\binom{t}{2}(n-1)+\sum_{r=2}^{t}\binom{t}{r}(r-1)(n-1)^r\right)\\&\quad= -\sqrt{q}\,F(n,t)\,,\end{aligned}$$

where

$$F(n,t)=1+n^t(t-1)-tn^{t-1}-\binom{t}{2}(n-1)\,.$$

Thus, from (2),

$$n^t|R_A|\geq q-(n-1)\binom{t}{2}-\sqrt{q}\,F(n,t)-tn^{t-1}\,,$$

and, similarly, from (3),

$$n^{t+1}|R_C|\leq q-(n-1)\binom{t+1}{2}+\sqrt{q}\,F(n,t+1)\,.$$

Subtraction yields

$$\begin{aligned}&n^{t+1}\big(|R_A|-|R_C|\big)\\&\quad\geq q(n-1)-\sqrt{q}\,\big(nF(n,t)+F(n,t+1)\big)\\&\qquad+(n-1)\left\{\binom{t+1}{2}-n\binom{t}{2}\right\}-tn^t\,.\end{aligned}$$

The last member above is positive for $q>Q(n,t)$, as desired.

References

[1] N. ITO: Note on Hadamard matrices of Pless type, Hokkaido Math. J. Vol. 9 No. 2, 1980.

[2] W. SCHMIDT: Equations over finite fields, Lecture Notes in Mathematics #536, Springer-Verlag, Berlin, 1976.

Ronald J. Evans, Dept. of Math.
University of California, San Diego
La Jolla, Ca. 92093