INFORMATION AND CONTROL 10, 499–508 (1967)

Enumeration of Finite Automata[1]

FRANK HARARY AND ED PALMER

Department of Mathematics, University of Michigan, Ann Arbor, Michigan

Harary (1960, 1964), in a survey of 27 unsolved problems in graphical enumeration, asked for the number of different finite automata. Recently, Harrison (1965) solved this problem, but without considering automata with initial and final states. With the aid of the Power Group Enumeration Theorem (Harary and Palmer, 1965, 1966) the entire problem can be handled routinely. The method involves a confrontation of several different operations on permutation groups.

To set the stage, we enumerate ordered pairs of functions with respect to the product of two power groups. Finite automata are then concisely defined as certain ordered pairs of functions. We review the enumeration of automata in the natural setting of the power group, and then extend this result to enumerate automata with initial and terminal states.

I. ENUMERATION THEOREM

For completeness we require a number of definitions, which are now given. Let A be a permutation group of order $m = |A|$ and degree d acting on the set $X = \{x_1, x_2, \cdots, x_d\}$. The *cycle index* of A, denoted $Z(A)$, is defined as follows. Let $j_k(\alpha)$ be the number of cycles of length k in the disjoint cycle decomposition of any permutation α in A. Let $a_1, a_2, \cdots, a_d$ be variables. Then the cycle index, which is a polynomial in the variables a_k, is given by

$$Z(A) = \frac{1}{m} \sum_{\alpha \in A} \prod_{k=1}^{d} a_k^{j_k(\alpha)}. \tag{1}$$

We sometimes write $Z(A; a_1, a_2, \cdots, a_d)$ to indicate the variables in $Z(A)$.

The following formula for the number of orbits determined by a permutation group can be found in Burnside (1911).

[1] This work was supported in part by the U.S. Air Force Office of Scientific Research under grant AF-AFOSR-754-65.

THEOREM 1. *The number of orbits determined by the permutation group* A *is*

$$N(A) = \frac{1}{|A|} \sum_{\alpha \in A} j_1(\alpha). \tag{2}$$

We will use several well known operations (see Harary, 1959) on permutation groups which produce other permutation groups. As above, let A be a permutation group of order $m = |A|$ and degree d, acting on the set X. Let B be another permutation group of order $n = |B|$ and degree e, acting on the set Y.

The *sum* of A and B, denoted $A + B$, is a permutation group which acts on the disjoint union $X \cup Y$. Its permutations are all the ordered pairs, written $\alpha\beta$, of permutations α in A and β in B. Any element z of $X \cup Y$ is permuted by $\alpha\beta$ according to

$$\alpha\beta(z) = \begin{cases} \alpha z, & z \in X \\ \beta z, & z \in Y. \end{cases}$$

Thus the order of $A + B$ is mn and the degree is $d + e$.

The next operation was introduced by Harary (1958). The *product* of A and B, denoted $A \times B$, acts on the cartesian product $X \times Y$. The permutations in $A \times B$ consist of all ordered pairs, written (α, β), of permutations α in A and β in B. Any element (x, y) in $X \times Y$ is permuted by (α, β) according to the equation

$$(\alpha, \beta)\,(x, y) = (\alpha x, \beta y).$$

Then the order of $A \times B$ is mn and the degree is $d + e$.

The *power group* was defined by Harary and Palmer (1965). This permutation group, denoted by B^A, acts on Y^X, the set of all functions from X into Y. Here we assume $|Y| > 1$ so that there are at least two functions. The permutations in B^A are the ordered pairs, written $(\alpha; \beta)$, of permutations α in A and β in B. Any function f in Y^X is permuted by $(\alpha\,; \beta)$ according to

$$(\alpha\,; \beta)\, f(x) = \beta f(\alpha x)$$

for all x in X. It is clear that the order of B^A is mn and the degree is e^d.

Following the terminology of Carmichael (1937), we write $A \cong B$ to mean only that A and B are *isomorphic* as abstract groups. But $A \equiv B$ means more, namely that A and B are *identical,* i.e., equivalent as permutation groups.

Our enumeration methods depend on formulas which give the cycle index of the sum, the product and the power group in terms of the constituent groups. It is well known (Pólya, 1937) that

$$Z(A + B) = Z(A)Z(B). \tag{3}$$

Harary (1958) has shown that for any permutation (α, β) in $A \times B$,

$$j_k(\alpha, \beta) = \sum_{p,q} j_p(\alpha) j_q(\beta) \langle p, q\rangle, \tag{4}$$

where $\langle p, q\rangle$ is the gcd of p and q, and the sum is over all p and q such that $k = [p, q]$, the lcm of p and q.

From Harary and Palmer (1965) we have the following formulas for each permutation $(\alpha ; \beta)$ in the power group:

$$j_1(\alpha ; \beta) = \prod_{k=1}^{d} \Big(\sum_{s|k} s j_s(\beta)\Big)^{j_k(\alpha)}, \tag{5}$$

where $b^0 = 1$ even when $b = 0$, and for $k > 1$

$$j_k(\alpha ; \beta) = \frac{1}{k} \sum_{s|k} \mu \left(\frac{k}{s}\right) j_1(\alpha^s ; \beta^s) \tag{6}$$

where μ is the Möbius function.

We find it convenient to use our formulation of the enumeration method discovered by deBruijn (1959, 1964). The constant form of the Power Group Enumeration Theorem (Harary and Palmer, 1965, 1966) which gives a formula for the number of equivalence classes (orbits) of functions determined by the power group, is stated as follows.

THEOREM 2. (*Power Group Enumeration Theorem, constant form*). *The number of equivalence classes of functions in Y^X determined by the power group B^A is*

$$N(B^A) = \frac{1}{|B|} \sum_{\beta \in B} Z[A ; m_1(\beta), m_2(\beta), \cdots, m_d(\beta)], \tag{7}$$

where

$$m_k(\beta) = \sum_{s|k} s j_s(\beta). \tag{8}$$

2. ORDERED PAIRS OF FUNCTIONS

The purpose of this section is to develop formulas for the enumeration of ordered pairs of functions under equivalence determined by the product of two power groups. The main result of this paper is Theorem

3, which has four corollaries that will serve by specialization to enumerate several types of automata.

It is convenient to denote a permutation group by an ordered pair (A, X), where A is the collection of permutations acting on the objects in the set X. Let (A_1, X_1), (A_2, X_2), (B_1, Y_1), and (B_2, Y_2) be permutation groups. Now consider the product of two power groups $B_1^{A_1} \times B_2^{A_2}$ acting on $Y_1^{X_1} \times Y_2^{X_2}$, the collection of pairs (f_1, f_2) of functions. Let $d_i = |X_i|$, for $i = 1, 2$. In accordance with our notation for both the power group and the product, each permutation in $B_1^{A_1} \times B_2^{A_2}$ can be written in the form $((\alpha_1; \beta_1), (\alpha_2; \beta_2))$.

Let $N(F)$ be the number of equivalence classes of pairs of functions determined by any subgroup F of $B_1^{A_1} \times B_2^{A_2}$. From Eq. (2) and the formulas for the cycle indexes of the power group and the product, the following result is obtained.

THEOREM 3. *The number of equivalence classes of pairs of functions determined by any subgroup F of $B_1^{A_1} \times B_2^{A_2}$ is*

$$N(F) = \frac{1}{|F|} \sum \left\{ \prod_{k=1}^{d_1} [\sum_{s|k} sj_s(\beta_1)]^{j_k(\alpha_1)} \right\} \left\{ \prod_{k=1}^{d_2} [\sum_{s|k} sj_s(\beta_2)]^{j_k(\alpha_2)} \right\}, \quad (9)$$

where the sum is taken over all permutations $[(\alpha_1; \beta_1), (\alpha_2; \beta_2)]$ in F.

In the special case when $F \equiv B_1^{A_1} \times B_2^{A_2}$, we can express this result by using the constant form of the Power Group Enumeration Theorem.

COROLLARY 1. *The number N of equivalence classes of pairs of functions determined by $B_1^{A_1} \times B_2^{A_2}$ is*

$$N = \frac{1}{|B_1| \cdot |B_2|} \sum Z[A_1; m_1(\beta_1), \cdots, m_{d_1}(\beta_1)] \cdot [Z[A_2; m_1(\beta_2), \cdots, m_{d_2}(\beta_2)], \quad (10)$$

where the sum is over all β_1 in B_1 and β_2 in B_2, and $m_k(\beta)$ is given by (8).

Now suppose each of the groups A_1 and A_2 is a product of groups. Let $A_1 \equiv C_1 \times D_1$ and $A_2 \equiv C_2 \times D_2$. For each i, let the degrees of C_i and D_i be c_i and d_i, respectively. We write the permutations of $C_i \times D_i$ as (γ_i, δ_i). Using the formulas for the cycle indexes of the power group and the product, and applying Theorem 3, we can enumerate more complicated ordered pairs of functions.

COROLLARY 2. *The number of equivalence classes of pairs of functions determined by any subgroup F of $(B_1^{C_1 \times D_1}) \times (B_2^{C_2 \times D_2})$ is*

$$N(F) = \frac{1}{|F|} \sum \prod_{i=1}^{2} \left\{ \prod_{p=1}^{c_i} \prod_{q=1}^{d_i} [\sum_{s|[p,q]} sj_s(\beta_i)]^{j_p(\gamma_i) j_q(\delta_i) \langle p,q \rangle} \right\}, \quad (11)$$

where the sum is over all permutations $(((\gamma_1, \delta_1); \beta_1), ((\gamma_2, \delta_2); \beta_2))$ in F.

These general results for ordered pairs of functions are easily applied to accomplish the enumeration of finite automata.

3. FINITE AUTOMATA

There are a number of ways in which (finite) automata can be defined. One formulation most convenient for enumeration purposes may be expressed in terms of ordered pairs of functions.

Let X, Y, and S be three sets with cardinalities k, m, and n, respectively. The elements of S will be called *states*; the sets X and Y the *input* and *output alphabets*, respectively. An *automaton* is an ordered pair of functions (f_1, f_2) with $f_1 : S \times X \to S$ and $f_2 : S \times X \to Y$. The map f_1 is called the *input function* and f_2, the *output function.* In conventional terminology, f_1 tells the next state and f_2 the output symbol when the automaton is in any given state and is presented with some input symbol.

Three types of equivalence for automata are described by Harrison (1965). We will discuss just one of these types here; the others may be handled similarly. Let S_k, S_m, and S_n be the symmetric groups of degrees k, m, and n acting on X, Y, and S, respectively. Thus there are n states, k input letters, and m output letters. Two automata (f_1, f_2) and (g_1, g_2) are simply called *isomorphic* if there are permutations α in S_n, β in S_k, and γ in S_m such that for all s in S and x in X

$$f_1(s, x) = \alpha^{-1} g_1(\alpha s, \beta x) \tag{12}$$

and

$$f_2(s, x) = \gamma^{-1} g_2(\alpha s, \beta x). \tag{13}$$

As we will illustrate in Fig. 2, Eq. (12) allows for changing the names of the states and input letters for the input function, while (13) admits permuting them for the output function.

In order to have an appropriate graph theoretic setting, we require the next concept. In a *net,* both loops and multiple directed lines are permitted; see Harary *et al.* (1965). If the outdegree of every point is k, and each of the k lines from a point is given a different label from the input alphabet X, then such a net represents the input function of an automaton. We also label the points of the net as the states of the automaton at hand. Figure 1 shows two such diagrams, which represent the same input function under the equivalence relation of isomorphism defined above. The symbols 0 and 1 are used for the input alphabet. Both the two state labels and the two input letters have been interchanged.

To further clarify the definition of isomorphic automata given above, consider Eq. (12), which defines equivalence for input functions f_1 and g_1. In the labeled net of f_1, there is a directed line with input label x from each state s to the state $f_1(s, x)$. Similarly, in the net of g_1 there is a directed line with input label βx from each state αs to the state $g_1(\alpha s, \beta x)$. Thus the permutation $[(\alpha, \beta) ; \alpha^{-1}]$ in the power group $S_n^{S_n \times S_k}$ sends the input function g_1 to f_1 and simply changes the names of the states along with appropriate changes in the input labels on the directed lines. The behavior of this permutation is described schematically in Fig. 2.

4. ENUMERATION OF AUTOMATA

For the enumeration of automata, we now let H_1 be the permutation group:

$$H_1 \equiv S_n^{S_n \times S_k} \times S_m^{S_n \times S_k}$$

which acts on

$$S^{S \times X} \times Y^{S \times X}.$$

Let $a(n, k, m)$ be the number of nonisomorphic automata with n

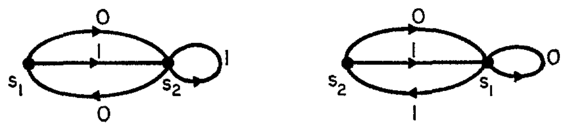

FIG. 1

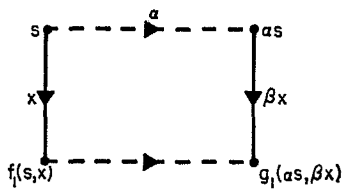

FIG. 2

states, k input symbols, and m output symbols. If F is the subgroup of H_1 which consists of all permutations of the particular form $\{[(\alpha, \beta); \alpha^{-1}], [(\alpha, \beta); \gamma]\}$, then the number of different automata is $N(F)$, given by formula (11) of Corollary 2, when the groups in (11) are taken as $B_1 \equiv C_1 \equiv C_2 \equiv S_n$, $B_2 \equiv S_m$, and $D_1 \equiv D_2 \equiv S_k$. Now the order of F is $n!\,k!\,m!$, and so the formula for $a(n, k, m)$ can be given as follows.

COROLLARY 3. *The number of finite automata with n states, k input symbols, and m output symbols is*

$$a(n, k, m) = \frac{1}{n!\,k!\,m!} \sum I(\alpha, \beta, a) I(\alpha, \beta, \gamma), \tag{14}$$

where the sum is over all permutations in H_1 of the form $\{[(\alpha, \beta); \alpha^{-1}], [(\alpha, \beta); \gamma]\}$ and where

$$I(\alpha, \beta, \gamma) = \prod_{p=1}^{n} \prod_{q=1}^{k} [\sum_{s|[p,q]} s j_s(\gamma)]^{j_p(\alpha) j_q(\beta) \langle p,q \rangle}. \tag{15}$$

Similar results for the two other types of equivalence are easily obtained from Corollary 2. Obviously (14) can be modified further by using the well-known formula for the number of permutations in the symmetric group S_p with a given partition. These numbers are precisely the coefficients in the cycle index

$$Z(S_p; a_1, a_2, \cdots, a_p) = \frac{1}{p!} \sum_{(j)} \frac{p!}{\prod_i i^{j_i} j_i!} \prod_i a_i^{j_i}. \tag{16}$$

where (j) is any vector $(j_1, j_2, \cdots, j_p)$ such that

$$1j_1 + 2j_2 + \cdots + pj_p = p. \tag{17}$$

As an illustration we give some of the details for finding $a(2, 2, 1)$, the number of automata with 2 states, 2 input symbols, and just one output symbol. Since there is only one output function, formula (14) is somewhat simplified:

$$a(2, 2, 1) = \tfrac{1}{4} \sum \prod_{p=1}^{2} \prod_{q=1}^{2} [\sum_{s|[p,q]} s j_s(\alpha)]^{j_p(\alpha) j_q(\beta) \langle p,q \rangle}$$

$$= \tfrac{1}{4}(2^4 + 2^2 + 2^2 + 2^2) = 7.$$

These seven automata are represented by the labeled nets in Fig. 3. The symbols 0 and 1 are used for the inputs.

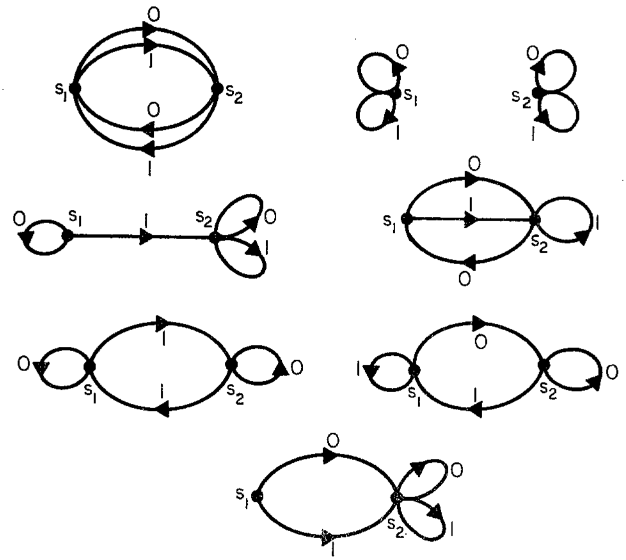

FIG. 3

5. AUTOMATA WITH AN INITIAL STATE AND TERMINAL STATES

A *rooted graph* is a graph in which one of the points is a distinguished point. In an automaton one usually distinguishes one of the states, calling it the *initial state* or *source*. Further, one may distinguish several other states called *terminal states*. Thus to enumerate these automata, we must enumerate appropriately rooted nets. More specifically we enumerate nets with one initial state and t terminal states by applying the power group to the original enumeration of rooted graphs given by Harary (1955).

The operations on permutation groups of forming the power group, product, and sum provide the means for an explicit description of the permutation group which accomplishes the enumeration. Let H_2 be the permutation group:

$$H_2 \equiv \{(E_1 + S_{n-t-1} + S_t^{(E_1+S_{n-t-1}+S_t)\times S_k})\} \times \{S_m^{(E_1+S_{n-t-1}+S_t)\times S_k}\}$$

acting on $S^{S\times X} \times Y^{S\times X}$.

Let $a(n, k, m, t)$ be the number of automata with $n = t + 1$ states, including one initial state and t terminal states, k input symbols, and m output symbols. Let F be the subgroup of H_2 which consists of all permutations of the previously encountered form

$$\{[(\alpha, \beta) \ ; \alpha^{-1}], \quad [(\alpha, \beta) \ ; \gamma]\}.$$

Then the order of F is $(n - t - 1)!\,t!\,k!\,m!$ As before, the number of such automata is $N(F)$, which is given by formula (11) of Corollary 2.

COROLLARY 4. *The number of automata with one initial state and t terminal states is*

$$a(n, k, m, t) = \frac{1}{(n - t - 1)!\,t!\,k!\,m!} \sum I(\alpha, \beta, \alpha) I(\alpha, \beta, \gamma), \quad (18)$$

where the sum is over all permutations in H_2 of the form

$$\{[(\alpha, \beta) \ ; \alpha^{-1}], [(\alpha, \beta) \ ; \gamma]\}$$

and $I(\alpha, \beta, \gamma)$ is given by (15).

Similar results are obtained when the other two types of equivalence are considered.

For a simple example, we take the case in which the number m of output symbols and the number t of terminal states are both 1, and the number of input symbols is 2. Then we have

$$a(n, 2, 1, 1) = \frac{1}{(n - 2)!\,2} \sum \prod_{p=1}^{n-2} \prod_{q=1}^{2} \Big[\sum_{s \mid [p,q]} s j_s(\alpha) \Big]^{j_p(\alpha) j_q(\beta) \, (p,q)}. \quad (19)$$

It is now easy to calculate that for $n = 2$, $a(2,2,1,1) = 10$ (see Table I). The ten rooted labeled nets which correspond to these automata may be obtained by observing that exactly three of the seven nets in Fig. 3 can be rooted in two ways.

We note that the enumeration given by Corollary 4 entails t terminal states different from the initial state. To admit the situation where the

TABLE I

VALUES OF $a(n, 2, 1, t)$[a]

n	t = 1	2	3	4
2	10			
3	378	198		
4	16,576	16,576	5614	
5	819,420	1,226,900	819,420	206,495

[a] In the table the values of $a(n, 2, 1, t)$ are shown for small n and $t = 1$ to n—1. The identical entries occur because $a(n, 2, 1, t) = a(n, 2, 1, n - t - 1)$ for $t = 1$ to $n - 2$.

initial state is itself one of the terminal states, one replaces each occurrence of t in (16) by $t - 1$. It is also easy to count automata with any number r of initial states and t terminal states, as well as any specified number of states which are both initial and terminal.

RECEIVED: March 10, 1966

REFERENCES

BURNSIDE, W. (1911). "Theory of Groups of Finite Order," second edition, p. 191, Theorem VII. Cambridge. Reprinted New York, 1955.

CARMICHAEL, R. D. (1937). "Introduction to the Theory of Groups of Finite Order", p. 22.

DEBRUIJN, N. G. (1959). Generalization of Pólya's fundamental theorem in enumerative combinatorial analysis. *Nederl. Akad. Wetensch. Proc. Ser. A* **62**, 59–69.

DEBRUIJN, N. G. (1964). Pólya's theory of counting. *In* "Applied Combinatorial Mathematics" (E. Beckenbach, ed.), Wiley, pp. 144–184.

HARARY, F. (1955). The number of linear, directed, rooted, and connected graphs. *Trans. Amer. Math. Soc.* **78**, 445–463.

HARARY, F. (1958). On the number of bicolored graphs. *Pacific J. Math.* **8**, 743–755.

HARARY, F. (1959). Exponentiation of permutation groups. *Amer. Math. Monthly* **66**, 572–575.

HARARY, F. (1960). Unsolved problems in the enumeration of graphs. *Publ. Math. Inst. Hungar. Acad. Sci.* **5**, 63–95.

HARARY, F. (1964). Combinatorial problems in graphical enumeration. *In* "Applied Combinatorial Mathematics" (E. Beckenbach, ed.), pp. 185–217. New York.

HARARY, F., AND PALMER, E. M. (1965). The power group of two permutation groups. *Proc. Nat. Acad. Sci. U.S.A.* **54**, 680–682.

HARARY, F., AND PALMER, E. M. (1966) The power group enumeration theorem. *J. Combinatorial Theory*, **1**, 157–173.

HARARY, F., NORMAN, R., AND CARTWRIGHT, D. (1965). "Structural Models: An Introduction to the Theory of Directed Graphs." Wiley, New York.

HARRISON, M. (1965). A census of finite automata. *Canad. J. Math.* **17**, 100–113.

PÓLYA, G. (1937). Kombinatorische Anzahlbestimmungen für Gruppen, Graphen, und chemische Verbindungen. *Acta Math.* **68**, 145–254.