A Note on Difference Sets with Group Characters*

Kimball Martin

December 10, 1997

Let G be a finite abelian group and $Ch(G)$ be the set of group characters of G. Let $\mathbf{V}$ be the vectorspace of complex-valued functions on G. Define an inner product on $\mathbf{V}$ by

$$\langle f, g\rangle = \sum_{x\in G} f(x)\overline{g(x)}.$$

(Notice this just the dot product of the truth tables of $f(x)$ and $\overline{g(x)}$.)

Theorem 1 (Orthogonality of Group Characters) *The set $Ch(G)$ forms a group isomorphic to G. Moreover, $Ch(G)$ is an orthogonal basis for $\mathbf{V}$.*

Proof First we show $Ch(G)$ forms a group isomorphic to G. It is easy to see $Ch(G)$ constitutes a group under multiplication. Take a minimal generating set $g_1, g_2, ..., g_r$ of G and a character χ of G. Then χ is completely determined by the images under χ of $g_1, g_2, ..., g_r$. Let d_i be the order of g_i for $i = 1, 2, ...r$. For any g_i, $\chi(g_i)$ must be a d_i^{th} root of unity. In fact for each $g_i, \chi(g_i)$ may be any d_i^{th} root of unity.

Now we will associate each element in G with a group character. For each d_i let ζ_i be a primitive d_i^{th} root of unity. For any element $x \in G$ write x as $g_1^{a_1} g_2^{a_2} \cdots g_r^{a_r}$. Let χ_x be determined by $\chi_x(g_i) = \zeta_i^{a_i}$ for $i = 1, 2, ..., r$. We claim the mapping $\phi : x \to \chi_x$ is an isomorphism of G onto $Ch(G)$. Take any $y = g_1^{b_1} g_2^{b_2} \cdots g_r^{b_r}$. Since

$$\chi_x(g_i)\chi_y(g_i) = \zeta_i^{a_i}\zeta_i^{b_i} = \zeta_i^{a_i+b_i} = \chi_{xy}(g_i)$$

for each g_i, ϕ is a homomorphism of G into $Ch(G)$.

Now suppose $\chi_x = \chi_y$. Thus for $i = 1, 2, ..., r$ we have

$$\begin{aligned} \chi_x(g_i) &= \chi_y(g_i) \Rightarrow \\ \zeta_i^{a_i} &= \zeta_i^{b_i} \Rightarrow \\ a_i &= b_i \Rightarrow \\ x &= y, \end{aligned}$$

*References: John F. Dillon; Ireland and Rosen, *A Classical Introduction to Modern Number Theory.*

i.e. ϕ is one-to-one. As x ranges through G, $\chi_x(g_1), \chi_x(g_2), ...\chi_x(g_r)$ range through all possible combinations of powers of $\zeta_1, \zeta_2, ..., \zeta_r$, respectively. Hence ϕ is onto and ϕ is in fact an isomorphism of G onto $Ch(G)$.

Now we show the orthogonality of group characters. If $|G| = 1$, this result holds trivially. So assume $n = |G| > 1$. Let χ and λ be two distinct characters in $Ch(G)$. First consider $\lambda = \chi_0$, the trivial character. Then

$$\langle \chi, \lambda \rangle = \sum_{x \in G} \chi(x).$$

Since χ is non-principal, for some $a \in G$, $\chi(a) \neq 1$. Then

$$\sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(ax) = \sum_{x \in G} \chi(a)\chi(x) = \chi(a) \sum_{x \in G} \chi(x).$$

Thus $(1 - \chi(a)) \sum_x \chi(x) = 0$ so $\langle \chi, \chi_0 \rangle = \sum_{x \in G} \chi(x)$ must be 0.

Now for any $\lambda \neq \chi$ we have

$$\overline{\lambda(xy)} = \overline{\lambda(x)\lambda(y)} = \overline{\lambda(x)\lambda(y)},$$

for all $x, y \in G$, i.e. $\overline{\lambda}$ is a character. In fact for any $x \in G$, $\lambda(x)\overline{\lambda(x)} = |\lambda(x)|^2$. Since $\lambda(x)$ is a root of 1, $|\lambda(x)|^2$ must be 1 and $\overline{\lambda}$ is the inverse of λ in $Ch(G)$. Then $\chi\overline{\lambda} = \chi\lambda^{-1} \neq \chi_0$. So

$$\langle \chi, \lambda \rangle = \sum_{x \in G} \chi(x)\overline{\lambda(x)} = \langle \chi\overline{\lambda}, \chi_0 \rangle = 0.$$

Thus $Ch(G)$ can be regarded as an set of n orthogonal vectors in $\mathbf{V}$. Since $dim\mathbf{V} = n$, $Ch(G)$ constitutes a basis for $\mathbf{V}$. ∎

Consider the group algebra $\mathbf{C}[G]$ and $D \subseteq G$. In $\mathbf{C}[G]$, we write D as $D = \sum_{g \in G} a_g g$. For a character χ, define $\chi(D)$ to be $\sum_{g \in G} a_g \chi(g)$. (We use D to mean both the subset D of G and the element in $\mathbf{C}[G]$ which is the characteristic function of D in G.)

Theorem 2 *For $D \subseteq G$, D is a (v, k, λ)-difference set in G if and only if*

$$\begin{array}{rcll} \chi_0(D) & = & k, & \text{and} \\ |\chi(D)| & = & \sqrt{n} & \forall \chi \in Ch(G), \chi \neq \chi_0. \end{array}$$

Proof Let $D = \sum_{g \in G} a_g g$ and $D^{(-1)} = \sum_{g \in G} a_g g^{-1}$. We use the characterization of a difference set in terms of the product of it with its inverse in the group algebra, i.e. the fact that D is a (v, k, λ)-difference set if and only if $DD^{-1} = n + \lambda G$, where $n = n \cdot 1$ represents n times the identity in G.

($\Longrightarrow$) Suppose $D \subseteq G$ is a (v, k, λ)-difference set. Take any $\chi \in Ch(G)$. Now

$$\chi(D^{(-1)}) = \chi(\sum_g a_g g^{-1}) = \sum_g a_g \chi^{-1}(g).$$

Earlier we noted $\chi^{-1} = \overline{\chi}$ for χ a group character. (This is not true for χ a character extended to the group algebra). So we have

$$\chi(D^{(-1)}) = \sum_g a_g \overline{\chi(g)} = \overline{\sum_g a_g \chi(g)} = \overline{\chi(D)}.$$

Thus

$$\begin{aligned} |\chi(D)|^2 &= \chi(D)\overline{\chi(D)} = \chi(D)\chi(D^{(-1)}) = \chi(DD^{(-1)}) \\ &= \chi(n + \lambda G) = \chi(n \cdot 1) + \lambda\chi(G) = n + \lambda\chi(G). \end{aligned}$$

If $\chi = \chi_0$, then $\chi(G) = v$ so

$$|\chi(D)|^2 = n + \lambda v = (n + \lambda) + \lambda(v - 1) = k + k(k - 1) = k^2.$$

Otherwise, $\chi(G) = 0$ and $|\chi(D)|^2 = n$. Hence our theorem holds in one direction.
($\Longleftarrow$) Suppose that, for all $\chi \in Ch(G)$,

$$|\chi(D)| = \begin{cases} k & \textit{if } \chi = \chi_0 \\ \sqrt{n} & \textit{otherwise}, \end{cases}$$

i.e., suppose $|\chi(D)|^2 = \chi(n + \lambda G)$ for all $\chi \in Ch(G)$. Above we showed $|\chi(D)|^2 = \chi(DD^{(-1)})$ for all $\chi \in Ch(G)$. Then we have

$$\chi(DD^{(-1)}) = \chi(n + \lambda G), \forall \chi \in Ch(G).$$

Take any real-valued $a = \sum_g a_g g, b = \sum_g b_g g \in \mathbf{C}[G]$ such that

$$\chi(a) = \chi(b), \forall \chi \in Ch(G).$$

We show it must be the case that $a = b$. This will imply $DD^{(-1)} = n + \lambda G$ and complete the proof. Now for any $\chi \in Ch(G)$,

$$0 = \chi(a) - \chi(b) = \sum_g a_g \chi(g) - b_g \chi(g) = \sum_g \chi(g)(a_g - b_g) = \langle \chi, c \rangle,$$

where $c \in \mathbf{V}$ is given by $c = \sum_g (a_g - b_g)g$. Thus c is orthogonal to every character of G, i.e. c is orthogonal to every element in a basis for $\mathbf{V}$, i.e. $c = 0$. So for all g in G, it must be that $a_g = b_g$, i.e. $a = b$. ∎

We use this characterization of a difference set to prove Maschietti's theorem, but first we will introduce Gauss and Jacobi sums. Take any finite field $\mathbf{F}_p$ of prime order and any extension $\mathbf{F}_q$ of $\mathbf{F}_p$. Let $tr(x)$ denote the trace of x from $\mathbf{F}_q$ down to $\mathbf{F}_p$. We will extend the characters $Ch(\mathbf{F}_q^*)$ to $\mathbf{F}_q$ by letting $\chi(0) = 1$ if $\chi = \chi_0$ and $\chi(0) = 0$ otherwise for all χ in $Ch(\mathbf{F}_q^*)$.

Definition 1 *For $a \in \mathbf{F}_q, \chi \in Ch(\mathbf{F}_q)$ we define the* Gauss sum *$g_a(\chi)$ to be*

$$g_a(\chi) = \sum_{x \in \mathbf{F}_q} \chi(x)\zeta^{tr(ax)},$$

where ζ is a primitive p^{th} root of unity.

We are concerned with the case $a = 1$ here and we will abbreviate $g_1(\chi)$ as $g(\chi)$.

Proposition 1 *For any non-principal $\chi \in Ch(\mathbf{F}_q)$, $|g(\chi)| = \sqrt{q}$.*

Proof Take any non-principal $\chi \in Ch(\mathbf{F}_q)$. We will show

$$\sum_a g_a(\chi)\overline{g_a(\chi)} = (q-1)|g(\chi)|^2,$$

and

$$\sum_a g_a(\chi)\overline{g_a(\chi)} = (q-1)q,$$

to prove our proposition.

If $a = 0$ then $g_a\chi = \sum_x \chi(x) = 0$. Otherwise $a \neq 0$. Then

$$\chi(a)g_a(\chi) = \chi(a)\sum_x \chi(x)\zeta^{tr(ax)} = \sum_x \chi(ax)\zeta^{tr(ax)} = g(\chi),$$

so $g_a(\chi) = \chi(a^{-1})g(\chi)$. Then $\overline{g_a(\chi)} = \overline{\chi(a^{-1})g(\chi)} = \underline{\chi(a)}\overline{g(\chi)}$. Hence $g_a(\chi)\overline{g_a(\chi)} = \chi(a^{-1})g(\chi)\chi(a)\overline{g(\chi)} = |g(\chi)|^2$ and the sum $\sum_a g_a(\chi)\overline{g_a(\chi)}$ is in fact $(q-1)|g(\chi)|^2$.

We also have

$$\begin{aligned}
\sum_a g_a(\chi)\overline{g_a(\chi)} &= \sum_a \sum_{x,y} \chi(x)\overline{\chi(y)}\zeta^{tr(ax-ay)} \\
&= \sum_{x,y} \chi(x)\overline{\chi(y)} \sum_{a \neq 0} \zeta^{tr(a(x-y))} \\
&= \sum_{x,y} \chi(x)\overline{\chi(y)}\delta_{x,y}q \\
&= q\sum_{x \neq 0} \chi(x)\overline{\chi(x)} \\
&= q(q-1). \quad \blacksquare
\end{aligned}$$

Definition 2 *Let χ, λ be characters of $\mathbf{F}_q$. Then we define the* Jacobi sum *$J(\chi, \lambda)$ to be*

$$J(\chi, \lambda) = \sum_{x+y=1} \chi(x)\lambda(y).$$

Proposition 2 *Suppose χ, λ and $\chi\lambda$ are non-principal characters of $\mathbf{F}_q$. Then*

$$J(\chi, \lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}.$$

Proof We have

$$\begin{aligned} g(\chi)g(\lambda) &= \left(\sum_x \chi(x)\zeta^{tr(x)}\right)\left(\sum_y \lambda(y)\zeta^{tr(y)}\right) \\ &= \sum_{x,y} \chi(x)\lambda(y)\zeta^{tr(x+y)} \\ &= \sum_t \left(\sum_{x+y=t} \chi(x)\lambda(y)\right)\zeta^{tr(t)}. \end{aligned}$$

If $t = 0$ this inner sum is just $\sum_x \chi(x)\lambda(-x) = \lambda(-1)\sum_x \chi\lambda(x) = 0$. Otherwise we can set $x = x't$ and $y = y't$ and the inner sum becomes $\sum_{x'+y'=1} \chi(tx')\lambda(ty') = \chi\lambda(t)\sum_{x'+y'=1} \chi(x')\lambda(y') = \chi\lambda(t)J(\chi, \lambda)$. Thus we now have

$$g(\chi)g(\lambda) = \sum_t \chi\lambda(t)J(\chi, \lambda)\zeta^{tr(t)} = J(\chi, \lambda)\sum_t \chi\lambda(t)\zeta^{tr(t)} = J(\chi, \lambda)g(\chi\lambda). \quad \blacksquare$$

In particular, if χ, λ and $\chi\lambda$ are all non-principal, then $|J(\chi, \lambda)| = |g(\chi)g(\lambda)/g(\chi\lambda)|$ which, by Proposition 1, is equal to $\sqrt{q}$.

Theorem 3 (Maschietti) *Let k be relatively prime to $q - 1, q = 2^m$. Suppose*

$$\sigma_k(x) = x^k + x$$

defines a two-to-one mapping on $\mathbf{F}_q$. Then $D = \{x^k + x : x \in \mathbf{F}_q\}\backslash\{0\}$ is a difference set in $\mathbf{F}_q^*$ with Singer parameters $(2^m - 1, 2^{m-1} - 1, 2^{m-2} - 1)$.

Proof Since σ_k is two-to-one on F_q, we have

$$\chi_0(D) = |D| = \frac{q}{2} - 1 = 2^{m-1} - 1.$$

Now take any nonprincipal $\chi \in Ch(\mathbf{F}_q)$. We can write

$$\chi(D) = \sum_{\sigma_k(x) \in D} \chi(\sigma_k(x)) = \frac{1}{2}\sum_{x \in \mathbf{F}_q} \chi(\sigma_k(x)).$$

Since $x^k + x = x(x^{k-1} + 1) = 0$ has only two solutions, namely 0 and 1, $x^{k-1} = 1$ has only the trivial solution in $\mathbf{F}_q$. Thus no $x \neq 1$ in $\mathbf{F}_q$ has order dividing $k - 1$, i.e. $k-1$ is relatively prime to $q-1$. Hence $x \mapsto x^{\frac{1}{k-1}}$ is an automorphism of $\mathbf{F}_q$ so we can define a character λ on $\mathbf{F}_q$ by $\lambda = \chi^{\frac{1}{k-1}}$. Then

$$\begin{aligned} \sum_x \chi(\sigma_k(x)) &= \sum_x \chi(x^k + x) \\ &= \sum_x \chi(x)\chi(x^{k-1}+1) \\ &= \sum_x \lambda(x^{k-1})\chi(x^{k-1}+1) \\ &= J(\chi, \lambda). \end{aligned}$$

Since χ is non-principal, so is λ. Also note $\chi\lambda = \chi^{1+\frac{1}{k-1}} = \chi^{\frac{k}{k-1}} \neq \chi_0$ since k is relatively prime to $q-1$. Thus

$$\begin{aligned} |\chi(D)| &= \frac{1}{2}\left|\sum x \in \mathbf{F}_q \chi(\sigma_k(x))\right| \\ &= \frac{1}{2}\left|J(\chi, \lambda)\right| \\ &= \frac{1}{2}\sqrt{q}. \end{aligned}$$

Hence D is a difference set with $n = q/4$ and D has the Singer parameters $(q-1, q/2-1, q/2-1-q/4) = (q-1, q/2-1, q/4-1) = (2^m-1, 2^{m-1}-1, 2^{m-2}-1)$.
$\blacksquare$