Construction of association schemes from difference sets

Sejeong Bang¹, Mitsugu Hirasaka²

¹Com2MaC, Pohang University of Science and Technology San 31, Hyoja-dong, Namgu, Pohang, 790-784, Republic of Korea
²Department of Mathematics College of Science, Pusan National University Kamjung, Pusan 609-735, Republic of Korea

Received 31 August 2003; received in revised form 1 February 2004; accepted 6 February 2004
Available online 10 March 2004

Abstract

Let $H$ and $F$ be two finite groups. In group theory it is known that an extension $G$ of $H$ by $F$ is characterized by the action of $F$ on $H$ and a factor set associated with the action, and the two-dimensional cohomology group with respect to the action is defined when $H$ is Abelian. In this paper we consider an analogy of the above for association schemes and construct such extensions of association schemes from a difference set when $H$ is an elementary Abelian group.

© 2004 Elsevier Ltd. All rights reserved.

1. Introduction

Let $\Gamma$ be a transitive permutation group on a finite set $X$. Then $\Gamma$ acts on $X \times X$ by its entrywise action, i.e. $(x, y)^\gamma := (x^\gamma, y^\gamma)$ for all $x, y \in X$ and $\gamma \in \Gamma$. We call an orbit of $\Gamma$ on $X \times X$ an orbital, and denote by $G_\Gamma$ the set of the orbitals. It is well known (for example, see [2]) that $G_\Gamma$ satisfies the following conditions:

(i) The diagonal set $1_X := \{(x, x) | x \in X\}$ is a member of $G_\Gamma$;
(ii) For each $g \in G_\Gamma$ $g^* := \{(x, y) | (y, x) \in g\}$ is a member of $G_\Gamma$;
(iii) For all $d, e, f \in G_\Gamma |xd \cap ye^*|$ is constant whenever $(x, y) \in f$ where $zr := \{w \in X | (z, w) \in r\}$ for each $z \in X$ and each $r \subseteq X \times X$, so that it is denoted by $a_{def}$.

The numbers $\{a_{def} | d, e, f \in G\}$ are called the intersection numbers.

E-mail addresses: sejong@euclid.postech.ac.kr (S. Bang), hirasaka@pusan.ac.kr (M. Hirasaka).
Let $G$ be a partition of $X \times X$ which does not contain the empty set, namely, a set of disjoint binary relations on $X$ whose union covers $X \times X$. We say that $(X, G)$ is an association scheme (or shortly scheme) if it satisfies the above three conditions replaced $G \Gamma$ by $G$. Taking such a view we can say that an association scheme is an object to generalize the orbitals of a transitive permutation group, which is a proper class of schemes called Schurian. The problem of determining whether or not a given class of schemes is Schurian has been discussed in a number of articles with various kinds of forms, for example, a series of characterizations of distance-regular graphs by its intersection numbers (see [3]). In this paper we consider extensions of schemes derived from two finite groups, and aim to take a general view of them. The following theorem is what we will generalize to association schemes:

**Theorem 1.1** (Theorem 7.6, [7]). Let $H$ and $F$ be two finite groups and $\{f(\sigma, \tau)\}$ be a factor set belonging to a family $\{T(\sigma)\}$ of automorphisms of $H$. Then, there is an extension $G$ of $H$ by $F$ such that, for a suitable choice of a transversal of $H$, $f$ is a factor set associated with the extension $G$.

Throughout this paper we use the same notation and terminology as given in [9]. For the remainder of this section we assume that $(X, G)$ is an association scheme.

First, we introduce a concept on schemes corresponding to a binary operation in group theory. For each $g \in G$ we define the adjacency matrix $A_g$ whose columns and rows are indexed by the elements of $X$ as follows:

$$(A_g)_{x, y} := \begin{cases} 1 & \text{if } (x, y) \in g \\ 0 & \text{otherwise.} \end{cases}$$

It is well known that the vector space over the complex field spanned by $\{A_g \mid g \in G\}$ forms a semisimple subalgebra of the full matrix algebra of degree $|X|$. We denote the subalgebra by $A$. Each element $\alpha \in A$ can be written as a linear combination of $\{A_g \mid g \in G\}$, so we define the support of $\alpha = \sum_{g \in G} a_g A_g$ to be $\{g \in G \mid a_g \neq 0\}$. Here we define the complex product on the power set $\mathcal{P}(G)$ of $G$ as follows:

$$\mathcal{P}(G) \times \mathcal{P}(G) \to \mathcal{P}(G), \quad (D, E) \mapsto DE,$$

where $DE := \bigcup_{d \in D, e \in E} de$ and $de := \{f \in G \mid a_{de} \neq 0\}$ and a singleton $\{g\}$ is often abbreviated as $g$ in the complex product. Taking an algebraic view the complex product $DE$ is the support of $A_DA_E$ where $A_F := \sum_{f \in F} A_f$ for each $F \subseteq G$, so that the complex product is associative and the singleton $\{1_X\}$ is the identity. Note that the complex product of two singletons of $G$ is not necessarily a singleton in general. The following is an example of schemes in which the complex product can be regarded as a binary operation on the set of binary relations:

\footnote{The notation $(X, \{R_i\}_{0<i<d})$ used to express an association scheme is given in many articles, and many readers must be familiar with the notation. Actually, it is very useful and powerful to use it when we need not rename the numbering of the relations like association schemes derived from distance-regular graphs. On the other hand, the notation given in Zieschang is derived from group theory and has an advantage when we deal with imprimitive blocks of association schemes and its quotients (see [2] or [9]). That is the reason why we use this notation in this paper, while these notations are essentially the same.}
Example 1.1. Let \( \Gamma \) be a finite group acting on itself by the right multiplication. Then \((\Gamma', G_{\Gamma'})\) forms an association scheme each of whose adjacency matrices is a permutation matrix, equivalently, \(G_{\Gamma}'\) forms a group isomorphic to \(\Gamma'\) with respect to the complex product. We call such a scheme thin.

Second, we introduce a concept on schemes corresponding to groups in group theory. For each \(D \subseteq G\) we set \(n_D := \sum_{d \in D} n_d\) called the valency of \(D\), where \(n_d := a_{dd^*1_x}\) is the constant rowsum of \(A_d\).

The following lemma shows that the ordinary product of two subsets of a group coincides with the complex product of the corresponding subsets of \(G_{\Gamma}\) in Example 1.1.

Lemma 1.2 ([1]). Let \((X, G)\) be an association scheme. For all \(d, e \in G\) with we have \(|de| \leq \gcd(n_d, n_e)\). In particular, a thin closed subset forms a group with respect to the complex product.

Third, we introduce a concept on schemes corresponding to subgroups in group theory. We say that a subset \(F\) of \(G\) is closed if \(\bigcup_{f \in F} f\) is an equivalence relation on \(X\), equivalently, \(A_F A_F = n_F A_F\), or, \(FF \subseteq F\).

Example 1.2. Clearly, \(G\) is closed, and so is \(\{1_X\}\). The subset \(T_G := \{t \in G \mid n_t = 1\}\) is a closed subset forming a group with respect to the complex product. We say that a closed subset \(F\) is thin if \(F\) is contained in \(T_G\).

For each closed subset \(F\) of \(G\) and \(x \in X\) the pair \((xF, (f_x)_{f \in F})\) forms an association scheme called the subscheme with respect to \(F\) and \(x\) denoted by \((X, G)_{xF}\). For all \(x, y \in X\) and each closed subset \(F\) if \((X, G)\) is Schurian, but it does not hold in general (see [6] for the details).

Fourth, we introduce a concept on schemes corresponding to quotient groups in group theory. Setting \(X/F := \{xF \mid x \in X\}\) and \(G/F := \{gF \mid g \in G\}\) where \(gF := \{xF, yF\} \cap f (see [9])\). Note that \((X, G)_{xF} \simeq (X, G)_{yF}\) for all \(x, y \in X\) and each closed subset \(F\) if \((X, G)\) is Schurian, but it does not hold in general (see [6] for the details).

Example 1.3. In Example 1.1 each subgroup \(\Delta\) of \(\Gamma\) induces the corresponding closed subset \(G_{\Delta}\) in \(G_{\Gamma}\). Then the factor scheme of \((\Gamma, G_{\Gamma})\) over \(G_{\Delta}\) is isomorphic to the orbitals of \(\Gamma\) acting on the right cosets \(\Gamma/\Delta\) by the right multiplication. Thus, we see that \((X, G)\) is Schurian if and only if \((X, G)\) is a factor scheme of a thin association scheme.

From now on we will show a way to generalize an extension of groups to that of association schemes. Let \((X, G), (Y, H)\) and \((Z, F)\) be three association schemes. We say that \((X, G)\) is an extension of \((Y, H)\) by \((Z, F)\) if there exists a closed subset \(N\) of \(G\) and \(x \in X\) such that \((Y, H) \simeq (X, G)_{xN}\) and \((Z, F) \simeq (X/N, G\|N)\). In short we say that \((X, G)\) is an extension of \(H\) by \(F\) if \(H, F\) are thin. In this paper we focus only on extensions of \(H\) by \(F\) where \(F\) and \(H\) are thin, namely, an extension of a group by another group, though it might be possible and deserved to consider other kinds of extensions. Here we will show some examples of extensions of \(H\) by \(F\).
Example 1.4. Let \( G \) be a finite group and \( H \trianglelefteq G \). For each \( g \in G \) we set \( \tilde{g} := \{(a, b) \in G \times G \mid ab^{-1} = g\} \). Then \((G, \{\tilde{g}\}_{g \in G})\) is an extension of \( H \) by \( F := G/H \).

Example 1.5. Let \( H \) and \( F \) be two finite groups. Then the orbitals of the standard wreath product of \( H \) by \( F \) is an extension of \( H \) by \( F \) (see [7] for the definition of the standard wreath product).

Example 1.6. Let \( G \) be a finite group, \( H \trianglelefteq G \) and \( H \leq M \leq G \). For each \( g \in G - M \) we define \( \tilde{g} := \{(a, b) \in G \times G \mid ab^{-1} \in Hg\} \). Then \((G, \{\tilde{g}\}_{g \in M} \cup \{\tilde{g}\}_{g \in G - M})\) is an extension of \( H \) by \( F := G/H \).

Note that Example 1.6 is the same as Example 1.4 if \( M = G \), and the same as Example 1.5 if \( M = H \). In addition, these three examples are Schurian (see [6] for the proof). The following example shows that there exists an extension of \( H \) by \( F \) which is not Schurian.

Example 1.7. In [4] the list of association schemes with at most 28 points is released. The association schemes indexed by as-28.no.175 and as-28.no.176 in the list are extensions of \( \mathbb{Z}_2 \times \mathbb{Z}_2 \) by \( \mathbb{Z}_7 \). These have the same intersection numbers, and as-28.no.175 is Schurian, but as-28.no.176 is not so.

Our study was started from the question whether as-28.no.176 is quite exceptional, otherwise, there is a systematic way to construct non-Schurian extensions like as-28.no.176. The question is related to the study of \( p \)-schemes, that are association schemes \((X, G)\) such that \(|X| \prod_{g \in G} n_g \) is a power of a prime \( p \). The authors were trying to classify \( p \)-schemes with \( p^3 \) points. Though the attempt was far from a success, it provided the idea to derive the construction given in this paper. In conclusion we have a construction including Example 1.7, which can be generalized to an extension of an elementary Abelian group by any finite group.

In this paper we prepare the notation in Section 2, give a way to generalize Theorem 1.1 in Section 3, introduce D-sequences in Section 4, show a construction including Example 1.7 in Section 5, and apply our results for \( p \)-schemes in Section 6.

2. Preliminary

In this paper we shall write the two function composite following the method given in [7], i.e. the composite \( fg \) of two functions \( f \) and \( g \) is defined such that \((fg)(x) := g(f(x)) \) for each \( x \in X \).

For the remainder of this paper we assume that \( H \) is a finite group and \( \mathcal{P}(H) \) is the power set of \( H \). If \( f \in \text{Aut}(H) \), then

\[
\begin{align*}
    f(A \cup B) &= f(A) \cup f(B), \\
    f(AB) &= f(A)f(B), \\
    f(H) &= H
\end{align*}
\]

for all \( A, B \in \mathcal{P}(H) \). Now we consider a generalization of automorphisms on a group to that on the power set of the group. We say that \( g : \mathcal{P}(H) \to \mathcal{P}(H) \) is an automorphism on \( \mathcal{P}(H) \) if it satisfies (1). Clearly, any automorphism on \( H \) induces the automorphism on \( \mathcal{P}(H) \), and the map from all subsets except the empty set to \( H \) is also an automorphism on \( \mathcal{P}(H) \). We denote the set of automorphisms on \( \mathcal{P}(H) \) by \( \text{SAut}(H) \). The following
lemma shows that there is a one-to-one correspondence between $\text{SAut}(H)$ and the set of all isomorphisms among the quotients group of $H$.

**Lemma 2.1.** Let $U, V$ be normal subgroups of $H$ such that $H/U \cong H/V$. Then, for any group isomorphism $f : H/U \to H/V$ there exists a unique $\tilde{f} \in \text{SAut}(H)$ such that $\tilde{f}(a) = f(aU)$ for each $a \in H$. Conversely, for any $g \in \text{SAut}(H)$ there exists a unique isomorphism $\tilde{g} : H/\text{Kerg} \to H/g(1)$ such that $\tilde{g}(a\text{Kerg}) = g(a)$ for each $a \in H$ where $1$ is the identity of $H$ and $\text{Kerg} := \{a \in H \mid g(1) = g(a)\}$.

**Proof.** It is routine to check that the restriction on the singletons has a unique extension on $\mathcal{P}(H)$ since any nonempty subset is the union of singletons, and that the extended one satisfies (1).

We will now prove the second part.

First, we claim that $g(1) \trianglelefteq H$. Since $g \in \text{SAut}(H)$, $g(1)g(1) = g(1 \cdot 1) = g(1)$. It follows from $|H| < \infty$ that $g(1)$ is a subgroup of $H$. For each $b \in H$ we have $g(b)g(b^{-1}) = g(1)$, whence, $|g(b)| \leq |g(1)|$. Combining it with the fact that $g(b) = g(b)g(1) = g(1)g(b)$ we conclude that $g(b)$ is a coset of $g(1)$. Since $g(H) = H$, for each $a \in H$ there exists $b \in H$ such that $a \in g(b)$. Thus, $ag(1) = g(b)g(1) = g(b) = g(1)g(b) = g(1)a$. This implies that $g(1) \trianglelefteq H$.

Second, we claim that $\text{Kerg} \trianglelefteq H$. For all $a, b \in \text{Kerg}$ we have

$$g(ab) = g(a)g(b) = g(1)g(1) = g(1).$$

Since $|H| < \infty$, it follows that $\text{Kerg}$ is a subgroup of $H$. For each $c \in \text{Kerg}$ and $a \in H$ we have

$$g(a^{-1}ca) = g(a^{-1})g(c)g(a) = g(a^{-1} \cdot 1 \cdot a) = g(1).$$

This implies that $\text{Kerg} \trianglelefteq H$.

If $a\text{Kerg} = b\text{Kerg}$, then $a = bc$ for some $c \in \text{Kerg}$, and

$$g(a) = g(bc) = g(b)g(c) = g(b)g(1) = g(b).$$

Therefore, $\tilde{g}$ is well defined. It is clear that $\tilde{g}(ab\text{Kerg}) = g(ab) = g(a)g(b) = \tilde{g}(a\text{Kerg})\tilde{g}(b\text{Kerg})$ for all $a, b \in H$. If $\tilde{g}(a\text{Kerg}) = \tilde{g}(b\text{Kerg})$, then $g(a) = g(b)$, whence,

$$g(ab^{-1}) = g(ab)g(b^{-1}) = g(b)g(b^{-1}) = g(bb^{-1}) = g(1).$$

This implies that $ab^{-1} \in \text{Kerg}$. Therefore, $\tilde{g}$ is injective. Since it is clear that $\tilde{g}$ is surjective, we conclude that $\tilde{g}$ is a group isomorphism. ☐

By Lemma 2.1, each $f \in \text{SAut}(H)$ induces a group isomorphism $\tilde{f} : H/\text{Kerf} \to H/f(1)$. Since $\tilde{f}^{-1}$ is also a group isomorphism from $H/f(1)$ to $H/\text{Kerf}$, it induces $\tilde{f}^{-1} \in \text{SAut}(H)$, denoted by $f^*$.

For each $A \in \mathcal{P}(H)$ we set $R(A) : \mathcal{P}(H) \to \mathcal{P}(H)$ by $B \mapsto R(A)(B) := BA$, and $L(A) : \mathcal{P}(H) \to \mathcal{P}(H)$ by $B \mapsto L(A)(B) := AB$. For each coset $C$ of a normal subgroup in $H$ we set $I(C) : \mathcal{P}(H) \to \mathcal{P}(H)$ by $B \mapsto I(C)(B) := C^{-1}AC$. Then $I(C) \in \text{SAut}(H)$.

Let $(X, G)$ be an association scheme. According to [8] we say that $Y \subseteq X$ if $X$ is a *transversal* of a closed subset $F$ in $X$ if $Y$ is a complete set of representatives of the
equivalence relation induced by \( F \). We say that \( T \subseteq G \) is a transversal of \( F \) in \( G \) if 
\[ FtF \cup FsF = \emptyset \]
for all \( s, t \in T \) with \( s \neq t \) and \( \bigcup_{t \in F} FtF = G \).

3. Analogy of group theory

Throughout this section we assume that \( F \) and \( H \) are two finite groups, and denote the identity of \( F \) and \( H \) by \( 1_F \) and \( 1_H \), respectively.

Let \((X, G)\) be an extension of \( H \) by \( F \). Then there exists a thin closed subset \( N \) of \( G \) such that \( N \cong H \) and \( G//N \cong F \) are groups. For convenience we identify \( N \) with \( H \), namely, we assume that \( G \) has a thin closed subset \( H \) with \( G//H \cong F \).

According to [9], for each \( g \in G \) we have
\[ g^*Hg = H, \quad gH = Hg, \quad gg^* = \{g\}, \quad gg^* \leq H \] (2)
under the complex product. Since \( G//H \cong F \), we can take a transversal of \( H \) in \( G \) according to the ordering of the elements of \( F \), i.e. \( G \) is the disjoint union of \( \{t_\sigma H \mid \sigma \in F\} \) so that
\[ t_\sigma t_\tau H = t_{\sigma \tau} H \quad \text{for all} \ \sigma, \tau \in F. \] (3)

For convenience we assume that
\[ t_1F = 1_X. \] (4)

For each \( \sigma \in F \) \( t_\sigma \) induces \( T_\sigma : \mathcal{P}(H) \to \mathcal{P}(H) \) such that
\[ T_\sigma (A) := t_\sigma^* A t_\sigma \quad \text{for each} \ \ A \in \mathcal{P}(H). \] (5)

The property (2) guarantees that \( T_\sigma \) is well defined and \( T_\sigma \in \text{SAut}(H) \) as follows:
\[ g^* ABg = g^* Abg^*g = g^* Agg^*Bg. \]

Combining Lemma 1.2 with (3), we obtain that, for all, \( \sigma, \tau \in F \) there exists \( E_{\sigma, \tau} \in \mathcal{P}(H) \) such that
\[ t_\sigma t_\tau = t_{\sigma \tau} E_{\sigma, \tau}. \] (6)

If \( G \) is thin, then \( E_{\sigma, \tau} \) is uniquely determined as \( t_{\sigma \tau}^* t_\sigma t_\tau \), and the set \( \{E_{\sigma, \tau} \mid \sigma, \tau \in F\} \) forms a factor set belonging to \( \{T_\sigma \mid \sigma \in F\} \subseteq \text{Aut}(H) \) in the sense of [7]. However, the same argument would not be suited for general cases since the set \( \{E_{\sigma, \tau} \mid \sigma, \tau \in F\} \) does not always induce a way to partition \( X \times X \) into binary relations.

For each \( \sigma \in F \) we take \( x_\sigma \in X \) such that
\[ (x_1F, x_\sigma) \in t_\sigma. \]

Then \( \{x_\sigma \mid \sigma \in F\} \) is a transversal of \( H \) in \( X \). Here we introduce \( f : F \times F \to H ((\sigma, \tau) \mapsto f_{\sigma, \tau}) \), which corresponds to the concept of a factor set in [7], so that
\[ x_{\sigma} f_{\sigma, \tau} x_{\tau} \in x_\sigma t_\sigma^{-1} t_\tau \quad \text{for all} \ \sigma, \tau \in F. \] (7)

Lemma 3.1. Let \( T : F \to \text{SAut}(H) \) and \( f : F \times F \to H \) be given in the above. Then we have the following:
(i) \( T_{1_F} \) is the identity map on \( \mathcal{P}(H) \);
(ii) For each \( \sigma \in F \) we have \( T_{\sigma^{-1}}(1_H) = \text{Ker}T_\sigma \);
(iii) For all \( \sigma, \tau \in F \) there exists a coset \( C_{\sigma, \tau} \) of \( (T_\sigma T_\tau)(1_H) \) in \( H \) such that \( T_\sigma T_\tau = T_{\sigma T_\tau}(C_{\sigma, \tau}) \);
(iv) For each \( \sigma \in F \) we have \( f_{\sigma, \sigma} = 1_H \).
(v) For all \( \sigma, \tau \in F \) there exists \( E_{\sigma, \tau} \in \mathcal{P}(H) \) such that \( T_\sigma L(f_{\rho, \rho \sigma})T_\tau L(f_{\rho \sigma, \rho \sigma \tau}) = T_{\sigma T_\tau}(f_{\rho, \rho \sigma T_\tau}(E_{\sigma, \tau})) \) for each \( \rho \in F \).

**Proof.**

(i) Since \( t_{1_F} = 1_H \), \( T_{1_F} \) is the identity map.

(ii) By (3) and (4), \( t_\sigma t_{\sigma^{-1}}, t_{\sigma^{-1}} t_\sigma \leq H \). Thus, \( t_{\sigma^{-1}} H = t_\sigma^* H \), i.e. \( t_{\sigma^{-1}} = t_\sigma^* h \) for some \( h \in H \). It follows from \( t_\sigma^* t_\sigma \leq H \) that

\[ T_{\sigma^{-1}}(1_H) = (t_\sigma^*)^* h^* h = h^* t_\sigma^* h = t_\sigma t_\sigma^* \subseteq \text{Ker}T_\sigma. \]

Note that \( h = x_\sigma f_{\sigma, \sigma} \), \( h \in \mathcal{P}(H) \).

We claim that \( C_{\sigma, \tau} := \langle t_\sigma t_\tau \rangle \), \( C_{\sigma, \tau} \) is the identity map on \( \mathcal{P}(H) \).

((iii)) Set \( C_{\sigma, \tau} := \langle t_\sigma t_\tau \rangle \). Then, by (2) and (6)

\[ t_\tau C_{\sigma, \tau} = t_\tau (t_\tau^* t_\tau E_{\sigma, \tau}) = t_\tau E_{\sigma, \tau} \leq t_\tau. \]

We claim that \( C_{\sigma, \tau} \) is a coset of \( (T_\sigma T_\tau)(1_H) \). By definition of \( T_\sigma T_\tau \),

\[ (T_\sigma T_\tau)(1_H) = C_{\sigma, \tau} \leq (T_\sigma T_\tau)(1_H). \]

Thus, \( C_{\sigma, \tau} \) is a coset of \( (T_\sigma T_\tau)(1_H) \). By definition of \( C_{\sigma, \tau} \),

\[ C_{\sigma, \tau} = (T_\sigma T_\tau)(1_H) \leq (T_\sigma T_\tau)(1_H). \]

Therefore, \( C_{\sigma, \tau} = (T_\sigma T_\tau)(1_H) \). By a direct calculation, we have

\[ C_{\sigma, \tau} C_{\sigma, \tau} = C_{\sigma, \tau}. \]

This implies that \( C_{\sigma, \tau} \) is a coset of \( (T_\sigma T_\tau)(1_H) \).

(iv) Since \( x_\sigma f_{\sigma, \sigma} \in x_\sigma t_{\sigma^{-1}} \), it follows from (4) that \( f_{\sigma, \sigma} \) must be 1_H.

(v) By (6), \( t_\sigma t_\tau = t_\tau E_{\sigma, \tau} \). This implies that, for each \( \rho \in F \) and \( h \in H \),

\[ x_\rho h t_\sigma t_\tau = x_\rho h t_\tau E_{\sigma, \tau}. \]

It follows from (2) that \( x_\rho h t_\sigma t_\tau = x_\rho t_\sigma T_\sigma(h) t_\tau \). Since \( x_\rho f_{\rho, \rho \sigma} \in x_\rho t_\sigma \) by (7) and \( |x_\rho f_{\rho, \rho \sigma} T_\sigma(h)| = |x_\rho t_\sigma T_\sigma(h)| \) by (2), we have

\[ x_\rho t_\sigma T_\sigma(h) t_\tau = x_\rho f_{\rho, \rho \sigma} T_\sigma(h) t_\tau. \]

Applying the same argument to \( t_\sigma \) we obtain that

\[ x_\rho f_{\rho, \rho \sigma} T_\sigma(h) t_\sigma = x_\rho t_\sigma T_\sigma f_{\rho, \rho \sigma} T_\sigma T_\tau(h) = x_\rho f_{\rho, \rho \sigma} f_{\rho \sigma, \rho \sigma \tau} T_\tau T_\sigma(h). \]

Similarly, the right-hand side of (8) is equal to \( x_\rho f_{\rho, \rho \sigma} T_\sigma(h) E_{\sigma, \tau} \). Since \( h \) is arbitrarily taken, the desired equation follows from (8) and the uniqueness of the presentation \( \{x h \mid h \in H \} \) (note that \( H \) is thin, i.e. each element of \( H \) is of valency one). □
We say that a map \( T : F \to \text{SAut}(H) \) is feasible if it satisfies (i), (ii), (iii) in Lemma 3.1, and a map \( f : F \times F \to H \) is called a factor set belonging to \( T \) if it satisfies (iv), (v) in Lemma 3.1.

**Theorem 3.2.** Let \( f : F \times F \to H \) be a factor set belonging to \( T : F \to \text{SAut}(H) \) where \( T \) is feasible. Then \( (F \times H, \{ \overline{\rho h} \}_{\rho \in F, h \in H}) \) is an extension of \( H \) by \( F \) where

\[
\overline{\rho h} := \{ (\sigma, \tau b) \mid \sigma^{-1} \tau = \rho, b \in f_{\sigma, \tau} T(a)h \}.
\]

Furthermore, \( T \) and \( f \) can be obtained by way of (5) and (7) with respect to a suitable pair of transversals of the closed subset \( \{ \overline{1_F H} \}_{h \in H} \) in the binary relations \( \{ \overline{\rho h} \}_{\rho \in F, h \in H} \) and the underlying set \( F \times H \).

**Proof.** We claim that \( \{ \overline{\rho h} \}_{\rho \in F, h \in H} \) is a partition of \( (F \times H) \times (F \times H) \). If \( (\sigma a, \tau b) \in \rho_1 h_1 \cap \rho_2 h_2 \), then \( \sigma^{-1} \tau = \rho_1, b \in f_{\sigma, \tau} T_{\rho_1}(a)h_1 \) for \( i = 1, 2 \). Hence, \( \rho_1 = \rho_2 \) and \( f_{\sigma, \tau} T_{\rho_1}(a)h_1 \cap f_{\sigma, \tau} T_{\rho_1}(a)h_2 \neq \emptyset \). Since \( T_{\rho_1}(1_H) \subseteq H \) and \( T_{\rho_1}(a)T_{\rho_1}(1_H) = T_{\rho_1}(a) \)

\[
f_{\sigma, \tau} T_{\rho_1}(a)h_1 = f_{\sigma, \tau} T_{\rho_1}(a)h_2.
\]

This implies \( \overline{\rho_1 h_1} = \overline{\rho_2 h_2} \). For all \( \sigma a, \tau b \in F \times H \) there exists \( \rho := \sigma^{-1} \tau \in F \) and \( h \in T_{\rho}(a)^{-1} b \) such that \( (\sigma a, \tau b) \in \overline{\rho h} \). Therefore, \( \{ \overline{\rho h} \}_{\rho \in F, h \in H} \) is a partition of \( (F \times H) \times (F \times H) \).

By definition

\[
1_F 1_H := \{ (\sigma a, \tau b) \mid \sigma^{-1} \tau = 1_F, b \in f_{\sigma, \tau} T_{\sigma^{-1} \tau}(a)1_H \}.
\]

By (i), (iv), we have \( 1_F 1_H = \{ (\sigma a, \sigma a) \mid \sigma a \in F \times H \} \).

For each \( \overline{\rho h} \in \{ \overline{\rho h} \}_{\rho \in F, h \in H} \) its transpose is

\[
(\tau b, \sigma a) \mid \sigma^{-1} \tau = \rho, b \in f_{\sigma, \tau} T_{\rho}(a)h \}.
\]

Let \( (\tau b, \sigma a) \in \overline{\rho h}^t \). Then \( \sigma^{-1} \tau = \rho, b \in f_{\sigma, \tau} T_{\rho}(a)h \).

By (v),

\[
T_{\rho} L(f_{\sigma, \rho \sigma})T_{\rho^{-1}} L(f_{\sigma \rho, \sigma}) = T_{\rho \rho^{-1}} L(f_{\sigma, \sigma}) R(E_{\rho, \rho^{-1}}).
\]

It follows from (i) and (iv) that

\[
T_{\sigma} L(f_{\sigma, \sigma \rho})T_{\rho^{-1}} L(f_{\sigma \rho, \sigma}) = R(E_{\rho, \rho^{-1}}). \tag{9}
\]

Mapping \( bh^{-1} \) by \( T_{\rho^{-1}} L(f_{\sigma \rho, \sigma}) \) we obtain from (9) and \( \tau = \sigma \rho \) that

\[
f_{\sigma \rho, \sigma \rho} T_{\rho^{-1}} (bh^{-1}) \leq a E_{\rho, \rho^{-1}}. \tag{10}
\]

Mapping \( 1_H \) by (9) and applying Lemma 2.1 with (ii) we obtain that \( a E_{\rho, \rho^{-1}} \) is exactly a coset of \( T_{\rho^{-1}}(1_H) \), whence, the equality of (10) holds. This implies that

\[
a \in f_{\tau, \sigma} T_{\rho^{-1}} (bh^{-1}) E_{\rho, \rho^{-1}}^{-1}.
\]

Taking \( m \in T_{\rho^{-1}} (h^{-1} E_{\rho, \rho^{-1}}^{-1}) \) we have \( a \in f_{\tau, \sigma} T_{\rho^{-1}} (b)m \). Hence, the transpose of \( \overline{\rho h} \) is contained in \( \overline{\rho^{-1} m} \). Since \( \overline{\rho h} \) is arbitrarily taken, it follows that \( \{ \overline{\rho h} \}_{\rho \in F, h \in H} \) is closed under the transposition.
For all \( \sigma, \tau \in F \) and each \( (\mu d, ve) \in \overline{\rho c} \) we will show that \( (\mu d)\overline{\sigma a} \cap (ve)\overline{\tau b} \neq \emptyset \) if and only if \( (\mu d)\overline{\sigma a} \cap (ve)\overline{\tau b} \neq \emptyset \).

Since \( 1_H \in T_\rho(1_H) \cap \text{Ker}T_\tau \), the “if” part is obvious. If \( \epsilon h \in (\mu d)\overline{\sigma a} \cap (ve)\overline{\tau b} \), then \( \epsilon = \mu a = v \tau^{-1} \), \( h \in f_{\mu,\epsilon}T_\sigma-da \) and \( e \in f_{\epsilon,\tau}T_\tau(b) \). Note that \( h \) lies in the intersection of a coset of \( T_\sigma(1_H) \) and that of \( \text{Ker}T_\tau \). From a basic knowledge of group theory the size of the intersection is equal to \( |T_\sigma(1_H) \cap \text{Ker}T_\tau| \). Furthermore, by (v),

\[
e \in f_{\epsilon,\tau}(f_{\mu,\epsilon}T_\sigma(d)a)b = (T_\sigma L(f_{\mu,\epsilon}T_\tau)L(f_{\epsilon,\tau}))(d)T_\tau(a)b \\
= (T_\sigma L(f_{\mu,\mu}\sigma)T_\tau L(f_{\mu,\mu}\sigma\tau))(d)T_\tau(a)b \\
= (T_\rho L(f_{\mu,\mu}\rho)R(E_{\sigma\tau}T_\tau(a)b))(d).
\]

Therefore, \( (\mu d)\overline{\sigma a} \cap (ve)\overline{\tau b} \neq \emptyset \) if and only if

\[
e \in f_{\mu,\tau}T_\rho(d)E_{\sigma\tau}T_\tau(a)b,
\]

or, equivalently, since \( (\mu d, ve) \in \overline{\rho c} \),

\[
c \in T_\rho(1_H)E_{\sigma\tau}T_\tau(a)b
\]

which does not depend on the choice of \( d \) and \( e \) and the choice of \( \mu \) and \( v \) with \( (\mu d, ve) \in \overline{\rho c} \).

It is obvious that \( N := \{1_H | h \in H\} \) is a thin closed subset such that \( N \cong H \) and the factor scheme over \( N \) is isomorphic to \( F \).

If you take a transversal \( \{\sigma \in F \} \) of \( N \) with \( t_\sigma := \overline{\sigma 1_H} \) and a transversal \( \{\sigma 1_H | \sigma \in F \} \) of \( N \) in \( F \times H \), then \( T \) and \( f \) can be obtained by way of (5) and (7) with respect to a suitable pair of transversals of \( N \) in \( \overline{\rho h} \) for \( h \in H \) and \( F \times H \).

This completes the proof. \( \square \)

Now we will prepare some lemma to define two-dimensional cohomology groups. For the remainder of this section we assume that \( H \) is Abelian and \( T : F \to \text{SAut}(H) \) is feasible.

**Lemma 3.3.** For all \( \sigma, \tau \in F \) we have \( T_\sigma T_\tau = T_{\sigma\tau}L((T_\sigma T_\tau)(1_H)) \). Furthermore, a map \( g : F \times F \to H \) is a factor set belonging to \( T \) if and only if \( g_{\sigma,\sigma} = 1_H \) for each \( \sigma \in F \) and \( T_\rho(g_{\rho,\rho\sigma})g_{\rho\sigma,\rho\sigma\tau}g_{\rho,\rho\sigma\tau}(T_\sigma T_\tau)(1_H) \) does not depend on the choice of \( \rho \).

**Proof.** Since \( H \) is Abelian, it follows from (iii) in **Lemma 3.1** that \( I(C_{\sigma,\tau}) = L((T_\sigma T_\tau)(1_H)) \), as desired.

If \( g : F \times F \to H \) is a factor set belonging to \( T \), then it is clear that \( g_{\sigma,\sigma} = 1_H \) for each \( \sigma \in F \). By (v) in **Lemma 3.1**, for all \( \sigma, \tau \in F \) there exists \( E_{\sigma,\tau} \in \mathcal{P}(H) \) such that

\[
T_\rho L(f_{\rho,\rho\sigma})T_\tau L(f_{\rho\sigma,\rho\sigma\tau}) = T_{\sigma\tau}L(f_{\rho,\rho\sigma\tau})(E_{\sigma,\tau})
\]

for each \( \rho \in F \). Mapping \( 1_H \) by both sides of the above we obtain

\[
(T_\rho T_\tau)(1_H)T_{\rho\sigma,\rho\sigma\tau} = T_{\sigma\tau}(1_H)g_{\rho,\rho\sigma\tau}E_{\sigma,\tau}.
\]

Since \( T_\tau(1_H) \subseteq (T_\sigma T_\tau)(1_H) \), \( T_\tau(g_{\rho,\rho\sigma})g_{\rho\sigma,\rho\sigma\tau}g_{\rho,\rho\sigma\tau}(T_\sigma T_\tau)(1_H) \) is a coset of \( (T_\sigma T_\tau)(1_H) \), which does not depend on the choice of \( \rho \in F \).
Conversely, if we take \( E_{\sigma, \tau} := T_t(g_{\rho, \rho\sigma}) g_{\rho\sigma, \rho\sigma\tau} g_{\rho, \rho\sigma\tau}^{-1} (T_\sigma T_\tau)(1_H) \), then (v) in Lemma 3.1 is satisfied so that \( g \) is a factor set. □

**Lemma 3.4.** For all factor sets \( f, g \) belonging to \( T \) we define an addition of \( f \) and \( g \) by \((f + g)_{\sigma, \tau} := f_{\sigma, \tau} g_{\sigma, \tau}^{-1} \). Then the set of all factor sets belonging to \( T \) forms an Abelian group with respect to the addition.

**Proof.** Since \( f_{\sigma, \sigma} g_{\sigma, \sigma} = 1_H 1_H = 1_H \) in Lemma 3.1 for \( f + g \) is satisfied.

Applying Lemma 3.3 for \( f + g \) we can show that \( f + g \) is a factor set belonging to \( T \). Therefore, the addition is well defined. It is obvious to check the associativity. If we take the constant map from \( F \times F \) to the identity of \( H \), then it is the identity with respect to the addition. For each factor \( g \) the inverse \(-g\) of \( g \) is the map defined by \(-g_{\sigma, \tau} := g_{\sigma, \tau}^{-1}\). This completes the proof. □

**Lemma 3.5.** For a given \( h : F \rightarrow H \) with \( h_{1_F} = 1_H \) we choose \( g : F \times F \rightarrow H \) such that \( g_{\rho, \rho\sigma} \in T_\rho(h_{\rho\sigma}^{-1}) h_{\rho\sigma} h_{\rho\sigma}^{-1} \) for all \( \rho, \sigma \in F \). Then \( g \) is a factor set belonging to \( T \). Furthermore, \( \{g : F \times F \rightarrow H \mid \exists h \in H \exists \sigma, \rho, g_{\rho, \rho\sigma} \in T_\rho(h_{\rho\sigma}^{-1}) h_{\rho\sigma} h_{\rho\sigma}^{-1} \} \) forms a group with respect to the addition given in Lemma 3.4.

**Proof.** Since \( g_{\sigma, \sigma} \in T_{1_F}(h_{\sigma}^{-1}) h_{\sigma} h_{\sigma}^{-1} \), it follows from (i) that \( g_{\sigma, \sigma} = 1_H \).

Applying Lemma 3.3 for \( g \) we can show that \( g \) is a factor set belonging to \( T \).

Let \( g \) and \( g' \) be factor sets derived from \( h : F \rightarrow H \) and \( h' : F \rightarrow H \), respectively. Then \( g + g' \) is a factor set derived from \( h + h' : F \rightarrow H \) such that \((h + h')_{\sigma} := h_{\sigma} h'_{\sigma}\) for each \( \sigma \in F \). Therefore, it is closed under the addition. Therefore, the second statement holds. □

**Definition 3.1.** Let \( \mathcal{F} \) denote the group consisting of all factor sets belonging to \( T \), and \( \mathcal{H} \) denote the group given in Lemma 3.5. We define the two-dimensional cohomology group with respect to \((T, F, H)\) to be \( \mathcal{F}/\mathcal{H} \).

**Lemma 3.6.** Let \( \mathcal{F}/\mathcal{H} \) denote the two-dimensional cohomology group with respect to \((T, F, H)\). For all factor sets \( f, g \in \mathcal{F} \), if \( f \mathcal{H} = g \mathcal{H} \), then the scheme derived from \( f \) by way of Theorem 3.2 is isomorphic to that from \( g \).

**Proof.** Let \((X, G)\) be the scheme derived from \( f \) by way of Theorem 3.2. Then there exists suitable transversals \( \{t_\sigma \mid \sigma \in F\} \) and \( \{x_\sigma \mid \sigma \in F\} \) such that \( f \) can be obtained by way of (5) and (7). Note that it suffices to show that, for each \( e \in \mathcal{H} \) the scheme derived from \( f + e \) is isomorphic to that from \( f \). Let \( e : F \times F \rightarrow H \) be obtained from \( h : F \rightarrow H \) such that \( e_{\rho, \rho\sigma} \in T_\rho(h_{\rho\sigma}^{-1}) h_{\rho\sigma} h_{\rho\sigma}^{-1} \) for all \( \rho, \sigma \in F \). Then \((f + e)_{\sigma, \tau} = f_{\sigma, \tau} e_{\sigma, \tau} \in f_{\sigma, \tau} T_{\sigma^{-1} \tau}(h_{\sigma}^{-1}) h_{\sigma^{-1} \tau}^{-1} h_{\tau} \). Taking a new transversal of \( H \) in \( G \) to be \( \{t_\sigma h_{\sigma}^{-1} \mid \sigma \in F\} \) and that in \( X \) to be \( \{x_\sigma h_{\sigma}^{-1} \mid \sigma \in F\} \) we obtain from (7) that

\[
(x_\tau h_{\tau}^{-1})(f + e)_{\sigma, \tau} = x_\tau h_{\tau}^{-1} f_{\sigma, \tau} T_{\sigma^{-1} \tau}(h_{\sigma}^{-1}) h_{\sigma^{-1} \tau}^{-1} h_{\tau} = (x_\sigma t_{\sigma^{-1} \tau}) T_{\sigma^{-1} \tau}(h_{\sigma}^{-1}) h_{\sigma^{-1} \tau}^{-1} = (x_\sigma h_{\sigma}^{-1}) t_{\sigma^{-1} \tau} h_{\sigma^{-1} \tau}^{-1}
\]
Thus, \( f + e \) is a factor set belonging to \( T \), which can be obtained with respect to the transversal \( \{ t \sigma h^{-1}_\sigma \mid \sigma \in F \} \) in \( G \) and the transversal \( \{ x \sigma h^{-1}_\sigma \mid \sigma \in F \} \) in \( X \). Therefore, we conclude from Theorem 3.2 that the scheme derived from \( f + e \) is isomorphic to that from \( f \).

The following is an immediate consequence of Lemma 3.1, Theorem 3.2 and Lemma 3.6.

**Corollary 3.7.** The number of the isomorphism classes of extensions of \( F \) by \( H \) with \( T \) is at most \(|F|/|H|\).

**Example 3.1.** Consider the extension of \( H \) by \( F \) given in Example 1.5 and its two-dimensional cohomology group where \( H \) is Abelian. Let \((X, G)\) be the orbitals of the wreath product of \( H \) by \( F \). Then there exists a closed subset \( N \) of \( G \) such that \( N \simeq H \) and \( G/N \simeq F \). Moreover, for each \( g \in G - N \) we have \( Ng = \{g\} \). This implies that \( G = N \cup \{t \sigma \mid \sigma \in F - \{1\} \} \). Since \( T^*_{\sigma}(1_H) = H \) for each \( \sigma \in F - \{1\} \), the induced map \( T : F \rightarrow \text{SAut} \) by (5) is feasible. Note that any map from \( F \times F \) to \( H \) satisfying (iv) in Lemma 3.1 forms a factor set belonging to \( T \). Therefore, the two-dimensional cohomology group with respect to \((T, F, H)\) is trivial. It follows from Corollary 3.7 that such an extension is uniquely determined by its intersection numbers.

### 4. D-sequences

In this section we assume that \( F \) is a finite group. Let \( (a_i \mid i \in \mathbb{Z}_n) \) be a sequence of length \( n \) over \( F \). Then the subset \( \{a_ia_{j+1}\cdots a_{j+k} \mid 1 \leq j \leq n, 0 \leq k \leq n-2\} \) consisting of the consecutive products according to the ordering of \( (a_i \mid i \in \mathbb{Z}_n) \) is called the range of \( (a_i \mid i \in \mathbb{Z}_n) \). We say that a sequence \( (a_i \mid i \in \mathbb{Z}_n) \) over \( F \) is a D-sequence if \( a_0a_1a_2\cdots a_{n-1} = 1_F \) and the range of the sequence has size \( n^2 - n \).

Let \( \mathcal{A} \) be a set of D-sequences. Then the sum of lengths of the sequences in \( \mathcal{A} \) is called the length of \( \mathcal{A} \), and the union of the ranges of the sequences in \( \mathcal{A} \) is called the range of \( \mathcal{A} \).

We say that \( \mathcal{A} \) is independent if the ranges of any two sequences in \( \mathcal{A} \) are disjoint.

**Example 4.1.** We have the following:

(i) The sequence \((1, 2, 4)\) over \( \mathbb{Z}_7 \) is a D-sequence with the range \( \{1, 2, 4, 1 + 2, 2 + 4, 4 + 1\} \).

(ii) The sequences \((1, 6), (2, 5)\) over \( \mathbb{Z}_7 \) are D-sequences with the ranges \( \{1, 6\}, \{2, 5\} \), respectively. Since \( \{1, 6\} \cap \{2, 5\} = \emptyset \), the set \( \{(1, 6), (2, 5)\} \) is independent.

**Remark 4.2** ([5]). We have the following:

(i) If \( (a_i \mid i \in \mathbb{Z}_n) \) is a D-sequence over \( F \) and \( |F| = n^2 - n + 1 \), then the subset \( \{a_0, a_0a_1, \ldots, a_0a_1\cdots a_{n-1}, 1_F\} \) of \( F \) is a \((|F|, n, 1)\)-difference set.

(ii) If \( \{s_1, s_2, \ldots, s_n\} \subseteq F \) is a \((|F|, n, 1)\)-difference set with \( s_n = 1_F \), then \( (s_1, s_1^{-1}s_2, s_2^{-1}s_3, \ldots, s_{n-1}^{-1}s_n) \) is a D-sequence.
In the next section we will construct association schemes from an independent set of D-sequences. In particular, each scheme given in Example 1.7 is constructed from the D-sequence \((1, 2, 4)\) which induces a difference set \(\{1, 3, 0\} \subseteq \mathbb{Z}_7\).

5. Construction from D-sequences

In this section we assume that \(F\) is a finite group and \(H\) is the elementary Abelian \(p\)-group of rank \(m\), i.e., \(H := \mathbb{Z}_p^m\). We often deal with \(H\) as a vector space over \(\mathbb{Z}_p\).

Let \(A\) be an independent set of D-sequences over \(F\) such that the length of \(A\) is at most \(\frac{p^m-1}{p-1}\). We set

\[ S_A := \{a_i \mid (a_i) \in A\}, \]

so that \(|S_A|\) is the length of \(A\). We denote by \(R_A\) the range of \(A\). Since \(\frac{p^m-1}{p-1}\) is the number of the hyperplanes of \(H\), we can take an injection \(\lambda\) from \(S_A\) to the set of the hyperplanes of \(H\), and an injection \(\kappa\) from \(S_A\) to \(H\) such that

\[ \lambda(\sigma) \oplus (\kappa(\sigma)) = H \quad \text{for each } \sigma \in S_A. \quad (11) \]

We will define \(T : F \rightarrow \text{SAut}(H)\) by the following steps:

(i) We set \(T_1\) to be the identity on \(\mathcal{P}(H)\);
(ii) If \((a_i \mid i \in \mathbb{Z}_m) \in A\), then, for each \(i\) with \(1 \leq i \leq n - 1\) we set \(T_{a_i}\) by

\[ \text{Ker}T_{a_i} = \lambda(a_i), \quad T_{a_i}(1_H) := \lambda(a_{i+1}) \quad \text{and} \quad T_{a_i}(\kappa(a_i)) := \kappa(a_{i+1}). \]

By \((11)\), \(T_{a_i}\) is uniquely extended to \(\mathcal{P}(H)\) so that \(T_{a_i} \in \text{SAut}(H)\).

(iii) If \((a_i \mid i \in \mathbb{Z}_m) \in A\), then we set \(T_{a_0} := (T_{a_1} \cdots T_{a_{n-1}})^*, \) so that \(\text{Ker}T_{a_0} = \lambda(a_0)\) and \(T_{a_0}(1_H) = \lambda(a_1)\).

(iv) If \(\sigma \in R_A\), then there exists a unique sequence \((a_i \mid i \in \mathbb{Z}_m) \in A\) and a unique pair of \(j, k \in \mathbb{Z}_m\) such that \(\sigma = a_ja_{j+1} \cdots a_{j+k}\). We set \(T_{\sigma} := T_{a_j}T_{a_{j+1}} \cdots T_{a_{j+k}}\), so that

\[ \text{Ker}T_{\sigma} = \lambda(a_j) \quad \text{and} \quad T_{\sigma}(1_H) = \lambda(a_{j+k+1}). \]

(v) If \(\sigma \in F - R_A\) with \(\sigma \neq 1_F\), then we set \(T_{\sigma}\) such that \(T_{\sigma}(A) = H\) for each \(A \in \mathcal{P}(H)\).

For the remainder of this section \(T : F \rightarrow \text{SAut}(H)\) is given in the above paragraph. Now we consider how to define \(f : F \times F \rightarrow H\) so that \(f\) is a factor set belonging to \(T\).

We set

\[ U_A := \{a_1, a_2, \ldots, a_{n-1} \mid (a_i) \in \mathbb{Z}_m\} \in A\],
\[ \tilde{U}_A := \{(\sigma, \tau) \in F \times F \mid \sigma^{-1}\tau \in U_A\}. \]

Lemma 5.1. For all \(\sigma, \tau \in R_A\), the following are equivalent:

(i) \(T_{\sigma}(1_H) = \text{Ker}T_{\tau}\);
(ii) There exist a unique \((a_i \mid i \in \mathbb{Z}_m) \in A\) and a unique \((j, k, l) \in \mathbb{Z}_3^3\) such that \(\sigma = a_ja_{j+1} \cdots a_{j+k}\) and \(\tau = a_{j+k+1}a_{j+k+2} \cdots a_{j+k+l}\);
(iii) \(T_{\sigma}T_{\tau} = T_{\sigma\tau}\) with \(\sigma \tau \in R_A\) or \(\sigma\tau = 1_F\).
Proof. Since $\mathcal{A}$ is independent, there exists a unique $(a_i \mid i \in \mathbb{Z}_n) \in \mathcal{A}$ whose range contains $\sigma$, and a unique $j, k \in \mathbb{Z}_n$ such that $\sigma = a_j a_{j+1} \cdots a_{j+k}$ by definition of D-sequences. Recall that $\text{Ker} T_\sigma = \lambda(a_j)$ and $T_\sigma(1_H) = \lambda(a_j a_{j+k+1})$.

Suppose $T_\sigma(1_H) = \text{Ker} T_\sigma$. By the property on the injection $\lambda$, there exists a unique $l \in \mathbb{Z}_n$ such that $\tau = a_j a_{j+k+1} \cdots a_{j+k+l}$. By the definition of $T$, (i) and (ii) are equivalent. Since $\sigma \tau = a_j a_{j+1} \cdots a_{j+k+l}$, it follows from the definition of $T$ that $T_{\sigma \tau} = T_{a_j} T_{a_{j+1}} \cdots T_{a_{j+k+l}} = T_\sigma T_\tau$ if $\sigma \tau \neq 1_F$. Therefore, (ii) implies (iii).

If $\sigma \tau = 1_F$, then $T_{\sigma}(1_H) = \text{Ker} T_\sigma$ by definition of $T$. If $T_\sigma T_\tau = T_{\sigma \tau}$ with $\sigma \tau \in R_\mathcal{A}$ and $T_\sigma(1_H) \neq \text{Ker} T_\tau$, then, by the definition of $T_\sigma$ and $T_\tau$, $T_{\sigma \tau}(1_H) = (T_\sigma T_\tau)(1_H) = H$, which contradicts $\sigma \tau \in R_\mathcal{A}$. Therefore, (iii) implies (i). □

**Lemma 5.2.** If $T_\sigma T_\tau = T_{\sigma \tau}$, then, for all $a, b \in H$ there exists $c \in H$ such that $T_\sigma L(a) T_\tau L(b) = T_{\sigma \tau} L(c)$.

**Proof.** Since $T_\sigma L(a) T_\tau L(b) = T_\sigma T_\tau L(T_\tau(a)b) = T_{\sigma \tau} L(T_\tau(a)b)$ and $T_\tau(a)b$ is contained in a coset of $(T_\sigma T_\tau)(1_H) = T_{\sigma \tau}(1_H)$, there exists $c \in T_\tau(a)b$ such that $T_\sigma L(a) T_\tau L(b) = T_{\sigma \tau} L(c)$. □

**Lemma 5.3.** The map $T : F \to \text{SAut}(H)$ is feasible.

**Proof.** It is obvious that (i) in Lemma 3.1 holds.

By the definition of $T$, (ii) in Lemma 3.1 holds.

We claim that (iii) in Lemma 3.1 holds. Since $H$ is Abelian, it suffices to show that $T_\sigma T_\tau = T_{\sigma \tau}(L(T_\tau(1_H)))$ for all $\sigma, \tau \in F$. If $1_F \in \{\sigma, \tau\}$, then it is trivial. If $\sigma, \tau \in F \setminus \{1_F\}$ with $T_\sigma(1_H) \neq \text{Ker} T_\tau$ or $H \in \{T_\sigma(1_H), \text{Ker} T_\tau\}$, then $(T_\sigma T_\tau)(1_H) = H$ by definition of $T$. If $\sigma, \tau \in F \setminus \{1_F\}$ with $T_\tau(1_H) = \text{Ker} T_\sigma$ and $H \notin \{T_\sigma(1_H), \text{Ker} T_\tau\}$, then $\sigma, \tau \in R_\mathcal{A}$. By Lemma 5.1, there exists a unique $(a_i \mid i \in \mathbb{Z}_n) \in \mathcal{A}$ and a unique $(j, k, l) \in \mathbb{Z}_n^3$ such that $\sigma = a_j a_{j+1} \cdots a_{j+k}$ and $\tau = a_{j+k+1} a_{j+k+2} \cdots a_{j+k+l}$. By the definition of $T$, it is complete. □

The following theorem shows that we can choose any value of $f$ on $\tilde{U}_A$, and such a variety of $f$ possibly provides the isomorphism classes of all extensions of $H$ by $F$ with $T$.

**Theorem 5.4.** Assume that $T$ is given in the above construction. Then each $\tilde{f} : \tilde{U}_A \to H$ extends $f : F \times F \to H$ such that $f$ is a factor set belonging to $T$.

**Proof.** We set $f_{\rho, \rho} = 1_H$ for each $\rho \in F$.

By Lemma 5.1, for each element $\mu \in R_\mathcal{A}$ there exists a unique $(a_i \mid i \in \mathbb{Z}_n) \in \mathcal{A}$ and $j, k \in \mathbb{Z}_n$ such that $\mu := a_j a_{j+1} \cdots a_{j+k}$. For each $\rho \in F$ the composite

$$T_{a_j} L(f_{\rho, \rho a_j}) T_{a_{j+1}} L(f_{\rho a_j, \rho a_j a_{j+1}}) \cdots T_{a_{j+k}} L(f_{\rho a_{j+k}, \rho a_{j+k} a_{j+k+1}})$$

can be written as $T_\mu L(c)$ for some $c \in H$ by Lemmas 5.1 and 5.2. We choose $f_{\rho, \rho \mu}$ as $c$ if $\mu \in R_\mathcal{A} - U_\mathcal{A}$. 

For each $\mu \in F - R_A$ and $\rho \in F$ we set $f_{\rho, \rho \mu} := 1_H$ for convenience, though we can take any value of $H$ in this case.

We will show that the extended map $f : F \times F \to H$ is a factor set belonging to $T$. By definition $f_{\sigma, \sigma} = 1_H$ for each $\sigma \in F$. By Lemma 3.3, it suffices to show that

$$T_t(f_{\rho, \rho \sigma}) f_{\rho, \rho \sigma} f_{\rho, \rho \sigma}^{-1} T_t(T_{\alpha}(1_H))$$

(12)
does not depend on the choice of $\rho$.

If $1_F \in \{\sigma, \tau\}$, then (12) is equal to $T_t(T_{\alpha}(1_H))$.

If $\sigma, \tau \in F - \{1_F\}$ with $T_{\alpha}(1_H) \neq \text{Ker}T_t$ or $H \notin \{T_{\alpha}(1_H), \text{Ker}T_t\}$, then $(T_{\alpha}T_t)(1_H) = H$ by definition of $T$. This implies that (12) is equal to $H$.

If $\sigma, \tau \in F - \{1_F\}$ with $T_{\alpha}(1_H) = \text{Ker}T_t$ and $H \notin \{T_{\alpha}(1_H), \text{Ker}T_t\}$, then $\sigma, \tau \in R_A$.

By Lemma 5.1, there exist a unique $(a_i | i \in \mathbb{Z}_n) \in A$ and a unique $(j, k, l) \in \mathbb{Z}_n^3$ such that $\sigma = a_ja_{j+1} \cdots a_{j+k}$ and $\tau = a_{j+k+1}a_{j+k+2} \cdots a_{j+l}$. By the definition of the extended map $f$, we see directly that (iii) in Lemma 3.1 holds, actually, (12) is equal to $T_t(1_H)$.

Since each case does not depend on the choice of $\rho$, we conclude that $f$ is a factor set belonging to $T$. □

**Remark 5.1.** Combining Theorem 3.2 with Theorem 5.4 we obtain an extension of $\mathbb{Z}_n^m$ by $F$ from an independent set of D-sequences over $F$ whose length is at most $(p^m - 1)/(p - 1)$.

Each factor set belonging to $T$ can be obtained by the above construction since $\tilde{f}$ on $\tilde{U}_A$ can be chosen arbitrarily and the arbitrarily chosen $\tilde{f}$ induces a unique association scheme by the construction.

6. Application

Let $(X, G)$ be an association scheme. For each $D \subseteq G$ we define the thin centralizer of $D$ to be $\bigcap_{g \in D} \{g \in G | n_g = 1, gd = dg\}$, and we define the thin center of $G$ to be the thin centralizer of $G$.

In this section we will show an application of our results for $p$-schemes where $p$ is a prime. Recall that $(X, G)$ is called a $p$-scheme if $|X| \prod_{g \in G} n_g$ is a power of $p$. Combining Sylow’s theorem in group theory and observation for $p$-schemes we obtain the following proposition.

**Proposition 6.1.** Let $(X, G)$ be a $p$-scheme. If $(X, G)$ is Schurian, then $G$ has a non-trivial thin center.

**Proof.** Since $(X, G)$ is Schurian, there exists a transitive permutation group $\Gamma$ on $X$ such that $G = \{(x, y)^\Gamma | xy \in X\}$ where $(x, y)^\Gamma := \{(x^\gamma, y^\gamma) | \gamma \in \Gamma\}$.

We claim that $\Gamma$ is a $p$-group. Suppose not, i.e. there exists a non-trivial Sylow subgroup $\Theta$ of $\Gamma$ whose order is prime to $p$. Since $|X|$ is a power of $p$, there exists $x \in X$ such that $x^\Theta = \{x\}$. Let $\Delta$ denote the stabilizer of $x \in X$ in $\Gamma$. Then $\Theta \leq \Delta$, so that $|y^\Theta|$ divides $|y^\Delta|$ for each $y \in X$. Recall that there exists a one-to-one correspondence between $G$ and the orbits of $\Delta$ on $X$, and that $|y^\Delta|$ is equal to the valency of $r(x, y)$ where $r(x, y)$ is the member of $G$ containing $(x, y)$. Since $(X, G)$ is a $p$-scheme, it follows that $|y^\Theta| = 1$ for each $y \in Y$. This implies that $|\Theta| = 1$, a contradiction.
We claim that $Z(\Gamma) \cap \Delta = 1_T$. Let $\sigma \in Z(\Gamma) \cap \Delta$ and $y \in X$. Since $\Gamma$ is transitive on $X$, there exists $t \in \Gamma$ such that $y = x^t$. Then we have

$$y^\sigma = (x^t)^\sigma = x^{t\sigma} = x^t = y.$$ 

This implies that $\sigma$ is the identity.

Since $\Gamma$ is a $p$-group, there exists a non-trivial center $\theta$. Then $r(x, x^\theta)$ is thin since $\{x^\theta\}$ is an orbit of $\Delta$. Moreover, $r(x, x^\theta)$ is a non-trivial thin center since $|\theta g| = 1$ for each $\theta \in G$ with $n_1 = 1$ and $g \in G$ so that, for each $\sigma \in \Gamma$

$$r(x^\theta, x^\sigma)r(x, x^\theta) = r(x^\theta x^\sigma, x) = r(x^\theta x^\sigma, x^\theta)$$

$$= r(x^\theta, x^\theta) = r(x, x^\sigma) = r(x, x^\theta) r(x^\theta, x^\sigma) \quad \Box$$

**Remark 6.1.** We can construct non-Schurian $p$-schemes by the construction given in Section 5. Let us take $\mathcal{A} = \{(1, 2, p - 3)\}$ over $\mathbb{Z}_p$ as a set of D-sequences and define a map $\lambda$ from $S_A$ to the set of hyperplanes of $\mathbb{Z}_p^2$ by $\lambda(1) := ((1, 0)), \lambda(2) := ((0, 1)), \lambda(p - 3) := (1, 1)$ where $p$ is a prime greater than 5. We define $\kappa : S_A \rightarrow \mathbb{Z}_p^2$ by $\kappa(1) := (0, 1), \kappa(2) := (1, 1), \kappa(p - 3) := (1, 0)$. Taking $f : \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p^2$ as the identity element of the factor sets belonging to $T$ we obtain from Theorem 3.2 that an extension $(\mathbb{Z}_p^2, \mathbb{Z}_p^2, \bigoplus \mathbb{Z}_p^2)$ of $\mathbb{Z}_p^2$ by $\mathbb{Z}_p$. Note that $\{0\} \in \mathbb{Z}_p^2$ is the largest thin closed subset and the thin centralizer of $0(0, 0)$ is $\{0(i, 0) | i \in \mathbb{Z}_p\}$ and that $\mathbb{Z}(0, 0)$ is $\{0(i, 0) | i \in \mathbb{Z}_p\}$. Therefore, the thin center of the scheme is trivial. It follows from Proposition 6.1 that the $p$-scheme obtained above is not Schurian.

**Acknowledgements**

In December of 2002 the second author gave a talk on a part of the result of this paper at a workshop in Kyoto (Japan). Though the authors did not notice the relationship between D-sequences and difference sets, A. Munemasa and S. Yoshiara gave their comments on it after the talk, and Y. Hiramine showed a note to prove Remark 4.2. At the banquet of the workshop A. Hanaki encouraged that the presented talk would be a first step to approach to extension theory of association schemes.

In July of 2003 the second author had a discussion with M. Muzychuk at a conference in Bled (Slovenia). Though the presented construction (see Section 5) was only for extensions of $\mathbb{Z}_p^2$, he suggested the author that it was possible to generalize it to $\mathbb{Z}_p^n$ and the idea was due to a paper by D.G. Fon-Der-Flaas.

The authors would like to thank A. Hanaki, Y. Hiramine, A. Munemasa, M. Muzychuk and S. Yoshiara for giving the authors their valuable and farsighted comments.

**References**