GL_n- orbits of minimal functions over finite fields

Francisco Rivero

1. This paper deals with the fourier transform over finite fields. Our main goal is to give a partial answer to a problem posed by McGehee (See [1]) . First we need some definitions .

Let G denote the additive group of a finite field of p^n elements A character on G is a map

$$\chi : G \longrightarrow \mathbb{C}^* ,$$

such that $\chi (a + b) = \chi (a).\ \chi (b)$ for a , b in G .

$\mathbb{C}^*$ denotes the multiplicative group of complex numbers.

Thus $\chi (0) = 0$, and for all a in G , its image $\chi (a)$ is a p-th root of unity.

The trivial character χ_0 is the map given by $\chi_0 (a) = 1$ for all a in G.

The set of all characters becomes a group under the multiplication of functions. We call this group the dual of G and we denoted it by $\hat{G}$.

McGehee considers functions

$$\mu : G \longrightarrow \{ 0 , 1 , -1 \} ,$$

with $\mu (x) = 0$ if and only if $x = 0$.

We denote the set of such functions by $\mathfrak{M}$ .For a function μ in $\mathfrak{M}$ its fourier transform is defined as

$$\hat{\mu}(\chi) = \sum_{g \in G} \mu(g)\,\chi(g) \quad \text{for } \chi \text{ in } \hat{G}.$$

The norm of μ is given by

$$\| \mu \| = \sup_{\chi \in \hat{G}} | \hat{\mu}(\chi) | ,$$

and this norm satisfies $\| \mu \| \leq p^{n/2}$.

We say that μ is minimal if $\| \mu \| = p^{n/2}$.

The basic examples of minimal functions are the quadratic function ψ and its negative $-\psi$, where

$$\psi(x) = \begin{cases} 1 & \text{if } x \text{ is a nonzero square} \\ -1 & \text{if } x \text{ is nonsquare} \\ 0 & \text{if } x = 0 . \end{cases}$$

McGehee question is to describe all minimal functions ; or at least to count them . When n = 1 or 2 , McGehee gave a complete count of all minimal functions.

The set of minimal functions will be denoted by $\mathfrak{M}_0$. We know two bounds for the number of elements in this set (See [2])

$$2 \leq | \mathfrak{M}_0 | \leq 2^{s} ,$$

where $s = \frac{p^n - 1}{p - 1}$.

The following theorem , due to McGehee , is a useful criterion to test a function in $\mathfrak{M}$ for minimality .

THEOREM 1 Let f be a function in $\mathfrak{M}$. Then $\| f \| = p^{n/2}$ if and only if

i) $\hat{f}(\chi_0) = 0$

ii) $| \hat{f}(\chi_0) | = p^{n/2}$ for $\chi \neq \chi_0$.

We will refer to i) and ii) as the minimality conditions for f

2. We now consider group actions on the set of minimal functions .

Let σ a group automorphism $\sigma : G \longrightarrow G$, and let χ be a character on G . Define the action of σ over χ as

$$\chi^{\sigma}(g) = \chi (\sigma (g)).$$

Thus the group Aut (G) acts over $\hat{G}$ and by means of this action , we can make Aut (G) act on on the set $\mathfrak{M}_0$ of minimal functions.

Let $f \in \mathfrak{M}_0$, then define

$$f^{\sigma} = f \sigma \quad \text{for } \sigma \text{ in Aut (G)} .$$

THEOREM 2 If f is a minimal function , then f^{σ} is minimal for all σ in Aut (G).

PROOF : Let f be in $\mathfrak{M}_0$ and let σ be in Aut (G) . In order to prove that f^{σ} is in $\mathfrak{M}_0$, we only need to verify the minimality conditions.

Thus

$$\hat{f}^{\sigma} (\chi_0) = \sum_{g \in G} f^{\sigma}(g) \chi_0 (g)$$

$$= \sum_{g \in G} f (\sigma (g)) \chi_0 (g) .$$

Making $\sigma (g) = s$, and using the fact that $\sigma (g)$ runs over all elements in G , as g runs over G , gives

$$\hat{f}^{\sigma} = \sum_{s \in G} f (s) = \hat{f} (\chi_0) = 0 .$$

Therefore the first minimality condition holds for f^{σ}. Now, let χ be any character on G, $\chi \neq \chi_0$. Then we have

$$| \hat{f^{\sigma}} (\chi) | = | \sum_{g \in G} f (\sigma (g)) \chi (g) |$$

$$= | \sum_{g \in G} f (\sigma (g)) \chi^{\sigma^{-1}} (\sigma (g)) |$$

$$= | \hat{f} (\chi^{\sigma^{-1}}) | = p^{n/2} . \qquad \square$$

There is a subgroup of Aut (G), which is of our interest, namely $GL_n (\mathbb{F}_p)$. If we look at the finite field $\mathbb{F}_{p^n}$ as a vector space over $\mathbb{F}_p$, then $GL_n (\mathbb{F}_p)$ is the group of all invertible $\mathbb{F}_p$- linear maps from $\mathbb{F}_{p^n}$ to itself.

We will study the action of this group on $\mathfrak{M}_0$ and in particular its action on Ψ. The size of the orbit of Ψ is given by

$$| GL_n (\mathbb{F}_p) . \Psi | = \frac{| GL_n (\mathbb{F}_p) |}{| \text{Stab } \Psi |} \qquad (1)$$

Here $\text{Stab } \Psi = \{ \sigma \in GL_n (\mathbb{F}_p) / \Psi \sigma = \Psi \}$.

REMARK There is a formula for the order of $GL_n (\mathbb{F}_p)$ (See [3])

$$| GL_n (\mathbb{F}_p) | = (p^n - 1) (p^n - p) \ldots . (p^n - p^{n-1}) \quad (2)$$

REMARK We found a formula for the order of Stab Ψ in [2]

$$| \text{Stab } \Psi | = n \frac{p^n - 1}{2} \qquad (3)$$

The above formula was verified for some numerical values of p^n. However we did not have a complete proof for that formula. While we

were trying to prove (3) , we arrived to the following interesting conjecture

CONJECTURE 1 Every σ in Stab Ψ is of the form :

$$\sigma = c \cdot \theta^i \qquad 1 \leq i \leq n \qquad (4)$$

where c is a non-zero square in G , and θ is an element in the Galois group Gal ($\mathbb{F}_{p^n} : \mathbb{F}_p$) .

Our conjecture can be restated as follows

CONJECTURE 2 Let σ be a $\mathbb{F}_p$- linear invertible map on $F = \mathbb{F}_{p^n}$

$\sigma : F \longrightarrow F$, such that

i) $\sigma (1) = 1$

ii) $\sigma (F^2) = F^2$.

Then $\sigma (xy) = \sigma (x) \sigma (y)$ for all x , y in F .

In a letter sent to the author , Dr Robert Perlis pointed out that this conjecture was a special case of a theorem of L. Carlitz , from 1960 (See [4]) . There is a more elegant proof of the same theorem , given by A. Bruen and B. Levinger (See [5])

<u>THEOREM 2</u> (Carlitz) Let F be a finite field of order $q = p^n$, and let $K = \{ x \in F / x^d = 1 \}$, for some proper divisor d of q-1 . Then a mapping f of F into itself satisfies

$$(x - y)^{-1} (f(x) - f(y)) \in K \qquad (6)$$

for $x \neq y$ in F , if and only if f(x) is given by

$$f(x) = a + b x^{p^j} , \qquad (7)$$

where $a \in F$, $b \in K$, and (q-1) divides $d (p^j - 1)$.

We will give a proof of the conjecture as stated in (4) .

PROOF OF THE CONJECTURE :

Take d = (q-1)/2 , then it follows K = squares in F .

Now , let σ be a map in Stab Ψ . We will show that σ satisfies condition (6) . Consider x,y two different elements in F and its difference x-y in F . We have two choices

I) If x-y is a square we get $\sigma(x-y) = \sigma(x) - \sigma(y) \in K$, thus $(x-y)^{-1} (\sigma(x) - \sigma(y)) \in K$.

II) If x-y is nonsquare we have $\sigma(x-y) = \sigma(x) - \sigma(y)$ is nonsquare, and from this we obtain : $(x-y)^{-1} (\sigma(x) - \sigma(y)) \in K$.

Thus by using Carlitz theorem we conclude

$$\sigma(x) = a + b\, x^{p^j} , \qquad (8)$$

where $a \in F$, $b \in K$, and $q-1$ divides $\frac{q-1}{2} (p^j - 1)$.

First we note that there is no restriction on j , since q-1 always divides $\frac{(q-1)}{2} (p^j - 1)$. Second we observe that if $j > n$, the element x^{p^j} is on the set x^p , $x^{p^2}, \ldots, x^{p^n}$, thus we can take $1 \leq j \leq n$. Moreover , putting $x^p = \theta \in Gal(F ; \mathbb{F}_p)$ in (8) gives

$$\sigma(x) = a + b\, \theta^j \quad 1 \leq j \leq n . \qquad (9)$$

Finally , observe that a = 0 , since $\sigma(0) = 0$. Thus

$$\sigma(x) = b\, \theta^j \quad 1 \leq j \leq n \quad , b \in K ,$$

and that finishes the proof . □

REMARK Once we prove the conjecture , the order of Stab Ψ can be

found easily by counting the choices for σ in (4)

$$| \text{ Stab } \Psi | = \#\text{ choices for b } . \#\text{ choices for j } = \frac{p^n-1}{2} n .$$

Thus we have shown

THEOREM 3 Let F be a finite field of p^n elements . Then we have

$$| GL_n (F ; \mathbb{F}_p) . \Psi | = \frac{2 (p^n-p) (p^n - p^2) \ldots (p^n - p^{n-1})}{n} \quad (8)$$

REMARK The above formula gives a good lower bound for the number of minimal functions . When p = 3 , n = 3 McGehee found exactly 288 of such functions by numerical computations . Also for n= 1 and any p there are only two minimal functions Ψ and $-\Psi$. Then in this two cases all minimal functions are in the orbit of Ψ . An open question is : Does $GL_n (\mathbb{F}_p)$ acts transitively on $\mathfrak{M}_0$, $n \geq 1$, n odd ?

REMARK When n = 2 and $p \neq 3,5$ we show in [2] that $GL_2 (\mathbb{F}_p)$ does not act transitively on the set of minimals . However , there is a larger group that acts transitively in this case .

We may consider G , the additive group of $\mathbb{F}_{p^n}$ as a vector space over $\mathbb{F}_p$. Then a line through the origin given by a in G is

$$\mathbb{F}_p . a = \{ x \in G / x = c.a \text{ for c in } \mathbb{F}_p \}$$

Then G can be seen as the union of lines through the origin . It can be shown that the set of all permutations σ of G , taking 0 to to 0 , and lines to lines is a group . Also this group , which is denoted by P_2 , acts transitively on $\mathfrak{M}_0$. Thus we obtain all minimal functions from the P_2 - orbit of Ψ . The number of such functions is

$$| \mathcal{M}_0 | = \binom{p+1}{\frac{p+1}{2}}.$$

In general when n = 2m is even , then the finite field $F = \mathbb{F}_{p^{2m}}$ contains the subfield $K = \mathbb{F}_{p^n}$, and G = (F , +) can be considered to be a K- vector space , and thus G is the union of K-lines through the origin . As before , we consider the group P_2 (K) of permutations of F , taking 0 to 0 and K-lines to K-lines . It is not known whether P_2 (K) acts transitively on minimals when n > 2 . But we can say that the action of P_2 (K) gives that the number N_0 of minimals functions satisfies

$$N_0 \geq \binom{t}{t/2},$$

where $t = p^m + 1$.

For example , for p = 7 and n = 6 we see

$$N_0 \geq \binom{344}{172}$$

which is a number with over 100 digits .

References

[1] O. Carruth McGehee - Gaussian Sums and Harmonic Analysis on finite fields . (To be published) , 1987

[2] Francisco Rivero - Group actions on minimal functions over finite fields . Umpublished dissertation . Louisiana State University , 1987.

[3] Nathan Jacobson - Basic Algebra . W.H. Freeman and company . San Francisco , 1974.

[4] L. Carlitz- A theorem on permutations in a finite field . Proc . Amer . Math . Soc 11 , 1960 .

[5] A.Bruen and B.Levinger . A theorem on permutations of a finite field . Can . J. Math , vol xxv , No 5 , 1973.

[6] C.C. Graham and O.C. Macgehee . Essays in commutative Harmonic analysis ; Springer Verlag , New York 1979 .