The University of Warwick

THEORY OF COMPUTATION

REPORT NO. 25

ON THE STRUCTURE OF FREE FINITE STATE MACHINES

BY

W. M. BEYNON

Department of Computer Science
University of Warwick
COVENTRY CV4 7AL
ENGLAND.

September 1978

On the structure of free finite state machines

1. Introduction

As explained by Birkhoff and Lipson in [1], a finite state machine M (without outputs) can be considered as an algebra with two "phyla":

$$S = \text{set of states}, \quad I = \text{input alphabet}$$

and a single operator: $T : S \times I \to S$, the transition function of M.

Given $M = (S,I)$ and a pair of integers (m,n) there is an associated machine $U_{m,n}(M)$ freely generated as an algebra by states $t_1,\ldots,t_m$ and input symbols $e_1,\ldots,e_n$ subject to the relations which hold within M. Explicitly $U_{m,n}(M) = (\mathcal{S},\mathcal{I})$ where

$$\mathcal{I} = \{e_1,\ldots,e_n\}$$

and each state in $\mathcal{S}$ consists of an equivalence class of expressions of the form

$$t_i w(e_1,\ldots,e_n) \text{ where } 1 \leq i \leq m,\ w \in \mathcal{I}^*$$

and $t_i w(e_1,\ldots,e_n)$ and $t_j v(e_1,\ldots,e_n)$ are equivalent if for all pairs of maps $\{t_1,\ldots,t_m\} \xrightarrow{f} S$ and $\{e_1,\ldots,e_n\} \xrightarrow{g} I$ the relation:

$$f(t_i)\ w(g(e_1),\ldots,g(e_n)) = f(t_j)\ v(g(e_1),\ldots,g(e_n))$$

holds in M. The transition function then maps $(t_i w(e_1,\ldots,e_n),e_i)$ to $t_i(w(e_1,\ldots,e_n)e_i)$.

Definition Using the notation introduced above, it will be convenient to refer to a pair of maps $f : \{t_1,\ldots,t_m\} \to S$ and $g : \{e_1,\ldots,e_n\} \to I$ as a phyla-preserving mapping from $\{t_1,\ldots,t_m,e_1,\ldots,e_n\}$ to M or an interpretation of $\{t_1,\ldots,t_m,e_1,\ldots,e_n\}$ in M.

The proof of the following theorem is to be found in [1].

<u>Theorem</u> (i) $U_{m,n}(M)$ is a finite state machine.

(ii) $U_{m,n}(M)$ is generated by the m states $t_1,\ldots,t_m$ and n input symbols $e_1,\ldots,e_n$.

(iii) If π denotes the canonical phyla-preserving map from the set $\{t_1,\ldots,t_m,e_1,\ldots,e_n\}$ to $U_{m,n}(M)$, and θ is any phyla-preserving map from $\{t_1,\ldots,t_m,e_1,\ldots,e_n\}$ to M, then there is an unique algebra homomorphism $\phi : U_{m,n}(M) \to M$ such that $\theta = \phi\pi$.

(iv) $U_{m,n}(M)$ is an epimorphic image of any other finite state machine having property (iii).

<u>Definition</u> If $t_i\ w(e_1,\ldots,e_n)$ and $t_j\ v(e_1,\ldots,e_n)$ are equivalent in $U_{m,n}(M)$, then

$$t_i\ w(e_1,\ldots,e_n) = t_j\ v(e_1,\ldots,e_n)$$

is a <u>universal relation</u> in M.

2. <u>The case $m \geqslant 1$</u>

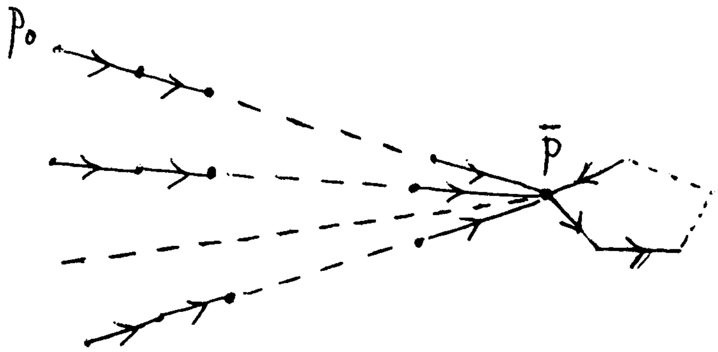
<u>Theorem 1</u>: For a machine $M = (S,I)$ to have a universal relation of the form

$$t_i\ w(e_1,\ldots,e_n) = t_j\ v(e_1,\ldots,e_n) \text{ with } i \neq j$$

it is necessary and sufficient that for each input α in I there should exist a state $t(\alpha)$ such that (a) $t(\alpha).\alpha = t(\alpha)$

and (b) for each s in S there is a non-negative integer $r(s)$ such that $s.\alpha^{r(s)} = t(\alpha)$

<u>Proof:</u> Suppose that M has a universal relation U of the form $t_i\ w(e_1,\ldots,e_n) = t_j\ v(e_1,\ldots,e_n)$ for $i \neq j$. If $\alpha \in I$, there is a submachine $M_\alpha = (S,\alpha^*)$ of M, which is a disjoint union of k machines of the following type:



Since U holds under all interpretations (f,g) for which $g(e_i) = \alpha$ for $1 \leqslant i \leqslant n$, it is clear that $k = 1$. Moreover, taking interpretations (f,g) such that $f(t_i) = p_o$, $f(t_j) = p_o\,\alpha^c$ for some non-negative integer c and $g(e_i) = \alpha$ for $1 \leqslant i \leqslant n$, it follows that

$$p_o\alpha^{\ell(w)} = p_o\alpha^{\ell(v)+c}$$

in M for $c = 0, 1, 2, \ldots$. This establishes that $\overline{p}\alpha = \overline{p}$, so that conditions (a) and (b) are satisfied with $t(\alpha) = \overline{p}$.

For the converse, suppose that given input α in I, there is a $t(\alpha)$ for which conditions (a) and (b) hold. Then let $r(\alpha) = \max_{s\epsilon S} r(s)$, and $r = \max_{\alpha\epsilon I} r(\alpha)$. It is clear that the relation $s\alpha^r = t\alpha^r$ holds for all s,t in S and all α in I; that is, the relation $t_1\, x_1^{\ r} = t_2\, x_1^{\ r}$ holds universally in M.

<u>Corollary to Theorem 1:</u>

Unless a relation of the form $t_1\, x_1^{\ r} = t_2\, x_1^{\ r}$ holds universally in the machine M, the finite state machine $U_{m,n}(M)$ is (up to isomorphism) m disjoint copies of $U_{1,n}(M)$.

3. <u>Structure of $U_{1,n}(M)$</u>

<u>Definition</u> Let K be a finite monoid generated by elements $x_1,\ldots,x_n$. The machine $\mathfrak{M}(K,X)$ <u>associated with the monoid K generated by X</u> has a set of states K, input alphabet $X = \{x_1,\ldots,x_n\}$ and transition function $K \times X \to K$ defined by multiplication in K. The machine $\mathfrak{M}(K,X)$ will be called a <u>monoid machine</u>. If K is a group, then $\mathfrak{M}(K,X)$ is a <u>group machine</u> or <u>Cayley diagram</u>.

Theorem 2: (i) If M is a finite state machine, then, for $n \geq 1$, $U_{1,n}(M)$ is isomorphic to the monoid machine $\mathcal{M}(K,X)$, where K is the monoid freely generated by $X = \{x_1,\ldots,x_n\}$ subject to the relations:

$$w(x_1,\ldots,x_n) = v(x_1,\ldots,x_n)$$

where $tw(e_1,\ldots,e_n) = tv(e_1,\ldots,e_n)$

is a universal relation in M.

(ii) Let K be a finite monoid generated by $X = \{x_1,\ldots,x_n\}$

For $\mathcal{M}(K,X)$ to be isomorphic with $U_{1,n}(M)$ for some finite state machine M, it is necessary and sufficient that for each relation $w(x_1,\ldots,x_n) = v(x_1,\ldots,x_n)$ in K and each map $f : \{1,2,\ldots,n\} \circlearrowleft$, the relation $w(x_{f(1)},\ldots,x_{f(n)}) = v(x_{f(1)},\ldots,x_{f(n)})$ also holds in K. If this condition is satisfied then $U_{1,n}(\mathcal{M}(K,X)) \simeq \mathcal{M}(K,X)$.

(iii) For $U_{1,n}(M)$ to be a group machine $(n \geq 1)$ it is necessary and sufficient that for some non-trivial w in $\mathcal{G}^*$, a relation of the form:

$$tw(e_1,\ldots,e_n) = t$$

holds universally in M.

Definition When the necessary and sufficient conditions (stated in (ii) above) for $\mathcal{M}(K,X)$ to be isomorphic with $U_{1,n}(M)$ for a finite state machine M are satisfied, X is said to generate K universally or to generate a universal presentation of K.

Proof: (i) The elements of $U_{1,n}$ are equivalence classes of expressions of the form:

$$tw(e_1,\ldots,e_n)$$

where $tw(e_1,\ldots,e_n)$ and $tv(e_1,\ldots,e_n)$ are equivalent if $tw(e_1,\ldots,e_n) = tv(e_1,\ldots,e_n)$ is a universal relation in M, with transition function defined by

$$(tw(e_1,\ldots,e_n),e_i) \mapsto t(w(e_1,\ldots,e_n)e_i)$$

The map $tw(e_1,\dots,e_n) \mapsto w(x_1,\dots,x_n)$ then clearly induces an isomorphism $U_{1,n}(M) \simeq K$.

(ii) Suppose $\mathfrak{M}(K,X) \simeq U_{1,n}(M)$. Then if the relation $w(x_1,\dots,x_n) = v(x_1,\dots,x_n)$ holds in K then $tw(e_1,\dots,e_n) = tv(e_1,\dots,e_n)$ is a universal relation in M. Thus given any map $f : \{1,2,\dots,n\}^{\circlearrowleft}$, the relation

$$tw(e_{f(1)},\dots,e_{f(n)}) = tv(e_{f(1)},\dots,e_{f(n)})$$

holds universally in M, whence $w(x_{f(1)},\dots,x_{f(n)}) = v(x_{f(1)},\dots,x_{f(n)})$ in K.

Conversely, suppose that if $w(x_1,\dots,x_n) = v(x_1,\dots,x_n)$ in K and f is a map $\{1,2,\dots,n\}^{\circlearrowleft}$, then $w(x_{f(1)},\dots,x_{f(n)}) = v(x_{f(1)},\dots,x_{f(n)})$. It follows that the relation $tw(e_1,\dots,e_n) = tv(e_1,\dots,e_n)$ holds universally in $\mathfrak{M}(K,X)$. Conversely if $tw(e_1,\dots,e_n) = tv(e_1,\dots,e_n)$ is a universal relation in $\mathfrak{M}(K,X)$ then certainly $w(x_1,\dots,x_n) = v(x_1,\dots,x_n)$ in K (interpreting t as 1, and e_i as x_i for $i = 1,2,\dots,n$). The isomorphism

$$U_{1,n}(\mathfrak{M}(K,X)) \simeq \mathfrak{M}(K,X)$$

follows from (i).

(iii) Let $x_1,\dots,x_n$ generate $U_{1,n}(M)$ freely subject to the relations:

$$w(x_1,\dots,x_n) = v(x_1,\dots,x_n)$$

where $tw(e_1,\dots,e_n) = tv(e_1,\dots,e_n)$

is a universal relation in M. Since $x_1{}^r = 1$ for some $r \geqslant 1$, the relation $te_i{}^r = t$ must hold universally in M for some r.

Conversely, suppose $tw(e_1,\dots,e_n) = t$ holds universally in M, with w non-trivial. Then given $f : \{1,2,\dots,n\}^{\circlearrowleft}$ the relation $w(x_{f(1)},\dots,x_{f(n)}) = 1$ holds in $U_{1,n}(M)$. In particular, $w(x_i,\dots,x_i) = 1$ for each i, which proves the existence of $x_i{}^{-1}$ for each i, as w is non-trivial.

Definition Let $M = (S,I)$ be a finite state machine, and let $F(S)$ denote the semigroup of mappings $S \to S$ under composition. For each α in I, let $T(\alpha)$ be the map $S \to S$ in $F(S)$. The map T extends naturally to a semigroup homomorphism $I^* \to F(S)$. The image of this homomorphism is the syntactic monoid $\mathcal{S}(M)$ of M.

Lemma: For each $n > 1$, $U_{1,n}(M)$ and $U_{1,n}(\mathcal{M}(\mathcal{S}(M), T(I)))$ are isomorphic.

Proof: Suppose that $sw(\alpha_1,\ldots,\alpha_n) = sv(\alpha_1,\ldots,\alpha_n)$ for all s in S and all α_i in I. Then $w(T(\alpha_1),\ldots,T(\alpha_n))$ and $v(T(\alpha_1),\ldots,T(\alpha_n))$ represent the same element of $\mathcal{S}(M)$, so that $fw(T(\alpha_1),\ldots,T(\alpha_n)) = fv(T(\alpha_1),\ldots,T(\alpha_n))$ for all f in $\mathcal{S}(M)$ and all α_i in I.

Conversely, if $fw(T(\alpha_1),\ldots,T(\alpha_n)) = fv(T(\alpha_1),\ldots,T\alpha_n))$ for all f in $\mathcal{S}(M)$ and all α_i in I, then $w(T(\alpha_1),\ldots,T(\alpha_n)) = v(T(\alpha_1),\ldots,T(\alpha_n))$ in $\mathcal{S}(M)$. Thus $sw(\alpha_1,\ldots,\alpha_n) = sv(\alpha_1,\ldots,\alpha_n)$ in M for all s in S and all α_i in I.

This proves the required isomorphism.

It is evident that a universal relation of the form $tw(e_1,\ldots,e_m) = tv(e_1,\ldots,e_m)$ holds in a monoid machine $\mathcal{M}(K,X)$ if and only if $w(x_1,\ldots,x_m) = v(x_1,\ldots,x_m)$ for all x_i in X. This result will be used in the proof of the next theorem, which describes a simple method for constructing $U_{1,m}(M)$ when M is a monoid machine.

Theorem 3: Let K be a finite monoid generated by $X = \{x_1,\ldots,x_m\}$. Let X^* be the set of rows of the n by m^n array whose columns are the elements of X^n. Then X^* has n elements $X_1,\ldots,X_n$, which generate a submonoid K^* of K^{m^n}, and $U_{1,n}(\mathcal{M}(K,X))$ and $\mathcal{M}(K^*,X^*)$ are isomorphic.

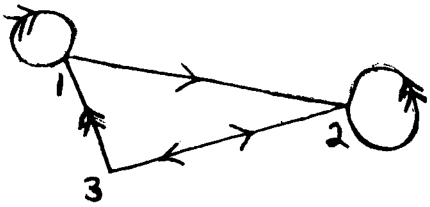
Proof: Suppose that $w(y_1,\ldots,y_n) = v(y_1,\ldots,y_n)$ in K for all interpretations of $y_1,\ldots,y_n$ in X. Then the identity $w(y_1,\ldots,y_n) = v(y_1,\ldots,y_n)$ necessarily holds in K^*.

Conversely $w(X_1,\ldots,X_n) = v(X_1,\ldots,X_n)$ in K^* entails $w(y_1,\ldots,y_n) = v(y_1,\ldots,y_n)$ for all interpretations of $y_1,\ldots,y_n$ in X, each interpretation corresponding to a projection of the identity $w(X_1,\ldots,X_n) = v(X_1,\ldots,X_n)$ onto a single component.

4. Illustrative Examples

Example 1:

Let M be the machine having three states, and input alphabet $\{a,b\}$, as indicated below:



(This machine is considered by Birkhoff and Lipson in [1]).

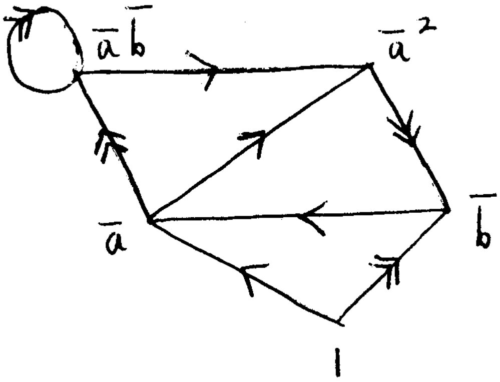
For this machine M, $\mathcal{S}(M)$ is the subsemigroup of maps $\{1,2,3\}^{\circlearrowleft}$ generated by a, b where

$\bar{a}(1) = 2, \quad \bar{a}(2) = 3, \quad \bar{a}(3) = 2$

and $\bar{b}(1) = 1, \quad \bar{b}(2) = 2, \quad \bar{b}(3) = 1$

The syntactic monoid then consists of five maps viz. $1, \bar{a}, \bar{b}, \bar{a}^2, \bar{a}\bar{b}$, and the additional relations $\bar{a}^3 = \bar{a}$, $\bar{b}^2 = \bar{b}$, $\bar{b}.\bar{a} = \bar{a}$, $\bar{a}^2\bar{b} = \bar{b}$, $\bar{a}\bar{b}\bar{a} = \bar{a}^2$ hold.

The machine $\mathcal{M} = \mathcal{M}(\mathcal{S}(M), \{\bar{a},\bar{b}\})$ is:



The free machine $U_{1,2}(\mathfrak{m}) \simeq U_{1,2}(M)$ is now the semigroup machine associated with the subsemigroup of $\mathcal{S}(M)^4$ generated by

$$A = (\bar{a},\bar{a},\bar{b},\bar{b}) \text{ and } B = (\bar{a},\bar{b},\bar{a},\bar{b})$$

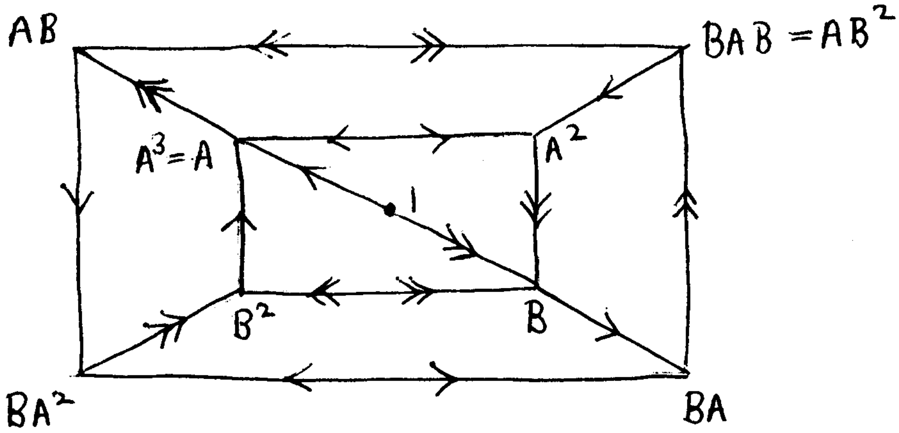
It has 9 elements viz.:

$$1,\ A,\ B,\ A^2 = (\bar{a}^2,\bar{a}^2,\bar{b},\bar{b}),\ B^2=(\bar{a}^2,\bar{b},\bar{a}^2,\bar{b}),$$

$$AB = (\bar{a}^2,\overline{ab},\bar{a},\bar{b}),\ BAB = (\bar{a},\overline{ab},\bar{a}^2,\bar{b})$$

$$BA = (\bar{a}^2,\bar{a},\overline{ab},\bar{b}) \text{ and } BA^2 = (\bar{a},\bar{a}^2,\overline{ab},\bar{b})$$

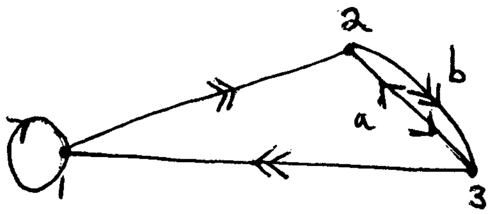
The resulting semigroup machine is:



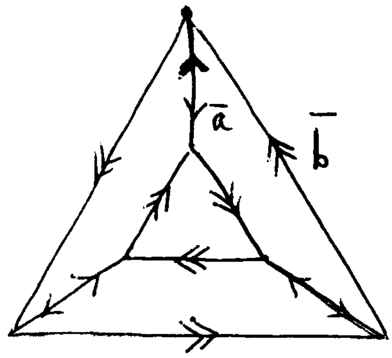
(Note that there is an error in the representation of $U_{1,n}(M)$ given by Birkhoff and Lipson in [1], and that a similar error occurs in [2]. The relation $AB^2 = BA^2$ does not hold universally in M as the diagrams in [1] and [2] suggest).

Example 2:

Let N be the machine with 3 states, and input alphabet {a, b}, as represented below:



In this case, $\mathcal{S}(N)$ is the subgroup of the semigroup of maps $\{1,2,3\}$ consisting of all permutations, with generators $\bar{a} = (23)$, $\bar{b} = (123)$. The machine $\mathcal{M}(\mathcal{S}(N), \{a,b\})$ is then a Cayley diagram for the symmetric group S_3 viz:



By the previous results, $U_{1,2}(M) \simeq U_{1,2}(\mathcal{M})$ is the group machine associated with the subgroup of $S_3^{\,4}$ generated by $A = (\bar{a},\bar{a},\bar{b},\bar{b},)$ and $B = (\bar{a},\bar{b},\bar{a},\bar{b})$ generated by $A = (\bar{a},\bar{a},\bar{b},\bar{b})$ and $B = (\bar{a},\bar{b},\bar{a},\bar{b})$. Since $(AB)^2 = (1,1,1,\bar{b})$, and it can be shown that $(\bar{a},\bar{a},\bar{b})$ and $(\bar{a},\bar{b},\bar{a})$ generate the subgroup of $C_1 \times S_3^{\,2}$ consisting of triples (c,p,q) such that pq and c are permutations of the same parity, it follows that $U_{1,2}(M)$ is (up to isomorphism) the group machine $\mathcal{M}(G,X)$ where $G = S_3 \times S_3 \times C_3$ and $X = \{(\bar{a},\bar{b},\bar{b}), (\bar{b},\bar{a},\bar{b})\}$. This result would be difficult to obtain by the direct method for computing $U_{1,2}(M)$ described in [1].

5. Monoids with a universal presentation

It has been shown in the previous section that every free finite state machine is of the form $\mathcal{M}(S,X)$ where S is a finite monoid, and X $\{x_1,\ldots,x_n\}$ is a set of generators for S. In this section, necessary conditions on S and X for $\mathcal{M}(S,X)$ to be a free finite state machine are described. For instance, it is evident that if X generates S universally then the set of relations between $x_1,\ldots,x_n$ holding in S is invariant under any permutation of $\{1,2,\ldots,n\}$. This fact is relevant for the interpretation of the results and proofs of this section.

Lemma 3: If the elements $x_1,\dots,x_n$ generate the finite monoid S universally, then either $x_1 = x_2 = \dots = x_n$ or $x_1,x_2,\dots,x_n$ are pairwise distinct and generate S irredundantly.

Proof: Suppose that $x_1 = w(x_2,\dots,x_n)$. Let f be the map $\{1,2,\dots,n\}$ such that $f(1) = 2$ and $f(i) = i$ for $i > 2$. Then $x_{f(1)} = x_2 = w(x_{f(2)},\dots,x_{f(n)}) = w(x_2,\dots,x_n) = x_1$, whence $x_1 = x_2 = \dots = x_n$.

Notation: Let P be a partition of $\{1,2,\dots,n\}$. The rank of P (the number of blocks in the partition P) will be denoted by $\rho(P)$.

Theorem 4: Let S be a finite monoid generated universally by distinct generators $x_1,\dots,x_n$. For each partition P let E(P) be the smallest congruence on S such that x_i and x_j are congruent for all (i,j) in P Then

(i) the map E is a join-preserving bijection from the lattice of partitions of $\{1,2,\dots,n\}$ (ordered by $P < Q$ if P is a refinement of Q), to the congruence lattice of S.

(ii) the quotient S/E(P) is isomorphic with the subsemigroup $S_{\rho(P)}$ of S generated by $x_1,\dots,x_{\rho(P)}$.

Proof: (ii) Let F be the monoid freely generated by $e_1,\dots,e_n$. Define $p : \{1,2,\dots,n\}$ by setting $p(i)$ = smallest integer in the block of P which contains i. There is a unique monoid homomorphism $\phi : F \to G$ such that $\phi(e_i) = x_{p(i)}$ for $i = 1,2,\dots,n$. Since $w(x_1,\dots,x_n) = v(x_1,\dots,x_n)$ implies $w(x_{p(1)},\dots,x_{p(n)}) = v(x_{p(1)},\dots,x_{p(n)})$ there is a monoid homomorphism $\phi' : G \to G$, induced by ϕ, such that $\phi'(w(x_1,\dots,x_n)) = w(x_{p(1)},\dots,x_{p(n)})$. Consider the equivalence relation E on S defined by $x \equiv y$ if and only if there exist w and v in F such that $w(x_1,\dots,x_n) = x$, $v(x_1,\dots,x_n) = y$ and $w(x_{p(1)},\dots,x_{p(n)}) = v(x_{p(1)},\dots,x_{p(n)})$. Clearly $(i,j) \in P$ implies $(x_i,x_j) \in E$, whilst it is easy to show that $\operatorname{Ker} \phi' = E \subseteq E(P)$. Since E(P) is the smallest congruence in which x_i and x_j are equivalent whenever $(i,j) \in P$, it follows that Ker $\phi' = E(P)$. Thus $S/E(P)$ is isomorphic to Im ϕ', the submonoid of S generated by $\{x_{p(1)},\ldots,x_{p(n)}\}$, and this set comprises $\rho(P)$ distinct elements.

(i) If P is a refinement of Q, then certainly $E(P) \subseteq E(Q)$. Moreover $P < Q$ ensures $\rho(P) > \rho(Q)$, so $S/E(P)$ and $S/E(Q)$ are non-isomorphic by (ii) and the previous lemma. Thus $P < Q$ entails $E(P) \underset{\neq}{\subset} E(Q)$.

Now $E(P \vee Q)$ is the congruence generated by the relations $x_i = x_j$ for $(i,j) \in P \vee Q$. Since $P \vee Q$ is the smallest equivalence relation which contains both P and Q, it follows that $E(P \vee Q) = E(P \cup Q) = E(P) \vee E(Q)$, showing that E is a join-preserving map.

Suppose that $E(P) = E(Q)$. Then $E(P) = E(P) \vee E(Q) = E(P \vee Q)$. Since $P \vee Q \geqslant P$, this implies $Q \leqslant P$. Similarly $P \leqslant Q$, so that E is a bijective map.

Note: The map E is not in general a lattice homomorphism.

Let S be universally generated by $x_1,\ldots,x_n$, and suppose that x_1 (and thus each generator) has stem of length c and period t.

Suppose that $w(e_1,\ldots,e_n)$ and $v(e_1,\ldots,e_n)$ are elements of length $\ell(w)$ and $\ell(v)$ respectively in F, the monoid freely generated by $e_1,\ldots,e_n$. If $w(x_1,\ldots,x_n) = v(x_1,\ldots,x_n)$ in S, then

$$x_1^{\ell(w)} = w(x_1,\ldots,x_1) = v(x_1,\ldots,x_1) = x_1^{\ell(v)}$$

whence either

(i) $\ell(w) = \ell(v) < c$

or (ii) $\min(\ell(w), \ell(v)) \geqslant c$

and $\ell(w) \equiv \ell(v) \pmod t$

Given an element x in S, it is then consistent to define the length of x as the unique number $\ell(x)$ such that if $w(x_1,\ldots,x_n) = x$ then $\ell(x) \equiv \ell(w) \pmod t$ and $\ell(x) < c + t$.

Corollary: Let U be the partition of $\{1,2,\ldots,n\}$ consisting of a single block. Then $(x,y) \in E(U)$ if and only if $\ell(x) = \ell(y)$.

Proof: Let $w(x_1,\ldots,x_n) = x$ and $v(x_1,\ldots,x_n) = y$. Then $\ell(x) = \ell(y)$ if and only if $w(x_1,\ldots,x_1) = v(x_1,\ldots,x_1)$, and this is equivalent to $(x,y) \in E(U)$ as observed in the proof of part (ii) of the theorem.

6. Algebras with a universal presentation

Necessary conditions for a finite monoid to possess a universal presentation have already been described. In this section, stronger conditions are derived for special varieties of monoid.

Theorem 5: Let S be an upper semilattice with least element 0 (i.e. a monoid $(S,\vee)$ in which the binary operation $\vee$ is commutative and idempotent and 0 is the identity element).

The generators $x_1,\ldots,x_n$ of S generate a universal presentation of S if and only if either $x_1 = x_2 = \ldots = x_n$ or $x_1,\ldots,x_n$ freely generate S as an upper semilattice with zero element.

Proof: The sufficiency of the stated conditions is clear. Accordingly, it suffices to show that if a relation of the form

$$(U) \quad \bigvee_{i \in A} x_i = \bigvee_{i \in B} x_i \qquad A,B \subseteq \{1,2,\ldots,n\}$$

holds in S then either $x_1 = x_2 = \ldots = x_n$ or $A = B$.

Assume without loss of generality that $A \neq \phi$. Then if $B = \phi$ the relation (U) is of the form

$$\bigvee_{i \in A} x_i = 0$$

whence $x_i = 0$ for all i in A, and $x_1 = x_2 = \ldots = x_n = 0$.

Suppose A, B both non-empty, and let $I = A \cap B$, $\overline{A} = A \setminus I$ and $\overline{B} = B \setminus I$. If $\overline{A} = \overline{B} = \phi$ then $A = B$. Otherwise assume without loss of generality that $\overline{A} \neq \phi$ and let $f : \{1,2,\ldots,n\}^{\circlearrowleft}$ be such that

$$f(i) = \begin{cases} 1 & \text{if } i \in \overline{A} \\ 2 & \text{otherwise} \end{cases}$$

Since (U) is a universal relation,

$\bigvee_{i \in A} x_{f(i)} = \bigvee_{i \in B} x_{f(i)}$ also holds in S. If $I = \phi$, this entails $x_1 = x_2$, whence $x_1 = x_2 = \ldots = x_n$. If $I \neq \phi$, then $x_2 \vee x_1 = x_2$ whence (by universality and commutativity)

$$x_1 = x_1 \vee x_2 = x_2 \vee x_1 = x_2 .$$

<u>Theorem 6</u>: Let G be a finite Abelian group. The elements $g_1,\ldots,g_n$ of G are the generators of a universal presentation if and only if for some t and some d dividing t, the group G is freely generated by $g_1,\ldots,g_n$ subject to the relations:

$$\left.\begin{array}{ll} \forall i & g_i^{\,t} = 1 \\ \forall i,j & g_i g_j = g_j g_i \\ \forall i,j & g_i^{\,d} = g_j^{\,d} \end{array}\right\} \quad (*)$$

<u>Proof</u>: The group G with free presentation on generators $g_1,\ldots,g_n$ subject to the relations (*) is universally presented on generators $g_1,\ldots,g_n$, since the set of relations (*) is closed under the application of any function $f : \{1,2,\ldots,n\}^{\circlearrowleft}$ to the indices of the g_i's.

Conversely, suppose that $g_1,\ldots,g_n$ universally generate G and have common order t. Then G has a free presentation on $g_1,\ldots,g_n$ with relations

$$\begin{array}{ll} \forall i & g_i^{\,t} = 1 \\ \forall i,j & g_i g_j = g_j g_i \end{array}$$

and other relations of the form $\prod_{i=1}^{n} g_i^{\,r_i} = 1$. Since $g_i^{\,t} = g_j^{\,t} = 1$, there is a least number d such that $g_i^{\,d} = g_j^{\,d}$ (for some, whence all pairs of indices (i,j)). As $g_i^{\,t} = g_j^{\,t}$ and $g_i^{\,d} = g_j^{\,d}$ ensure $g_i^{\,HCF(d,t)} = g_j^{\,HCF(d,t)}$, it must be that d divides t. If the relation $\prod_{i=1}^{n} g_i^{\,r_i} = 1$ holds in G, then $\prod_{i=1}^{n} g_{f(i)}^{\,r_i} = 1$ for all maps $f : \{1,2,\dots,n\}$. In particular, if $r = \sum_{i=1}^{n} r_i$ then $g_1^{\,r} = 1$, whence t divides r. Moreover, $g_1^{\,r_1} g_2^{\,r-r_1} = 1$, showing that $g_1^{\,r_1} = g_2^{\,r_1}$ and thus that d divides r_1. By symmetry, d divides r_i for each i, so that the relation $\prod_{i=1}^{n} g_i^{\,r_i} = 1$ is a consequence of the set of relations $g_i^{\,d} = g_j^{\,d}$ for all i and j.

Cor.1:

G is an Abelian group universally generated by elements $g_1,\dots,g_n$ of order t if and only if G and $C_t \times C_d^{\,n-1} \equiv \langle\alpha\rangle \times \langle\beta\rangle^{n-1}$ are isomorphic via the mapping ϕ such that $\phi(g_1) = (\alpha,1,\dots,1)$ and $\phi(g_i) = (\alpha,1,\dots,1,\beta,1,\dots,1)$ (ith component) for $i = 2,3,\dots,n$.

Proof: It is not difficult to show that the group freely generated by $g_1,\dots,g_n$ subject to the relations (*) is indeed isomorphic to $C_t \times C_d^{\,n-1}$ via the mapping ϕ.

7. Groups with a universal presentation

Necessary and sufficient conditions for a finite Abelian group to have a universal presentation are given in Theorem 6. The results and examples in this section relate to the harder (and unresolved) problem of determining which finite non-Abelian groups admit a universal presentation.

The following result is a corollary to Theorem 6:

Cor 2 to Thecrem 6:

Suppose that $g_1,\ldots,g_n$ generate a universal presentation for the finite group G. Let G' be the commutator subgroup of G. The images $\bar{g}_1,\ldots,\bar{g}_n$ of $g_1,\ldots,g_n$ generate a universal presentation of G/G'. In particular, G/G' is isomorphic with $C_t \times C_d^{\,n-1}$ for some positive integers k and d where d divides k.

Proof: The elements of G' are products of commutators. Thus if $w(g_1,\ldots,g_n) \in G'$ and $f : \{1,2,\ldots,n\}$ is any map, then $w(g_{f(1)},\ldots,g_{f(n)}) \in G'$. That is, the relations imposed upon $g_1,\ldots,g_n$ by taking the quotient by G' hold universally in G/G'. By Theorem 6, G/G' (being a finite Abelian group) is isomorphic with some $C_t \times C_d^{\,n-1}$.

The next result is the analogue for groups of Theorem 4.

Theorem 7: Let G be a finite group generated universally by distinct generators $g_1,\ldots,g_n$. For each partition P, let N(P) be the normal subgroup of G generated by all elements of the form $g_i g_j^{-1}$ such that $(i,j) \in P$.

Then

(i) the map N is a join-preserving bijection from the lattice of partitions of $\{1,2,\ldots,n\}$ (ordered by refinement) to the lattice of normal subgroups of G.

(ii) the quotient G/N(P) is isomorphic with the subgroup $G_{\rho(P)}$ of G generated by $g_1,\ldots,g_{\rho(P)}$, and G is isomorphic to a semi-direct product of $G_{\rho(P)}$ and N(P).

Proof: It suffices to show that $G \cong G_{\rho(P)} * N(P)$; the other results are interpretations of Theorem 4.

For $i = 1,2,\ldots,n$ let $q(i)$ be the least integer such that $(i,q(i)) \in P$. Let $\theta : G \to G$ be the group homomorphism such that $\theta(g_i) = g_{q(i)}$ (c.f. proof of Theorem 4 (ii)). Then $\mathrm{Ker}\theta = N(P)$, and $\mathrm{Im}\theta = \langle g_{q(1)},\ldots,g_{q(n)}\rangle$. Note that $g_i = g_{q(i)}(g_{q(i)}^{-1} g_i) \in \mathrm{Im}\theta.\mathrm{Ker}\theta$

so that $G = Im\theta . Ker\ \theta$. Moreover, if $g \in Ker\theta \cap Im\theta$, then $\theta(g) = g = 1$. Thus $G = Im\ \theta * Ker\ \theta \simeq G_{\rho(P)} * N(P)$

Corollary 1: If G has a universal presentation by generators $g_1,\dots,g_n$ of common order t then the elements of G of length 0 form a normal subgroup N of G, and $G \simeq C_t * N$.

Proof: See the corollary to Theorem 4, and apply Theorem 7 (ii).

Corollary 2: If $k \geqslant 4$, then the symmetric group S_k has no universal presentation.

Proof: Suppose $g_1,\dots,g_n$ are permutations generating S_k universally, and let $g_1,\dots,g_n$ have common order t. Since $S_k \simeq C_t * N$ for some normal subgroup N, it must be that $N = A_k$ and $t = 2$. On the other hand, in view of Theorem 7 (i), $n \leqslant 2$. But, if a group is generated by two elements of order 2 it is dihedral (see [4] p.49 Ex.1).

8. Examples of groups with universal presentations

Example 1:

As suggested by the proof of the previous corollary, the dihedral group D_n of order 2n has a universal presentation by two generators of order 2, viz. $< x,y \mid x^2 = y^2 = (xy)^n = 1 >$. In particular $S_3 (\simeq D_3)$ is universally generated by a pair of transpositions.

Example 2:

Every finite Burnside group B(t,n) (which is generated by n elements $x_1,\dots,x_n$ subject to relations $g^t = 1$ for every g in B(t,n))is universally generated by its canonical generating set.

The Burnside group B(3,3) of order 2187 illustrates that the map N in Theorem 7 (and likewise the map E in Theorem 4) is not in general a lattice homomorphism. As described in [3], evey element of B(3,3) has a unique representation of the form:

$$x_1^{a_1} x_2^{a_2} x_3^{a_3} (x_1,x_2)^{b_3} (x_1,x_3)^{b_2} (x_2,x_3)^{b_1} (x_1,x_2,x_3)^{c}$$

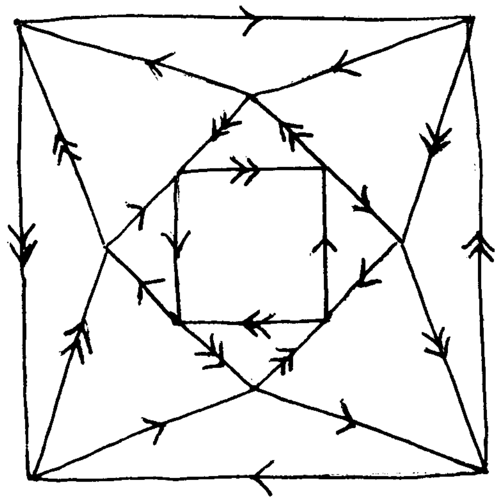
where $0 \leq a_i, b_i, c \leq 2$. Let P be the partition (12)(3) and Q the partition (1)(23). The partition $P \wedge Q$ is (1)(2)(3) whence $N(P \wedge Q) = \{1\}$ But $(x_1,x_2)^2 (x_1,x_3) (x_2,x_3)^2 \in N(P) \cap N(Q)$ (it reduces to 1 under adjunction of the relation $x_1 = x_2$ or $x_2 = x_3$) whence $N(P) \cap N(Q) \neq N(P \wedge Q)$.

Example 3:

The group A_4 is universally generated by x and y subject to the relations:

$$x^3 = y^3 = (xy)^3 = (xy^2)^2 = 1$$

The Cayley diagram associated with this presentation is:



Example 4:

The group G of order 56 generated by x and y subject to the relations

$$x^2y\ xy^3 = y^2xyx^3 = 1$$

is universally generated by x and y, which are elements of order 7 (see [4] p.60). The semi-direct product decomposition of G referred to in Corollary 2 to Theorem 7 exhibits G as $C_7 * C_2^3$.

References

[1] G. Birkhoff and J.D. Lipson, Heterogeneous Algebras, J. Combinatorial Theory 8(1970) 115-133.

[2] G. Birkhoff and J.D. Lipson, Universal Algebra and Automata, AMS Colloquium publications in Pure Mathematics (Tarski Symposium 1974).

[3] M. Hall, The Theory of Groups, New York, Macmillan 1959.

[4] D.L. Johnson, Presentation of Groups, LMS Lecture note series No. 22, Cambridge University Press.