Semigroup Forum Vol. 13 (1977) 253-259

RESEARCH ARTICLE

BOUNDS ON THE INDEX AND PERIOD OF A BINARY RELATION ON A FINITE SET

George Markowsky

Communicated by A. H. Clifford

§0 INTRODUCTION

In this paper, we show that no binary relation on a set of n elements can have its index greater than $(n-1)^2+1$ or its period greater than the size (call it c_n) of the largest cyclic subgroup of the symmetric group on n letters. Furthermore, we show that these bounds are sharp. As a consequence, it follows that the order of any binary relation is bounded by $c_n + (n-1)^2$, which is dominated by c_n.

As an application of these results, we derive Mandl's result [6] that any n-state, one symbol, nondeterministic automation has an equivalent one symbol, deterministic automaton which requires no more than $c_n + (n-1)^2+1$ states. Furthermore, it can be shown that this is "essentially" the best one can do in general.

§1 PRELIMINARIES

All the basic semigroup concepts which we will use are defined in Clifford and Preston [3]. In particular, the following result is found on p. 20.

Theorem 1.1 Let S be a finite semigroup and $a \in S$. Let $\langle a \rangle = \{a, a^2, a^3, \ldots\}$ be the cyclic subsemigroup generated by a. Then, there exist two positive integers, the index r and the period m of a, such that $a^{m+r} = a^r$ and $\langle a \rangle = \{a, a^2, \ldots, a^{m+r-1}\}$, the order of $\langle a \rangle$ being m+r-1. The set $K_a = \{a^r, a^{r+1}, \ldots, a^{m+r-1}\}$ is a cyclic subgroup of S of order m. □

Remark It is well known that any subgroup of a semigroup is contained in an H-class of the semigroup and that, if the product of two elements of an H-class of a semigroup is in the same H-class, then that

$\mathcal{H}$-class is a subgroup of the semigroup. For more details, see [3; pp. 47-66].

Definition 1.2

(a) Let n be an integer. By $\underline{n}$ we mean $\{1,\ldots,n\}$.

b) By B_n we mean $\{X \subset \underline{n} \times \underline{n}\}$. B_n is the semigroup of binary relations on $\underline{n}$, where for $A,B \in B_n$ $AB = \{(i,k) \in \underline{n} \times \underline{n} \mid$ there exists $j \in \underline{n}$ such that $(i,j) \in A$ and $(j,k) \in B\}$. We assume throughout that whenever we discuss B_n, $n \geq 2$. If X is a set, we will use B_X to denote the semigroup of binary relations on X. If X is finite, B_X is obviously isomorphic to $B_{|X|}$.

(c) Let $\Delta \subset \underline{n}$, $A \in B_n$. By ΔA ($A\Delta$) we mean $\{j \in \underline{n} \mid$ for some $i \in \Delta, (i,j) \in A\}$ ($\{i \in \underline{n} \mid$ for some $j \in \Delta$, $(i,j) \in A\}$). If W is a singleton, e.g., $W = \{j\}$, we write jA (Aj) rather than $\{j\}A$ ($A\{j\}$).

(d) Let $A \in B_n$. By the row space of A, R(A), we mean $\{\Delta A \mid \Delta \subset \underline{n}\}$. By the column space of A, C(A), we mean $\{A\Delta \mid \Delta \subset \underline{n}\}$.

Remark. For $A \in B_n$, R(A) and C(A) are complete lattices when ordered by inclusion. The sup in R(A) and C(A) is simply union. Also, every set in R(A) (C(A)) is the union of "rows" ("columns"), i.e., sets of the form xA (Ax) for $x \in \underline{n}$.

§2 THE PERIOD OF A BINARY RELATION

The following seemingly irrelevant results will in short order provide a very good bound on the period of a binary relation. For a basic reference on Lattice Theory, see Birkhoff [1].

Definition 2.1 Let L be a finite lattice and $a \in L$. We say that a is join-irreducible if $a = \sup F$, $F \subset L$, imply $a \in F$.

Lemma 2.2 Let L be a finite lattice ($L \neq \emptyset$) and let $J = \{a \in L \mid$ a is join-irreducible$\}$. Then for all $b \in L$, $b = \sup J_b$, where $J_b = \{a \in J \mid a \leq b\}$. Furthermore, Aut(L), the automorphism group of L, is isomorphic to a subgroup of S_J, the permutation group on the set J.

Proof: Suppose for some $b \in L$, $b \neq \sup J_b$. Thus b cannot be join-irreducible. Thus there exist $b_1,\ldots,b_k \in L$ such that $b = b_1 \vee \ldots \vee b_k$ and $b \neq b_i$ for all i. If $b_i = \sup J_{b_i}$ for all i, then since $J_b \supset \bigcup_{i=1}^{k} J_{b_i}$, we would have $b = \sup J_b$. Since $b \neq \sup J_b$, for some i_o, $b > b_{i_o}$ and $b_{i_o} \neq \sup J_{b_{i_o}}$. Proceeding in this way we would get an infinite chain $a_1 > a_2 > a_3 > \ldots$ ($a_1 = b$, $a_2 = b_{i_o}$) with $a_i \neq \sup J_{a_i}$. This is impossible since L is finite.

Observe that any automorphism of L maps join-irreducible elements into join-irreducible elements. Furthermore, if we are given the values of an automorphism of L on J, we can uniquely reconstruct the automorphism since every element is a sup of join-irreducibles. Thus we have an injective group homomorphism F: $Aut(L) \to S_J$, given by $F(f) = f|J$ (f restricted to J). F is an isomorphism between Aut(L) and a subgroup of S_J. □

Theorem 2.3 Let $A \in B_n$. Then the period of $A \leq c_n$, where c_n is the largest order of any cyclic subgroup of the symmetric group S_n. This bound is "tight", since $S_n \subset B_n$ (any permutation is a binary relation).

Proof: From Section §1, the period of A is bounded by the size of the most numerous cyclic subgroup of the H-class, H, containing all "large enough" powers of A.

K.A. Zaretskii [9] showed that $H \simeq Aut(R(B))$, where $B \in H$ (see Brandon, Hardy, Markowsky [2] for a proof of a more general result and for additional references). By Lemma 2.2, we know that H is thus essentially a subgroup of S_J where J is the set of join-irreducibles of R(B). From the remark following Definition 1.2 it is clear that for $B \in B_n$, $|J| \leq n$. Thus H is essentially a subgroup of S_n. Thus the period of $A \leq c_n$. □

Landau [5] proved the following result which gives a rough idea of the size of c_n. Additional results about c_n and references can be found in [6].

Proposition 2.4 $$\lim_{n\to\infty} \frac{\ln c_n}{\sqrt{n \ln n}} = 1.$$ □

§3 THE INDEX OF A BINARY RELATION

Lemma 3.1 Let $A \in B_n$ and $i, j \in \underline{n}$. If for some $k_k \geq 1$, $(i,j) \in A^k$, then there exists k_o, with $1 \leq k_o \leq n$, such that $(i,j) \in A^{k_o}$.

Proof: Let k_o be the smallest integer ≥ 1, such that $(i,j) \in A^{k_o}$. Thus there must exist exist $i=p_0, p_1, \ldots, p_{k_o} = j \in \underline{n}$, such that $(p_0,p_1), (p_1, p_2), \ldots, (p_{k_o-1}, p_{k_o}) \in A$. We claim that the k_o elements $p_o, \ldots, p_{k_o-1}$ are distinct. If not, say $p_\alpha = p_{\alpha+\delta}$ with $0 \leq \alpha < \alpha+\delta \leq k_o-1$. Then $(p_o,p_\alpha) \in A^\alpha$ and $(p_\alpha,p_{k_o}) = (p_{\alpha+\delta},p_{k_o}) \in A^{k_o-\alpha-\delta}$. Thus we would have $(p_o,p_{k_o}) \in A^{k_o-\delta}$ with $\delta>0$, contradicting the minimality of k_o. Thus the elements are all distinct, since the number of

elements in $\underline{n}$ is $\leq n$, we have $k_o \leq n$. □

Remark: Lemma 3.1 is essentially just the fact that in a directed graph of size n, there is a path between two points if and only if there is a path of length $\leq n$.

Theorem 3.2 Let $A \in B_n$; then the index of A is $\leq (n-1)^2+1$. Furthermore, there exists a binary relation whose index is exactly $(n-1)^2+1$.

Proof: We will proceed by induction on n. Clearly, the theorem is true for n=2. Thus, $n \geq 3$. What we will actually show is that for all $j \in \underline{n}$ and $\alpha=(n-1)^2+1$, jA^{α}, $jA^{\alpha+1}$,.... (the j-th rows of the $A^{\alpha+i}$'s) repeat, i.e., each term appears infinitely often and with a definite period. From this fact it follows that the sequence A^{α}, $A^{\alpha+1}$,..... repeats with period equal to the least common multiple of the periods of the rows. By Theorem 1.1 then, $\alpha \geq$ index of A.

The first case we consider is when $j \notin jA^k$ for all $k \geq 1$. To reduce notation, we may renumber things so that j=n. Let $\Delta = j\ A$ and $\bar{A} \in B_{n-1}$ be given by $\{(i_1,i_2) \in A \mid i_1,i_2 \neq n\}$. A little reflection shows that for $k \geq 0$, $y \in \Delta\ \bar{A}^k$ if and only if $y \in j\ A^{k+1}$. By the induction hypothesis, the index of $\bar{A}$ is $\leq (n-2)^2+1$. Thus $j\ A^{k+1}$ begins to cycle with jA^{α}, $jA^{\alpha+1}$, ... where $\alpha = (n-2)^2+2 \leq (n-1)^2+1$ for $n \geq 2$.

The last case we consider is when $j \in j\ A^k$ for some $k \geq 1$. Let k be such that $j \notin j\ A^i$ for all $1 \leq i \leq k-1$. By Lemma 3.1 it follows that $k \leq n$. Notice that we have $jA^o=\{j\} \subset jA^k \subset jA^{2k} \subset \ldots\ldots \subset jA^{(n-2)k}$ $\ldots\ldots \subset jA^{(n-1)k} \subset \ldots\ldots \subset jA^{nk}$, by induction and the fact that $S,T \subset \underline{n}$, $S \subset T$, implies that $SB \subset TB$ for all $B \in B_n$. If $j\ A^{\ell k} = jA^{\ell k+k}$, then $j\ A^{\alpha}$,.... begins to cycle with $\alpha=\ell k$.

We claim that $j\ A^{(n-1)k} = j\ A^{nk}$. If not we have $1=|\{j\}| < |jA^k| < |jA^k|\ldots. < |jA^{nk}|$, which implies that $j\ A^{nk} = n+1$, which is impossible since $j\ A^{nk} \subset \underline{n}$. Thus jA^{α},... begins to cycle with $\alpha=(n-1)k$. Thus the index is $\leq (n-1)k$. We further consider three subcases.

a. $k \leq n-1$. Then the index $\leq (n-1)^2 < (n-1)^2+1$ and we are done.

b. $|jA^k| \geq 3$. Then arguing as above we see that $j\ A^{(n-2)k} = j\ A^{(n-1)k}$ and the index is $\leq (n-2)k \leq (n-2)n < (n-1)^2+1$.

c. It only remains to consider the case when k=n and $|jA^n|=2$. Since $j \notin jA^i$ for $1 \leq i \leq n-1$, there exist $j = p_0, \ldots, p_n = j$, with $p_0, \ldots, p_{n-1}$ all different and $(p_i, p_{i+1}) \in A$ for i=0,..., n-1. For simplicity, we can renumber everything so that $p_0=1$, $p_1=2$, ..., $p_{n-1}=n$ and $p_n=1$.

There is much more information which we can get about A in this case. First observe that if $(i,1) \in A$, then $i=n$, else $(1,1) \in A^i$ with $i<n$, contradicting our assumption. Furthermore, suppose $(i,j) \in A$ with $i < j$, then $(1,i) \in A^{i-1}$ (since $(\alpha,\alpha+1)\in A$ for $\alpha=1, \ldots, i-1$), $(i,j) \in A$ and $(j,1) \in A^{n-j+1}$. Thus $(1,1) \in A^{n-j+i+1}$. Since $(1,1) \notin A^q$ for all $1\leq q\leq n-1$, $j=i+1$.

Let $\Delta = \{(i,j) \in A \mid i \geq j > 1\}$. Note that if $(i,j)\in\Delta$, $(1,i)\in A^{i-1}$, $(i,j)\in A$ and $(j,n+j-i)\in A^{n-i}$. Thus $(1, n+j-i)\in A^n$. Hence $\{1\} \cup \{n+j-i \mid (i,j)\in\Delta\} \subset 1A^n$. Since $|1A^n|=2$ and $n+j-i>1$, we see that $i-j$ is constant (call it c) for all $(i,j)\in\Delta$. Note that $c \leq n-2$.

Let $i_o = \min \{i \mid$ there exists j, such that $i > j$ and $(i,j) \in\Delta\}$. Then $1A^{i_o} = \{j_o, i_o+1\}$. Let $d=c+1 = i_o + 1-j_o$. Then by induction one can easily see that $1A^{i_o+td} = \{j_o, i_o+1, \alpha_1, \ldots, \alpha_t\}$ where $\alpha_1 \equiv i_o+d \pmod n$ and $\alpha_{j+1} \equiv \alpha_{j+d} \pmod n$ (Note: here we use the residue classes $1, \ldots, n$ rather than $0,1,\ldots,n-1$.). Clearly $1A^{i_o+td} \subset 1A^{i_o+td+d}$ for all t. If $1A^{i_o+td} = 1A^{i_o+td+d}$ for some t, then $1A^{\alpha}, \ldots$, certainly is periodic for $\alpha = i_o+td$. Arguing as we did at the start of the consideration of this case, we see that $1A^{i_o+(n-2)d} = 1A^{i_o+(n-1)d}$. Thus the index is bounded above by $i_o + (n-2)d$. Since $i_o \leq n$ and $d \leq n-1$, $i_o+(n-2)d \leq n+(n-2)(n-1)=(n-1)^2+1$.

The proof above tells us exactly how to achieve the upper bound, i.e., $i_o = n$ and $d = n-1 = c+1$. Thus up to renumbering, the only binary relation achieving this bound on the index is $\{(i,i+1) \mid i\in n-1\}\cup \{(n,1),(n,2)\}$. □

Theorem 3.3 Let c_n be as in Theorem 2.3. Then for all $A \in B_n$, $|< A >| \leq c_n + (n-1)^2$. Furthermore, $\lim_{n\to\infty} \frac{\max\{|<A>| \mid A \in B_n\}}{c_n} = 1$.

Proof: That $|<A>| \leq c_n + (n-1)^2$ follows from Theorems 1.1, 2.3, and 3.2. The rest of the theorem follows from the fact that $\max \{|<A>| \mid A \in B_n\} \geq c_n$ and Proposition 2.4. □

Remark. The binary relation with maximal index produced in Theorem 3.2 is equivalent to the automata example used by Moore [7].

§4 FINITE AUTOMATA OVER A SINGLE LETTER ALPHABET

The definitions we present here have been modified so as to enable us to relate the preceding results to automata theory as quickly as

possible. For more general definitions see any book on automata, such as Hopcraft and Ullman [4].

Definition 4.1

(a) By an n-state, one symbol, nondeterministic automation N we mean a triple (A,I,F) where $A \in B_n$ and $I,F \subset \underline{n}$. I is the set of initial statesand F is the set of final states. Of course, we can use any n-element set in place of $\underline{n}$.

(b) An integer $j \geq 0$ is said to be good for N if $IA^j \cap F \neq \emptyset$. Otherwise, j is said to be bad for N.

(c) An n-state, one symbol, deterministic automaton $\mathcal{D}$ is a triple (θ, i, F) where $\theta:\underline{n} \to \underline{n}$, $i \in \underline{n}$ and $F \subset \underline{n}$. Here i is the initial state and F the set of final states. Of course, we can use any n-element set in place of $\underline{n}$.

(d) An integer $j \geq 0$ is said to be good for $\mathcal{D}$ if $\theta^j(i) \in F$. Otherwise, j is said to be bad for $\mathcal{D}$.

(e) Two n-state, one symbol automata are said to be equivalent if an integer is good for one automaton if and only if it is good for the other.

Remark. The basic question here is, given an n-state, one symbol nondeterministic automaton, what is the smallest number of states for which it is possible to have an equivalent one symbol deterministic automaton? A number of people have shown that for an alphabet of more than one symbol, we must (in the worst case) use 2^n states to realize an n-state, nondeterministic automaton by an equivalent deterministic automaton (see [6] for references). Mandl [6] shows that at least c_n states (in the worst case) are necessary in the one symbol case and that $c_n + (n-1)^2+1$ states is always sufficient. We will use Theorem 3.3 to obtain the same upper bound. The construction we use is a slight modification of a standard automata theory construction.

Theorem 4.2 Let $N = (A,I,F)$ be an n-state, one symbol, nondeterministic automaton. Let $\mathcal{D} = (\theta, i, F')$ be given by $\theta(IA^j) = IA^{j+1}$ (where $\theta:J \to J$ with $J = \{IA^j \mid j = 0,1,\ldots\}$), $i = I$, and $F' = \{X \in J \mid X \cap F \neq \emptyset\}$. Then $\mathcal{D}$ is equivalent to N and the number of states in $\mathcal{D}$ (i.e., $|J|$) is $\leq c_n + (n-1)^2+1$. (Note: The extra 1 comes from considering A^0.)

Proof: Note that j is good for N, if and only if, $IA^j \cap F \neq \emptyset$, if and only if, $\theta^j(I) \in F'$, if and only if, j is good for D. That

$|J| \leq c_m + (n-1)^2+1$ follows from Theorem 3.3. □

Remark. Since c_n dominates n^2, we see that in the worst case the transition from nondeterministic, one symbol automata to deterministic, one symbol automata involves a transition from n to essentially c_n states.

The author would like to acknowledge some stimulating discussions with and valuable references from L. Kou and A. Chandra, and to note that in [8], B. M. Schein discusses the related problem of finding the smallest n such that some cyclic subsemigroup of B_n is isomorphic to some given cyclic semigroup.

REFERENCES

1. Birkhoff, G., Lattice Theory, AMS Colloq. Publ. Vol XXV, Providence, RI, 1967.
2. Brandon, R.L., D.W. Hardy and G. Markowsky, The Schützenberger Group of an H-class in the Semigroup of Binary Relations, Semigroup Forum, Vol. 5 (1972), 45-53.
3. Clifford, A.H. and G.B. Preston, The Algebraic Theory of Semigroups, AMS Surveys, Vol. I, Providence, RI, 1961.
4. Hopcroft, J.E. and J.D. Ullman, Formal Languages and Their Relation to Automata, Addison-Wesley, Reading, MA, 1969.
5. Landau, E., Handbuch Verteilung der Primzahlen 1 1909, 222-229.
6. Mandl, R., Precise Bounds Associated With the Subset Construction on Various Classes of Nondeterministic Finite Automata, Proc. 7th Annual Princeton Conf. on Info. Sciences and Systems, 1973, 263-267.
7. Moore, F.R., On the Bounds for State-Set Size in the Proofs of Equivalence Between Deterministic, Nondeterministic, and Two-Way Automata, IEEE Trans. on Computers 20, 1211-1214.
8. Schein, B. M., Remarks on Research Problem T45, Semigroup Forum, Vol. 4, p. 373.
9. Zaretskii, K.A., The Semigroup of Binary Relations, (In Russian) Mat. Sbornik 61 (1963), 291-305.

Computer Science Department
IBM Thomas J. Watson Research Center
Yorktown Heights, New York 10598

Received January 16, 1976; and, in revised form, June 14, 1976.
In final form, October 1, 1976.