数理解析研究所講究録
第1687巻 2010年 71-76

Difference families and Frobenius groups

Marco Buratti*

March 15, 2010

Abstract

In his famous cyclotomic paper [9] R.M. Wilson gave a *difference family* construction over finite fields which was subsequently extended to commutative rings with unity by S. Furino [5].
Here we prove that the constructions of both Wilson and Furino are obtainable as special cases of a more general difference family construction over groups G admitting an automorphism group with suitable properties. In particular, we prove that the existence of a Frobenius group with abelian complement of order k and kernel G of order v implies the existence of a *disjoint* $(v, k, k-1)$ difference family over G. Equivalently, it implies the existence of a $(v, k, k-1)$ *near resolvable design* admitting G as an automorphism group acting sharply transitively on the points.

1 Preliminaries

This paper gives some difference family constructions in groups G exploiting suitable properties of $Aut(G)$, the automorphism group of G.
Our main result contains, as particular cases, a difference family construction over finite fields by R.M. Wilson [9] and its generalization over commutative rings with unity by S. Furino [5].
We shall use the following exponential notation. For $g \in G$ and $\phi \in Aut(G)$, the image of g under ϕ is denoted by g^{ϕ}. If Φ is a subset of $Aut(G)$, then g^{Φ} denotes the set $\{g^{\phi} \mid \phi \in \Phi\}$. Hence, in the case where Φ is a subgroup of $Aut(G)$, g^{Φ} is the orbit of g under Φ.
An element $\phi \in Aut(G)$ is said to be *semiregular* on G if it fixes only the identity element of G. A subset or multisubset Φ of $Aut(G)$ is *semiregular* on G if every $\phi \in \Phi - \{id_G\}$ is such.
Let G be a group and let A be a subgroup of $Aut(G)$. By $A.G$ we denote the group with elements in the cartesian product set $A \times G$ and composition law defined by the rule

$$(\alpha, x).(\beta, y) = (\alpha\beta, x^{\beta}y) \, \forall \alpha, \beta \in A, \forall x, y \in G.$$

If A is semiregular on G, then $A.G$ is said to be a *Frobenius group* with *kernel* G and *complement* A.

As a classical example of Frobenius group we may take the *group of affinities* of a finite field F_q, namely the group $A.G$ where G and A respectively are the additive and multiplicative group of F_q.
For general background on Frobenius groups see e.g. [7].

Throughout the paper, every union will be understood as *multiset union* and the union of μ copies of a multiset A will be denoted by ${}^{\mu}A$.
Given a subset B of a group G, by *list of differences* from B one means the multiset

$\Delta B = \{bc^{-1} \mid b, c \in B, b \neq c\}$ when G is multiplicative

or the multiset

$\Delta B = \{b - c \mid b, c \in B, b \neq c\}$ when G is additive.

Let R be a ring with unity and let $U(R)$ be the group of units of R. Of course $u \in U(R)$ may be considered as an automorphism of the additive group of R, the action of u being defined by $r^u = ru$ for any $r \in R$. We note that if B is a subset of $U(R)$, then to speak of ΔB is ambiguous. In fact in this case

*Dipartimento di Matematica e Informatica, Universita di Perugia, I-06123, Italy. Email: buratti@mat.uniroma1.it

both of the above expressions of ΔB make sense. To avoid this ambiguity, we denote them by $\Delta_U B$ and $\Delta_R B$ respectively.
We point out the following elementary observations.

Proposition 1.1 *Let R be a ring with unity. If B is a subset of $U(R)$ such that $\Delta_R B$ is also contained in $U(R)$, then $\Delta_U B$ is semiregular on the additive group of R.*

Proof. An element of $\Delta_U B$ is of the form bc^{-1} with b and c distinct elements of B. If we have $x(bc^{-1}) = x$ for some $x \in R$, then we have $xb = xc$ and hence $x(b-c) = 0$. But $b - c \in \Delta_R B \subset U(R)$ so that we necessarily have $x = 0$, i.e. x is the identity element of the additive group of R. □

Proposition 1.2 *If Φ is a subset of a group G such that $\Delta\Phi$ is semiregular on G, then any set of the form g^Φ with g a nonidentity element of G has the same size as Φ.*

Proof. It suffices to note that if g is a non-identity element of G, then for distinct elements ϕ and ψ of Φ we have $g^\phi \neq g^\psi$ otherwise $\phi\psi^{-1}$ should be an element of $\Delta\Phi$ fixing g. □

If $\mathcal{F}$ is a family of subsets of a group G then the list $\Delta\mathcal{F}$ of differences from $\mathcal{F}$ is defined by $\Delta\mathcal{F} = \bigcup_{F\in\mathcal{F}} \Delta F$.

A (v, k, λ) difference family (briefly DF) over a group G of order v is a multiset $\mathcal{F}$ of k-subsets of G called *base blocks* such that $\Delta\mathcal{F}$ covers $G - \{1\}$ exactly λ times. In other words, each element x of $G - \{1\}$ is representable in exactly λ ways in the form $x = ab^{-1}$ with both a and b belonging to some base block. Such a difference family generates the $2-(v, k, \lambda)$ design $(G, dev\mathcal{F})$ where $dev\mathcal{F}$ is the *development* of $\mathcal{F}$, i.e. the multiset defined by $dev\mathcal{F} = \{F + g \mid F \in \mathcal{F}, g \in G\}$.
A difference family is said to be *disjoint* when its base blocks are pairwise disjoint.

A group of *multipliers* of a difference family $\mathcal{F}$ over a group G, is a subgroup M of $Aut(G)$ such that $F^\mu \in dev\mathcal{F}$ for any $F \in \mathcal{F}$ and any $\mu \in M$.
It is straightforward to check that if M is a group of multipliers of $\mathcal{F}$, then $M.G$ is an automorphism group of $(G, dev\mathcal{F})$.

For general background on difference families one can see [1] or [2].

2 The theorem of Wilson

In his fundamental cyclotomic paper [9], R.M. Wilson proved the following result.

Theorem 2.1 *Let $k > 1$ and $\lambda > 0$ be integers such that 2λ is a multiple of either k or $k-1$. Then, for prime powers $q \geq k+1$, the necessary condition*

$$\lambda(q-1) \equiv 0 \,(\mathrm{mod}\, k(k-1))$$

for the existence of a (q, k, λ)-DF is also sufficient.

Observe that by replicating m times each base block of a (v, k, λ)-DF one obviously obtains a $(v, k, \lambda m)$-DF. With this in mind, it is easy to recognize that the above theorem may be equivalently formulated as follows.

Theorem 2.2 *For any prime power $q \geq k+1$ there exist $(q, k, e(k-1))$- and $(q, k+1, e(k+1))$-DF's where $e = \frac{k}{gcd(q-1,k)}$. Also, in the case of both q and k odd, there exist $(q, k, \frac{e(k-1)}{2})$- and $(q, k+1, \frac{e(k+1)}{2})$-DF's.*

Sketch of proof. Let F be a union of e distinct cosets of the group, say H, of $\frac{k}{e}$-roots of unity and let S be a set of representatives for the cosets of H. Then, $\mathcal{F} = \{sF \mid s \in S\}$ and $\mathcal{F}' = \{sF \cup \{0\} \mid s \in S\}$ are $(q, k, e(k-1))$- and $(q, k+1, e(k+1))$-DF's respectively.
When both q and k are odd we may take S of the form $S_1 \cup S_2$ with $|S_1| = |S_2| = \frac{|S|}{2}$. For $i = 1, 2$ the families $\mathcal{F}_i = \{sF \mid s \in S_i\}$ and $\mathcal{F}'_i = \{sF \cup \{0\} \mid s \in S_i\}$ are $(q, k, \frac{e(k-1)}{2})$- and $(q, k+1, \frac{e(k+1)}{2})$-DF's respectively. □

Note, in particular, that applying the above theorem with $q \equiv 3 \pmod 4$ and $k = \frac{q-1}{2}$ one recovers the $(q, \frac{q-1}{2}, \frac{q-3}{4})$ *Paley difference sets.*

3 The theorem of Furino

The difference family construction over finite fields by R.M. Wilson was extended to commutative rings with unity by S. Furino [5]. His main result may be reformulated as follows.

Theorem 3.1 *Let R be a commutative ring with unity, $|R| = v$, and let F be a k-subset of $U(R)$ which is union of e distinct cosets of a subgroup B of $U(R)$ (hence $|B| = k/e$). Let us denote by S a complete system of representatives for the B-orbits on $R - \{0\}$ (that is, S is a subset of R with the property that for any $r \in R - \{0\}$ there is exactly one pair $(s, b) \in S \times B$ such that $r = sb$). Then, in the hypothesis that $\Delta_R F \subset U(R)$, we have that the families $\mathcal{F} = \{sF \mid s \in S\}$ and $\mathcal{F}' = \{sF \cup \{0\} \mid s \in S\}$ respectively are $(v, k, e(k-1))$- and $(v, k+1, e(k+1))$-DF's over the additive group of R.*

Furino also observes that when k is odd and R has no involutions, then $\mathcal{F}$ and $\mathcal{F}'$ are splittable into two $(v, k, \frac{e(k-1)}{2})$- and $(v, k+1, \frac{e(k+1)}{2})$ difference families respectively.

4 A more general construction

We will recover both the constructions of Wilson and Furino as particular cases of the following new general construction.

Theorem 4.1 *Let $B.G$ be a Frobenius group with abelian complement B and kernel G of order v.*
Let C be the centralizer of B in $Aut(G)$ and let Φ be a k-subset of C which is union of e distinct cosets of B in C and such that $\Delta\Phi$ is semiregular on G.
Then there exist $(v, k, e(k-1))$- and $(v, k+1, e(k+1))$-DF's over G.
With the additional hypothesis that both v and k are odd and that G is abelian, the above difference families split into two $(v, k, \frac{e(k-1)}{2})$- and $(v, k+1, \frac{e(k+1)}{2})$ difference families, respectively.

Proof. Let S be a complete system of representatives for the B-orbits on $G - \{1\}$. We prove that $\mathcal{F} = \{s^\Phi | s \in S\}$ is a $(v, k, e(k-1))$-DF over G.
First of all, since $\Delta\Phi$ is semiregular on G, by Proposition 1.2, any member of $\mathcal{F}$ actually is a k-subset of G.
By definition, we have $\Phi = \Theta B$ where Θ is a set of e distinct representatives for the cosets of B in C.
It is easy to see that for any $s \in S$ we have

$$\Delta s^\Phi = \bigcup_{\substack{(\phi,\theta)\in\Phi\times\Theta \\ \phi\neq\theta}} [s^\phi (s^{-1})^\theta]^B$$

Hence we have:

$$\Delta\mathcal{F} = \bigcup_{s\in S} \Delta s^\Phi = \bigcup_{\substack{(\phi,\theta)\in\Phi\times\Theta \\ \phi\neq\theta}} \bigcup_{s\in S} [s^\phi (s^{-1})^\theta]^B$$

Now note that for any fixed pair $(\phi, \theta) \in \Phi \times \Theta$ with $\phi \neq \theta$ the list $\{s^\phi (s^{-1})^\theta \mid s \in S\}$ is a complete system of representatives for the B-orbits on $G - \{1\}$. To show this, it suffices to prove that if s and t are distinct elements of S, then $s^\phi (s^{-1})^\theta$ and $t^\phi (t^{-1})^\theta$ belong to distinct B-orbits. In fact, assuming the contrary, we would have $[s^\phi (s^{-1})^\theta]^\beta = t^\phi (t^{-1})^\theta$ for some $\beta \in B$ so that, taking into account that $\beta\phi = \phi\beta$ and $\theta\beta = \beta\theta$ since Φ is contained in the centralizer of B, we have $(t^{-1}s^\beta)^\phi = (t^{-1}s^\beta)^\theta$. Then, since B is semiregular on G and $\phi \neq \theta$, we have $t^{-1}s^\beta = 1$, i.e., $s^\beta = t$ which, by definition of S, would imply $s = t$, a contradiction.
By the above paragraph, for any pair $(\phi, \theta) \in \Phi \times \Theta$ with $\phi \neq \theta$ we have $\bigcup_{s\in S} [s^\phi (s^{-1})^\theta]^B = G - \{1\}$. Hence, since $|\{(\phi, \theta) \in \Phi \times \Theta \mid \phi \neq \theta\}| = e(k-1)$, we have $\Delta\mathcal{F} = {}^{e(k-1)}(G - \{1\})$, i.e. $\mathcal{F}$ is a $(v, k, e(k-1))$-difference family over G.
Now, let $\mathcal{F}'$ be the family obtained by appending the identity element of G to each base block of $\mathcal{F}$, namely $\mathcal{F}' = \{s^\Phi \cup \{1\} \mid s \in S\}$. We have:

$$\Delta\mathcal{F}' = \Delta\mathcal{F} \cup \bigcup_{s\in S}\{s, s^{-1}\}^{\Phi}$$

Recalling that $\Phi = B\Theta$, we have $\bigcup_{s\in S} s^{\Phi} = \bigcup_{s\in S}\bigcup_{\theta\in\Theta}(s^{\theta})^{B}$.

On the other hand it is easy to see that for any fixed $\theta \in \Theta$ the list $\{s^{\theta} \mid s \in S\}$ is a complete system of representatives for the B-orbits on $G - \{1\}$ so that $\bigcup_{s\in S}(s^{0})^{B} = G - \{1\}$. Hence, since $|\Theta| = e$, we have

$\bigcup_{s\in S}\bigcup_{\theta\in\Theta}(s^{\theta})^{B} = {}^{e}(G - \{1\})$.

It follows that $\bigcup_{s\in S}\{s, s^{-1}\}^{\Phi} = {}^{2e}(G - \{1\})$ and hence that $\Delta\mathcal{F}'$ covers $G - \{1\}$ exactly $e(k+1)$ times.

Now assume that kv is odd and that G is abelian. By the first hypothesis we can choose as system S of representatives for the B-orbits on $G - \{1\}$ a set of type $S_1 \cup S_2$ with $|S_1| = |S_2| = \frac{|S|}{2}$ and $S_2 = \{s^{-1} \mid s \in S_1\}$.

This is because if $s \in G - \{1\}$, then s and s^{-1} are in distinct B-orbits otherwise we should have $s^{\beta} = s^{-1}$ for a suitable $\beta \in B$. This would imply $s = (s^{\beta^{-1}})^{-1}$, i.e. $s^{\beta^{-1}} = s^{-1}$ so that, since B is semiregular on G, we would have $\beta = \beta^{-1}$. Hence $\beta = id_G$ or β is an involution. But $\beta = id_G$ would imply $s = s^{-1}$ which is absurd since v is odd and β cannot be an involution since k is odd.

We have $\mathcal{F} = \mathcal{F}_1 \cup \mathcal{F}_2$ where, for $i = 1, 2$, $\mathcal{F}_i = \{s^{\Phi} \mid s \in S_i\}$. Also, since G is abelian, we have $\Delta\mathcal{F}_1 = \Delta\mathcal{F}_2$. Then, since $\Delta\mathcal{F} = {}^{e(k-1)}(G - \{1\})$, we have $\Delta\mathcal{F}_i = {}^{e(k-1)/2}(G - \{1\})$ for $i = 1, 2$. This means that each $\mathcal{F}_i$ is a $(v, k, \frac{e(k-1)}{2})$-DF.

Analogously, it is easy to see that each of the families $\mathcal{F}'_i = \{s^{\Phi} \cup \{1\} \mid s \in S_i\}$, $i = 1, 2$ is a $(v, k+1, \frac{e(k+1)}{2})$-DF. □

Taking into account of Proposition 1.1, it is easy to see that the theorem of Furino is a particular case of the above theorem.

Applying Theorem 4.1 with $B = \{1\}$ we get the following corollary.

Corollary 4.2 *If G is a group of order v admitting a k-set Φ of automorphisms such that $\Delta\Phi$ is semiregular on G, then there exists a $(v, k, k(k-1))$-DF over G.*

Furino states the above corollary only in the case where G is the additive group of a commutative ring R with unity and Φ is a subset of $U(R)$.

Corollary 4.3 *Let $A.G$ be a Frobenius group with kernel G of order v and abelian complement A of order $\geq k$. Then there exist $(v, k, e(k-1))$- and $(v, k+1, e(k+1))$-difference families over G where $e = \frac{k}{gcd(k, |A|)}$.*

Proof. It suffices to apply Theorem 4.1 taking as B a subgroup of A of order $\frac{k}{e}$ (which exists since A is abelian and $\frac{k}{e}$ divides its order) and taking as Φ a union of e distinct cosets of B in A. □

Note that taking G and A as the additive and the multiplicative groups of a finite field, the above corollary gives exactly our equivalent reformulation of Theorem 2.2 of Wilson's Theorem 2.1.

A particular but remarkable case of Corollary 4.3 is the following.

Corollary 4.4 *If $A.G$ is a Frobenius group with kernel G of order v and abelian complement A of order k, then there exist $(v, k, k-1)$- and $(v, k+1, k+1)$-difference families over G.*

The following proposition, where we use the same notation as in Theorem 4.1, gives us more informations about the automorphism group of the designs associated with the obtained $(v, k, e(k-1))$- and $(v, k+1, e(k+1))$-DF's.

Proposition 4.5 *Let M be the normalizer of $< \Phi >$ in $Aut(G)$. Then both $(G, dev\mathcal{F})$ and $(G, dev\mathcal{F}')$ admit $M.G$ as an automorphism group.*

Proof. Let us consider, for instance, the design $(G, dev\mathcal{F})$. Let s^Φ be a block of $\mathcal{F}$, let $\mu \in M$, and let t be the element of S representing the B-orbit containing s^μ. Since M normalizes $< \Phi >$, we have $\Phi\mu = \mu\Phi$ so that $(s^\Phi)^\mu = (s^\mu)^\Phi = t^\Phi$ which also is a block of $\mathcal{F}$. It follows that M is a group of multipliers of $\mathcal{F}$ and hence that $M.G$ is a group of automorphisms of $(G, dev\mathcal{F})$. □

5 An application to near resolvable designs

We recall that a $(v, k, k-1)$-*near resolvable design* (briefly NRB) is a triple $(V, \mathcal{B}, \mathcal{R})$ where $(V, \mathcal{B})$ is a $2-(v, k, k-1)$ design and $\mathcal{R}$ is a partition of $\mathcal{B}$ (*near resolution*) into v classes (*near parallel classes*) each of which consists of $\frac{v-1}{k}$ pairwise disjoint blocks.

An automorphism group of such an NRB is a group of permutations on V leaving invariant $\mathcal{R}$. We say that $(V, \mathcal{B}, \mathcal{R})$ is *regular* over a group G if it admits G as an automorphism group acting regularly on the points.

It is an easy matter to prove the following proposition.

Proposition 5.1 *There exists a regular $(v, k, k-1)$-NRB over a group G if and only if there exists a disjoint $(v, k, k-1)$-DF over G.*
More precisely, the regular $(v, k, k-1)$-NRB's over G are, up to isomorphisms, all the triples of type $(G, dev\mathcal{F}, \mathcal{R})$ where $\mathcal{F}$ is a disjoint $(v, k, k-1)$-DF and $\mathcal{R} = \{\{Fg \mid F \in \mathcal{F}\} \mid g \in G\}$.

In view of the above proposition it is natural to say that a disjoint $(v, k, k-1)$-DF is the *starter parallel class* of its associated NRB.
Since the $(v, k, k-1)$-DF's of Corollary 4.4 are disjoint (their base blocks are the A-orbits on $G - \{1\}$) we may state the following theorem.

Theorem 5.2 *If there exists a Frobenius group with abelian complement A of order k and kernel G of order v, then there exists a regular $(v, k, k-1)$-NRB over G admitting the set of A-orbits on $G - \{1\}$ as a starter near parallel class.*

As a consequence, if v is an integer of the form $q_1 q_2 ... q_n$ where the q_i's are prime powers $\equiv 1 \pmod{k}$ then there exists a regular $(v, k, k-1)$-NRB over the additive group $G(v)$ of the *Galois ring* of order v, that is the direct product of the fields of orders $q_1, ..., q_n$. In fact it is easy to see that $G(v)$ possesses a semiregular group of automorphisms of order k.
This has been already observed by Furino [6] and it may be obtained also combining the theorem of Wilson 2.1 with a recursive technique making use of the concept of *difference matrix* [3]. But Theorem 5.2 allows to get many new NRB's, even over nonabelian groups. In fact, it is known that there exist Frobenius groups with abelian complement and nonabelian kernel (see, e.g. [8]).

Example 1.
Let $G = Z_4 \times Z_4$ and let α be the automorphism of G defined by $\alpha(x, y) = (y, 3x + 3y)$. One can see that the group $A = \{id, \alpha, \alpha^2\}$ generated by α acts semiregularly on $G - \{0\}$ so that $A.G$ is a Frobenius group.
Applying Theorem 5.2 we have that the set of A-orbits on $G - \{0\}$

$$\mathcal{F} = \Big\{01, 13, 30\}, \{10, 03, 31\}, \{11, 12, 21\}, \{20, 02, 22\}, \{23, 33, 32\}\Big\}$$

is the starter near parallel class of a regular (16,3,2)-NRB over G.

Example 2.
Let G be the additive group of the ring $R = M_{2\times 2}(Z_2)$ of square matrices of order 2 with entries in Z_2. Let $A = \left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}, \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\right\}$ be the subgroup of $U(R)$ generated by $\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}$. One can check that A is semiregular on G so that $A.G$ is a Frobenius group.
Then, applying Theorem 5.2 we have that

$$\mathcal{F} = \left\{ \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}, \left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}, \right.$$
$$\left\{ \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \right\}, \left\{ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\},$$
$$\left. \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \right\} \right\}$$

is the starter near parallel class of a regular (16,3,2)-NRB over G.

We finally point out that many regular $(q^2, k, k-1)$-NRB's over F_{q^2} with k a multiple of $q-1$ are obtainable using a difference family construction given in [4].

References

[1] R.J.R. Abel and M. Buratti, *Difference families*, Handbook of Combinatorial Designs, Second Edition, C.J. Colbourn and J.H. Dinitz (Editors), Chapman & Hall/CRC, Boca Raton, FL, 2006, 392-409.

[2] T. Beth, D. Jungnickel and H. Lenz, Design Theory. Cambridge University Press, 1999.

[3] M. Buratti, *Recursive constructions for difference matrices and relative difference families*, J. Combin. Designs **6** (1998), 165-182.

[4] M. Buratti, *Two new classes of difference families*, J. Combin. Theory A **90** (2000), 353-355.

[5] S. Furino, *Difference families from rings*, Discrete Math. **97** (1991), 177-190.

[6] S. Furino, *Existence results for near resolvable designs*, J. Combin. Designs **3** (1995), 101-113.

[7] D. Gorenstein, *Finite Groups*, Evanston-London Harper and Row Publ., New York, 1968.

[8] D.J.S. Robinson, *A Course in the Theory of Groups*, 2nd edition, Berlin, Springer, 1996.

[9] R.M. Wilson, *Cyclotomy and difference families in elementary abelian groups*, J. Number Theory **4** (1972), 17-47.