Известия Гомельского государственного университета
имени Ф.Скорины, №2(41), 2007

УДК 519.6

Association schemes and automorphisms of finite groups

V. M. Sidelnikov[1]

1. Introduction

Association schemes are one of the main fields of research in algebraic combinatorial analysis. This research is stimulated by applications of association schemes in coding theory, combinatorial designs and cryptography.

Let X be a finite set. Elements of X (of $X \times X$) are called vertices (edges).

An association scheme $\boldsymbol{C}(X)$ on X is a partition of the Cartesian square $X \times X$ into $1+m$ subsets $R_0, \ldots, R_m$ (relations) satisfying the following conditions [14, 16]:

a $R_0 = \{(x,x) | x \in X\}$.

b Let $(x,y) \in X \times X$. The number $r_{i,j}(x,y)$ of pairs of edges $(x,z),(z,y)$ such that $(x,z) \in \in R_i$, $(z,y) \in R_j$, is the same for any $(x,y) \in R_k$, i.e. the number $r_{i,j}(x,y) = r^k_{i,j}$ does not depend on the choice of (x,y) in R_k.

c The reciprocal relation $R_j^T = \{(y,x) | (x,y) \in R_j\}$ also belongs to the set $R_0, \ldots, R_m$, i.e. $R_j^T = R_{j'}$ for some j'.

If, in addition to the items **a**, **b** and **c**, condition $r^k_{i,j} = r^k_{j,i}$ holds, then the association scheme is called commutative.

The well-known example is the Hamming association scheme $\mathcal{H}_q^n$ with $n+1$ relations where X, $|X| = q$, $q \geq 2$,. The relation R_j consists of all pairs of vectors $(\boldsymbol{x}, \boldsymbol{y}) \in X^n \times X^n$ such that $d(\boldsymbol{x}, \boldsymbol{y}) = j$, where d is the Hamming distance.

For extended bibliography on association schemes the reader is referred to [8, 14, 16].

The usual item of study in the theory of association schemes is the Bose-Mesner algebra of an association scheme. This algebra has two basic bases: basis formed by incidence matrices of the relations R_j and the basis formed by its idempotents [16]. The theory concentrates on the interrelation of these two bases.

Another topic in the theory of commutative association schemes is the so-called Krein's formal duality [8], [16].

One more direction of research is studying codes $Y \subset X$ on an association scheme $\boldsymbol{C}(X)$. The theory is developed for the general case, but for expository purposes we shall confine ourselves to the Hamming scheme $\mathcal{H}_q^n$. Let N_j be a number of pairs $y, y' \in Y$ such that $(y, y') \in R_j$. One of the main results of the theory is the inequality $\sum_{j=0}^n N_j q_k(j) \geq 0$ where $q_k(j)$ are entries of a matrix transforming the basis of idempotents into the basis of incidence matrices of Bose-Mesner algebra. This inequality is a base for deriving upper bounds on the code size using linear programming techniques.

It is convenient to treat the Hamming association scheme $\mathcal{H}_q^n$ as follows. First, consider an association scheme $\boldsymbol{C}(X)$, $|X| = q \geq 2$, which has two relations R_0, R_1. All pairs $(f,f) \in \in X \times X$ are in R_0, and R_1 includes all other pairs $(f,g) \in X \times X$. We define an association scheme $\boldsymbol{C}(X^n)$ having $n+1$ relations $R_{(n-j,j)}$, $j = 0, \ldots, n$. We put $(\boldsymbol{x}, \boldsymbol{x}') \in R_{(n-j,j)}$, if and

[1]This work is supported by the Russian Fund of Basic Researches (the grant No 05-01-01018)

only if the relation R_1 holds for j pairs of entries of vectors $\boldsymbol{x}, \boldsymbol{x}' \in X^n$, while R_0 holds for $n-j$ remaining pairs, i.e. $d(\boldsymbol{x}, \boldsymbol{x}') = j$. It is obvious, that $\boldsymbol{C}(X) = \mathcal{H}_q^n$.

In the present work we study composition association schemes $\boldsymbol{C}(X^n)$, generally noncommutative, which generalize the Hamming association scheme $\mathcal{H}_q^n$ treated as above. Namely, let $\boldsymbol{C}(X)$ be a scheme with $m+1$ relations $R_0, \ldots, R_m \subset X \times X$, which is called a coordinate scheme. The relations $R_{\boldsymbol{c}} \subset X^n \times X^n, \boldsymbol{c} = (c_0, \ldots, c_m)$, $c_i \in \{0, \ldots, n\}$, $c_0 + \cdots + c_m = n$, of the composition scheme $\boldsymbol{C}(X^n)$, are defined as follows. Suppose, that the number of pairs of coordinates $x_s, x_s', s = 1, \ldots, n$, of vectors $\boldsymbol{x}, \boldsymbol{x}' \in X^n$ such that the relation R_j holds is equal to c_j, $j = 0, \ldots, m$. Then $(\boldsymbol{x}, \boldsymbol{x}') \in R_{(c_0, \ldots, c_m)}$. Delsarte [6], [14] shows that if $\boldsymbol{C}(X)$ is an association scheme then $\boldsymbol{C}(X^n)$ is also an association scheme.

Obviously, the number m_n of classes of relations in the scheme $\boldsymbol{C}(X^n)$ is $\binom{n+m}{n}$.

1.1 Elementary properties of the scheme $\boldsymbol{C}_H(\mathfrak{G}^n)$.

Let $\mathfrak{G}$ be a finite group and H be a subgroup of its automorphism group $Aut(\mathfrak{G})$. We consider association schemes $S_H(\mathfrak{G})$ with relations R_j, $j = 0, \ldots, m$, defined as follows. If $\mathfrak{g}'\mathfrak{g}^{-1} \in C_j$, where C_j is a class of conjugate elements of $\mathfrak{G}$ relative to a group H of automorphisms of $\mathfrak{G}$, then $(\mathfrak{g}, \mathfrak{g}') \in R_j$. The composition association scheme $\boldsymbol{C}(\mathfrak{G}^n) = \boldsymbol{C}_H(\mathfrak{G}^n)$ has the above mentioned structure (see also definition 2.2).

It should be noted that in the book [16] the association scheme $S_H(\mathfrak{G})$ was considered in the case, when the group H is the group of inner automorphisms of $\mathfrak{G}$, and in the paper [14] in the case, when $\mathfrak{G}$ is an Abelian group and H is the trivial group. i.e. it consists of identity mapping only. For these cases there is (see [16], [14]) a series of brilliant and nontrivial results connecting properties of the scheme S_H with properties of linear representations of the group $\mathfrak{G}$ in the vector space $\mathbb{C}^u$. The class of schemes S_H (see definition 2.2) is somewhat wider than the class of schemes studied in the work [14].

We define a function $\lambda(\boldsymbol{x}, \boldsymbol{x}')$ over the scheme $\boldsymbol{C}(X^n)$ which assumes a value $\widetilde{\boldsymbol{c}} = (c_1, \ldots, c_m)$, if $(\boldsymbol{x}, \boldsymbol{x}') \in R_{(c_0, \ldots, c_m)}$. Thus, $\widetilde{\boldsymbol{c}}$ is just the vector $\boldsymbol{c}$ with the first coordinate dropped. Note, that the function λ is constant on all edges (x, x') belonging to the same relation of the scheme $C(X^n)$, i.e. λ is a central function with respect to the relations of the scheme $\boldsymbol{C}(X^n)$.

The scheme $\boldsymbol{C}_H(\mathfrak{G}^n)$ has the following distinguishing property. If $(\mathfrak{g}, \mathfrak{g}') \in R_{\boldsymbol{c}}$ then $(\mathfrak{e}, \mathfrak{g}'\mathfrak{g}^{-1}) \in R_{\boldsymbol{c}}$, where $\mathfrak{e}$ is the unity of the group $\mathfrak{G}^n$. Hence, the value of the function $wt(\mathfrak{g}) = \lambda(\mathfrak{e}, \mathfrak{g})$ can be considered as a pseudo-weight of $\mathfrak{g}$. The function λ which we call pseudo-distance, is defined using the pseudo-weight $wt(\mathfrak{g})$ in the usual way: $\lambda(\mathfrak{g}, \mathfrak{g}') = wt(\mathfrak{g}'\mathfrak{g}^{-1})$ or if the group operation in $\mathfrak{G}^n$ is written in additive form, it is defined as $\lambda(\mathfrak{g}, \mathfrak{g}') = wt(\mathfrak{g}' - \mathfrak{g})$.

We consider codes $\mathfrak{K} \subseteq \mathfrak{G}^n$ and pseudo-distances $\lambda(\mathfrak{y}, \mathfrak{y}')$. $\mathfrak{y}, \mathfrak{y}' \in \mathfrak{K}$, defined on them. A code $\mathfrak{K}$ which is a subgroup $\mathfrak{H}$ of the group $\mathfrak{G}^n$ is called a group code.

Enumerator of the set of pseudo-distances $\lambda(\mathfrak{g}, \mathfrak{g}')$ of a group code $\mathfrak{K}$ is determined uniquely by enumerator of the set of pseudo-weights $wt(\mathfrak{g})$ of elements of this code because the number $N_{\boldsymbol{c}}(\mathfrak{K})$ of vectors of pseudo-weight $\boldsymbol{c}$ of a group code $\mathfrak{K}$ is equal to the number $|\mathfrak{K}| N_{\boldsymbol{c}}(\mathfrak{K})$ of pairs of vectors $\mathfrak{g}, \mathfrak{g}'$, for which $\lambda(\mathfrak{g}, \mathfrak{g}') = c$. Thus, the situation is roughly the same as for linear codes.

Let Ψ_n be a group of certain mappings $\psi : \mathfrak{G}^n \to \mathfrak{G}$ and $\widehat{H} = H_n$ be the group of automorphisms of the group Ψ_n generated by the group of automorphisms $H \wr S_n \leq Aut(\mathfrak{G}^n)$. Definitions of Ψ_n and H_n are given in section 1.2. Note, that the group operation in Ψ_n is multiplication of functions instead of their superposition.

The association scheme $\boldsymbol{C}_{\widehat{H}}(\Psi_n)$ is called dual to $\boldsymbol{C}_H(\mathfrak{G}^n)$.

Since the group Ψ_n is defined in a nonunique way, there are generally multiple dual schemes $\boldsymbol{C}_{\widehat{H}}(\Psi_n)$ for a given scheme of relations $\boldsymbol{C}_H(\mathfrak{G}^n)$. Note, that for the Abelian group $\mathfrak{G}^n$ its dual group Ψ_n is isomorphic to a group that is dual to $\mathfrak{G}^n$ under the commonly used definition of duality.

In this paper we obtain novel results in the following lines of research.

i For non-Abelian group $\mathfrak{G}$ we construct an association scheme $\boldsymbol{C}_{\widehat{H}}(\mathfrak{A}_n)$ dual to $\boldsymbol{C}_H(\mathfrak{G}^n)$.

ii We derive identities which express the number $N_c(\mathfrak{K}) = \#\{\mathfrak{g} | \mathfrak{g} \in \mathfrak{K}, wt(\mathfrak{g}) = c\}$ (element of a weight spectrum of a code $\mathfrak{K}$) by means of a weight spectrum of its dual code $\mathfrak{K}^{\perp} \subseteq \mathfrak{A}_n$.

1.2 Dual schemes of relations $\boldsymbol{C}_{\widehat{H}}(\Psi_n)$

Let $\Phi_{\mathfrak{G}}$ be the set of all maps $f : \mathfrak{G} \to \mathfrak{G}$. On the set $\Phi_{\mathfrak{G}}$ we define a group operation to be pointwise multiplication of functions. Thus, $\Phi_{\mathfrak{G}}$ becomes a finite group. Obviously, $|\Phi_{\mathfrak{G}}| = |\mathfrak{G}|^{|\mathfrak{G}|}$. In what follows, we consider subgroups of the group $\Phi_{\mathfrak{G}}$, which act identically on a unity $\mathfrak{e}$ of the group $\mathfrak{G}$.

Definition 1.1. *A subgroup Ψ of the group $\Phi_{\mathfrak{G}}$ is called an ambivalent group of the group $\mathfrak{G}$ if for any $f \in \Psi$, $f(\mathfrak{e}) = \mathfrak{e}$.*

As an example of ambivalent group Ψ consider a group $\widetilde{\mathfrak{G}}$, defined as follows.

Definition 1.2. *Denote by $\widetilde{\mathfrak{G}}$ the subgroup of $\Phi_{\mathfrak{G}}$ consisting of all "linear"functions of the form*

$$f(\mathfrak{x}) = f_{\mathfrak{g}_1,\dots,\mathfrak{g}_k,\mathfrak{g}_0}(\mathfrak{x}) = \mathfrak{g}_1\mathfrak{x}\mathfrak{g}_2\mathfrak{x}\cdots\mathfrak{g}_k\mathfrak{x}\mathfrak{g}_0,\ k = 0, 1, \dots,\ \mathfrak{x} \in \mathfrak{G}, \tag{1.1}$$

defined on the group $\mathfrak{G}$, such that $f(\mathfrak{e}) = \mathfrak{e}$, where $\mathfrak{g}_0, \mathfrak{g}_1, \dots, \mathfrak{g}_k \in \mathfrak{G}$.

It is easy to show, that if $\mathfrak{G}$ is a cyclic group of order u, then $\widetilde{\mathfrak{G}}$ is composed by all the functions $f(\mathfrak{x}) = \mathfrak{x}^s$, $\mathfrak{x} \in \mathfrak{G}$, $s = 0, \dots, u-1$. It is obvious, that $\widetilde{\mathfrak{G}}$ and $\mathfrak{G}$ are isomorphic. If $\mathfrak{G} = \mathfrak{H}_1 \times \dots \times \mathfrak{H}_n$ is a direct product of cyclic groups $\mathfrak{H}_i$, then $\widetilde{\mathfrak{G}}$ is composed by various products of functions $f_{i,s}(\mathfrak{x}_1 \cdots \mathfrak{x}_n) = \mathfrak{x}_i^s$, $s = 0, \dots, u_i - 1$, $\mathfrak{x}_i \in \mathfrak{H}_i$, $|\mathfrak{H}_i| = u_i$, $i = 1, \dots, n$. Therefore the groups $\widetilde{\mathfrak{G}}$ and $\mathfrak{G}$ are also isomorphic. Thus, if $\mathfrak{G}$ is an Abelian group then the groups $\widetilde{\mathfrak{G}}$ and $\mathfrak{G}$ are isomorphic .

One more example of a nontrivial ambivalent group is the group $\Psi_{Aut(\mathfrak{G})}$ generated by all functions $\sigma \in Aut(\mathfrak{G})$, i.e $\Psi_{Aut(\mathfrak{G})} = \langle Aut(\mathfrak{G})\rangle$. Recall, that the group operation $\cdot$ in $\Psi_{Aut(\mathfrak{G})}$ is defined to be pointwise multiplication of automorphisms.

If $\mathfrak{G}$ is noncommutative, then the function $\sigma \cdot \sigma' \in \Psi_{Aut(\mathfrak{G})}$, $\sigma, \sigma' \in Aut(\mathfrak{G})$, in general is not an automorphism. Therefore in this case $\Psi_{Aut(\mathfrak{G})}$ contains also elements that are not automorphism.

It should be noted that one could also define another operation $\circ$ in the group $\Psi_{Aut(\mathfrak{G})}$ namely superposition of functions. It is easy to prove that $\Psi_{Aut(\mathfrak{G})}$ is closed under the operation $\circ$. Thus, $\Psi_{Aut(\mathfrak{G})}$ is a near-ring with a group operation $\cdot$ (usually denoted as $+$) and a multiplicative semigroup operation $\circ$.

We denote by $\Psi_{\mathfrak{g}_1,\dots,\mathfrak{g}_k}$ a normal subgroup of the group Ψ, composed by all functions $f \in \Psi$ such that $f(\mathfrak{g}_j) = \mathfrak{e}$, $j = 1, \dots, k$. If $\{\mathfrak{g}_1, \dots, \mathfrak{g}_k\} = \mathcal{R}$ is a subgroup of $\mathfrak{G}$, then we denote by $\Psi_{\mathcal{R}}$ the subgroup $\Psi_{\mathfrak{g}_1,\dots,\mathfrak{g}_k}$.

Consider a linear representation Γ of an ambivalent group Ψ in the vector space $V = \mathbb{C}^r$.

A special case of Γ is a representation of the form $\Gamma^{\mathfrak{g}} = \Gamma^{\mathfrak{g}}_{\phi} = \{\phi(f(\mathfrak{g})),\ f \in \Psi\}$, where $\phi = \{\phi(\mathfrak{h}),\ \mathfrak{h} \in \mathfrak{G}\}$ is the representation of the group $\mathfrak{G}$ in the space $W = \mathbb{C}^t$ and $\mathfrak{g}$

is a fixed element of $\mathfrak{G}$. In particular, $\Gamma^{\mathfrak{e}}$ is the trivial representation formed by the identity $t \times t$–matrix I_t where $t = \chi(\mathfrak{e})$ and χ is a character of ϕ.

Definition 1.3. *Let $\mathcal{R}$ be a subgroup of the group $\mathfrak{G}$. A subgroup $\mathcal{R}^{\perp}$ of an ambivalent group Ψ, composed by all functions $f(\mathfrak{x}) \in \Psi$ such that $f(\mathfrak{x}) = \mathfrak{e}$ for all $\in \mathfrak{x} \in \mathcal{R}$, is called dual to $\mathcal{R}$ in the group Ψ.*

It is easy to show that $\mathcal{R}^{\perp}$ is a normal subgroup of the group Ψ.

Let $\Gamma^{\mathfrak{g}}_{\mathcal{R}^{\perp}}$ be a restriction of the representation $\Gamma^{\mathfrak{g}}$ to the subgroup $\mathcal{R}^{\perp}$. We denote by $l_{\mathfrak{g}}$ a multiplicity factor of the principal representation (equal to 1 in $\mathcal{R}^{\perp}$) ϕ_0 in the representation $\Gamma^{\mathfrak{g}}_{\mathcal{R}^{\perp}}$. In particular, $l_{\mathfrak{g}} = \chi(\mathfrak{e})$ for $\mathfrak{g} \in \mathcal{R}$.

For simplicity, we take the following assumption.

A *If $\mathfrak{g} \notin \mathcal{R}$, then $l_{\mathfrak{g}} = 0$, i.e. for $\mathfrak{g} \notin \mathcal{R}$ the representation $\Gamma^{\mathfrak{g}}_{\mathcal{R}^{\perp}}$ does not contain the principal representation.*

If the assumption **A** holds then the characteristic function of a subgroup $\mathcal{R}$ is as stated in the next lemma.

Lemma 1.1. *Let $l_{\mathfrak{g}} = 0$ for $\mathfrak{g} \notin \mathcal{R}$. Then*

$$\psi_{\mathcal{R}}(\mathfrak{x}) = \frac{1}{|\mathcal{R}^{\perp}|} \sum_{f \in \mathcal{R}^{\perp}} \chi(f(\mathfrak{x})) = \begin{cases} \chi(\mathfrak{e}), & \text{if } \mathfrak{x} \in \mathcal{R} \\ 0, & \text{if } \mathfrak{x} \notin \mathcal{R} \end{cases}, \tag{1.2}$$

where χ is a character of a representation ϕ of the group $\mathfrak{G}$.

Proof. Obvious.

Let σ be an automorphism of the group $\mathfrak{G}$. The transformation $\widehat{\sigma} : f(\mathfrak{x}) \to f(\mathfrak{x}^{\sigma^{-1}})$ is an automorphism of the group Ψ if $f(\mathfrak{x}^{\sigma^{-1}}) \in \Psi$ for all $f \in \Psi$. We assume that this property always holds for all $\sigma \in H$.

We call $\widehat{\sigma}$ automorphism induced by the automorphism σ. Thus, to a subgroup of automorphisms $H \subseteq Aut(\mathfrak{G})$ there corresponds a subgroup $\widehat{H} = \langle\{\widehat{\sigma}|\sigma \in H\}\rangle \subseteq Aut(\Psi)$ generated by all automorphisms $\widehat{\sigma}$.

The preimage $\{\widehat{\sigma}\}^{-1} \subseteq H$ of an automorphism $\widehat{\sigma}$ is a set of automorphisms σ such that $f^{\widehat{\sigma}}(\mathfrak{x}) = f(\mathfrak{x}^{\sigma^{-1}})$. In general, cardinalities of these preimages may differ for different $\widehat{\sigma}$. I.e., generally the transformation $\sigma \to \widehat{\sigma}$ is not a homomorphism from the group H to the group $\widehat{H}$.

The interrelation of classes $\widehat{C}_i$ of conjugate elements of the group Ψ with respect to a group of automorphisms $\widehat{H}$ and classes C_i of conjugate elements of the group $\mathfrak{G}$ with respect to a group of automorphisms H, depends on the structure of the group Ψ and in general case is unknown. In particular, the relation between the numbers $1 + m$ and $1 + l$ (amounts of classes of the conjugate elements of the groups $\mathfrak{G}$ and Ψ respectively) is unknown. We can answer these questions only in the case when $\mathfrak{G}$ and, hence, Ψ are Abelian groups.

Definition 1.4. *We denote by Ψ_n the group formed by all functions $f(\mathfrak{x}_1, \ldots, \mathfrak{x}_n) : \mathfrak{G}^n \longrightarrow \mathfrak{G}$ of the following form*

$$\begin{gathered} f(\mathfrak{x}_1, \ldots, \mathfrak{x}_n) = \mathfrak{g}_1 h_1(\mathfrak{x}_{i_1})\mathfrak{g}_2 h_2(\mathfrak{x}_{i_2})\mathfrak{g}_3 \cdots \mathfrak{g}_k h_k(\mathfrak{x}_{i_k})\mathfrak{g}_{k+1}, \\ i_s \in \{1, \ldots, n\},\ k = 0\ldots,\ h_j \in \Psi,\ f(\mathfrak{e}, \ldots, \mathfrak{e}) = \mathfrak{e}. \end{gathered} \tag{1.3}$$

It is easy to show, that if Ψ is an Abelian group, then Ψ_n coincides with Ψ^n.

Let τ be a permutation of the tuple of indices $\{1, \ldots, n\}$ and $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_n)$ be an automorphism of the group $\mathfrak{G}^n$. A group $H \wr S_n$ (S_n is the symmetric group) is the group of automorphisms of the group $\mathfrak{G}^n$. It is formed by all transformations

$$(\boldsymbol{\sigma}, \tau) : \mathfrak{g} = (\mathfrak{g}_1, \ldots, \mathfrak{g}_n) \to (\mathfrak{g}_{i_1}^{\sigma_1}, \ldots, \mathfrak{g}_{i_n}^{\sigma_n}),\ \boldsymbol{\sigma} \in H^n,\ \tau = \begin{pmatrix} 1 & , \ldots, & n \\ i_1 & , \ldots, & i_n \end{pmatrix} \in S_n.$$

It is easy to see, that the scheme of relations $S_{H \wr S_n}(\mathfrak{G}^n)$ coincides with the composition scheme $\boldsymbol{C}_H(\mathfrak{G}^n)$. The group $H \wr S_n$ is called a wreath product of groups H and S_n.

Definition 1.5. *We define the group of automorphisms $\widehat{H}_n$ of the group Ψ_n as the group formed by all transformations*

$$\boldsymbol{f}(\mathfrak{x}_1, \ldots, \mathfrak{x}_n) \to \boldsymbol{f}(\mathfrak{x}_{i_1}^{\sigma_1^{-1}}, \ldots, \mathfrak{x}_{i_n}^{\sigma_n^{-1}}), \text{ where } \boldsymbol{\sigma} \in H^n,\ \tau \in S_n. \tag{1.4}$$

Definition 1.6. *Relation scheme $S_{\widehat{H}_n}(\Psi_n)$ is called dual to the scheme $\boldsymbol{C}_H(\mathfrak{G}^n)$. To simplify notation we denote it by $\boldsymbol{C}_{\widehat{H}}(\Psi_n)$.*

Generally the scheme $\boldsymbol{C}_{\widehat{H}}(\Psi_n)$ is not composition in the sense of definition 3.2. If $\mathfrak{G}$ is an Abelian group and, hence, $H \sim \widehat{H}$, then the group $\widehat{H}_n$ is isomorphic to the group $H^n \wr S_n$. In particular, the association scheme $\boldsymbol{C}_{\widehat{H}}(\Psi_n)$ is composite. In this case the association schemes $\boldsymbol{C}_H(\mathfrak{G}^n)$ and $\boldsymbol{C}_{\widehat{H}}(\Psi_n)$ are isomorphic in the commonly accepted sense. All the above claims are easy to prove.

We denote by $wt(\boldsymbol{f})$, $\boldsymbol{f} \in \Psi_n$ the index $\boldsymbol{w}$ of a relation $\widehat{R}_{\boldsymbol{w}}$ of the scheme $\boldsymbol{C}_{\widehat{H}}(\Psi_n)$ to which the pair $(\boldsymbol{e}, \boldsymbol{f})$ belongs. This notation agrees with the above defined function (pseudo-weight) $wt(\mathfrak{g})$, $\mathfrak{g} \in \mathfrak{G}^n$, of the composition scheme $\boldsymbol{C}_H(\mathfrak{G}^n)$.

1.3 The main theorem.

The next theorem underlie all the claims about MacWilliams identities for the schemes $\boldsymbol{C}_H(\mathfrak{G}^n)$ and $\boldsymbol{C}_{\widehat{H}}(\Psi_n)$.

Theorem 1.1. *Let $\boldsymbol{C}_{\widehat{H}}(\Psi_n)$ be the association scheme dual to the scheme $\boldsymbol{C}_H(\mathfrak{G}^n)$, and $N_{\boldsymbol{c}}(\mathfrak{K})$ be a number of elements $\mathfrak{g}$ in a subgroup (code) $\mathfrak{K} \leq \mathfrak{G}^n$ with pseudo-weight $wt(\mathfrak{g})$ equal to $\boldsymbol{c} = (c_1, \ldots, c_m)$. Let $M_{\boldsymbol{w}}(\mathfrak{K}^{\perp})$ be a number of elements $\boldsymbol{f}$ in a subgroup (code) $\mathfrak{K}^{\perp} \leq \Psi_n$ with pseudo-weight $wt(\boldsymbol{f})$ equal to $\boldsymbol{w}$.*

Suppose , that for the subgroup $\mathfrak{K}$ of the group $\mathfrak{G}^n$ assumption **A** *holds, i.e. for $\mathfrak{g} \notin \mathcal{R}$ the representation $\Gamma_{\mathcal{R}^{\perp}}^{\mathfrak{g}}$ does not contain the principal representation.*

Then

i *The sum*

$$P(\boldsymbol{f}, \boldsymbol{c}) = \sum_{wt(\mathfrak{g})=\boldsymbol{c}} \chi(\boldsymbol{f}(\mathfrak{g})) \tag{1.5}$$

depends only on the value $\boldsymbol{w}$ of the pseudo-weight $wt(\boldsymbol{f})$, i.e. $P(\boldsymbol{f}, \boldsymbol{c}) = P(\boldsymbol{f}', \boldsymbol{c})$ if $wt(\boldsymbol{f}) = wt(\boldsymbol{f}')$.

ii

$$\chi(\mathfrak{e}) N_{\boldsymbol{c}}(\mathcal{R}) = \frac{1}{|\mathfrak{K}^{\perp}|} \sum_{\boldsymbol{w}} M_{\boldsymbol{w}}(\mathfrak{K}^{\perp}) p(\boldsymbol{w}, \boldsymbol{c}), \tag{1.6}$$

where $p(\boldsymbol{w}, \boldsymbol{c}) = P(\boldsymbol{f}, \boldsymbol{c})$, if $wt(\boldsymbol{f}) = \boldsymbol{w}$, and χ is the character of a representation of the group $\mathfrak{G}$.

Note, that the right-hand side of equality (1.6) (more precisely the function $p(\boldsymbol{w},\boldsymbol{c})$) depends also on a choice of representation ϕ of the group $\mathfrak{G}$, i.e. the number $N_{\boldsymbol{c}}(\mathcal{R})$ has in general nonunique representation in terms of numbers $M_{\boldsymbol{w}}(\mathfrak{K}^{\perp})$.

It should be noted, that Camion [14] proved an identity, formulated in terms of a group algebra, somewhat weaker than (1.6) in the case, when $\mathfrak{G}$ is an Abelian group and H is the trivial group of automorphisms.

We can show that if Ψ is an Abelian group then the function $p(\boldsymbol{z},\boldsymbol{c})$ is an orthogonal polynomial $p_{\boldsymbol{c}}(\boldsymbol{z})$ in m integer-valued variables $\boldsymbol{z} = (z_0,\ldots,z_m)$. As a consequence, we obtain an identity for association schemes which is analogous to the well-known MacWilliams identity. In the case of non-Abelian group Ψ evaluation of the function $p(\boldsymbol{w},\boldsymbol{c})$ is more complicated.

1.4 Extension of the theorem 1.1.

We substantially generalize definitions 1.4, 1.5, 1.6 and theorem 1.1 (see theorem 5.1).

Consider a homomorphism π of the group $\mathfrak{G}$ into some group $\mathfrak{G}' = \pi(\mathfrak{G})$. The homomorphism π induces a homomorphism π' of the group Ψ into the group $\mathfrak{A}$ (see section 4). The elements of $\mathfrak{A}$ are functions $\widehat{f} = \pi'(f)$ mapping the group $\mathfrak{G}$ to the group $\pi(\mathfrak{G})$. A group operation in $\mathfrak{A}$ is multiplication of values of the functions in the group $\pi(\mathfrak{G})$.

On the group $\mathfrak{A}$ act automorphisms $\widehat{\sigma}'$, induced by automorphisms $\widehat{\sigma}$ of the group Ψ (see section 4).

We shall omit primes ($'$) in notation for the automorphisms $\widehat{\sigma}'$ of the group $\mathfrak{A}$, homomorphism π' and the group of automorphisms $\widehat{H}'$ of $\mathfrak{A}$ i.e. we shall use the same symbols, as for corresponding objects for the group Ψ. This could not cause confusion since the object being considered, Ψ or $\mathfrak{A}$ will always be clear from the context.

By $\mathfrak{A}_n$ we denote a group, formed by all functions $\widehat{\boldsymbol{f}} = \pi(\boldsymbol{f})$, $\boldsymbol{f} \in \Psi_n$, (see (1.4)) which map the group $\mathfrak{G}^n$ into the group $\pi(\mathfrak{G})$.

Accordingly, by $\widehat{H}_n'$ we denote a subgroup of the group $Aut(\mathfrak{A}_n)$ comprised by all automorphisms of the form $\pi(\boldsymbol{f}(\mathfrak{x}_1,\ldots,\mathfrak{x}_n)) \to \pi(\boldsymbol{f}(\mathfrak{x}_{i_1}^{\sigma_1^{-1}},\ldots,\mathfrak{x}_{i_n}^{\sigma_n^{-1}}))$, $\sigma_j \in H$, $(i_1,\ldots,i_n) \in$ $\in S_n$.

To simplify notation we denote the scheme $S_{\widehat{H}_n'}(\mathfrak{A}^n)$ by $\boldsymbol{C}_{\widehat{H}}(\mathfrak{A}^n)$.

Definition 1.7. *The association scheme $\boldsymbol{C}_{\widehat{H}}(\mathfrak{A}_n)$ is called dual to the scheme $C_H(\mathfrak{G}^n)$.*

Definition 1.8. *Let $\mathcal{R}$ be a subgroup of the group $\mathfrak{G}^n$ and let $\mathcal{R}'^{\perp}$ be a subgroup of the group $\mathfrak{A}_n$, formed by all elements $\pi(\boldsymbol{f}) \subseteq \mathfrak{A}_n$ such that $\pi(\boldsymbol{f}(\mathfrak{g})) = \pi(\mathfrak{e})$ for all $\mathfrak{g} \in \mathcal{R}$. The group $\mathcal{R}'^{\perp}$ is called dual to $\mathcal{R}$ in the group $\mathfrak{A}_n$.*

Thus, $\mathcal{R}'^{\perp}$ is formed by all elements $\pi(\boldsymbol{f})$ for which $\boldsymbol{f}(\mathfrak{x}) \in \ker\pi(\Psi_n/\mathcal{R}^{\perp})$, if $\mathfrak{g} \in \mathcal{R}$, where $\mathcal{R}^{\perp}$ is a group dual to $\mathcal{R}$ in the group Ψ_n. To simplify notation we shall omit primes ($'$) in $\mathcal{R}'^{\perp}$.

Theorem 5.1 (see section 5) is a straightforward generalization of the theorem 1.1 with the group Ψ_n replaced by $\mathfrak{A}_n$

1.5 MacWilliams identity for association schemes and orthogonal polynomials

In the case when $\mathfrak{A}$ is an Abelian group, the function $p(\boldsymbol{w},\boldsymbol{c})$ is determined by a matrix Λ of structural constants (see identity 1.7). In this case the association scheme $\boldsymbol{C}_{\widehat{H}}(\mathfrak{A}_n)$ is composition ($\mathfrak{A}_n = \mathfrak{A}^n$). Therefore the indices $\boldsymbol{w}$ of its relations $\widehat{R}_{\boldsymbol{w}}$ can be considered as vectors $\boldsymbol{w} = (w_0, \dots, w_l)$, where w_j is a number of coordinates of the vector $\widehat{\boldsymbol{f}} \in \mathfrak{A}^n$ which belong to a class $\widehat{C}_j$ of conjugate elements of $\mathfrak{A}$ with respect to its group of automorphisms $\widehat{H}$.

For a group code $\mathcal{R} \leq \mathfrak{G}^n$ and its dual code $\mathcal{R}^\perp \trianglelefteq \mathfrak{A}^n$ we derive an identity (see (5.4)) which relates a number $N_{\boldsymbol{c}}(\mathfrak{K})$ to numbers $M_{\boldsymbol{w}}(\mathfrak{K}^\perp)$ in a similar fashion as the MacWilliams identity does in the case of the Hamming space.

If $\mathfrak{G}$ is an Abelian group and π is an isomorphism, then the number $N_{\boldsymbol{c}}(\mathfrak{K})$ can be expressed as a sum of the numbers $M_{\boldsymbol{w}}(\mathfrak{K}^\perp)$ multiplied by values of a polynomial $p_{\boldsymbol{c}}(\boldsymbol{w}; \Lambda) = p(\boldsymbol{w}, \boldsymbol{c})$, $\boldsymbol{w} = (w_0, \dots, w_m)$, (see (1.6)), which is an orthogonal (with some weight function) polynomial in $1 + m$ integer variables w_j such that $w_0 + \dots + w_m = n$. A polynomial $p_{\boldsymbol{c}}(\boldsymbol{z}; \Lambda)$ is determined by a matrix $\Lambda = \Lambda_\chi(\boldsymbol{C}_H(\mathfrak{G}), \boldsymbol{C}_{\widehat{H}}(\mathfrak{A}))$ of structural constants of the group $\mathfrak{A}$ with respect to the group $\mathfrak{G}$. The entries of $\Lambda = |r_{i,j}|_{i=0,\dots,m, j=0,\dots,l}$ are as follows.

Let R_i and $\widehat{R}_j$ be relations of schemes $\boldsymbol{C}_H(\mathfrak{G})$ and $\boldsymbol{C}_{\widehat{H}}(\mathfrak{A})$ respectively. Then

$$r_{i,j} = \sum_{\mathfrak{x} \in C_i} \chi(\pi(f(\mathfrak{x}))) = \frac{1}{|St(\mathfrak{g})|} \sum_{\sigma \in H} \chi(\pi(f(\mathfrak{g}^\sigma))), \ (\pi(e), \pi(f(\mathfrak{g}))) \in \widehat{R}_j, \tag{1.7}$$

where $St(\mathfrak{g})$ is the stabilizer of $\mathfrak{g}$ in the group H and χ is a character of the linear representation ϕ of the group $\mathfrak{G}$.

If we put $z_1 = \dots = z_l = z$, $z_0 = n - z$, then the polynomial $\sum_{c_1 + \dots + c_m = s} p_{\boldsymbol{c}}(n - z, z, \dots, z; \Lambda) = p_s(z)$ turns out to be Krawtchuok polynomial $K_s^{(|\mathfrak{G}|)}(z)$ of degree s.

We propose several nontrivial examples, illustrating all the above concepts. Some of these examples are of independent interest.

1.6 Example

Let $\mathfrak{G} = \mathbb{Z}_{p^2}$ be an additive group of residues modulo p^2. As a group Ψ we take a group of functions $f(\mathfrak{x}) = u\mathfrak{x}$, $0 \leq u < p^2$ with the group operation $+$ being addition of functions modulo p^2. As a group of automorphisms H we take all transformations $x \to ax, p \nmid a$. The group operation in H is superposition of two transformations. The order of H is equal to $p(p-1)$ and it is isomorphic to the group $\mathbb{Z}^*_{p^2}$.

Obviously, the association scheme $\boldsymbol{C}_H(\mathfrak{G})$ has three relations ($m = 2$): $R_0 = \{(g, g) | g \in \mathfrak{G}\}$, $R_p = \{(g, g + ph) | g, h \in \mathfrak{G}, ph \neq 0\}$, $R_1 = \{(g, g + h) | g, h \in \mathfrak{G}, p \nmid h\}$. We take as π an isomorphism mapping $\mathfrak{G}$ into multiplicative group of characters $\mathfrak{A} = \{\varrho_a(x) = \exp\left(\frac{2\pi i a x}{p^2}\right) | a \in \mathfrak{G}\}$, and finally, as a group of automorphisms $\widehat{H}$ of the group $\mathfrak{A}$ induced by H we choose the group, formed by all transformations $\varrho_b(x) \to \varrho_{ab}(x), p \nmid a$.

As $\Gamma^{\mathfrak{g}} = \Gamma^a$, $a \in \mathbb{Z}_{p^2}$, we take one-dimensional representation $\varrho_y(a) = \varrho_a(y)$ of the group Ψ.

The group $\mathfrak{A}_n = \mathfrak{A}^n$ is formed by all functions $\varrho_{\boldsymbol{a}}(\boldsymbol{x}) = \exp\left(\frac{2\pi i a_1 x_1}{p^2}\right) \cdots \exp\left(\frac{2\pi i a_n x_n}{p^2}\right)$, $\boldsymbol{a} = (a_1, \dots, a_n)$, $\boldsymbol{x} = (x_1, \dots, x_n) \in \mathbb{Z}^n_{p^2}$. We consider as a subgroup $\mathcal{R} \trianglelefteq \mathfrak{G}^n$ a group $\mathcal{R} = \mathfrak{G}^n_{\boldsymbol{a}_1} \bigcap \dots \bigcap \mathfrak{G}^n_{\boldsymbol{a}_r}$, where $\mathfrak{G}^n_{\boldsymbol{a}} = \ker \varrho_{\boldsymbol{a}}(\boldsymbol{x})$ is the kernel of homomorphism $\varrho_{\boldsymbol{a}}(\boldsymbol{x})$ of the group $\mathfrak{G}^n$ into the group of roots of unity.

In this case the group $\mathcal{R}^\perp \trianglelefteq \mathfrak{A}_n$ is a linear space spanned by $\varrho_{\boldsymbol{a}_r}(\boldsymbol{x}), \dots, \varrho_{\boldsymbol{a}_r}(\boldsymbol{x})$. Note that group operation in $\mathcal{R}^\perp$ is multiplication. Obviously, this space coincides with a linear code, which is dual to the linear code $\mathcal{R} \trianglelefteq \mathfrak{G}^n$ under the commonly used definition of duality.

Collection $[\boldsymbol{a}_1, \dots, \boldsymbol{a}_r]$ can be treated as the set of the rows of the parity-check matrix of the code $\mathcal{R}$.

The matrix of structural constants in the example being considered looks as follows

$$\Lambda = \begin{Vmatrix} 1 & p-1 & p(p-1) \\ 1 & p-1 & -p \\ 1 & -1 & 0 \end{Vmatrix}, \tag{1.8}$$

and the derived identity is

$$\sum_{c_0+c_p+c_1=n} N_{(c_0,c_p,c_1)}(\mathfrak{K};\, z_0^{c_0} z_p^{c_p} z_1^{c_1} = \frac{1}{|\mathfrak{K}^{\perp}|} \sum_{w_0+w_p+w_1=n} M_{(w_0,w_p,w_1)}(\mathfrak{K}^{\perp})\,(z_0+(p-1)z_p+p(p-1)z_1)^{w_0} (z_0+(p-1)z_p-pz_1)^{w_p}\,(z_0-z_p)^{w_1}, \tag{1.9}$$

where $N_{(c_0,c_p,c_1)}(\mathfrak{K})$ is the number of vectors $\boldsymbol{g}$ in the code $\mathfrak{K}$, which contain c_0 zero coordinates, c_p nonzero coordinates which are multiples of p, and c_1 coordinates coprime with p. Accordingly, $M_{(w_0,w_p,w_1)}(\mathfrak{K}^{\perp})$ is the number of functions (vectors) $\varrho_{\boldsymbol{a}}(\boldsymbol{x})$, $\boldsymbol{a} = (a_1, \dots, a_n)$, in the code $\mathfrak{K}^{\perp} \subseteq \mathfrak{A}^n$ such that $\boldsymbol{a}$ has w_0 zero coordinates, w_p nonzero coordinates which are multiples of p, and w_1 coordinates coprime with p.

2. Background

Let Γ be an exact (one-to-one) representation of a finite group $\mathfrak{G}$ in the unitary space $\mathbb{C}^f$, $Aut(\mathfrak{G})$ be the group of all automorphisms of $\mathfrak{G}$, $H = \{\sigma_0, \dots, \sigma_t\}$ be a subgroup of $Aut(\mathfrak{G})$, $C_j^H = \{\mathfrak{h}_j^{\sigma} | \sigma \in H\}$, $j = 0, \dots, m$, $C_0^H = \{\mathfrak{e}\}$, be the classes of conjugate elements relative to the subgroup H, and $\mathfrak{h}_j$ be the representative of C_j^H. We use Latin letters for elements (matrices) of Γ. We assume implicitly, that to an element $\mathfrak{g} \in \mathfrak{G}$ there corresponds a matrix g. We suppose, that Γ does not contain a principal representation, i.e. that $\sum_{\mathfrak{g}\in G} g = 0$. For simplicity we omit the superscript H in C_j^H.

2.1 The association scheme

To any subgroup H of $Aut(\mathfrak{G})$ there corresponds a scheme $\mathcal{S}_H(\mathfrak{G})$, which, as will be shown later, is a noncommutative association scheme (association scheme) under the commonly accepted definition.

Definition 2.1 (The scheme $\mathcal{S}$). . *A scheme $\mathcal{S}$ is a pair $\{X, \boldsymbol{R}\}$, where X is a finite set of vertices of $\mathcal{S}$, and $\boldsymbol{R} = \{R_0, \dots, R_m\}$ is a partition on the set $X \times X$ ($X \times X = \cup_{j=0}^{m} R_j$), $R_0 = \{(\mathfrak{g}, \mathfrak{g}) | \mathfrak{g} \in \mathfrak{G}\}$. The elements of the set $X \times X$ are called edges of the scheme $\mathcal{S}$.*

Definition 2.2 (The scheme $\mathcal{S}_H(\mathfrak{G})$). .

The set of vertices X of a scheme $\mathcal{S}_H(\mathfrak{G})$ is the set of elements of the group $\mathfrak{G}$ i.e. $X = \mathfrak{G}$.

The set $\mathfrak{G} \times \mathfrak{G}$ is partitioned into classes R_j, $j = 0, \dots, m$ ($\mathfrak{G} \times \mathfrak{G} = \cup_{j=0}^{m} R_j$), defined as follows: $R_j = \{(\mathfrak{g}, \mathfrak{h}\mathfrak{g}) | \, \mathfrak{h} \in C_j, \mathfrak{g} \in \mathfrak{G}\}$.

Thus, R_j consists of edges $(\mathfrak{g}, \mathfrak{g}')$, for which $\mathfrak{g}'\mathfrak{g}^{-1} \in C_j$. Obviously, $|R_j| = |G||C_j|$. We assume, that the edge $(\mathfrak{e}, \mathfrak{h}_j)$ is a representative of the class R_j is , where $\mathfrak{h}_j$ is a representative of the class of conjugate elements C_j.

Sometimes we use $\mathcal{S}_H$ as a shorthand for $\mathcal{S}_H(\mathfrak{G})$.

Lemma 2.1. . *For the scheme $\mathcal{S}_H(\mathfrak{G})$ the following holds.*

i *The scheme $\mathcal{S}_H(\mathfrak{G})$ is an association scheme.*

ii *If edges $(\mathfrak{g}, \mathfrak{g}')$ and $(\mathfrak{g}'^{-1}, \mathfrak{g}^{-1})$ belong to the same class of relations for any $\mathfrak{g}$, then the association scheme $\mathcal{S}_H(\mathfrak{G})$ is a commutative association scheme.*

iii *Let $(\mathfrak{e}, \mathfrak{h}_j)$ be a representative of the class R_j. The reciprocal relation $R_j^T = \{(y, x)|(x, y) \in \in R_j\}$ is a relation $R_{j'}$ of the scheme $\mathcal{S}_H(\mathfrak{G})$ such that $(\mathfrak{e}, \mathfrak{h}_j^{-1}) \in R_{j'}$.*

Proof. (i.) We need to show that the number $r_{i,j}(\mathfrak{g}, \mathfrak{g}')$ of those $\mathfrak{h} \in \mathfrak{G}$, for which $(\mathfrak{g}, \mathfrak{h}) \in R_j$, $(\mathfrak{h}, \mathfrak{g}') \in R_i$ is the same for all $(\mathfrak{g}, \mathfrak{g}') \in R_k$, i.e. the number $r_{i,j}(\mathfrak{g}, \mathfrak{g}') = r_{i,j}^k$ is determined uniquely by a class R_k, to which the edge $(\mathfrak{g}, \mathfrak{g}')$ belongs.

If $(\mathfrak{g}, \mathfrak{h}) \in R_j$, $(\mathfrak{h}, \mathfrak{g}') \in R_i$, then $(\mathfrak{g}\mathfrak{h}', \mathfrak{h}\mathfrak{h}') \in R_j$, $(\mathfrak{h}\mathfrak{h}', \mathfrak{g}'\mathfrak{h}') \in R_i$ for any $\mathfrak{h}' \in \mathfrak{G}$. Therefore the numbers $r_{i,j}(\mathfrak{g}, \mathfrak{g}')$ and $r_{i,j}(\mathfrak{g}\mathfrak{h}', \mathfrak{g}'\mathfrak{h}')$ are equal for all $\mathfrak{h}' \in \mathfrak{G}$. If we put $\mathfrak{h}' = \mathfrak{g}^{-1}$ then $r_{i,j}(\mathfrak{g}, \mathfrak{g}') = r_{i,j}(\mathfrak{e}, \mathfrak{g}'\mathfrak{g}^{-1})$.

Obviously, $r_{i,j}(\mathfrak{g}, \mathfrak{g}') = r_{i,j}(\mathfrak{g}^\sigma, \mathfrak{g}'^\sigma)$ for any $\sigma \in H$. If $\mathfrak{h}_k$ is a representative of a class of conjugate elements C_k and $(\mathfrak{g}, \mathfrak{g}') \in R_k$, then there exists $\sigma \in H$, such that $(\mathfrak{g}'\mathfrak{g}^{-1})^\sigma = = \mathfrak{h}_k$. Therefore $r_{i,j}(\mathfrak{g}, \mathfrak{g}') = r_{i,j}(\mathfrak{e}, \mathfrak{g}'\mathfrak{g}^{-1}) = r_{i,j}(\mathfrak{e}, \mathfrak{h}_k)$, i.e. the number $r_{i,j}(\mathfrak{g}, \mathfrak{g}')$ is determined uniquely by a class of relations R_k, to which the edge $(\mathfrak{g}, \mathfrak{g}')$ belongs.

To finish the proof of item **i** it suffices to show that reciprocal relations R_j^T belong to the scheme $\mathcal{S}_H(\mathfrak{G})$. This is follows from item **iii**.

(**ii**.) We need to show that if the edge $(\mathfrak{g}, \mathfrak{g}')$ belongs to the same class of relations as $(\mathfrak{g}^{-1}, \mathfrak{g}'^{-1})$ then $r_{i,j}(\mathfrak{g}, \mathfrak{g}') = r_{j,i}(\mathfrak{g}, \mathfrak{g}')$ for all $(\mathfrak{g}, \mathfrak{g}') \in \mathfrak{G} \times \mathfrak{G}$.

Let $(\mathfrak{e}, \mathfrak{h}) \in R_i$ and $(\mathfrak{h}, \mathfrak{h}_k) \in R_j$. Then $(\mathfrak{e}, \mathfrak{h}_k\mathfrak{h}^{-1}) \in R_j$. We show, that if the condition of item **ii**. holds, then $(\mathfrak{h}_k\mathfrak{h}^{-1}, \mathfrak{h}_k) \in R_i$. Indeed, the condition of **ii**. implies, that edges $(\mathfrak{h}_k^{-1}, (\mathfrak{h}_k\mathfrak{h}^{-1})^{-1})$ and $(\mathfrak{e}, \mathfrak{h})$ belong to the same class of relations R_i. This implies the claim being proved.

Thus, substituting $\mathfrak{h}_k\mathfrak{h}^{-1}$ for $\mathfrak{h}$ in $(\mathfrak{e}, \mathfrak{h}) \in R_i$ and $(\mathfrak{h}, \mathfrak{h}_k) \in R_j$ we in fact permute indices of classes R_i and R_j. Therefore $r_{i,j}(\mathfrak{g}, \mathfrak{g}') = r_{j,i}(\mathfrak{g}, \mathfrak{g}')$ for all $(\mathfrak{g}, \mathfrak{g}')$.

(**iii**.) It is easy to show that the set $R_j^T = \{(\mathfrak{h}_j\mathfrak{g}, \mathfrak{g})|\mathfrak{h}_j \in C_j, \mathfrak{g} \in \mathfrak{G}\}$ coincides with the class of relations $R_{j'}$ which has a representative $(\mathfrak{e}, \mathfrak{h}_j^{-1})$. □

It is easy to show, that $\mathcal{S}_H$ is an commutative association scheme provided that $\mathfrak{G}$ is an Abelian group, or H is a group of inner automorphisms.

If edges $(\mathfrak{g}, \mathfrak{g}'), (\mathfrak{g}', \mathfrak{g})$ belong to the same class of relations, then the scheme $\mathcal{S}_H$ is called symmetric association scheme.

It is easy to see, that the association scheme $\mathcal{S}_H$ is symmetric association scheme, provided that elements $\mathfrak{g}, \mathfrak{g}^{-1}$ belong to the same class of conjugate elements of the group $\mathfrak{G}$.

Higman [10], Bannai [16] and Delsarte [8] considered association schemes with orbits $R_j = \{(x^\sigma, y^\sigma)|\sigma \in \tilde{H}\}$ playing the role of classes R_j, where $\tilde{H}$ is a group of substitution automorphisms of the set X and $(x, y) \in X \times X$. Our association scheme $\mathcal{S}_H(\mathfrak{G})$ is a special case of this, since we may take X to be the group $\mathfrak{G}$ and $\tilde{H}$ to be the the semidirect product of H with $\mathfrak{G}$.

The scheme $\mathcal{S}_H(\mathfrak{G})$ with Abelian group $\mathfrak{G}$ and H formed by trivial homomorphism only is usually called Hecke scheme. Such schemes were studied by Camion [14].

Remark 2.1. *It is possible to prove (mathematical folklore), that only an elementary Abelian group $\mathfrak{G}$ can have two classes of conjugate elements relative to a group $Aut(\mathfrak{G})$. All other groups $\mathfrak{G}$ are partitioned into three or more classes of conjugate elements.*

3. Relation schemes on $\mathfrak{G}^n$

We assume, that elements of a group H^n act coordinate-wise on $\mathfrak{G}^n$. A class of conjugate elements C_j, where $\boldsymbol{j} = (j_1, \dots, j_n)$, is formed by all vectors $\boldsymbol{\mathfrak{g}} = (\mathfrak{g}_1, \dots, \mathfrak{g}_n)$ such that $\mathfrak{g}_s \in C_{j_s}$.

Definition 3.1 (Definition of scheme $S_{H^n}(\mathfrak{G}^n)$). .

A set of the vertices X of the scheme $S_{H^n}(\mathfrak{G}^n)$ is defined to be a group $\mathfrak{G}^n$.

A set $\mathfrak{G}^n \times \mathfrak{G}^n$ is partitioned into $(1+m)^n$ classes $\{R_{\boldsymbol{j}} | \boldsymbol{j} = (j_1, \dots, j_n); 0 \leq j_s \leq m\}$, where $(\boldsymbol{\mathfrak{g}}, \boldsymbol{\mathfrak{g}}') \in R_{\boldsymbol{j}}$, if $\boldsymbol{\mathfrak{g}}'\boldsymbol{\mathfrak{g}}^{-1} \in C_{\boldsymbol{j}}$.

We call the scheme $S_{H^n}(\mathfrak{G}^n)$ an nth degree of the scheme $S_H(\mathfrak{G})$.

>From the lemma 2.1 follows

Theorem 3.1. *The scheme $S_{H^n}(\mathfrak{G}^n)$ is a association scheme.*

The composition association scheme $\boldsymbol{C}_H(\mathfrak{G}^n)$, defined below, is obtained from $S_{H^n}(\mathfrak{G}^n)$ by taking unions of some of its classes $R_{\boldsymbol{j}}$. For $n = 1$ the schemes $\boldsymbol{C}_H(\mathfrak{G}^n)$ and $S_{H^n}(\mathfrak{G}^n)$ are identical.

Define $c_j(\boldsymbol{\mathfrak{g}})$ to be a number of coordinates $\mathfrak{g}_s$ of a vector $\boldsymbol{\mathfrak{g}} = (\mathfrak{g}_1, \dots, \mathfrak{g}_n)$ such, that $\mathfrak{g}_s \in C_j$. Vector $\boldsymbol{c}(\boldsymbol{\mathfrak{g}}) = (c_0(\boldsymbol{\mathfrak{g}}), \dots, c_m(\boldsymbol{\mathfrak{g}}))$, where $1+m$ is a number of classes of conjugate elements in G relative to a group of automorphisms H, is called composition of the vector $\boldsymbol{\mathfrak{g}}$.

Definition 3.2 (Definition of the composition scheme $C_H(\mathfrak{G}^n)$).

A set of vertices X of the scheme $C_H(\mathfrak{G}^n)$ is the set of all elements of the group $\mathfrak{G}^n$.

A set $\mathfrak{G}^n \times \mathfrak{G}^n$ is partitioned into classes $\{R_{\boldsymbol{c}} | \boldsymbol{c} = (c_0, \dots, c_m); c_0 + \dots + c_n = n\}$, where $(\boldsymbol{\mathfrak{g}}, \boldsymbol{\mathfrak{g}}') \in R_{\boldsymbol{c}}$, if $\boldsymbol{c}(\boldsymbol{\mathfrak{g}}'\boldsymbol{\mathfrak{g}}^{-1}) = \boldsymbol{c}$.

Thus, a class $R_{\boldsymbol{c}}$ consists of all edges $(\boldsymbol{\mathfrak{g}}, \boldsymbol{\mathfrak{g}}')$ which have identical compositions $\boldsymbol{c}(\boldsymbol{\mathfrak{g}}'\boldsymbol{\mathfrak{g}}^{-1}) = \boldsymbol{c}$. As it was mentioned above, $C_H(\mathfrak{G}) = S_H(\mathfrak{G})$.

The scheme $\boldsymbol{C}_H(\mathfrak{G}^n)$ was defined by Delsarte [6]. Camion [14] (p. 1506) defined $C_H(\mathfrak{G}^n)$ in a different way as compared to the definition 3.2. In the same paper Camion suggested to call it a Delsarte expansion of the scheme $\boldsymbol{C}_H(\mathfrak{G})$.

Definition 3.3 (Definition of the scheme $S_{H^n \wr S_n}(\mathfrak{G}^n)$ from the paper [14]).

The group $H^n \wr S_n$ of automorphisms of $\mathfrak{G}^n$ is defined as follows. Let $\tau = (i_1, \dots, i_n)$ be a permutation of the tuple $(1, \dots, n)$ and $\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_n)$ be an automorphism of the group $\mathfrak{G}^n$. A group $H^n \wr S_n$ is formed by all transformations $(\boldsymbol{\sigma}, \tau) : \boldsymbol{\mathfrak{g}} = (\mathfrak{g}_1, \dots, \mathfrak{g}_n) \to (\mathfrak{g}_{i_1}^{\sigma_1}, \dots \dots, \mathfrak{g}_{i_n}^{\sigma_n})$, $\boldsymbol{\sigma} \in H^n$, $\tau \in S_n$.

The scheme $S_{H^n \wr S_n}(\mathfrak{G}^n)$ is defined according to the definition 2.2.

It is easy to see, that the association scheme $S_{H^n \wr S_n}(\mathfrak{G}^n)$ coincides with the composition association scheme $\boldsymbol{C}_H(\mathfrak{G}^n)$ (definition 3.2).

Theorem 3.2. *The composition scheme $\boldsymbol{C}_H(\mathfrak{G}^n)$ is a association scheme.*

Proof follows from definition 3.3 and lemma 2.1.

4. Relation scheme $C_{\widehat{H}}(\mathfrak{A}_n)$, dual to $C_H(\mathfrak{G}^n)$

Consider a homomorphism π of the group $\mathfrak{G}$ to a group $\mathfrak{G}' = \pi(\mathfrak{G})$. We call functions $f, f' \in \Psi$ where Ψ is an ambivalent group of the group $\mathfrak{G}$, equivalent with respect to the homomorphism π, if $\pi(f(\mathfrak{g})) = \pi(f'(\mathfrak{g}))$ for all $\mathfrak{g} \in \mathfrak{G}$. Obviously, a set of functions $f \in \Psi$ such that $\pi(f(\mathfrak{g})) = \pi(\mathfrak{e})$ for all $\mathfrak{g} \in \mathfrak{G}$, is a normal subgroup Ψ_π of the group Ψ.

We consider the group $\mathfrak{A} = \Psi / \Psi_\pi$. Its elements can be considered as classes of equivalent functions $f \in \Psi$. The group Ψ as well as $\mathfrak{A}$ is called an ambivalent group of the group $\mathfrak{G}$.

A homomorphism π' mapping Ψ to $\mathfrak{A}$ is determined as follows $\pi' : f \to \pi(f)$. An image of an element $f \in \Psi$ under the homomorphism π' is denoted by $\widehat{f} = \pi'(f)$. An element $\widehat{f}$ of $\mathfrak{A}$ can be considered as a function mapping elements of the group $\mathfrak{G}$ into elements of the group $\pi(\mathfrak{G})$. Group operation in $\mathfrak{A}$ is a product of functions (in $\pi(\mathfrak{G})$).

On the group $\mathfrak{A}$ act automorphisms $\widehat{\sigma}' = \widehat{\sigma}'(\mathring{\sigma})$, induced by automorphisms $\mathring{\sigma}$ of the group Ψ. Namely, $\widehat{f}^{\,\widehat{\sigma}'} = \pi'(f)^{\widehat{\sigma}'} = \pi'(f^{\mathring{\sigma}}) = \pi'(f(\mathfrak{x}^{\sigma}))$. The group formed by automorphisms $\widehat{\sigma}'$, $\sigma \in H$, is denoted by $\widehat{H}'$.

In notation for automorphisms of the group $\mathfrak{A}$, homomorphism $\pi'(f)$ and group of automorphisms $\widehat{H}'$ we shall omit the symbol $'$ i.e. we shall use the same symbols, as for corresponding objects defined for the group Ψ. It should not cause any confusion for it will always be clear what object, Ψ or $\mathfrak{A}$ we deal with.

Accordingly, by $\mathfrak{A}_n$ we denote a group, formed by all functions

$$\begin{gathered} \widehat{\boldsymbol{f}}(\mathfrak{x}_1, \ldots, \mathfrak{x}_n) = \pi(\boldsymbol{f}) = \pi(\mathfrak{g}_1)\pi(h_1(\mathfrak{x}_{i_1}))\pi(\mathfrak{g}_2)\cdots\pi(\mathfrak{g}_k)\pi(h_k(\mathfrak{x}_{i_k}))\pi(\mathfrak{g}_{k+1}), \\ h_j \in \Psi,\ \mathfrak{g}_i \in \mathfrak{G},\ \pi(\boldsymbol{f}(\mathfrak{e})) = \pi(\mathfrak{e}), \end{gathered} \tag{4.1}$$

which map the group $\mathfrak{G}^n$ to the group $\pi(\mathfrak{G})$.

Let $\tau = (i_1, \ldots, i_n)$ be a permutation of the tuple $(1, \ldots, n)$ and let $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_n)$ be an automorphism of the group $\mathfrak{G}^n$. Group $H^n \wr S_n$ of automorphisms of the group $\mathfrak{G}^n$ is formed by all transformations $(\boldsymbol{\sigma}, \tau) : \boldsymbol{\mathfrak{g}} = (\mathfrak{g}_1, \ldots, \mathfrak{g}_n) \to (\mathfrak{g}_{i_1}^{\sigma_1}, \ldots, \mathfrak{g}_{i_n}^{\sigma_n})$, $\boldsymbol{\mathfrak{g}} \in H^n$, $\tau \in S_n$. As it was already mentioned, the association scheme $S_{H \wr S_n}(\mathfrak{G}^n)$ coincides with the composition association scheme $\boldsymbol{C}_H(\mathfrak{G}^n)$.

Definition 4.1. *A group of all mappings*

$$\widehat{\boldsymbol{f}}(\mathfrak{x}_1, \ldots, \mathfrak{x}_n) \to \widehat{\boldsymbol{f}}(\mathfrak{x}_{i_1}^{\sigma_1}, \ldots, \mathfrak{x}_{i_n}^{\sigma_n}),\ (\sigma_1, \ldots, \sigma_n) \in H^n,\ (i_1, \ldots, i_n) \in S_n. \tag{4.2}$$

is called a group of automorphisms of the group $\mathfrak{A}_n$, induced by automorphisms $H^n \wr S_n$ of the group $\mathfrak{G}^n$. It is denoted by $\widehat{H}_n$. The group operation in $\widehat{H}_n$ is a superposition of mappings.

In other words, $\widehat{H}_n$ is a group of automorphisms of the group $\mathfrak{A}_n$, induced by the group of automorphisms $H^n \wr S_n$ of the group $\mathfrak{G}^n$.

Definition 4.2 (Definition of dual scheme $\boldsymbol{C}_{\widehat{H}}(\mathfrak{A}_n)$). *The association scheme $S_{\widehat{H}^n \wr S_n}(\mathfrak{A}_n)$ is called dual to the scheme $\boldsymbol{C}_H(\mathfrak{G}^n)$ and is denoted by $\boldsymbol{C}_{\widehat{H}}(\mathfrak{A}_n)$.*

The scheme $\boldsymbol{C}_{\widehat{H}}(\mathfrak{A}_n)$ generally speaking is not a composition scheme according to the definition 3.2. The number of its relations $\widehat{R}_w$ and its structure in general case remain unknown.

If $\mathfrak{A}$ is an Abelian group, then $\widehat{H}_n$ is a composition scheme according to the definition 3.2, i.e it is isomorphic to $\widehat{H}^n$ where $\widehat{H}$ is the group of automorphisms of $\mathfrak{A}$ induced by the group H. Furthermore if in this case $\mathfrak{G}$ and $\mathfrak{A}$ are isomorphic, then the groups H and $\widehat{H}$ as well as $\mathfrak{G}^n$ and $\mathfrak{A}_n$ are pairwise isomorphic. These claims are easy to prove.

5. Main identity

Let $\mathcal{R}$ be a subgroup of the group $\mathfrak{G}^n$. Subgroup $\widehat{\mathcal{R}}^{\perp} \trianglelefteq \mathfrak{A}_n$ of the group $\mathfrak{A}_n$, composed by all elements $\widehat{f} = \pi(f)$, such that $\pi(\boldsymbol{f}(\mathfrak{g})) = \pi(\mathfrak{e})$ for all $\mathfrak{g} \in \mathcal{R}$, is called dual to $\mathcal{R}$ in the group $\mathfrak{A}_n$. Thus, $\widehat{\mathcal{R}}^{\perp}$ is composed by all elements $\widehat{\boldsymbol{f}} = \pi(\boldsymbol{f})$, such that $\boldsymbol{f}(\mathfrak{g}) \in \ker \pi(\Psi_n / \mathcal{R}^{\perp})$ for all $\mathfrak{g} \in \mathcal{R}$, where $\mathcal{R}^{\perp}$ is a group, dual to $\mathcal{R}$ in the group Ψ_n. It is easy to see, that $\widehat{\mathcal{R}}^{\perp}$ is a normal subgroup of the group $\mathfrak{A}_n$.

Let $\widehat{\phi}$ be a representation of the group $\pi(\mathfrak{G})$, $\widehat{\chi}$ be a character of the representation $\widehat{\phi}$ and $\widehat{\Gamma}^{\mathfrak{g}} = \{\widehat{\phi}(\pi(f(\mathfrak{g})))|\pi(f(\mathfrak{x})) \in \mathfrak{A}\}$, where $\mathfrak{g}$ is a fixed element of $\mathfrak{G}$, be a representation of the group $\mathfrak{A}$. As above, by $\widehat{\Gamma}^{\mathfrak{g}}_{\widehat{\mathcal{R}}^{\perp}}$ we denote restriction of the representation $\widehat{\Gamma}^{\mathfrak{g}}$ to the subgroup $\widehat{\mathcal{R}}^{\perp}$.

We denote by $\widehat{l}_{\mathfrak{g}}$ multiplicity of the main representation $\widehat{\phi}_0$ in $\widehat{\Gamma}^{\mathfrak{g}}_{\widehat{\mathcal{R}}^{\perp}}$. In particular, $\widehat{l}_{\mathfrak{g}} = \widehat{\chi}(\pi(\mathfrak{e}))$ for $\mathfrak{g} \in \mathcal{R}$.

We require that for ambivalent group $\mathfrak{A}_n$, a subgroup $\mathcal{R} \subseteq \mathfrak{G}^n$ and representation $\widehat{\phi}$ of the group $\pi(\mathfrak{G})$ the following assumption holds

$\widehat{A}_n$ *If* $\mathfrak{g} \notin \mathcal{R}$, *then* $\widehat{l}_{\mathfrak{g}} = 0$, *i.e. for* $\mathfrak{g} \notin \mathcal{R}$ *the main representation does not enter into* $\widehat{\Gamma}^{\mathfrak{g}}_{\widehat{\mathcal{R}}^{\perp}}$.

The next lemma follows from the well-known claim about orthogonality of distinct characters of a finite group (see, for example, [15], pp. 12).

Lemma 5.1. *Let* $\widehat{l}_{\mathfrak{g}} = 0$ *for* $\mathfrak{g} \notin \mathcal{R}$. *Then*

$$\psi_{\mathcal{R}}(\mathfrak{x}) = \frac{1}{|\widehat{\mathcal{R}}^{\perp}|} \sum_{\pi(f) \in \widehat{\mathcal{R}}^{\perp}} \widehat{\chi}(\pi(f(\mathfrak{x}))) = \begin{cases} \widehat{\chi}(\mathfrak{e}) & , \text{if } \mathfrak{x} \in \mathcal{R} \\ 0 & , \text{if } \mathfrak{x} \notin \mathcal{R} \end{cases} \tag{5.1}$$

To simplify notation, we use for pseudo-weight $wt(\pi(\boldsymbol{f}))$ and pseudo-distance $\lambda(\pi(\boldsymbol{f}), \pi(\boldsymbol{f}'))$, $\boldsymbol{f}, \boldsymbol{f}' \in \mathfrak{A}_n$, on the association scheme $C_{\widehat{H}}(\mathfrak{A}^n)$ the same symbols wt and λ, as for the scheme $C_H(\mathfrak{G}^n)$. Thus, $wt(\pi(\boldsymbol{f}))$ is an index of the class $\widehat{C}_{\boldsymbol{w}}$ of conjugate elements of the group $\mathfrak{A}_n$ to which function $\widehat{\boldsymbol{f}} = \pi(\boldsymbol{f})$ belongs.

Next theorem generalizes the theorem 1.1.

Theorem 5.1. *Let* $C_{\widehat{H}}(\mathfrak{A}_n)$ *be the association scheme dual to the scheme* $C_H(\mathfrak{G}^n)$, $N_{\boldsymbol{c}}(\mathfrak{K})$ *be a number of elements* $\mathfrak{g}$ *of a subgroup (code)* $\mathfrak{K} \leq \mathfrak{G}^n$ *such that* $wt(\mathfrak{g}) = \boldsymbol{c} = (c_1, \dots, c_m)$, *and* $M_{\boldsymbol{w}}(\mathfrak{K}^{\perp})$ *be a number of elements* $\widehat{\boldsymbol{f}} = \pi(\boldsymbol{f})$ *of a subgroup (code)* $\mathfrak{K}^{\perp} \leq \mathfrak{A}_n$ *such that* $wt(\boldsymbol{f}) = \boldsymbol{w}$.

Suppose, that for a subgroup $\mathfrak{K}$ *of the group* $\mathfrak{G}^n$ *assumption* $\widehat{A}_n$ *holds.*

Then

i_a *the value of the function*

$$P(\widehat{\boldsymbol{f}}, \boldsymbol{c}) = \sum_{wt(\mathfrak{g}) = \boldsymbol{c}} \widehat{\chi}(\widehat{\boldsymbol{f}}(\mathfrak{g})), \tag{5.2}$$

where the sum is taken over all $\mathfrak{g}$ *such that* $wt(\mathfrak{g}) = \boldsymbol{c}$, *is determined unambiguously by the value of the pseudo-weight* $\boldsymbol{w} = wt(\widehat{\boldsymbol{f}})$, *i.e.* $P(\widehat{\boldsymbol{f}}, \boldsymbol{c}) = P(\widehat{\boldsymbol{f}}', \boldsymbol{c})$, *if* $wt(\widehat{\boldsymbol{f}}) = wt(\widehat{\boldsymbol{f}}')$.

i_b *the value of the function*

$$Q(\boldsymbol{w}, \mathfrak{g}) = \sum_{wt(\widehat{\boldsymbol{f}}) = \boldsymbol{w}} \widehat{\chi}(\widehat{\boldsymbol{f}}(\mathfrak{g})), \tag{5.3}$$

is determined unambiguously by the value of the pseudo-weight $\boldsymbol{c} = wt(\mathfrak{g})$, *i.e.* $Q(\boldsymbol{w}, \mathfrak{g}) = Q(\boldsymbol{w}, \mathfrak{g}')$, *if* $wt(\mathfrak{g}) = wt(\mathfrak{g}')$.

ii

$$\widehat{\chi}(\mathfrak{e})N_{\boldsymbol{c}}(\mathcal{R}) = \frac{1}{|\widehat{\mathfrak{R}}^{\perp}|}\sum_{\boldsymbol{w}} M_{\boldsymbol{w}}(\widehat{\mathfrak{R}}^{\perp})p(\boldsymbol{w},\boldsymbol{c}), \tag{5.4}$$

where $p(\boldsymbol{w},\boldsymbol{c}) = P(\widehat{\boldsymbol{f}},\boldsymbol{c})$, $\boldsymbol{w} = wt(\widehat{\boldsymbol{f}})$, and $\widehat{\chi}$ is a character of the representation $\widehat{\phi}$.

iii

$$|\widehat{R}_{\boldsymbol{w}}|p(\boldsymbol{w},\boldsymbol{c}) = |R_{\boldsymbol{c}}|q(\boldsymbol{w},\boldsymbol{c}), \tag{5.5}$$

where $q(\boldsymbol{w},\boldsymbol{c}) = Q(\boldsymbol{w},\mathfrak{g})$ if $wt(\mathfrak{g}) = \boldsymbol{c}$, and $R_{\boldsymbol{c}}$ $(\widehat{R}_{\boldsymbol{w}})$ is the subset of $\mathfrak{G}^n$ $(\mathfrak{A}_n)$ formed by elements $\mathfrak{g}$ $(\widehat{\boldsymbol{f}})$ such that $wt(\mathfrak{g}) = \boldsymbol{c}$ $(wt(\widehat{\boldsymbol{f}}) = \boldsymbol{w})$.

Proof of item $\mathbf{i}_a$. If $wt(\widehat{\boldsymbol{f}})) = wt(\widehat{\boldsymbol{f}}\,')$, then there is $\widehat{\boldsymbol{\sigma}} \in \widehat{H}_n$ such that $\widehat{\boldsymbol{f}}\,' = \widehat{\boldsymbol{f}}^{\,\widehat{\boldsymbol{\sigma}}}$. Let $\boldsymbol{\sigma}$ be a preimage of the automorphism $\widehat{\boldsymbol{\sigma}}$, i.e. $\widehat{\boldsymbol{f}}^{\,\widehat{\boldsymbol{\sigma}}} = \pi(\boldsymbol{f}(\mathfrak{x}^{\,\boldsymbol{\sigma}}))$. This implies that

$$P(\widehat{\boldsymbol{f}},\boldsymbol{c}) = \sum_{wt(\mathfrak{g})=\boldsymbol{c}} \widehat{\chi}(\pi(\boldsymbol{f}(\mathfrak{g}^{\boldsymbol{\sigma}}))) = \sum_{wt(\mathfrak{g})=\boldsymbol{c}} \widehat{\chi}(\widehat{\boldsymbol{f}}^{\,\widehat{\boldsymbol{\sigma}}}(\mathfrak{g})) = P(\widehat{\boldsymbol{f}}\,',\boldsymbol{c}). \tag{5.6}$$

Thus, the function $P(\widehat{\boldsymbol{f}},\boldsymbol{c}) = p(\boldsymbol{w},\boldsymbol{c})$ depends only on the relation $\widehat{R}_{\boldsymbol{w}}$, to which the pair $(\widehat{\mathfrak{e}},\widehat{\boldsymbol{f}})$ belongs, where $\widehat{\mathfrak{e}}$ is the unity of the group $\mathfrak{A}_n$, and $\widehat{\boldsymbol{f}} \in \mathfrak{A}_n$.

Proof of item $\mathbf{i}_b$. is analogous to the proof of item $\mathbf{i}_a$.

Proof of item ii follows from the lemma 5.1, item $\mathbf{i}_a$ and the following obvious identities

$$\begin{aligned} \widehat{\chi}(\mathfrak{e})N_{\boldsymbol{c}}(\mathcal{R}) &= \sum_{wt(\mathfrak{g})=\boldsymbol{c}} \psi_{\mathcal{R}}(\mathfrak{g}) = \frac{1}{|\mathcal{R}^{\perp}|}\sum_{\widehat{\boldsymbol{f}}\in\mathcal{R}^{\perp}}\ \sum_{wt(\mathfrak{g})=\boldsymbol{c}} \widehat{\chi}(\widehat{\boldsymbol{f}}(\mathfrak{g})) = \\ &= \frac{1}{|\mathfrak{R}^{\perp}|}\sum_{\boldsymbol{w}}\ \sum_{\widehat{\boldsymbol{f}}\in\mathfrak{R}^{\perp}\&wt(\widehat{\boldsymbol{f}})=w}\ \sum_{wt(\mathfrak{g})=\boldsymbol{c}} \widehat{\chi}(\widehat{\boldsymbol{f}}(\mathfrak{g})) = \frac{1}{|\mathfrak{R}^{\perp}|}\sum_{\boldsymbol{w}} M_{\boldsymbol{w}}(\mathfrak{R}^{\perp})p(\boldsymbol{w},\boldsymbol{c}). \quad \square \end{aligned} \tag{5.7}$$

Proof of item iii. follows from the definitions of functions $P(\widehat{\boldsymbol{f}},\boldsymbol{c})$ and $Q(\boldsymbol{w},\mathfrak{g})$, items $\mathbf{i}_a$, $\mathbf{i}_b$ and the following obvious identities

$$|\widehat{R}_{\boldsymbol{w}}|p(\boldsymbol{w},\boldsymbol{c}) = \sum_{wt(\widehat{\boldsymbol{f}})=w} P(\widehat{\boldsymbol{f}},\boldsymbol{c}) = \sum_{wt(\mathfrak{g})=\boldsymbol{c}} Q(\boldsymbol{w},\mathfrak{g}) = |R_c|q(\boldsymbol{w},\boldsymbol{c}). \quad \square \tag{5.8}$$

In the next section we evaluate the function $p(\boldsymbol{w},\boldsymbol{c})$ explicitly in the case, when $\mathfrak{A}$ is an Abelian group. Explicit evaluation of $p(\boldsymbol{w},\boldsymbol{c})$ in the case of noncommutative group $\mathfrak{A}$ is also possible but postponed to the forthcoming paper.

6. An analogue of the MacWilliams identity

If $\mathfrak{A}$ is an Abelian group, then the identity (4.1) can be rewritten as follows

$$\widehat{\boldsymbol{f}}(\mathfrak{x}_1,\ldots,\mathfrak{x}_n) = \pi(h_1(\mathfrak{x}_1))\cdots\pi(h_n(\mathfrak{x}_n)), h_j \in \Psi, \quad \widehat{\boldsymbol{f}}(\mathfrak{e}) = \pi(\boldsymbol{f}(\mathfrak{e})) = \pi(\mathfrak{e}). \tag{6.1}$$

This implies, that $\mathfrak{A}_n = \mathfrak{A}^n$ i.e. the association scheme $\boldsymbol{C}_{\widehat{H}}(\mathfrak{A}_n)$ is composite. Therefore its relations $R_{\boldsymbol{w}}$ can be indexed by tuples $\boldsymbol{w} = (w_0,\ldots,w_l)$, $w_0 + \cdots + w_l = n$, where w_j is a number of pairs $(\widehat{f}_s, \widehat{f}'_s)$ of coordinates of vectors $(\widehat{\boldsymbol{f}}, \widehat{\boldsymbol{f}}') \in R_w$ which belong to the relation R_j, and $1+l$ is the number of relations in the coordinate association scheme $\mathcal{S}_{\widehat{H}}(\mathfrak{A})$.

Let $\Lambda = \Lambda(H) = \|r_{i,j}\|_{i=0,\dots,l,j=0,\dots,m}$ be a matrix of structural constants of the group $\mathfrak{A}$ with respect to the group $\mathfrak{G}$ where $r_{i,j}$ are determined by the equality (1.7). Using notation defined above, constant $r_{i,j}$ can be expressed as follows

$$r_{i,j} = \sum_{\mathfrak{g}\in C_j} \widehat{\chi}(\pi(f(\mathfrak{g}))), \tag{6.2}$$

where $\pi(f(\mathfrak{x})) = \widehat{f}$ is a representative of a class $\widehat{C}_i$ of conjugate elements of the group $\mathfrak{A}$ and $\widehat{H}$ is its group of automorphisms induced by the group of automorphisms H.

Lemma 6.1. *Let $\mathfrak{A}$ be an Abelian group, $\widehat{\boldsymbol{f}} \in \mathfrak{A}_n = \mathfrak{A}^n$, $wt(\widehat{\boldsymbol{f}}) = \boldsymbol{w} = (w_0, \dots, w_l)$ and $P(\widehat{\boldsymbol{f}}, \boldsymbol{c})$ be the function defined by (5.2).*

Then

$$P(\widehat{\boldsymbol{f}}, \boldsymbol{c}) = p_{\boldsymbol{c}}(\boldsymbol{w}, \Lambda) =$$
$$\sum_{\boldsymbol{c};\boldsymbol{w}} \binom{w_0}{c_{0,0}, \dots, c_{m,0}} \cdots \binom{w_l}{c_{0,l}, \dots, c_{m,l}} \left(\prod_{s=0}^{m} r_{0,s}^{\,c_{s,0}}\right) \cdots \left(\prod_{s=0}^{m} r_{l,s}^{\,c_{s,l}}\right), \tag{6.3}$$

where sum is over all tuples $\{c_{0,0}, \dots, c_{m,0}\}, \dots, \{c_{0,l}, \dots, c_{m,l}\}$ such that $c_{0,j} + \dots + c_{m,j} = w_j$, $j = 0, \dots, l$, and $c_{s,0} + \dots + c_{s,l} = c_s$, $s = 0, \dots, m$.

Proof. Since $\mathfrak{A}$ is an Abelian group, the function $\widehat{\boldsymbol{f}}$, determined by the equality (4.1), can be written as

$$\widehat{f}(\mathfrak{x}_1, \dots, \mathfrak{x}_n) = \prod_{j=1}^{n} \pi(f_j(\mathfrak{x}_j)), \quad f_j \in \Psi. \tag{6.4}$$

Let $wt(\widehat{\boldsymbol{f}}) = wt(\pi(\boldsymbol{f})) = \boldsymbol{w}$ and let $\mathcal{N} = \bigcup_{j=0}^{l} M_j$, $|M_j| = w_j$, be a partition of the set of indices $\mathcal{N} = \{1, \dots, n\}$ such that if $s \in M_j$ then $\pi(f_s(\mathfrak{x}_s)) \in \widehat{C}_j$. In this notation the equality (6.4) can be written as follows

$$\widehat{f}(\mathfrak{x}_1, \dots, \mathfrak{x}_n) = \prod_{s\in M_0} \pi(f_s(\mathfrak{x}_s)) \cdots \prod_{s\in M_l} \pi(f_s(\mathfrak{x}_s)). \tag{6.5}$$

Let $wt(\mathfrak{g}) = \boldsymbol{c}$ and $\mathcal{N} = \bigcup_{j=0}^{m} N_j$, $|N_j| = c_j$, be a partition of the set of indices $\mathcal{N}$. Denote by $S(N_0, \dots, N_m)$ the set of all elements $\mathfrak{g} = (\mathfrak{g}_1, \dots, \mathfrak{g}_n) \in \mathfrak{G}^n$ such that $\mathfrak{g}_i \in C_j$ for $i \in N_j$.

Put $c_{i,j} = |M_i \bigcap N_j|$. Obviously,

$$\sum_{(\mathfrak{x}_1,\dots,\mathfrak{x}_n)\in S(N_0,\dots,N_m)} \widehat{f}(\mathfrak{x}_1, \dots, \mathfrak{x}_n) = \prod_{i=1}^{l}\prod_{j=1}^{m}\prod_{s\in M_i}\prod_{s\in N_j}\sum_{\mathfrak{x}_s\in C_j} \pi(f_s(\mathfrak{x}_s)) = \prod_{i=1}^{l}\prod_{j=1}^{m} r_{i,j}^{c_{i,j}}. \tag{6.6}$$

Taking the sum of the identity (6.6) over all partitions $\mathcal{N} = \bigcup_{j=0}^{m} N_j$, $|N_j| = c_j$, of the set of indices $\mathcal{N}$ we get the equation (6.3). □

Let $z_0, \dots, z_m$ be formal variables. It is easy to see, that

$$p_{\boldsymbol{c}}(\boldsymbol{w}) = p_{\boldsymbol{c}}(\boldsymbol{w}, \Lambda) = \operatorname{coeff}_{z_0^{c_0}\dots z_m^{c_m}} \prod_{j=0}^{l} \left(\sum_{s=0}^{m} r_{s,j} z_s\right)^{w_j}. \tag{6.7}$$

From (6.3) it follows that the function $p_{\boldsymbol{c}}(\boldsymbol{x})$ is a polynomial of total degree at most $c_1 + \dots + c_l$ in variables $x_0, \dots, x_m$ where $x_0 = n - x_1 - \dots - x_m$.

Theorem 6.1. *Let $\mathfrak{A}$ be an Abelian group, $C_{\widehat{H}}(\mathfrak{A}^n)$ be the association scheme dual to $C_H(\mathfrak{G}^n)$. Let $\mathfrak{K}$ be a subgroup (group code) of the group $\mathfrak{G}^n$ and $\mathfrak{K}^{\perp}$ be a subgroup (the dual code) of the group $\mathfrak{A}^n$ dual to $\mathfrak{K}$.*

The numbers $N_{\boldsymbol{c}}(\mathfrak{K})$ (an amount of elements $\mathfrak{g} \in \mathfrak{K}$ of pseudo-weight $wt(\mathfrak{g}) = \boldsymbol{c} = (c_0, \ldots, c_m)$), and $M_{\boldsymbol{w}}(\mathfrak{K}^{\perp})$ (an amount of elements $\pi(\boldsymbol{f}) \in \mathfrak{K}^{\perp}$ of pseudo-weight $wt(\pi(\boldsymbol{f})) = \boldsymbol{w} = (w_0, \ldots, w_l)$), satisfy

$$\sum_{c_0+\cdots+c_m=n} N_{c_0,\ldots,c_m}(\mathfrak{K}) z_0^{c_0} \cdots z_m^{c_m} =$$
$$\frac{1}{|\mathfrak{K}^{\perp}|} \sum_{w_0+\cdots w_l=n} M_{w_0,\ldots,w_l}(\mathfrak{K}^{\perp}) \prod_{s=0}^{l} (r_{0,s}z_0 + r_{1,s}z_1 + \cdots + r_{m,s}z_m)^{w_s}. \tag{6.8}$$

Proof follows directly from theorem 5.1, lemma 6.1 and equality (6.7). □

Mizukawa and Tanaka have shown that polynomials $p_{\boldsymbol{c}}(\boldsymbol{w})$ could be to expressed in term of hypergeometric functions. They also printed out orthogonality of these polynomials.

In our opinion some particular cases of equality (6.8) deserve special attention. Below we consider some of them.

7. Theorem 6.1 for dihedral group with eight elements

Consider a set of matrices with rational entries

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$
$$S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad TS = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{7.1}$$

The set of matrices

$$\mathcal{E} = \{\pm E, \quad \pm T, \quad \pm S, \quad \pm ST\} \tag{7.2}$$

is a finite non-Abelian group of order 8, which is called extraspecial 2−group or a dihedral group (more precisely, its irreducible two-dimensional representation).

The group $\mathcal{E}$ has 4 inner automorphisms $\sigma_D : \ X \to DXD^{-1}$, $D = E, T, S, TS$, and 4 external automorphisms $\overline{\sigma}\sigma_D$ each being a product of all inner automorphisms σ_D and the external homomorphism $\overline{\sigma}$ generated by the following mapping $\overline{\sigma} : \pm S \to \pm T$, $\pm T \to \pm S$, $\pm ST \to \pm TS = \mp ST, \pm E \to \pm E$. Obviously, $\overline{\sigma}^2$ is the identity mapping. Thus, $|Aut(\mathcal{E})| = 8$.

The group $\mathcal{E}$ has one irreducible two-dimensional representation and 4 one-dimensional representations. Nontrivial one-dimensional representations ψ, ψ_1, ψ_2 are summarized in the following table

	E	T	S	ST	$-E$	$-T$	$-S$	$-ST$
ψ	1	−1	−1	1	1	−1	−1	1
ψ_1	1	−1	1	−1	1	−1	1	−1
ψ_2	1	1	−1	−1	1	1	−1	−1

(7.3)

Obviously, $\psi = \psi_1\psi_2$ and $\psi_1(x^{\overline{\sigma}}) = \psi_2(x)$, $\psi(x^{\overline{\sigma}}) = \psi(x)$.

The group $\mathcal{E}$ has four ($m = 3$) classes of conjugate elements with respect to the group $Aut(\mathcal{E})$: $C_0 = \{E\}$, $C_1 = \{-E\}$, $C_2 = \{\pm T, \pm S\}$, $C_3 = \{\pm ST\}$. It has five classes of conjugate elements with respect to the group of inner automorphisms $\mathrm{Inn}(\mathcal{E})$.

Let ξ be an isomorphism of the four-element Abelian group $\mathcal{E}/\{\pm E\}$ into a group of characters which is isomorphic to $\mathcal{E}/\{\pm E\}$, and let δ be a homomorphism of $\mathcal{E}$ into $\mathcal{E}/\{\pm E\}$. Put $\pi = \delta\xi$. As a group $\mathfrak{A}$ we take a group $\pi(\Psi) = \{\psi_0, \psi_1, \psi_2, \psi_1\psi_2\}$ of one-dimensional representations of the group $\mathcal{E}$.

The group $\mathfrak{A}$ is an elementary Abelian group of order 4, isomorphic to the additive group of the finite field $\mathbb{F}_4$.

The group $\widehat{H}$ of automorphisms of $\mathfrak{A}$ induced by $H = Aut(\mathcal{E})$, consists of trivial homomorphism and a homomorphism $\widehat{\overline{\sigma}} : \psi_1 \to \psi_2$ for which the element $\psi_1\psi_2$ is a fixed point. Thus, $\mathfrak{A}$ has three classes ($l = 2$) of conjugate elements: $\widehat{C}_0 = \{\psi_0\}$, $\widehat{C}_1 = \{\psi_1\psi_2\}$, $\widehat{C}_2 = \{\psi_1, \psi_2\}$.

Consider an isomorphism of the group $\mathfrak{A}$ into an additive group of the field $\mathbb{F}_4$ which maps the element $\psi_1\psi_2$ to an element $1 \in \mathbb{F}_2 \subset \mathbb{F}_4$. The group of automorphisms $\widehat{H}$ is transformed by this isomorphism into Galois group of the field $\mathbb{F}_4$. The automorphism $\overline{\sigma}$ of the group $\mathfrak{G}$ induces automorphism $\widehat{\overline{\sigma}}$ of $\mathfrak{A}$, which we call Frobenius automorphism of the group $\mathfrak{A}$.

The association scheme $\mathcal{S}_{\widehat{H}}(\mathfrak{A})$ with three relations is dual to the association scheme $\mathcal{S}_H(\mathcal{E})$, $H = Aut(\mathcal{E})$, with four relations.

Further we shall consider the association scheme $\boldsymbol{C}_H(\mathcal{E}^n)$, $H = Aut(\mathcal{E})$, and its dual scheme $\boldsymbol{C}_{\widehat{H}}(\mathfrak{A}_n)$. Note, that $\boldsymbol{C}_H(\mathcal{E}^n)$ and $\boldsymbol{C}_{\widehat{H}}(\mathfrak{A}_n)$ are composition association schemes for $\mathfrak{A}_n = \mathfrak{A}^n$.

The elements of $\mathfrak{A} = \{\psi_0, \psi_1, \psi_1, \psi = \psi_1\psi_2\}$ are indexed by elements of the 2-dimensional space $\mathbb{F}_2^2$ in such a manner that $\psi_0 = \psi_{(0,0)}, \psi_1 = \psi_{(1,0)}, \psi_2 = \psi_{(0,1)}$, and $\psi_{(1,1)} = \psi$. The elements of $\mathbb{F}_2^2$ will also be considered as element of the field $\mathbb{F}_4$. Thus, $\mathfrak{A} = \{\psi_\alpha | \alpha \in \mathbb{F}_2^2\}$.

We denote by $\psi_{\boldsymbol{\alpha}}$, $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_2^{2n}$, the function $\psi_{\boldsymbol{\alpha}} = \psi_{\alpha_1}(\mathfrak{x}_1) \cdots \psi_{\alpha_n}(\mathfrak{x}_n)$, $(\mathfrak{x}_1, \ldots, \mathfrak{x}_n) \in \mathfrak{G}^n$, which maps $\mathfrak{G}^n$ into $\mathfrak{A}$.

As a code $\mathcal{R} \subseteq \mathcal{E}^n$ we consider a subgroup of $\mathcal{E}^n$ of the following form

$$\mathcal{R} = \ker \psi_{\boldsymbol{\alpha}_1} \bigcap \cdots \bigcap \ker \psi_{\boldsymbol{\alpha}_r}, \ 1 \leq r \leq 2n, \tag{7.4}$$

where vectors $\boldsymbol{\alpha}_j \in \mathbb{F}_2^{2n}$, $j = 1, \ldots, r$, are linear-independent over $\mathbb{F}_2$. An $r \times 2n$–matrix A with the rows $\boldsymbol{\alpha}_j$, $j = 1, \ldots, r$, can be considered as a parity-check matrix of the code $\mathcal{R}$. A 4-ary code $\mathcal{R}^\perp \subseteq \mathfrak{A}_n$ with generator matrix A is composed by all functions (characters of the group $\mathcal{E}^n$) $\psi_{\boldsymbol{\alpha}}$ whose indices $\boldsymbol{\alpha}$ are vectors of r–dimensional space over $\mathbb{F}_2$ spanned by the rows of A.

The matrix of structural constants is as follows

$$\Lambda = \begin{Vmatrix} 1 & 1 & 4 & 2 \\ 1 & 1 & -4 & 2 \\ 1 & 1 & 0 & -2 \end{Vmatrix}. \tag{7.5}$$

A pseudo-weight of an element $\psi_{\boldsymbol{\alpha}} \in \mathfrak{A}_n$, $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$, of the association scheme $\boldsymbol{C}_{\widehat{H}}(\mathfrak{A}_n)$ is a three-dimensional vector $\boldsymbol{w} = (w_0, w_1, w_2)$, $w_0 + w_1 + w_2 = n$, whose coordinate w_j is a number of characters in the product $\psi_{\boldsymbol{\alpha}}$, belonging to the class $\widehat{C}_j$ of conjugate elements. As it has been noticed above, classes $\widehat{C}_j$, $j = 0, 1, 2$. and the classes of conjugate elements relative to the Galois group of the field $\mathbb{F}_4$ are in a one-on-one correspondence.

Note, that a pseudo-weight $wt(\mathbf{g})$ of an element $\mathbf{g} \in \mathcal{E}^n$ is a three-dimensional vector (c_1, c_2, c_3), $c_1 + c_2 + c_3 \le n$ with integer entries (see section 1.1).

Note, that it is possible to specify by a homogeneous system of linear equations (7.4) only those subgroups of $\mathfrak{G}^n$ which contain the direct product of n copies of the commutator of $\mathfrak{G}$. Therefore the considered example of Abelian group $\mathfrak{A}$ is included for illustrative purposes only.

The results would be stronger if one takes as $\mathfrak{A}_n$ a non-Abelian group of mappings. In particular, as $\mathfrak{A}_n$ we can consider the group $\Psi_{Aut(D_4)}$ (see section (1.2)). I.V. Filimonov showed using computer $|\Psi_{Aut(D_4)}| = 32$ and $|\Psi_{End(D_4)}| = 256$, where $\Psi_{End(D_4)} = \langle End(D_4)\rangle$. The group $\Psi_{Aut(D_4)}$ has 14 classes of conjugate elements with respect to the group of its automorphisms $\widehat{Aut}(D_4)$ (see Definition 1.5) induced by $Aut(D_4)$ (two classes of cardinality eight, four classes of cardinality two and eight classes of cardinality one). In the case being considered, the structure of the group Ψ_n, $n > 1$, and the number $|\Psi_n|$ are unknown.

One can prove that $\Psi_{Aut(D_4)} = \langle \tau_0(\mathfrak{x}), \tau_1(\mathfrak{x}), \tau_2(\mathfrak{x})\rangle$ where $\tau_0(\mathfrak{x}) = \mathfrak{x}$ is the identity automorphism (identity function) and

$$\begin{array}{c|c|c|c|c} \mathfrak{x} & \pm E & \pm TS & \pm S & \pm T \\ \tau_1 & E & E & E & -E \\ \tau_2 & E & E & TS & TS \\ \tau_3 & E & -E & E & E \\ \tau_4 & E & E & -E & E \end{array} \tag{7.6}$$

Note, that $[\tau_0, \tau_2] = \tau_3 \neq E$ where the function τ_3 belongs to the center $C(\Psi_{Aut(D_4)}) = \langle \tau_1, \tau_3, \tau_4\rangle$ of $\Psi_{Aut(D_4)}$. Thus, the group $\Psi_{Aut(D_4)}$ is non-Abelian. Moreover a function (commutator) $[\mathfrak{x}, \mathfrak{y}]$, $\mathfrak{x}, \mathfrak{y} \in \Psi_{Aut(D_4)}$, in two variables $\mathfrak{x}, \mathfrak{y}$ commutes with any function $f \in \Psi_{Aut(D_4)}$.

It easy to see that each element $\boldsymbol{f}(\mathfrak{x}_1, \dots, \mathfrak{x}_n)$ of the ambivalent group Ψ_n (see Definition 1.4) has the following form

$$\boldsymbol{f}(\mathfrak{x}_1, \dots, \mathfrak{x}_n) = \prod_{s=1}^{n} \mathfrak{x}_s^{i_s} \tau_1^{j_s}(\mathfrak{x}_s) \tau_2^{k_s}(\mathfrak{x}_s) \tau_3^{l_s}(\mathfrak{x}_s) \prod_{i<j} [\mathfrak{x}_i, \mathfrak{x}_j]^{t_{i,j}}, \qquad t_{i,j}, i_s, j_s, k_s, l_s \in \{0, 1\},\ \mathfrak{x}_s \in D_4. \tag{7.7}$$

In what follows we consider functions $\boldsymbol{f}(\mathfrak{x}_1, \dots, \mathfrak{x}_n) \in \Psi_n$ such that $i_s = 0$, $s = 1, \dots, n$. All such functions form an Abelian group $\widetilde{\Psi}_n$. Note, that $\widetilde{\Psi}_n \neq \widetilde{\Psi}_1^n$.

The following statements are easy to prove.

i. If $j = 1, 2, 3, 4$, then $\tau_j(a\mathfrak{x}) = a'_j \tau_{a,j}(\mathfrak{x}) \tau_j(\mathfrak{x})$, $a \in D_4$, $a'_j \in \{\pm E, \pm TS\}$, $\tau_{a,j}(\mathfrak{x}) \in C(\Psi_{Aut(D_4)})$. All functions $\tau_j(\mathfrak{x})$, $j = 1, 2, 3, 4$ commute with constant functions $\tau(\mathfrak{x}) = c$, $c \in \{\pm E, \pm TS\}$:

ii. $[a\mathfrak{x}, b\mathfrak{y}] = [a, b]\tau_{a,b}(\mathfrak{x})\tau'_{a,b}(\mathfrak{y})[\mathfrak{x}, \mathfrak{y}]$, $a, b \in D_4$, $\tau_{a,b}(\mathfrak{x}), \tau'_{a,b}(\mathfrak{y}) \in C(\Psi_{Aut(D_4)})$, $[a, b] \in C(D_4)$.

This implies, that the functions $\boldsymbol{f}(\boldsymbol{a}\mathfrak{x})$, $\boldsymbol{f}(\boldsymbol{b}\mathfrak{x})$, $\boldsymbol{a}, \boldsymbol{b} \in \mathfrak{G}^n$, commute. Therefore

$$F(\mathfrak{x}) = \prod_{a \in \mathcal{R}} \boldsymbol{f}(\boldsymbol{a}\mathfrak{x}) \tag{7.8}$$

is a correctly defined function, because different orders of the sequence of factors in (7.8) give the same function.

Obviously, $F(\mathfrak{x})$ is constant on all right cosets $\mathcal{R}\boldsymbol{b}$ of $\mathcal{R}$. Note, that this function is similar to the invariant polynomials relative $\mathcal{R}$ in classic algebra. We assume that $F(\mathfrak{e}) = \mathfrak{e}$. Otherwise one can to take as $F(\mathfrak{x})$ the function $F(\mathfrak{x})F(\mathfrak{e})^{-1}$.

Suppose that $\mathfrak{F} = \{F_1(\boldsymbol{x}), \ldots, F_k(\boldsymbol{x})\}$, $F_s(\mathfrak{e}) = \mathfrak{e}$, $s = 1, \ldots, k$, is a set of functions which are a constant on each right coset of $\mathcal{R}$. If for every $\boldsymbol{b} \notin R$ there exists an index s (depending on $\boldsymbol{b}$) such that $F_s(\boldsymbol{b}) \neq \mathfrak{e}$ then $\mathfrak{F}$ is called $\mathcal{R}$–set. The group $\langle\mathfrak{F}\rangle \leq \Psi_n$ generated by a set $\mathfrak{F}$ which is a $\mathcal{R}$–set, is a dual subgroup (code) $\mathcal{R}^{\perp}$ (see Definition 1.3) to the group R.

It is natural to specify the subgroup $\mathcal{R}(\mathfrak{F}) \leq D_4^n$ using the above set $\mathfrak{F}$, i.e $\mathcal{R}(\mathfrak{F}) = \{\mathfrak{g} | F_j(\mathfrak{g}) = \mathfrak{e}, j = 1, \ldots, k\}$. It is similar to the well-known definition a linear code using its parity-check matrix (see 7.4).

8. Acknowledgment

The author thanks Lev Kazarin, Nick Varnovsky and Akihiro Munemasa for very useful remarks which have essentially improved the contents of this paper.

Abtract. The paper presents noncommutative association schemes $\mathcal{S}_H(\mathfrak{G})$ defined by a pair $\mathfrak{G}, H$, where $\mathfrak{G}$ is a finite group and H is a subgroup of its automorphism group.

References

1. Kostrikin A. I. // Introduction in algebra. M.: Science, 1977.
2. MacWilliams F. W. and Sloane N. W. A. The Theory of Error-Correcting Codes. North-Holland, Amsterdam, 1977.
3. Bannai E., Ito T. Algebraic Combinatorics I. — Tsukuba University, 1984.
4. Simonis J. MacWilliams Identities and Coordinate Partitions // Linear Algebra and its Applications. — 1995. — Vol 216. — P. 81–91.
5. David Forney G. Jr. Transforms and Groups, Codes, curves, and signals (Urbana, IL, 1997), 79–97, Kluwer Acad. Publ., Boston. MA. 1998.
6. Delsarte Ph. An algebraic approach to association schemes in coding, Philips Res. Reps. Suppl. — 1973. — P. 10.
7. Delsarte Ph. Application and Generalization of the MacWilliams Transform in Coding Theory. In Proc. 15th Symp. Information Theory in the Benelux (Belgium, 1994).
8. Delsarte Ph., Levenshtein V. Association Schemes and Coding Theory // IEEE Trans., IT. — 1998. — Vol 44. — No 6. — P. 2477–2504.
9. Lidl R., Neiderreiter H. Finite Fields // Encyclopedia of Math. and its App. Vol 20, Addison-Wesley Pabl. Comp. 1983.
10. Higman D.G. Intersection matrices for finite permutation groups // J. Algebra. — 1967. — Vol. 6. — P. 22–42.
11. Sidelnikov V.M., Strunkov S. P. About a spectrum Orbital codes in space of matrixes // Proc. Mosc. univ, Mathematics, mechanics, sulfurs. — 1998. — No 1. — P. 58–61.
12. Neumaier A. Duality in coherent configurations // Combinatorics. — 1989. — vol 9. — P. 59–67.
13. Neumaier A. Distances, graphs and designs // Europ. J. Combin. — 1980. — vol. 1. — P. 163–174.

14. Camion P. Codes and association schemes: Basic properties of association schemes relevant to coding, Handbook of Coding Theory, V. II. — 1998. — P. 1441-1568, Elsevier.

15. Feit W. Characters of finite groups // W. A. Benjamin, Inc., 1967.

16. Bannai E., Ito T. Algebraic Combinatorics I. Benjamin/Cummings, Menlo Park, California, USA, 1984.

Ярославский государственный
университет

Поступило 12.10.06