NEW NECESSARY CONDITIONS ON THE EXISTENCE OF ABELIAN DIFFERENCE SETS

ALEXANDER POTT

Received January 20, 1989

In this paper we develop a new method to obtain identities in a group algebra $GF(p)G$ if an
abelian difference set of order $n \equiv 0 \pmod{p}$ exists in $G$. We give an explicit formula if $p^2$ or $p^3$
is the exact $p$-power dividing $n$. This generalizes the approach of Wilbrink, Arasu and the author.
The proof presented here uses some knowledge about field extensions of the $p$-adic numbers.

1. Preliminaries

In this paper $G$ is always a multiplicatively written abelian group of order $v$
with exponent $v^*$ and unit element 1. An abelian $(v, k, \lambda)$-difference set of order
$n := k - \lambda$ in $G$ is a $k$-subset of $G$ such that every element $\neq 1$ in $G$ has exactly
$\lambda$ representations as a “difference” $d_1 d_2^{-1}$ with $d_1, d_2 \in D$. It is well known that
the existence of $(v, k, \lambda)$-difference sets is equivalent to the existence of symmetric
$(v, k, \lambda)$-designs with a regular or sharply transitive automorphism group. For the
basic definitions and results on designs and difference sets we refer the reader to [4]
and [7].

To study difference sets we identify subsets of $G$ with elements in a group ring
$RG$ ($R$ a ring) in the following way:

$$ T \subseteq G \leftrightarrow \sum_{g \in T} g \in RG. $$

If

$$ A = \sum_{g \in G} r_g g \in RG, \quad r_g \in R, $$

we define

$$ A^{(t)} := \sum_{g \in G} r_g g^t $$

for every integer $t$. Thus we obtain for difference sets

$$ DD^{(-1)} = n + \lambda G \in \mathbb{Z}G. $$

AMS subject classification (1991): 05 B 10
We call an integer a \textit{(numerical) multiplier} of $D$ if
\[\Phi_t : G \rightarrow G \]
\[g \mapsto g^t\]
is a group automorphism and $D(t) = Dg$ in $\mathbb{Z}G$ for a suitable $g \in G$. It is well known that a prime divisor $p$ of $n$ is a multiplier if $(p, v) = 1$ and $p > \lambda$, see [4], [7], [8]. The latter condition is conjectured to be unnecessary. If $t$ is a multiplier we may assume $D(t) = D$ and say that $D$ is fixed by $t$, see [4]. Now let $K$ be a field that contains a primitive $v^*$-th root of unity. If $\text{char} K \nmid |G|$ the group algebra $KG$ is semisimple, thus there exist $v$ distinct homomorphisms $\chi : G \rightarrow K^*$, since $G$ is abelian. These homomorphisms are called characters and they form (under multiplication) a group $\hat{G}$ isomorphic to $G$. The identity of $\hat{G}$ is denoted by $\chi_0$ and is called the principal character. For the algebraic background see [5], for instance. We extend the character $\chi \in \hat{G}$ to a homomorphism
\[\chi : KG \rightarrow K\]
\[\sum k_g g \mapsto \sum k_g \chi(g),\]
which is, by abuse of notation, also denoted by $\chi$. It is well known that
\[(*) \quad \chi(G) = 0 \quad \text{if} \quad \chi \neq \chi_0 \quad \text{and} \quad \chi_0(G) = v.\]

We define a $(v \times v)$-matrix
\[X = (x_{\chi, g})_{\chi \in \hat{G}, g \in G}\]
where $x_{\chi, g} := \chi(g)$. It is an easy consequence of (*) that $XX^T = vP$ with a suitable permutation matrix $P$ (here $X^T$ is the transpose of $X$); thus $X$ is non-singular. In other words: An element in $KG$ is uniquely determined by the values of the “extended” characters. The matrix $X$ is called the matrix of the \textit{Discrete Fourier Transform} (DFT). For a more detailed discussion of the relation between the DFT and difference sets see [8].

\section{Difference sets in $\hat{G}$}

First we remark that there are many good textbooks in algebraic number theory that explain the theory of $p$-adic numbers. One also finds a short summary of the facts that we need here in [7]. We denote by $\hat{\mathbb{Z}}_p$ the ring of $p$-adic integers and by $\hat{\mathbb{Q}}_p$ the field of $p$-adic numbers. If $\hat{\mathbb{Q}}_p(\omega)$ is the splitting filed of $x^{v^*-1}$ over $\hat{\mathbb{Q}}_p[x]$ where $\omega$ is a primitive $v^*$-th root of unity, then the Galois group of $\hat{\mathbb{Q}}_p(\omega)/\hat{\mathbb{Q}}_p$ is cyclic with the Frobenius automorphism
\[\Psi : \hat{\mathbb{Q}}_p(\omega) \rightarrow \hat{\mathbb{Q}}_p(\omega)\]
\[\omega \mapsto \omega^p\]
as a generator. We call two elements $A = \sum a_g g$ and $B = \sum b_g g$ \textit{congruent modulo} $p_i$ ($A \equiv B \pmod{p^i}$) if $a_g \equiv b_g \pmod{p^i}$ for every $g \in G$ in the usual sense.