A NOTE ON SPLIT DILATIONS DEFINED BY HIGHER RESIDUES

JAY P. FILLMORE

1. **Introduction.** Let p be an odd prime, F_p the field of p elements. Given a, $b \in F_p$ the mapping

$$\begin{aligned} x &\to 0 && \text{if } x = 0, \\ &\to ax && \text{if } (x/p) = 1, \\ &\to bx && \text{if } (x/p) = -1. \end{aligned}$$

where (x/p) is the quadratic residue symbol, has been called a split dilation by W. H. Mills. If $ab \neq 0$ and $(a/p) = (b/p)$, it is a permutation of the elements of F_p.

Two maps P, Q of F_p into itself are called equivalent if $Q(x) = P(x+a)+b$ for some a, b and all x in F_p. Two split dilations have the property that they are equivalent only when they are equal.

In this note we discuss split dilations of a field with q elements where the splitting is defined for any divisor of $q-1$. Such split dilations are equivalent only when they are equal. The attractive conjecture that every permutation is equivalent to some split dilation is shown false by enumerating the split dilations and comparing this with the total number of equivalence classes.

2. **Split dilations.** Let F be the field with q elements and characteristic p, d a divisor of $q-1$, κ a primitive dth root of unity in F, $r = (q-1)/d$.

Let $a = (a_1, \cdots, a_d) \in F^d$. The map D_a defined by

$$\begin{aligned} D_a(x) &= 0 && \text{if } x = 0 \\ &= a_1 x && \text{if } x^r = \kappa \\ &= a_2 x && \text{if } x^r = \kappa^2 \\ &\;\;\vdots && \;\;\vdots \\ &= a_d x && \text{if } x^r = \kappa^d = 1 \end{aligned}$$

is said to be a *d-split dilation* of F.

Every mapping of F into itself is given by a unique polynomial of degree less than q. To see that a d-split dilation D_a may be put into the form

Received by the editors May 2, 1966.

$$D_a(x) = A_{d-1}x^{r(d-1)}x + A_{d-2}x^{r(d-2)}x + \cdots + A_1x^rx + A_0x$$

it is only necessary to solve the system

$$\sum_{i=0}^{d-1} A_i\kappa^{ji} = a_j, \qquad j = 1, 2, \cdots, d.$$

The determinant is a nonvanishing Vandermonde determinant and the system has a solution.

Call two maps P, Q of F into itself equivalent if there are α, $\beta \in F$ such that $Q(x) = P(x+\alpha)+\beta$ for all x. If Q and P are written as polynomials of degree less than q, their degrees are equal (the zero polynomial being assigned the degree 0).

THEOREM 1. *Let $d \mid q-1$, $d \neq q-1$. Let D_a be d-split and suppose the degree of the polynomial representing D_a is not divisible by p. Then any d-split dilation which is equivalent to D_a equals D_a.*

PROOF. Suppose $D_a(x)$ is given by the polynomial

$$A_{s-1}x^{r(s-1)+1} + A_{s-2}x^{r(s-2)+1} + \cdots + A_1x^{r+1} + A_0x$$

where $A_{s-1} \neq 0$ and $1 \leqq s \leqq d$. Then $D_a(x+\alpha)+\beta$ is given by the polynomial

$$A_{s-1}x^{r(s-1)+1} + (r(s-1)+1)A_{s-1}\alpha x^{r(s-1)} + \cdots .$$

If $s=1$ the theorem is trivial, so assume that $s>1$.

Since $d \neq q-1$, $r(s-1) > r(s-2)+1$ and the coefficient of the $r(s-1)$st degree term is $(r(s-1)+1)A_{s-1}\alpha$. If $D_a(x+\alpha)+\beta$ is to be d-split, this coefficient $=0$. Since $r(s-1)+1 \neq 0$, $A_{s-1} \neq 0$, it follows $\alpha = 0$. $\beta = 0$ comes from setting $x=0$.

REMARK. The hypothesis on the degree of the polynomial representing D_a is satisfied in two important instances:

1° $q=p$,

2° the degree of the polynomial representing D_a is maximal, i.e., the degree is $r(d-1)+1 = (q(d-1)+1)/d$ and hence never $\equiv 0 \bmod p$.

Special cases of split dilations are:

(1) p arbitrary, $d=1$. $D_a(x) = a_1x$ is a dilation of F in the usual sense.

(2) p odd, $d=2$, $D_a(x)=0$ if $x=0$, a_1x is $x^{(q-1)/2} = -1$, and a_2x if $x^{(q-1)/2} = 1$ ($a_1a_2 \neq 0$, $a_1{}^{(q-1)/2} = a_2{}^{(q-1)/2}$) is a split dilation as defined by Mills.

(3) p arbitrary, $d = q-1$. D_a, for suitable choice of the a_i, can be any map of F into itself which sends 0 into 0.

3. The group of split dilations. Let $K_i = \{x \in F - \{0\} \mid x^r = \kappa^i\}$

$i=1, \cdots, d$ (notation as in §2). K_d is a subgroup of $F-\{0\}$, the K_i are its cosets.

Let D_a, $a=(a_1, \cdots, a_d)$, be d-split. Suppose $a_i \in K_{\pi(i)-i}$ where the map π of 1, 2, $\cdots$, d into itself is determined by a. If $x \in K_i$, then $D_a(x)=a_i x \in K_{\pi(i)}$. Furthermore, the map $x \to a_i x$ from the set K_i to the set $K_{\pi(i)}$ is bijective. Thus D_a is a permutation if, and only if, π is a permutation of 1, 2, $\cdots$, d. Clearly every π in the symmetric group S_d comes from some D_a.

Let D_a, $D_{a'}$ be d-split dilations which permute the classes K_i according to π, π' respectively. Then $D_{a'} \cdot D_a$ is a d-split dilation $D_{a''}$ where $a_i''=a_{\pi(i)}' \cdot a_i$, $i=1, 2, \cdots, d$. $D_{a''}$ permutes the K_i according to $\pi' \cdot \pi$. If we denote by G_d the d-split dilations of F which are permutations we have:

THEOREM 2. *G_d is a group of order $d!((q-1)/d)^d$. It is a subgroup of index d^d of the semidirect product by S_d of d copies of the multiplicative group of F.*

The order of G_d is computed by knowing that S_d contains $d!$ elements and that each class K_i contains $(q-1)/d$ elements. The other assertions follow easily from the preceding discussion.

Now let ω be a primitive $(q-1)$st root of unity in F. Put $\kappa_d=\omega^{(q-1)/d}$ so that κ_d is a primitive dth root of unity.

Let $d \mid d'$, $d' \mid q-1$. There is then a natural inclusion $G_d \subseteq G_{d'}$ given by

$$D_{(a_1, \ldots, a_d)} \to D_{(\underbrace{a_1, \ldots, a_d}_{\text{repeated } d'/d \text{ times}}, a_1, \ldots, a_d, a_1, \ldots, a_d)}.$$

Since $\kappa_d=(\kappa_{d'})^{d'/d}$, the two maps agree on all of F.

Let d', d'' be two divisors of $q-1$. Then $G_d \subseteq G_{d'} \cap G_{d''}$ where $d=(d', d'')$ is the greatest common divisor of d' and d''. Our claim is that the inclusion is an equality. This is seen as follows.

Let $P \in G_{d'} \cap G_{d''}$. Since P is d'-split, it is given by a polynomial with exponents of the form $k'((q-1)/d')+1$ ($k'=0, 1, \cdots, d'-1$) only. Since P is d''-split, the same holds with exponents $k''((q-1)/d'')+1$. Thus each $k'((q-1)/d')+1$ is of the form $k''((q-1)/d'')+1$ for suitable k''. Putting $k=k'd/d'=k''d/d''$ we have $k'((q-1)/d')+1 = k''((q-1)/d)+1=k((q-1)/d)+1$, whence P is also d-split. Hence the assertion.

4. **Enumerations.** By Theorem 2 the number of elements in G_d is $d!((q-1)/d)^d$. Denote this by g_d. Let $d_1, d_2, \cdots, d_r$ be the divisors of $q-1$ which are $\neq q-1$. By repeated application of the fact that

$G_{d'} \cup G_{d''}$ contains $g_{d'} + g_{d''} - g_{(d',d'')}$ elements, we obtain

$$\sum_{\rho=1}^{r} (-1)^{\rho-1} \sum_{1 \leq i_1 < \cdots < i_\rho \leq r} g_{(d_{i_1}, \cdots, d_{i_\rho})}$$

for the number of elements of

$$\bigcup_{\rho=1}^{r} G_{d_\rho}.$$

If $p=q$, these elements are inequivalent under the equivalence relations defined in §2.

Assume now, $p=q$. The $(p-1)$-split dilations are just arbitrary permutations of F which send 0 into itself. Every equivalence class of permutations of F contains a $(p-1)$-split dilation.

If $p=q=7$, there are 60 permutations which are either 1-, 2-, or 3-split, thus 60 equivalence classes containing a permutation which is d-split with $d \neq 6$. However, we can compute directly that there are 108 equivalence classes of permutations on the 7 elements of F_7. Thus equivalence classes containing nontrivial $(d \neq p-1)$ split dilations do not exhaust all equivalence classes.

In fact, for large p equivalence classes containing nontrivial split dilations are quite scarce and their relative number appears to go to 0 as $p \to \infty$.

p	(Number of equivalence classes containing nontrivial split dilations)/(Total number of equivalence classes)
3	1
5	1
7	5.56×10^{-1}
11	1.18×10^{-2}
13	1.30×10^{-3}
17	8.39×10^{-6}
19	5.53×10^{-7}

DEPARTMENT OF DEFENSE