NUMBER OF INVERTIBLE TRANSFORMATIONS
IN MULTIVALUED LOGICS

E. A. Primenko

Let \( R \) be a finite set and \(| R | = k \geq 2\). The sum of all single-valued mappings from \( R^n \) into \( R \) forms the set of \( P_k \)-functions of \( k \)-valued logic [1]. An ordered system \( f = \{ f_1, f_2, \ldots, f_n \} \) of \( n \) functions from \( P_k \) defines the mapping \( f: R^n \to R^n \), which usually is called the mapping of the set \( R^n \) [2]. The sum of all transformations of the set \( R^n \) forms a semigroup, while the set of all single-valued transformations forms a symmetric group of degree \( k^n \), which we denote by \( C_n \).

The group of all mutually single-valued transformations of an arbitrary finite set \( \Omega \) is denoted by \( S^{\Omega} \). Let \( S^{\Omega} = G, H_1 \leq G, H_2 \leq G \) (i.e., \( H_1 \) and \( H_2 \) are subgroups of \( G \)).

Two elements \( f_1 \) and \( f_2 \) from \( G \) are said to be of the same type relative to the groups \( H_1 \) and \( H_2 \) if there exist \( h_1 \in H_1, h_2 \in H_2 \) such that \( f_2 = h_1 f_1 h_2^{-1} \) [3].

All elements that are of the same type relative to one another form a type (equivalence class). The number of types in \( G \) relative to \( H_1 \) and \( H_2 \) will be denoted by \( t(H_1, H_2) \).

For the case \( k = 2, \Omega = R^n \) in [4] there is given a classification of groups of transformations corresponding to the closed class of Post [5] (of fundamental groups of transformations). For the same case in [3] there is found the number of types of transformations (invertible Boolean functions), depending on two-four variables, relative to all pairs of fundamental groups. For an arbitrary \( n \) and \( k = 2 \), for certain pairs of fundamental groups the number of types was calculated in [6-8]. These results were obtained by direct application of the basic combinatorial theorem of De Bruijn [9] and in fact did not use the properties of fundamental groups as groups of transformations.

In the present work in an arbitrary finite-valued logic we consider the following transformation groups that are analogous to the fundamental groups: \( C_n^G, \ldots, C_n^G \) is a group leaving in position each \( \alpha_i \in R^n, i = 1, \ldots, k \); \( K_n, T_n, S_n, \) and \( N_n \) are, respectively, a self-dual group and groups of renaming, permutation, and shift of the variables [10]; \( L_n \) is a group of affine transformations \( (R \) is a finite field) [2]. Taking into account their specific features as groups of transformations, we calculate the number of types of transformations in a \( k \)-valued logic.

Let \( \Omega \) be a finite set, \( S^{\Omega} = G \). The sum of all \( \alpha = (\alpha_1, \ldots, \alpha_r) \in \Omega^r \) such that \( \alpha_i \neq \alpha_j \) for \( i \neq j, i, j = 1, \ldots, r \) is denoted by \( \tilde{\Omega} \). If \( H < G \), \( h \in H \), then the mapping \( \tilde{h}: \tilde{\Omega} \to \tilde{\Omega} \) given by the expression \( \tilde{h}(\alpha) = (\alpha h, \ldots, \alpha h) \) is the substitution \( \tilde{h} \) on the set \( \tilde{\Omega} \). It is obvious that \( \{ h(\tilde{\Omega}) | h \in H \} = \tilde{\Omega} \). \( \tilde{\Omega} \).

**Lemma 1.** Let \( H < G \) and \( \Delta \subseteq \Omega \). Then \( t(H, G \Delta) \) is the number of orbits of the group \( \tilde{H} \) on \( \tilde{\Omega} \). \( \Delta \).

**Proof.** From the definition of the property of being of the same type it follows that \( f_1, f_2 \) from \( G \) belong to the same type (relative to \( H \) and \( G \)) if and only if there exists an \( h \in H \) such that \( \alpha h = \alpha h \) for any \( \alpha \in \Delta \). Hence and from the definition of \( \tilde{H} \) we obtain the required result.

**Lemma 2.** Let \( \Delta \subseteq \Omega, \Gamma \subseteq \Omega, | \Gamma | \geq | \Delta |, \) and \( G_1 < G_\Delta \), with \( G_1 \) being \( | \Gamma | \)-transitive on \( \Omega \setminus \Delta \). Then \( t(G_1, G_\Delta) = \sum_{i=0}^{\left| \frac{|\Delta|}{\left| \Gamma \right|} \right|} \left( \left| \frac{|\Delta|}{\left| \Gamma \right|} \right| \right)^i \).

**Proof.** Let \( \Delta_1 \subseteq \Delta \), \( \Gamma_1 \subseteq \Gamma \), \( | \Delta_1 | = | \Gamma_1 | \) and \( w \) is a bijection from \( \Delta_1 \) to \( \Gamma_1 \). We consider the set \( \) the set of all substitutions \( \alpha \) satisfying the conditions

\[
\alpha^x = \alpha^w, \quad \alpha \in \Delta_1,
\]

\[
\alpha^x \notin \Gamma_1, \quad \alpha \notin \Delta \setminus \Delta_1.
\]

We denote this set by $K^w_{\Delta_1, \Gamma_1}$. It is obvious that the sets $K^w_{\Delta_1, \Gamma_1}$ do not intersect in pairs, their union coincides with $G$, and their number equals $\sum_{i=0}^{n} (\binom{m}{i}) (\binom{n}{i})$. We shall show that $K^w_{\Delta_1, \Gamma_1}$ is the type relative to the groups $G_i$ and $G_1$. Let $v_1 \in K^w_{\Delta_1, \Gamma_1}, v_2 \in K^w_{\Delta_1, \Gamma_1}$. We choose $g \in G_1$ so that for any $\gamma \in \Gamma, \gamma v_1^{-1} g^{-1} = \gamma v_2^{-1}$. This can be done, since $v_1$ and $v_2$ satisfy the conditions (1), while $G_i | \Gamma$ transitive on $\Omega \setminus \Delta$. Having chosen $g$, we put $h = v_1^{-1} g^{-1} v_2$. It is not difficult to show that $h \in G_1$ and, consequently, $v_1$ and $v_2$ are of the same type. Let now $v_1 \in K^w_{\Delta_1, \Gamma_1}, v_2 \in K^w_{\Delta_2, \Gamma_2}; g \in G_1, h \in G_1, |\Delta_1| > 0, (\Delta_1, \Gamma_1, v_1) \neq (\Delta_1, \Gamma_2, v_2)$. Then there exists an $\alpha \in \Delta_1$ such that $\alpha v_1 \in \Gamma_1, \alpha v_1 \neq \alpha v_2$. Therefore, $\alpha v_1 h = \alpha v_1 \neq \alpha v_2$. Consequently, $v_1$ and $v_2$ belong to different types. By this, Lemma 2 is completely proved.

Let $R$ be a commutative ring with a unity. Then we can consider the group $K_n, T_n, N_n$ [10]. Since they are transitive on $\Omega = R^n$, from Lemma 1 we obtain the following theorem.

**THEOREM 1.** For any $\alpha, \beta \in R^n, t(K_n, C_n^\alpha) = t(K_n, C_n^\beta) = t(N_n, C_n^\alpha) = 1$.

If $R$ is a Galois field, $k = p^m$, and $p$ is simple, then on $R^n$ we can define a group of affine transformations $L_n$ [2] which is twice transitive on $R^n$. Taking into account this fact, from Lemmas 1 and 2 we obtain the following theorem.

**THEOREM 2.** For any $\alpha, \beta$ from $R^n, t(L_n, C_n^\alpha) = 1, t(L_n, C_n^\alpha) = 2 (L_n = C_n^\alpha \cap L_n)$.

Further, from Lemma 2 follow the next theorems.

**THEOREM 3.** For any $\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_r$ from $R^n (0 \leq s \leq r \leq k^n - 1)$,

$$t(C_n^{\alpha_1 \cdots \alpha_s}, C_n^{\beta_1 \cdots \beta_r}) = \sum_{i=0}^{r} (t)(i).$$

**THEOREM 4.** For any $\alpha_1, \ldots, \alpha_r$ from $R^n (R$ is a ring, $0 \leq r \leq k^n - 1)$,

$$t(N_n, C_n^{\alpha_1 \cdots \alpha_r}) = (k^n - 1).$$

**Proof.** We denote by $\omega$ an element from $R^n$ each coordinate of which is a zero of the ring $R$. We consider the set $\tilde{\Omega}_R$, where $\Omega = R^n$, and a group of substitutions $\tilde{N}_n$ acting on this set. It is obvious that different elements $\tilde{\alpha}_R$ of the form $(\omega, \beta_1, \ldots, \beta_r)$ belong to different orbits of the group $\tilde{N}_n$. On the other hand, an arbitrary element $(\beta_1, \ldots, \beta_r)$ belongs to the orbit of the element $(\omega, \beta_1, \ldots, \beta_r)$. Consequently, the number of orbits of the group $\tilde{N}_n$ equals to the number of different elements of $\tilde{\alpha}_R$ of the form $(\omega, \beta_1, \ldots, \beta_r)$. Therefore, according to Lemma 1 we obtain $t(N_n, C_n^{\alpha_1 \cdots \alpha_r}) = (k^n - 1)_R$.

**THEOREM 5.** For any $\alpha \in R^n, t(S_n, C_n^\alpha) = \binom{n}{i-1} (i)!$.

**Proof.** Let $R = \{\alpha_1, \ldots, \alpha_k\};$ $\beta = (b_1, b_2, \ldots, b_n)$ is an arbitrary element from $R^n$. We denote by $l_1$ the number of coordinates of the element $\beta$ equal to $\alpha_1, i = 1, k$. Then an ordered collection of integers $l(\beta) = (l_1, l_2, \ldots, l_k)$ will be called the structure of the element $\beta$. From the definition of $S_n$ it follows that the group $S_n$ does not alter the structure of elements $\beta \in R^n$. Consequently, the number of orbits of $S_n$ is equal to all possible structures. Since the structure is determined by an ordered partition of the number $n$ into $i$ parts and a selection (without repetition) from the set $R$ of $i$ elements, the number of orbits of the group $S_n$ and, consequently (according to Lemma 1), also $t(S_n, C_n^\alpha) = \sum_{i=1}^{n} (i-1) (i)!$.

**THEOREM 6.** For any $\alpha$ and $\beta$ from $R^n = \Omega (R$ is a ring),

$$t(T_n, C_n^\alpha)^\beta = \sum_{i=1}^{n} (i-1) (i)! - 1.$$