Factorisation of semiregular relative difference sets*

A. A. I. Perera† and K. J. Horadam

Department of Mathematics, RMIT University
Melbourne, VIC 3001, AUSTRALIA

Abstract

Pott has shown that the product of two semiregular relative difference sets in commuting groups E_1 and E_2 relative to their intersection subgroup C is itself a semiregular relative difference set in their amalgamated direct product. We generalise this result in the case that C is central in E_1 and in E_2 by using an equivalence with corresponding cocycles ψ_1 and ψ_2. We prove that in the central case the converse of this product construction holds: if there is a relative difference set in the central extension corresponding to $\psi_1 \otimes \psi_2$ it factorises as a product of relative difference sets in E_1 and E_2.

1 Introduction

Relative difference sets (RDSs) have been found by a number of techniques, and there are iterative methods which construct a larger relative difference set as the product of given smaller relative difference sets. For instance, an abelian RDS in E relative to a subgroup N may be (set-) multiplied by an abelian RDS in N relative to U to give an abelian RDS in E relative to the smaller subgroup U provided suitable parametric conditions on the RDSs hold (Pott [11, Prop. 3.2.1]). J. A. Davis [1] and A. Pott [11] have shown how to construct a RDS in a larger group relative to N by taking the product of RDSs in smaller groups relative to the same N, given suitable conditions on the groups. Recently Jungnickel and Tonchev [5] have shown that the former of these iterative techniques can sometimes be reversed when $U = 1$; that is, they give sufficient conditions under which a given difference set in E (an RDS relative to 1) factorises as a product of an RDS in E relative to N and a difference set in N.

*Presented in the Combinatorics Special Session, AMS/AustMS Joint Meeting, Melbourne, July 1999.

†Current address: Department of Mathematics, University of Peradeniya, Peradeniya, Sri Lanka.

Here we give sufficient conditions under which the second iterative technique can be reversed; that is, we show how to decompose a given RDS in E relative to N as a product of RDS in suitable subgroups of E, relative to N.

We work in the group algebra $R[G]$, where R is a commutative ring with identity and G is a finite group, and in the twisted group algebra $R^\alpha[G]$, where α is a cocycle over G. We will follow standard practice and identify any subset X of G with the group algebra element $X = \sum_{x \in X} x$ in $R[G]$. For more background on relative difference sets, the reader is referred to [11, 12], and on cocycles and twisted algebras, to [6, 7].

2 Product constructions for relative difference sets

Under certain conditions it is possible to multiply two relative difference sets together and obtain a new relative difference set in a larger group. Before we describe these constructions, let us recall the required definitions.

Definition 2.1 (Elliott and Butson [2]) A *relative* (v, w, k, λ)*-difference set* (RDS) in a finite group E of order vw relative to a normal subgroup N of order w, is a k-element subset D of E such that the multiset of quotients $d_1 d_2^{-1}$ of distinct elements d_1, d_2 of D contains each element of $E \backslash N$ exactly λ times, and contains no elements of N. (The ordinary (v, k, λ)-difference sets correspond to the case $N = 1$.)

It is easily seen that the definition of a relative difference set translates into an equation in the group algebra: D is a relative (v, w, k, λ)-difference set in E if and only if the following equation holds in $R[E]$:

$$DD^{(-1)} = k1_E + \lambda(E - N). \tag{1}$$

There is always a short exact sequence $1 \to N \to E \to E/N \to 1$. We will be concerned with relative difference sets having $k = v$ and therefore also $k = w\lambda$. A relative difference set with the latter property is termed *semiregular*. Note that any semiregular RDS in E relative to N is a transversal of N in E.

The simplest product construction for RDS is due to Davis [1, Theorem 2.1]: if E_1 has a (v_1, w, k_1, λ_1)-RDS D_1 with respect to N and $N \times E_2$ has a (v_2, w, k_2, λ_2)-RDS D_2 with respect to $N \times 1$ then the product $D_1 \times D_2$ is a $(v_1 v_2, w, k_1 k_2, \lambda_1 \lambda_2 w)$-RDS in $E = E_1 \times E_2$ relative to $N \times 1$.

When D_1 and D_2 are semiregular, so is $D_1 \times D_2$, and we will term this the *direct product* construction for semiregular RDS.

A slight generalisation of the direct product construction for semiregular RDS is due to Pott.

Proposition 2.1 (Pott [11, Lemma 2.2.3]) *Let E be a group of order $v_1 v_2 w$ containing a normal subgroup N of order w. Let E_1 and E_2 be subgroups of E of order $v_1 w$ and $v_2 w$, such that*

(i) $\langle E_1, E_2 \rangle = E$
(ii) $[E_1, E_2] = 1$ *(i.e. E_1 and E_2 commute.)*
(iii) $E_1 \cap E_2 = N$.

If E_i contains a $(v_i, w, v_i, v_i/w)$-difference set D_i relative to N, $i = 1, 2$, then

$$D_1 D_2 = \{d_1 d_2 : d_1 \in D_1, d_2 \in D_2\}$$

is a $(v_1 v_2, w, v_1 v_2, v_1 v_2/w)$-difference set in E relative to N. □

We will term this the *amalgamated direct product* construction of semiregular RDS. The choice of nomenclature is based on the next observation. Recall that if N is a subgroup of two groups E_1 and E_2, the *amalgamated direct product* of E_1 and E_2 with respect to N, denoted by $E_1 \curlyvee_N E_2$, is the group $E_1 \curlyvee_N E_2 = E_1 \times E_2/\widehat{N}$, where $\widehat{N}$ is the normal closure of $\{(n^{-1}, n) : n \in N\}$. If N is abelian and normal in each of E_1 and E_2, then $\widehat{N} = \{(n^{-1}, n) : n \in N\}$. If E is the group of Proposition 2.1, N is abelian, and E is isomorphic to the amalgamated direct product $E_1 \curlyvee_N E_2$ under the isomorphism defined by $e_1 e_2 \mapsto (e_1, e_2)\widehat{N}$.

In order to relate this to the cocyclic construction of semiregular RDS given in [10] we must restrict to *central* semiregular RDS; that is, those for which the forbidden subgroup N is central (hence abelian) in E, not just normal. This is only a restriction if we are interested in nonabelian RDS: in the abelian case, it is automatically satisfied. Any central semiregular RDS is isomorphic to one with a particularly simple form, which we can describe in terms of a corresponding *cocycle.*

3 Central semiregular relative difference sets

Hereafter, G will be a finite group of order v and C will be a finite abelian group of order w. A (2-dimensional) *cocycle* is a mapping $\psi : G \times G \to C$ satisfying the *cocycle equation*

$$\psi(g,h)\,\psi(gh,k) \;=\; \psi(g,hk)\,\psi(h,k), \quad \forall g,h,k \in G. \tag{2}$$

This implies $\psi(g,1) = \psi(1,h) = \psi(1,1)$, $\forall g,h \in G$, so we follow standard usage and consider only *normalised* cocycles, for which $\psi(1,1) = 1$.

An *extension* of C by G (sometimes called an extension of G by C) is a short exact sequence of groups

$$1 \to C \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1 \ . \tag{3}$$

Each cocycle ψ determines a *central* extension of C by G,

$$1 \to C \to E_\psi \to G \to 1,$$

in which the *extension group* E_ψ of order vw is the set $C \times G$ with ψ-twisted multiplication:

$$E_\psi = \{(c,g) : c \in C,\ g \in G\}\ ,\ (c,g)(d,h) = (cd\psi(g,h), gh), \tag{4}$$

and the image $C \times 1$ of C lies in the centre of E_ψ. The set $T(\psi) = \{(1, g),\ g \in G\}$ is a normalised transversal of $C \times 1$ in E_ψ. Conversely, if in (3), $\iota(C)$ is central in E, each normalised transversal $T = \{e_g : g \in G\}$ of C in E determines a cocycle ψ_T by $\psi_T(g, h) = \iota^{-1}(e_g e_h (e_{gh})^{-1}),\ g, h \in G$.

Theorem 3.1 (Canonical Form) [10, Theorem 3.1] *Suppose there is a central extension* (3) *of C by G. There exists a relative $(v, w, v, v/w)$-difference set in E relative to $\iota(C)$, if and only if there exists a cocycle $\psi : G \times G \to C$ such that $E \cong E_\psi$ and $T(\psi) = \{(1, g) : g \in G\}$ is a relative $(v, w, v, v/w)$-difference set in E_ψ, relative to $C \times 1$.* □

The cocycles for which such a central semiregular RDS exists have been characterised.

Definition 3.1 Let $w|v$. The cocycle $\psi : G \times G \to C$ is *orthogonal* if, for each $g \neq 1 \in G$ and each $c \in C$, $|\{h \in G : \psi(g, h) = c\}| = v/w$, or equivalently, if in $\mathbf{Z}C$, for each $g \neq 1 \in G$, $\sum_{h \in G} \psi(g, h) = v/w\ (\sum_{c \in C} c)$.

Theorem 3.2 (Equivalence Theorem) [10, Lemma 2.2, Theorem 4.1] *Let $w|v$ and let $\psi : G \times G \to C$ be a cocycle. Then $T(\psi) = \{(1, g),\ g \in G\} \subset E_\psi$ is a relative $(v, w, v, v/w)$-difference set relative to the central subgroup $C \times 1$, if and only if the cocycle ψ is orthogonal.* □

A cocycle is a *coboundary* $\partial\phi$ if it is derived from a set mapping $\phi : G \to C$ having $\phi(1) = 1$ by the formula $\partial\phi(g, h) = \phi(g)^{-1}\phi(h)^{-1}\phi(gh)$.

The orthogonal coboundaries correspond to the splitting RDS ([10, p. 196]).

Two cocycles ψ and ψ' are *cohomologous* if there exists a coboundary $\partial\phi$ such that $\psi' = \psi \cdot \partial\phi$. Two cohomologous cocycles ψ and ψ' are *shift equivalent* [3] if $\psi' = \psi \cdot \partial\psi_g$ for some $g \in G$, where $\psi_g(h) = \psi(g, h),\ \forall h \in G$.

Definition 3.2 If $\alpha : K \times K \to C$ and $\beta : H \times H \to C$ are cocycles, then their *tensor product* $\alpha \otimes \beta : (K \times H) \times (K \times H) \to C$ is the cocycle defined by

$$(\alpha \otimes \beta)\Big((k_1, h_1), (k_2, h_2)\Big) = \alpha(k_1, k_2)\beta(h_1, h_2). \tag{5}$$

We will simplify notation, without any loss of generality, by making the following identifications of elements in $E_{\alpha\otimes\beta}$ as needed, without further comment: $(a, (k, h)) \equiv (a, k, h)$ in $E_{\alpha\otimes\beta}$; $(a, k, 1) \equiv (a, k)$ in E_α; $(a, 1, h) \equiv (a, h)$ in E_β and $(a, 1, 1) \equiv a$ in C. Under these identifications, E_α and E_β are commuting subgroups of $E_{\alpha\otimes\beta}$ which intersect in the central subgroup C of $E_{\alpha\otimes\beta}$.

Lemma 3.1 *With the identifications above, $T(\alpha \otimes \beta) = T(\alpha)T(\beta)$ as sets in $E_{\alpha\otimes\beta}$.*

Proof: Note that $T(\alpha) \cap T(\beta) = \{(1,1,1)\}$ and $| T(\alpha \otimes \beta) | = | T(\alpha) | \, | T(\beta) |$.

$$\begin{aligned}(1,k,1)(1,1,h) &= ((\alpha \otimes \beta)((k,1),(1,h)),(k,1)(1,h)) \\ &= (\alpha(k,1)\beta(1,h),k,h) \\ &= (1,k,h)\end{aligned}$$

since α and β are normalised. □

It is readily checked that if α and β are orthogonal, so is $\alpha \otimes \beta$ (cf. [10, Theorem 5.1]). Consequently the product $T(\alpha \otimes \beta)$ of central semiregular RDSs $T(\alpha)$ in E_α and $T(\beta)$ in E_β is a central semiregular RDS in $E_{\alpha\otimes\beta}$. This is the same result as we obtain by applying the amalgamated direct product construction in the case that C is central in $E_{\alpha\otimes\beta}$ and using the Equivalence Theorem and the identifications above.

Using the Equivalence Theorem and applications of the Canonical Form, we obtain a slight generalisation of the amalgamated direct product construction for central semiregular RDS.

Lemma 3.2 (Central Extension Construction of RDS) *Let E_1 and E_2 be groups of order $v_1 w$ and $v_2 w$, respectively, with $w|v_1$ and $w|v_2$, for which there are central extensions*

$$1 \to C \xrightarrow{\iota_i} E_i \xrightarrow{\pi_i} G_i \to 1, \quad i = 1, 2.$$

If D_i is a $(v_i, w, v_i, v_i/w)$-difference set in E_i relative to $N_i = \iota_i(C)$, $i = 1, 2$, there is a relative $(v_1v_2, w, v_1v_2, v_1v_2/w)$-difference set $D \cong \pi_1(D_1) \times \pi_2(D_2)$ in a central extension of C by $G_1 \times G_2$.

Proof: Let $\psi_i : G_i \times G_i \to C$ be the orthogonal cocycles determined by the transversals D_i, $i = 1, 2$. Thus $\{(1, (\pi_1(d_1), \pi_2(d_2))),\ d_i \in D_i,\ i = 1, 2\}$ is an RDS in $E_{\psi_1\otimes\psi_2}$ relative to C. Let E be a central extension of C by $G_1 \times G_2$. For any isomorphism $\theta : E_{\psi_1\otimes\psi_2} \to E$ which preserves the image of C, the isomorphic image under θ of the canonical RDS is an RDS D in E relative to C. □

For central semiregular RDS, we can prove the converse of this central extension construction of RDS.

4 Factorisation of central semiregular RDS

¿From now on, R will denote a commutative ring with identity, with multiplicative group of units R^*, and we will assume $C \leq R^*$. We write the twisted group algebra $R^\alpha[G]$ as a free R-module with basis $\{\overline{g} : g \in G\}$. Multiplication is defined distributively from $\overline{g}\,\overline{h} = \alpha(g,h)\,\overline{gh}$, $\forall g, h \in G$.

Proposition 4.1 [7, cf. Proposition 1.3], [8, cf. Lemma 6.1].

Let K and H be finite groups, let $\alpha : K \times K \to C$ and $\beta : H \times H \to C$ be cocycles over K and H respectively, and let $\{\bar{k} : k \in K\}$ and $\{\bar{h} : h \in H\}$ be bases *for $R^{\alpha}[K]$ and $R^{\beta}[H]$ respectively. Then $R^{\alpha}[K]\otimes R^{\beta}[H]$ is a free R-module with basis $\{\bar{k}\otimes\bar{h} : k\in K, h\in H\}$ and the mapping $\theta(\overline{(k,h)}) = \bar{k}\otimes\bar{h}$ extends to an R-algebra isomorphism $\theta : R^{\alpha\otimes\beta}[K\times H]\to R^{\alpha}[K]\otimes R^{\beta}[H]$.* □

Theorem 4.1 (Factorisation) *Let $G = K\times H$ be a finite group with $|K| = v_1$ and $|H| = v_2$, let C be a finite abelian group of order w such that $w|v_1$ and $w|v_2$, and let $\alpha : K\times K\to C$ and $\beta : H\times H\to C$ be cocycles.*

If $T(\alpha\otimes\beta) = \{(1,g) : g\in G\}$ is a relative $(v_1v_2, w, v_1v_2, v_1v_2/w)$-difference set in $E_{\alpha\otimes\beta}$ relative to $C\times 1$, then $T(\alpha\otimes\beta)$ factorises as a product $T(\alpha)T(\beta)$ of RDSs; that is, $T(\alpha)$ is a relative $(v_1, w, v_1, v_1/w)$-difference set in E_α relative to $C\times 1$ and $T(\beta)$ is a relative $(v_2, w, v_2, v_2/w)$-difference set in E_β relative to $C\times 1$.

Proof: Take $R = \mathbf{Z}[C]$ and write $D = T(\alpha\otimes\beta)$. By Equation (1), in $R[E_{\alpha\otimes\beta}]$,

$$\begin{aligned} DD^{(-1)} &= v_1v_2.1_{E_{\alpha\otimes\beta}} + v_1v_2/w(E_{\alpha\otimes\beta} - C\times 1)\\ &= v_1v_2.1_{E_{\alpha\otimes\beta}} + v_1v_2/w\sum_{1\neq g\in G}\sum_{a\in C}(a,g).\end{aligned}$$

Since $\pi : R[E_{\alpha\otimes\beta}]\to R^{\alpha\otimes\beta}[G]$ defined by $(a,g)\to a\bar{g}$ is a ring homomorphism, in $R^{\alpha\otimes\beta}[G]$, D satisfies

$$\begin{aligned}\pi(DD^{(-1)}) &= v_1v_2\bar{1} + v_1v_2/w\sum_{1\neq g\in G}\sum_{a\in C} a\,\bar{g}\\ &= v_1v_2.\overline{(1,1)} + v_1v_2/w\sum_{(1,1)\neq(k,h)\in K\times H}\ \sum_{a\in C} a\,\overline{(k,h)}.\end{aligned}$$

So, by Proposition 4.1, in $R^{\alpha}[K]\otimes R^{\beta}[H]$,

$$\begin{aligned}\theta\circ\pi(DD^{(-1)}) &= v_1v_2(\bar{1}\otimes\bar{1}) + v_1v_2/w\sum_{(1,1)\neq(k,h)\in K\times H}\ \sum_{a\in C} a\,(\bar{k}\otimes\bar{h})\\ &= v_1v_2(\bar{1}\otimes\bar{1}) + v_1v_2/w\sum_{1\neq k\in K}\sum_{a\in C} a\,(\bar{k}\otimes\bar{1})\\ &\quad + v_1v_2/w\sum_{1\neq h\in H}\sum_{a\in C} a\,(\bar{1}\otimes\bar{h}) + v_1v_2/w\sum_{1\neq k\in K, 1\neq h\in H}\ \sum_{a\in C} a\,(\bar{k}\otimes\bar{h}).\end{aligned}$$

But $DD^{(-1)} = \sum_{(k,h)\in K\times H}\sum_{(k',h')\in K\times H}(1,(k,h))(1,(k',h'))^{-1}$ in $R[E_{\alpha\otimes\beta}]$. By (2) (compare with the proof of Lemma 4.1 of [10]), in $R^{\alpha\otimes\beta}[K\times H]$,

$$\begin{aligned}\pi(DD^{(-1)}) &= v_1v_2\overline{(1,1)} + \sum_{(1,1)\neq(k,h)}\Big(\sum_{(k',h')}(\alpha\otimes\beta)((k,h),(k',h'))^{-1}\Big)\overline{(k,h)}\\ &= v_1v_2\overline{(1,1)} + \sum_{(1,1)\neq(k,h)}\Big(\sum_{(k',h')}\alpha(k,k')^{-1}\beta(h,h')^{-1}\Big)\overline{(k,h)}.\end{aligned}$$

So, by Proposition 4.1, in $R^{\alpha}[K] \otimes R^{\beta}[H]$,

$$
\begin{aligned}
&\theta \circ \pi(DD^{(-1)}) \\
&= v_1 v_2(\bar{1} \otimes \bar{1}) + \textstyle\sum_{(1,1)\neq(k,h)} \left(\sum_{(k',h')} \alpha(k,k')^{-1}\beta(h,h')^{-1} \right) (\bar{k} \otimes \bar{h}) \\
&= v_1 v_2(\bar{1} \otimes \bar{1}) + \textstyle\sum_{1\neq k, 1\neq h} \left(\sum_{(k',h')} \alpha(k,k')^{-1}\beta(h,h')^{-1} \right) (\bar{k} \otimes \bar{h}) \\
&\quad + \textstyle\sum_{1\neq k} \left(\sum_{(k',h')} \alpha(k,k')^{-1}\beta(1,h')^{-1} \right) (\bar{k} \otimes \bar{1}) \\
&\quad + \textstyle\sum_{1\neq h} \left(\sum_{(k',h')} \alpha(1,k')^{-1}\beta(h,h')^{-1} \right) (\bar{1} \otimes \bar{h}) \\
&= v_1 v_2(\bar{1} \otimes \bar{1}) + \textstyle\sum_{1\neq k, 1\neq h} \left(\sum_{(k',h')} \alpha(k,k')^{-1}\beta(h,h')^{-1} \right) (\bar{k} \otimes \bar{h}) \\
&\quad + \textstyle\sum_{1\neq k} \left(v_2 \sum_{k'\in K} \alpha(k,k')^{-1} \right) (\bar{k} \otimes \bar{1}) + \sum_{1\neq h} \left(v_1 \sum_{h'\in H} \beta(h,h')^{-1} \right) (\bar{1} \otimes \bar{h}).
\end{aligned}
$$

Since $R^{\alpha}[K] \otimes R^{\beta}[H]$ is a free R-module, we can equate coefficients of basis elements, and since $v_1 \neq 0$ and $v_2 \neq 0$ in $R = \mathbf{Z}[C]$,

$$
\text{for each} \quad 1 \neq k \in K, \quad v_1/w\Big(\sum_{a\in C} a\Big) = \sum_{k'\in K} \alpha(k,k')^{-1} \quad \text{and}
$$

$$
\text{for each} \quad 1 \neq h \in H, \quad v_2/w\Big(\sum_{a\in C} a\Big) = \sum_{k'\in K} \beta(h,h')^{-1}.
$$

Hence the result follows from Definition 3.1 and Theorem 3.2. □

In terms of the corresponding cocycles, by Theorem 3.2 this means that $\alpha \otimes \beta$ is orthogonal if and only if α and β are both orthogonal. A direct proof of this result appears in Hughes [4, Thm. 4.iii].

With notation as in Theorem 4.1, suppose there is an isomorphism $\theta : E_{\alpha\otimes\beta} \to E$. Then $D^* = \theta(D)$ is a relative $(v_1 v_2, w, v_1 v_2, v_1 v_2/w)$-difference set in E relative to $\theta(C)$, and D^* factorises as $D^* = \theta(T(\alpha))\theta(T(\beta))$ into relative difference sets in $\theta(E_{\alpha\otimes 1})$ and $\theta(E_{1\otimes\beta})$ respectively. In particular, if $\theta \in Aut(E_{\alpha\otimes\beta})$ then the isomorphic relative difference set $\theta(D)$ factorises into relative difference sets in $\theta(E_{\alpha})$ and $\theta(E_{\beta})$.

Now suppose that $E = E_{\psi}$ for some cocycle ψ.

Case (i): ψ is cohomologous to $\alpha \otimes \beta$.

Since cohomology need not preserve orthogonality, ψ need not be orthogonal. Therefore, the relative difference set $D^* = \theta(D)$ in E_{ψ} corresponding to the relative difference set D in $E_{\alpha\otimes\beta}$ is not necessarily equivalent to the canonical transversal $T(\psi)$ corresponding to ψ. Hence $T(\psi)$ need not always factorise in E_{ψ}. Indeed, it need not be a relative difference set.

Case (ii): ψ is shift-equivalent to $\alpha \otimes \beta$.

By the proof of Theorem 3.3 of [3], the relation between the corresponding transversals is that $T(\psi)$ is a shift of $T(\alpha \otimes \beta)$, say $T(\psi) = e\,T(\alpha \otimes \beta)$ where $e \in E_{\alpha\otimes\beta}$. We will prove that $T(\psi)$ factorises.

Write $e = (c, (x, y))$, so if $(1, (k, h)) \in T(\alpha \otimes \beta)$, then

$$\begin{aligned}(c, (x, y))\,(1, (k, h)) &= (c\,(\alpha \otimes \beta)((x, y), (k, h)), (x, y)(k, h)) \\ &= (c\,\alpha(x, k)\beta(y, h), (xk, yh)) \\ &= (c\,\alpha(x, k), (xk, 1))(\beta(y, h), (1, yh)) \\ &= [(c,\ (x, 1))(1, (k, 1))]\,[(1, (1, y))(1, (1, h))].\end{aligned}$$

We can easily see that $(c, x)\,\{(1, k) : k \in K\}$ and $(1, y)\,\{(1, h) : h \in H\}$ are relative difference sets in E_α and E_β respectively, equivalent by a shift to $T(\alpha)$ and $T(\beta)$ respectively. Therefore $T(\psi) = e\,T(\alpha \otimes \beta)$ factorises, into the relative difference sets $(c, x)T(\alpha)$ and $(1, y)T(\beta)$.

In view of the remarks above, we have proved the following.

Lemma 4.1 *Under the conditions of Theorem 4.1, if $T(\alpha \otimes \beta)$ is a RDS then any element of its equivalence class factorises into RDSs in E_α and E_β.* □

Theorem 4.1 clearly extends by induction to a direct product of n finite groups.

Theorem 4.2 *Let $G = G_1 \times G_2 \times \cdots \times G_n$ where G_i is a finite group of order v_i and let C be a finite abelian group of order w such that $w|v_i$ for all $i = 1, 2, \cdots, n$. Let α_i be a cocycle over G_i, $i = 1, 2, \cdots, n$, and let $E_{\alpha_1 \otimes \alpha_2 \otimes \cdots \otimes \alpha_n}$ be the central extension of C by G corresponding to $\alpha_1 \otimes \alpha_2 \otimes \cdots \otimes \alpha_n$. If $D = \{(1, g) : g \in G\}$ is a relative $\left(\prod_{i=1}^n v_i, w, \prod_{i=1}^n v_i, (\prod_{i=1}^n v_i)/w\right)$-difference set in $E_{\alpha_1 \otimes \alpha_2 \otimes \cdots \otimes \alpha_n}$ relative to C, then D factorises as a product $T(\alpha_1)T(\alpha_2) \cdots T(\alpha_n)$ of RDSs; that is, for each $i = 1, 2, \cdots, n$, $T(\alpha_i)$ is a relative $(v_i, w, v_i, v_i/w)$-difference set in the central extension E_{α_i} of C by G_i, relative to C.* □

Let us now prove the converse of Pott's Proposition 2.1 in the case that C is central.

Theorem 4.3 *Let E be a group of order $v_1 v_2 w$ containing a central subgroup C of order w. Let E_1 and E_2 be subgroups of E of order $v_1 w$ and $v_2 w$ respectively with*
(i) $\langle E_1, E_2 \rangle = E$
(ii) $[E_1, E_2] = 1$ (i.e. E_1 and E_2 commute)
(iii) $E_1 \cap E_2 = C$,
and let D_1 be a transversal of C in E_1 and D_2 be a transversal of C in E_2. The transversal $D = D_1 D_2$ is a relative $(v_1 v_2, w, v_1 v_2, v_1 v_2/w)$-difference set in E relative to C if and only if D_1 is a relative $(v_1, w, v_1, v_1/w)$-difference set in E_1 relative to C and D_2 is a relative $(v_2, w, v_2, v_2/w)$-difference set in E_2 relative to C.

Proof: Let $E_1/C = K$ and $E_2/C = H$, $D_1 = \{e_k, k \in K\}$ and $D_2 = \{e_h, h \in H\}$. Let $\alpha : K \times K \to C$ be the cocycle determined by D_1 and let $\beta : H \times H \to C$ be the cocycle determined by D_2. The mapping $c\,e_k \to (c, k)$ gives an isomorphism $E_1 \to E_\alpha$ and the mapping $c\,e_h \to (c, h)$ gives an isomorphism $E_2 \to E_\beta$.

Furthermore, $E/C \cong K \times H$: consider the short exact sequences

$$1 \to C \to E_1 \to K \to 1 \text{ and } 1 \to C \to E_2 \to H \to 1.$$

These short exact sequences give the short exact sequence

$$1 \to C \times C \to E_1 \times E_2 \to K \times H \to 1.$$

Therefore, $1 \to C \curlyvee_C C \to E_1 \curlyvee_C E_2 \to K \times H \to 1$ is a short exact sequence, and the result follows from the fact that $C \curlyvee_C C \cong C$ and $E_1 \curlyvee_C E_2 \cong E$.

Consequently the mapping $c\, e_k\, e_h \to (c,(k,h))$ gives an isomorphism $E \to E_{\alpha\otimes\beta}$ which takes D to $\{(1,(k,h)) : k \in K,\ h \in H\}$. If D is a RDS in E, $\{(1,(k,h)) : k \in K,\ h \in H\}$ is a RDS in $E_{\alpha\otimes\beta}$ relative to $C \times 1$. By Theorem 4.1 there are RDSs $T(\alpha)$ in E_α and $T(\beta)$ in E_β. Their isomorphic inverse images in E_1 and E_2 are D_1 and D_2, respectively. □

We close with an application to the case $G = \mathbf{Z}_v^n$ for v odd. By using the Factorisation Theorem we can show that many non-splitting abelian extensions of $\mathbf{Z}_v$ by $\mathbf{Z}_v^n$, cannot contain a semiregular RDS.

Let $G = \mathbf{Z}_v^n$, $C = \mathbf{Z}_v$ and $\alpha_i : \mathbf{Z}_v \times \mathbf{Z}_v \to \mathbf{Z}_v$ be cocycles, $i = 1, 2, \cdots, n$, for v odd, and let E_α be the (necessarily abelian) central extension of $\mathbf{Z}_v$ by $\mathbf{Z}_v^n$ corresponding to $\alpha = \alpha_1 \otimes \alpha_2 \cdots \otimes \alpha_n$. ¿From (4) we see that E_α has exponent at most v^2. If $T(\alpha) = \{(1,g) : g \in G\}$ is a relative (v^n, v, v^n, v^{n-1})-difference set in E_α relative to $\mathbf{Z}_v$ then by Theorem 4.1, it factorises; that is, for each $i = 1, 2, \cdots n$, there exists a relative $(v, v, v, 1)$-difference set D_i in the central extension E_{α_i} of $\mathbf{Z}_v$ by $\mathbf{Z}_v$ relative to $\mathbf{Z}_v$. Therefore the α_i, for $i = 1, 2, \cdots, n$, are orthogonal cocycles, and by [10, Prop. 5.3] each α_i is a coboundary. It is then easy to check that α is a coboundary, so that $T(\alpha)$ is splitting.

We have proved the following Lemma.

Lemma 4.2 *Let $\alpha = \alpha_1 \otimes \alpha_2 \cdots \otimes \alpha_n$ where $\alpha_i : \mathbf{Z}_v \times \mathbf{Z}_v \to \mathbf{Z}_v$ is any cocycle, $1 \le i \le n$, and v is odd. If $T(\alpha)$ is a RDS in the abelian group E_α relative to $\mathbf{Z}_v$, then $E_\alpha \cong \mathbf{Z}_v^{n+1}$ and $T(\alpha)$ must be a splitting relative (v^n, v, v^n, v^{n-1})-difference set.* □

The total number of cocycles of the form $\alpha_1 \otimes \alpha_2 \cdots \otimes \alpha_n$ is only $(|\mathbf{Z}_v|^{v-1})^n = |v|^{nv-n}$. However, the total number of cocycles $\mathbf{Z}_v^n \times \mathbf{Z}_v^n \to \mathbf{Z}_v$ which determine abelian extension groups is $|\mathbf{Z}_v|^{|G|-1} = |v|^{v^n-1}$, and all of these abelian extension groups will have exponent at most v^2.

If $n > 1$, orthogonal cocycles which are not tensor products do exist, and equate with other relative (v^n, v, v^n, v^{n-1})-difference sets, including non-splitting RDS. For instance, all the abelian relative (p^2, p, p^2, p)-difference sets in $\mathbf{Z}_{p^2} \times \mathbf{Z}_p$ relative to $\mathbf{Z}_p$, for p an odd prime power, are characterised in [9, Theorem 3.2], and some of these are non-splitting. Each of these non-splitting abelian RDS corresponds to some orthogonal cocycle $\mathbf{Z}_p^2 \times \mathbf{Z}_p^2 \to \mathbf{Z}_p$, which by Lemma 4.2 cannot be a tensor product.

Acknowledgement. This work forms part of the Ph. D. thesis of the first author, taken under the supervision of the second author.

References

[1] J. A. Davis, A note on products of relative difference sets, *Des. Codes Cryptogr.* 1 (1991), 117–119.

[2] J. E. H. Elliott and A. T. Butson, Relative difference sets, *Illinois J. Math.* 10 (1966), 517–531.

[3] K. J. Horadam, Equivalence classes of central relative difference sets, *J. Combin. Designs* (2000), to appear.

[4] G. Hughes, Characteristic functions of relative difference sets, correlated sequences and Hadamard matrices, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, M. Fossorier et al (eds), Lecture Notes in Computer Science 1719, Springer, 1999.

[5] D. Jungnickel and V. D. Tonchev, Decompositions of difference sets, *J. Algebra* 217 (1999), 21–39.

[6] G. Karpilovsky, *Projective Representations of Finite Groups*, Marcel Dekker, New York, 1985.

[7] G. Karpilovsky, *Algebraic Structure of Crossed Products*, North- Holland, 1987.

[8] G. Karpilovsky, *Group Representations Vol. 2*, Elsevier, North- Holland, 1993.

[9] S.-L. Ma and A. Pott, Relative difference sets, planar functions and generalised Hadamard matrices, *J. Algebra* 175 (1995), 505–525.

[10] A. A. I. Perera and K. J. Horadam, Cocyclic generalised Hadamard matrices and central relative difference sets, *Des. Codes Cryptogr.* 15 (1998) 187–200.

[11] A. Pott, *Finite Geometry and Character Theory*, LNM 1601, Springer, Berlin, 1995.

[12] A. Pott, A survey on relative difference sets, in *Groups, Difference Sets and the Monster*, K. T. Arasu et al, Eds, de Gruyter, Berlin (1996), pp. 195–232.

(Received 4/10/99)