Introduction to Universal Algebra

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 400

Subsection 1

Steiner Triple Systems, Squags and Sloops

Steiner Triple Systems

Definition

A **Steiner triple system** on a set A is a family $\mathscr{S}$ of three-element subsets of A, such that each pair of distinct elements from A is contained in exactly one member of $\mathscr{S}$. $|A|$ is called the **order** of the Steiner triple system.

- If $|A| = 1$, then $\mathscr{S} = \emptyset$.
- If $|A| = 3$, then $\mathscr{S} = \{A\}$.
- If $|A| = 2$, there are no Steiner triple systems on A.

Necessary Conditions on $|A|$ and $|\mathscr{S}|$

Theorem

If $\mathscr{S}$ is a Steiner triple system on a finite set A, then:

(a) $|\mathscr{S}| = \frac{|A|(|A|-1)}{6}$;

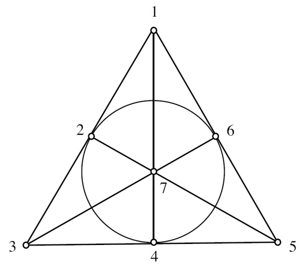
(b) $|A| \equiv 1$ or $3 \pmod 6$.

(a) Note that each member of $\mathscr{S}$ contains three distinct pairs of elements of A. Each pair of elements appears in only one member of S. Thus, the number of pairs of elements from A is exactly $3|S|$, i.e., $\binom{|A|}{2} = 3|\mathscr{S}|$. This gives $\frac{|A|(|A|-1)}{2} = 3|\mathscr{S}|$ whence the conclusion follows.

(b) Fix $a \in A$ and let $T_1, \ldots, T_k$ be the members of $\mathscr{S}$ to which a belongs. No pair of elements of A is contained in two distinct triples of $\mathscr{S}$. Thus, the doubletons $T_1 - \{a\}, \ldots, T_k - \{a\}$ are mutually disjoint. Each member of $A - \{a\}$ is in some triple along with the element a. So $A - \{a\} = (T_1 - \{a\}) \cup \cdots \cup (T_k - \{a\})$. Thus, $2 \mid |A| - 1$, so $|A| \equiv 1 \pmod 2$. From (a), $|A| \equiv 0$ or $1 \pmod 3$; hence, $|A| \equiv 1$ or $3 \pmod 6$.

The Steiner Triple System of Order 7

- After $|A| = 3$, the next possible size $|A|$ is 7.
- The figure shows a Steiner triple system of order 7, where we require that three numbers be in a triple iff they lie on one of the lines drawn or on the circle.
  This is the only Steiner triple system of order 7 (up to a relabeling of the elements).



Steiner Quasigroups

- To construct new Steiner triple systems from old ones,
  - we convert it to an algebraic system;
  - use standard constructions in universal algebra.
- A natural way of introducing a binary operation $\cdot$ on A is to require

$$a \cdot b = c \quad \text{if} \quad \{a, b, c\} \in \mathscr{S}.$$

  Since $a \cdot a$ is left undefined, we define $a \cdot a = a$.
- The associative law for $\cdot$ fails (look at the system of order 3).
- Nonetheless, we have the identities:

(Sq1) $x \cdot x \approx x$;
(Sq2) $x \cdot y \approx y \cdot x$;
(Sq3) $x \cdot (x \cdot y) \approx y$.

Definition

A groupoid satisfying the identities (Sq1)-(Sq3) above is called a **squag** (or **Steiner quasigroup**).

Squads Correspond to Steiner Triple Systems

Theorem

If $\langle A, \cdot \rangle$ is a squag, define $\mathscr{S}$ to be the set of three-element subsets $\{a, b, c\}$ of A, such that the product of any two elements gives the third. Then $\mathscr{S}$ is a Steiner triple system on A.

- Suppose $a \cdot b = c$ holds. Then $a \cdot (a \cdot b) = a \cdot c$, so by (Sq3), $b = a \cdot c$. Similarly, $b \cdot c = a$. Thus, in view of (Sq1), if any two are equal, all three are equal. Consequently, for any two distinct elements of A, there is a unique third element (distinct from the two) such that the product of any two gives the third. Thus, $\mathscr{S}$ is indeed a Steiner triple system on A.

Steiner Loops

- Another approach to converting a Steiner triple system $\mathscr{S}$ on A to an algebra is to adjoin a new element, called 1, and replace $a \cdot a = a$ by

$$a \cdot a = 1, \qquad a \cdot 1 = 1 \cdot a = a.$$

- This leads to a groupoid with identity $\langle A \cup \{1\}, \cdot, 1\rangle$, satisfying the identities:

(Sℓ1) $x \cdot x \approx 1$;
(Sℓ2) $x \cdot y \approx y \cdot x$;
(Sℓ3) $x \cdot (x \cdot y) \approx y$.

Definition

A groupoid with a distinguished element $\langle A, \cdot, 1\rangle$ is called a **sloop** (or **Steiner loop**) if the identities (Sℓ1)-(Sℓ3) hold.

Sloops and Steiner Triple Systems

Theorem

If $\langle A, \cdot, 1\rangle$ is a sloop and $|A| \geq 2$, define $\mathscr{S}$ to be the three-element subsets of $A - \{1\}$, such that the product of any two distinct elements gives the third. Then $\mathscr{S}$ is a Steiner triple system on $A - \{1\}$.

- Similar to the preceding theorem.

Subsection 2

Quasigroups, Loops and Latin Squares

Quasigroups Formalisms

- A quasigroup is usually defined to be a groupoid $\langle A, \cdot\rangle$, such that, for any elements $a, b \in A$, there are unique elements c, d, satisfying

$$a \cdot c = b, \qquad d \cdot a = b.$$

- The previously adopted definition of quasigroups has two extra binary operations $\backslash$ and $/$, left division and right division respectively, which allow us to consider quasigroups as an equational class.
- Recall that the axioms for quasigroups $\langle A, /, \cdot, \backslash\rangle$ are given by

$$\begin{array}{ll} x\backslash(x \cdot y) \approx y & (x \cdot y)/y \approx x \\ x \cdot (x\backslash y) \approx y & (x/y) \cdot y \approx x. \end{array}$$

- To convert a quasigroup $\langle A, \cdot\rangle$ in the usual definition to one in our definition we let
  - a/b be the unique solution c of $c \cdot b = a$;
  - $a\backslash b$ be the unique solution d of $a \cdot d = b$.

Quasigroups Formalisms (Cont'd)

- Conversely, let $\langle A, /, \cdot, \backslash \rangle$ be a quasigroup by our definition.
  - If $a, b \in A$, we have $a \cdot (a \backslash b) = b$. So there is a $c := a \backslash b$, such that $a \cdot c = b$.
  - Suppose $a, b \in A$ and c is such that $a \cdot c = b$. Then $a \backslash (a \cdot c) = a \backslash b$. Hence $c = a \backslash b$. So only one such c is possible.

Similarly, we can show that there is exactly one d, such that $d \cdot a = b$, namely $d = b / a$.

Thus, the two definitions of quasigroups are, in an obvious manner, equivalent.

Quasigroups with Identity and Squags

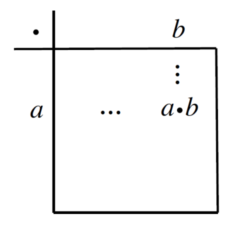
- A loop is usually defined to be a quasigroup with an identity element $\langle A, \cdot, 1\rangle$. In our definition, we have an algebra $\langle A, /, \cdot, \backslash, 1\rangle$ and such loops form an equational class.
- Suppose $\mathscr{S}$ is a Steiner triple system on A.

  The associated squag $\langle A, \cdot\rangle$ is a quasigroup: If $a \cdot c = b$, then $a \cdot (a \cdot c) = a \cdot b$. So $c = a \cdot b$. Furthermore, $a \cdot (a \cdot b) = b$. Hence, if we are given a, b, there is a unique c, such that $a \cdot c = b$. Similarly, there is a unique d, such that $d \cdot a = b$.
- In the case of squags we do not need to introduce the additional operations $/$ and $\backslash$ to obtain an equational class:

  In this case $/, \backslash$ and $\cdot$ are all the same.
- Squags are sometimes called **idempotent totally symmetric quasigroups**.

Cayley Tables and Quasigroups

- Given any finite groupoid $\langle A, \cdot \rangle$, we can write out the multiplication table of $\langle A, \cdot \rangle$ in a square array, giving the **Cayley table** of $\langle A, \cdot \rangle$.



Theorem

A finite groupoid $\mathbf{A}$ is a quasigroup iff every element of A appears exactly once in each row and in each column of the Cayley table of $\langle A, \cdot \rangle$.

- If we are given $a, b \in A$, then there is exactly one c satisfying $a \cdot c = b$ iff b occurs exactly once in the a-th row of the Cayley table of $\langle A, \cdot \rangle$ and there is exactly one d, such that $d \cdot a = b$ iff b occurs exactly once in the a-th column of the Cayley table.

Latin Squares

Definition

A **Latin square** of **order** n is an $n \times n$ matrix (a_{ij}) of elements from an n element set A, such that each member of A occurs exactly once in each row and each column of the matrix.

- The figure shows a Latin square of order 4:

a	b	c	d
d	c	a	b
b	a	d	c
c	d	b	a

- From the theorem, Latin squares are in an obvious one-to-one correspondence with quasigroups by using Cayley tables.

Subsection 3

Orthogonal Latin Squares

Orthogonal Latin Squares

Definition

If (a_{ij}) and (b_{ij}) are two Latin squares of order n with entries from a set A with the property that, for each $\langle a, b \rangle \in A \times A$, there is exactly one index ij, such that $\langle a, b \rangle = \langle a_{ij}, b_{ij} \rangle$, then we say that (a_{ij}) and (b_{ij}) are **orthogonal Latin squares**.

- The figure shows an example of orthogonal Latin squares of order 3.

a	b	c
b	c	a
c	a	b

a	b	c
c	a	b
b	c	a

- Euler conjectured that, if $n \equiv 2 \pmod 4$, then there do not exist orthogonal Latin squares of order n.
  - In 1900 Tarry verified the conjecture for $n = 6$
  - Macneish gave a construction for all orders n, where $n \not\equiv 2 \pmod 4$.
  - Bose, Parker, and Shrikhande showed that $n = 2, 6$ are the only values for which Euler's conjecture is actually true.

Pairs of Orthogonal Latin Squares

- Two orthogonal Latin squares on a set A correspond to two quasigroups $\langle A, /, \cdot, \backslash\rangle$ and $\langle A, /\!\!\!\circ, \circ, \circ\!\!\!\backslash\rangle$, such that the map $\langle a, b\rangle \mapsto \langle a \cdot b, a \circ b\rangle$ is a permutation of $A \times A$.
- For a finite set A, this will be a bijection iff there exist functions $*_\ell$ and $*_r$ from $A \times A$ to A, such that $*_\ell(a \cdot b, a \circ b) = a$, $*_r(a \cdot b, a \circ b) = b$.

Definition (Evans)

A **pair of orthogonal Latin squares** is an algebra $\langle A, /, \cdot, \backslash, /\!\!\!\circ, \circ, \circ\!\!\!\backslash, *_\ell, *_r\rangle$, with eight binary operations such that:

(i) $\langle A, /, \cdot, \backslash\rangle$ is a quasigroup;

(ii) $\langle A, /\!\!\!\circ, \circ, \circ\!\!\!\backslash\rangle$ is a quasigroup;

(iii) $*_\ell(x \cdot y, x \circ y) \approx x$;

(iv) $*_r(x \cdot y, x \circ y) \approx y$.

The **order** of such an algebra is the cardinality of its universe. Let POLS be the variety of pairs of orthogonal Latin squares.

Existence of POLS of Prime Power

Lemma

If q is a prime power and $q \geq 3$, then there is a member of POLS of order q.

- Let $\langle K, +, \cdot \rangle$ be a finite field of order q, and let e_1, e_2 be two distinct nonzero elements of K. Then define two binary operations $\Box_1$ and $\Box_2$ on K by

$$a \Box_i b = e_i \cdot a + b, \quad i = 1, 2.$$

Claim: The two groupoids $\langle K, \Box_1 \rangle$ and $\langle K, \Box_2 \rangle$ are quasigroups.

$a \Box_i c = b$ iff $c = b - e_i \cdot a$, and $d \Box_i a = b$ iff $d = e_i^{-1} \cdot (b - a)$.

Also we have that $\langle a \Box_1 b, a \Box_2 b \rangle = \langle c \Box_1 d, c \Box_2 d \rangle$ implies $e_1 \cdot a + b = e_1 \cdot c + d$, $e_2 \cdot a + b = e_2 \cdot c + d$. Hence, $e_1 \cdot (a - c) = d - b$, $e_2 \cdot (a - c) = d - b$. Thus, as $e_1 \neq e_2$, $a = c$ and $b = d$.

Thus, the Cayley tables of $\langle K, \Box_1 \rangle$ and $\langle K, \Box_2 \rangle$ give rise to orthogonal Latin squares of order q.

Existence of POLS

Theorem

If $n \equiv 0, 1$, or $3 \pmod 4$, then there is a pair of orthogonal Latin squares of order n.

- Note that $n \equiv 0, 1$ or $3 \pmod 4$ iff $n = 2^\alpha p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, with $\alpha \neq 1$, $\alpha_i \geq 1$, and each p_i is an odd prime.
  - The case $n = 1$ is trivial;
  - For $n \geq 3$, use the preceding lemma to construct $\mathbf{A}_0, \mathbf{A}_1, \ldots, \mathbf{A}_k$ in POLS of order $2^\alpha, p_1^{\alpha_1}, \ldots, p_k^{\alpha_k}$ respectively.
    Then $\mathbf{A}_0 \times \mathbf{A}_1 \times \cdots \times \mathbf{A}_k$ is the desired algebra.

The Class IPOLS

Definition

An algebra $\mathbf{A} = \langle A, F \rangle$ is a **binary algebra** if each of the fundamental operations is binary.

A binary algebra $\mathbf{A} = \langle A, F \rangle$ is **idempotent** if $f(x,x) \approx x$ holds in $\mathbf{A}$, for each function symbol f.

Definition

Let IPOLS be the variety of idempotent algebras in POLS.

Binary Idempotent Varieties and 2-Designs

Definition

A variety V of algebras is **binary idempotent** if:

(i) the members of V are binary idempotent algebras;

(ii) V can be defined by identities involving at most two variables.

- Note that IPOLS is a binary idempotent variety.

Definition

A 2-**design** is a tuple $\langle B, B_1, \ldots, B_k \rangle$ where:

(i) B is a finite set;

(ii) each B_i is a subset of B (called a **block**);

(iii) $|B_i| \geq 2$, for all i;

(iv) each two-element subset of B is contained in exactly one block.

2-Designs and Binary Idempotent Algebras in a Variety

Lemma

Let V be a binary idempotent variety and let $\langle B, B_1, \ldots, B_k \rangle$ be a 2-design. Let $n = |B|$, $n_i = |B_i|$. If V has members of size n_i, $1 \le i \le k$, then V has a member of size n.

- Let $\mathbf{A}_i \in V$, with $|A_i| = n_i$. We can assume $A_i = B_i$. Then, for each binary function symbol f in the type of V, we can find a binary function f^B on B, such that, when we restrict f^B to B_i, it agrees with $f^{\mathbf{A}_i}$ (essentially we let f^B be the union of the $f^{\mathbf{A}_i}$). As V can be defined by two variable identities $p(x,y) \approx q(x,y)$ which hold on each $\mathbf{A}_i$, it follows that we have constructed an algebra $\mathbf{B}$ in V, with $|B| = n$.

Existence of IPOLS of Prime Power Order

Lemma

If q is a prime power and $q \geq 4$, then there is a member of IPOLS of size q. In particular, there are members of sizes 5, 7 and 8.

- Let $\mathbf{K}$ be a field of order q, let e_1, e_2 be two distinct elements of $K - \{0,1\}$.

  Define two binary operations $\Box_1, \Box_2$ on K by

  $$a \Box_i b = e_i \cdot a + (1 - e_i) \cdot b.$$

  - $a \Box_i c = b$ iff $e_i \cdot a + (1 - e_i) \cdot c = b$ iff $c = (1 - e_i)^{-1}(b - e_i \cdot a)$
    $d \Box_i a = b$ iff $e_i \cdot d + (1 - e_i) \cdot a = b$ iff $d = e_i^{-1}(b - (1 - e_i) \cdot a)$;
  - $a \Box_i a = e_i \cdot a + (1 - e_i) \cdot a = a$.

  Thus, the Cayley tables of $\langle K, \Box_1 \rangle$ and $\langle K, \Box_2 \rangle$ give rise to idempotent Latin squares.

Existence of IPOLS of Prime Power Order (Cont'd)

- If $a\Box_1 b = c\Box_1 d$ and $a\Box_2 b = c\Box_2 d$, we get $e_1 \cdot a + (1 - e_1) \cdot b = e_1 \cdot c + (1 - e_1) \cdot d$ and $e_2 \cdot a + (1 - e_2) \cdot b = e_2 \cdot c + (1 - e_2) \cdot d$, whence $e_1 \cdot (a - c) = (1 - e_1) \cdot (d - b)$ and $e_2 \cdot (a - c) = (1 - e_2) \cdot (d - b)$. Since $e_1, e_2 \neq 0, 1$ and $e_1 \neq e_2$, we must have $a = c$ and $b = d$.

  Hence, the Cayley tables of $\langle K, \Box_1 \rangle$ and $\langle K, \Box_2 \rangle$ give rise to an idempotent pair of orthogonal Latin squares.

Projective Plane of Order n

- Given a finite field F of cardinality n, we form a **projective plane** $\mathscr{P}_n$ **of order** n by letting:
  - the **points** be the 1-dimensional subspaces U of the vector space F^3;
  - the **lines** be the 2-dimensional subspaces V of F^3.

  A point U **belongs** to a line V if $U \subseteq V$.
- One can readily verify that:
  - every line of $\mathscr{P}_n$ has $n+1$ points;
  - every point of $\mathscr{P}_n$ belongs to $n+1$ lines;
  - there are n^2+n+1 points and n^2+n+1 lines.
- Finally, we have:
  - Any two distinct points belong to exactly one line;
  - Any two distinct lines meet in exactly one point.

An IPOL of Order 54

Lemma

There is a 2-design $\langle B, B_1, \ldots, B_k \rangle$, with $|B| = 54$ and $|B_i| \in \{5,7,8\}$, for $1 \le i \le k$.

- Let π be the projective plane of order 7. This has 57 points and each line contains 8 points. Choose three points on one line and remove them. Let B be the set of the remaining 54 points, and let the B_i be the sets obtained by intersecting the lines of π with B. Then $\langle B, B_1, \ldots, B_k \rangle$ is easily seen to be a 2-design, since each pair of points from B lies on a unique line of π, and $|B_i| \in \{5,7,8\}$.

Theorem

There is an idempotent pair of orthogonal Latin squares of order 54.

- Combine the preceding three lemmas.

Subsection 4

Finite State Acceptors

Finite State Acceptors and Unary Terms

Definition

A **finite state acceptor** (abbreviated **f.s.a.**) of type $\mathscr{F}$ (where the type is finite with unary symbols) is a 4-tuple $\mathbf{A} = \langle A, F, a_0, A_0 \rangle$, where:

- $\langle A, F \rangle$ is a finite unary algebra of type $\mathscr{F}$;
- $a_0 \in A$;
- $A_0 \subseteq A$.

The set A is the set of **states** of $\mathbf{A}$, a_0 is the **initial state**, and A_0 is the set of **final states**.

Definition

If we are given a finite type $\mathscr{F}$ of unary algebras, let $\langle \mathscr{F}^*, \cdot, 1 \rangle$ be the monoid of strings on $\mathscr{F}$. Given a string $w \in \mathscr{F}^*$, an f.s.a. $\mathbf{A}$ of type $\mathscr{F}$, and an element $a \in A$, let $w(a)$ be the element resulting from applying the "term" $w(x)$ to a. E.g., if $w = fg$, then $w(a) = f(g(a))$, and $1(a) = a$.

Accepted Languages and Regular Languages

Definition

A **language** of type $\mathscr{F}$ is a subset of $\mathscr{F}^*$. A string w from $\mathscr{F}^*$ is **accepted** by an f.s.a. $\mathbf{A} = \langle A, F, a_0, A_0 \rangle$ of type $\mathscr{F}$ if $w(a_0) \in A_0$.
The **language accepted** by $\mathbf{A}$, written $\mathscr{L}(\mathbf{A})$, is the set of strings from $\mathscr{F}^*$ accepted by $\mathbf{A}$.

Definition

Given languages L, L_1 and L_2 of type $\mathscr{F}$ let

$$\begin{array}{rcl} L_1 \cdot L_2 & = & \{w_1 \cdot w_2 : w_1 \in L_1, w_2 \in L_2\}, \\ L^* & = & \text{the subuniverse of } \langle \mathscr{F}^*, \cdot, 1 \rangle \text{ generated by } L. \end{array}$$

The set of **regular languages** of type $\mathscr{F}$ is the smallest collection of subsets of $\mathscr{F}^*$ which contains the singleton languages $\{f\}, f \in \mathscr{F} \cup \{1\}$, and is closed under the set-theoretic operations, $\cup, \cap, '$ and the operations $\cdot$ and *, defined above.

Partial Algebras and Partial f.s.a.'s

Definition

A **partial unary algebra** of type $\mathscr{F}$ is a pair $\langle A, F\rangle$, where F is a family of partially defined unary functions on A indexed by $\mathscr{F}$, i.e., the domain and range of each function f are contained in A.

Definition

A **partial finite state acceptor (partial f.s.a.)** $\mathbf{A} = \langle A, F, a_0, A_0\rangle$ of type $\mathscr{F}$ has the same definition as an f.s.a. of type $\mathscr{F}$, except that we only require that $\langle A, F\rangle$ be a partial unary algebra of type $\mathscr{F}$.
The **language accepted by A**, $\mathscr{L}(\mathbf{A})$, is defined as for an f.s.a. (but, for a given $w \in \mathscr{F}^*$, $w(a)$ might not be defined, for some $a \in A$).

Languages Accepted by Partial f.s.a's and Ranges

Lemma

Every language accepted by a partial f.s.a. is accepted by some f.s.a.

- Let $\mathbf{A} = \langle A, F, a_0, A_0 \rangle$ be a partial f.s.a. Choose $b \notin A$ and let $B = A \cup \{b\}$. For $f \in \mathscr{F}$ and $a \in A \cup \{b\}$, if $f(a)$ is not defined in $\mathbf{A}$, let $f(a) = b$. This gives an f.s.a. which accepts the same language as $\mathbf{A}$.

Definition

If $\langle A, F, a_0, A_0 \rangle$ is a partial f.s.a., then, for $a \in A$ and $w \in \mathscr{F}^*$, the **range of** w **applied to** a, written $\mathrm{Rg}(w, a)$, is the set

$$\mathrm{Rg}(w, a) = \begin{cases} \{f_n(a), f_{n-1}f_n(a), \ldots, f_1 \cdots f_n(a)\}, & \text{if } w = f_1 \cdots f_n \\ \{a\}, & \text{if } w = 1 \end{cases}$$

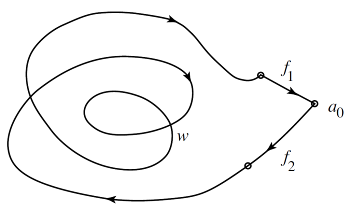
f.s.a.'s and Regular Languages

Lemma

The language accepted by any f.s.a. is regular.

- Let L be the language of the partial f.s.a. $\mathbf{A} = \langle A, F, a_0, A_0 \rangle$. We will prove the lemma by induction on $|A|$.
  - First note that $\varnothing$ is a regular language as $\varnothing = \{f\} \cap \{f\}'$, for any $f \in \mathscr{F}$. For the ground case suppose $|A| = 1$. If $A_0 = \varnothing$, then $\mathscr{L}(\mathbf{A}) = \varnothing$, a regular language. If $A_0 = \{a_0\}$, let $\mathscr{G} = \{f \in \mathscr{F} : f(a_0) \text{ is defined}\}$. Then $\mathscr{L}(\mathbf{A}) = \mathscr{G}^* = (\bigcup_{f \in \mathscr{G}} \{f\})^*$, also a regular language.
  - For the induction step assume that $|A| > 1$, and for any partial f.s.a. $\mathbf{B} = \langle B, F, b_0, B_0 \rangle$, with $|B| < |A|$ the language $\mathscr{L}(\mathbf{B})$ is regular. If $A_0 = \varnothing$, then, as before, $\mathscr{L}(\mathbf{A}) = \varnothing$, a regular language. So assume $A_0 \neq \varnothing$. The crux of the proof is to decompose any acceptable word into: (a) a product of words which one can visualize as giving a sequence of cycles when applied to a_0; (b) followed by a noncycle, mapping from a_0 to a member of A_0 if $a_0 \notin A_0$.

f.s.a.'s and Regular Languages (Cont'd)



- Let $C = \{\langle f_1, f_2\rangle \in \mathscr{F} \times \mathscr{F} : f_1 w f_2(a_0) = a_0$, for some $w \in \mathscr{F}^*, f_2(a_0) \neq a_0$ and $\mathrm{Rg}(w, f_2(a_0)) \subseteq A - \{a_0\}\}$. For $\langle f_1, f_2\rangle \in C$, let $C_{f_1 f_2} = \{w \in \mathscr{F}^* : f_1 w f_2(a_0) = a_0, \mathrm{Rg}(w, f_2(a_0)) \subseteq A - \{a_0\}\}$. Then $C_{f_1 f_2}$ is the language accepted by $\langle A - \{a_0\}, F, f_2(a_0), f^{-1}(a_0) - \{a_0\}\rangle$. Hence, by induction, $C_{f_1 f_2}$ is regular. Set $\mathscr{H} = \{f \in \mathscr{F} : f(a_0) = a_0\} \cup \{1\}$, $\mathscr{D} = \{f \in \mathscr{F} : f(a_0) \neq a_0\}$. For $f \in \mathscr{D}$, let $E_f = \{w \in \mathscr{F}^* : wf(a_0) \in A_0, \mathrm{Rg}(w, f(a_0)) \subseteq A - \{a_0\}\}$. We see that E_f is the language accepted by $\langle A - \{a_0\}, F, f(a_0), A_0 - \{a_0\}\rangle$. Hence, by induction, it is also regular. Let

$$E = \begin{cases} \bigcup_{f \in \mathscr{D}} E_f \cdot \{f\}, & \text{if } a_0 \notin A_0 \\ (\bigcup_{f \in \mathscr{D}} E_f \cdot \{f\}) \cup \{1\}, & \text{if } a_0 \in A_0 \end{cases}.$$

Then $L = E \cdot (\mathscr{H} \cup \bigcup_{\langle f_1, f_2\rangle \in C} \{f_1\} \cdot C_{f_1 f_2} \cdot \{f_2\})^*$, a regular language.

Deletion Homomorphisms

Definition

Given a type $\mathscr{F}$, $t \notin \mathscr{F}$, the **deletion homomorphism** $\delta_t : (\mathscr{F} \cup \{t\})^* \to \mathscr{F}^*$ is the homomorphism defined by $\delta_t(f) = f$, for $f \in \mathscr{F}$, $\delta_t(t) = 1$.

Lemma

If L is a language of type $\mathscr{F} \cup \{t\}$, where $t \notin \mathscr{F}$, which is also the language accepted by some f.s.a., then $\delta_t(L)$ is a language of type $\mathscr{F}$ which is the language accepted by some f.s.a.

- Let $\mathbf{A} = \langle A, F \cup \{t\}, a_0, A_0 \rangle$ be an f.s.a. with $\mathscr{L}(\mathbf{A}) = L$. For $w \in \mathscr{F}^*$, define $S_w = \{\overline{w}(a_0) : \overline{w} \in (\mathscr{F} \cup \{t\})^*, \delta_t(\overline{w}) = w\}$, $B = \{S_w : w \in \mathscr{F}^*\}$. This is of course finite as A is finite. For $f \in \mathscr{F}$, define $f(S_w) = S_{fw}$. This makes sense as S_{fw} depends only on S_w, not on w. Next let $b_0 = S_1$, and let $B_0 = \{S_w : S_w \cap A_0 \neq \emptyset\}$. Then $\langle B, F, b_0, B_0 \rangle$ accepts w iff $w(S_1) \in B_0$ iff $S_w \cap A_0 \neq \emptyset$ iff $\overline{w}(a_0) \in A_0$, for some $\overline{w} \in \delta_t^{-1}(w)$, iff $\overline{w} \in L$, for some $\overline{w} \in \delta_t^{-1}(w)$, iff $w \in \delta_t(L)$.

Kleene's Theorem

Theorem (Kleene)

Let L be a language. Then L is the language accepted by some f.s.a. iff L is regular.

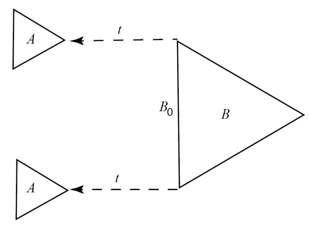
($\Rightarrow$) This has already been proven.

($\Leftarrow$) By induction.

- If $L = \{f\}$, then we can use the partial f.s.a. $a \xleftarrow{f} a_0$, where all functions not drawn are undefined, and $A_0 = \{a\}$.
- If $L = \{1\}$ use $A = A_0 = \{a_0\}$, with all f's undefined.
- Next suppose L_1 is the language of $\langle A, F, a_0, A_0 \rangle$ and L_2 is the language of $\langle B, F, b_0, B_0 \rangle$. Then $L_1 \cap L_2$ is the language of $\langle A \times B, F, \langle a_0, b_0 \rangle, A_0 \times B_0 \rangle$, where $f(\langle a, b \rangle)$ is defined to be $\langle f(a), f(b) \rangle$.
- L_1' is the language of $\langle A, F, a_0, A - A_0 \rangle$.
- Combining these we see by De Morgan's law that $L_1 \cup L_2$ is the language of a suitable f.s.a..

Kleene's Theorem (Cont'd)

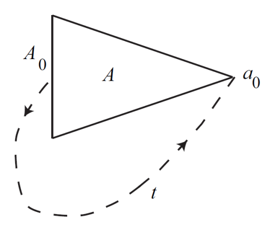
- To handle $L_1 \cdot L_2$, we first expand our type to $\mathscr{F} \cup \{t\}$. Then, mapping each member of B_0 to the input of a copy of A, we see that $L_1 \cdot \{t\} \cdot L_2$ is the language of some f.s.a. Hence, if we use the preceding lemma, it follows that $L_1 \cdot L_2$ is the language of some f.s.a..



- Similarly for L_1^*, let t map each element of A_0 to a_0. Then $(L_1 \cdot \{t\})^* \cdot L_1$ is the language of this partial f.s.a.; Hence,

$$L_1^* = \delta_t[(L_1 \cdot \{t\})^* \cdot L_1 \cup \{1\}]$$

is the language of some f.s.a..



Monoid of Words and Free Algebra

Definition

Let τ be the mapping from $\mathscr{F}^*$ to $T(x)$, the set of terms of type $\mathscr{F}$ over x, defined by $\tau(w) = w(x)$.

Lemma

The mapping τ is an isomorphism between the monoid $\langle \mathscr{F}^*, \cdot, 1\rangle$ and the monoid $\langle T(x), \circ, x\rangle$, where $\circ$ is "composition".

- If $w_1 \neq w_2$, then, in $T(x)$, $w_1(x) \neq w_2(x)$. Thus τ is 1-1;
  If $w(x) \in T(x)$, then $\tau(w) = w(x)$ and τ is also onto.
  Thus τ is a bijection.
  Finally, we have
  - $\tau(1) = 1(x) = x$;
  - $\tau((f_1 \cdots f_n) \cdot (g_1 \cdots g_m)) = f_1(\cdots(f_n(g_1 \cdots (g_m(x))\cdots))\cdots) = (f_1 \cdots f_n)((g_1 \cdots g_m)(x)) = \tau(f_1 \cdots f_n) \circ \tau(g_1 \cdots g_m)$.

Congruences

Definition

For $\theta \in \text{Con}\langle \mathscr{F}^*, \cdot, 1\rangle$, let $\theta(x) = \{\langle w_1(x), w_2(x)\rangle : \langle w_1, w_2\rangle \in \theta\}$.

Lemma

The map $\theta \mapsto \theta(x)$ is a lattice isomorphism from the lattice of congruences on $\langle \mathscr{F}^*, \cdot, 1\rangle$ to the lattice of fully invariant congruences on $\mathbf{T}(x)$.

- Suppose $\theta \in \text{Con}\langle \mathscr{F}^*, \cdot, 1\rangle$ and $\langle w_1, w_2\rangle \in \theta$.

  For $u \in \mathscr{F}^*$, we have $\langle uw_1, uw_2\rangle \in \theta$. Thus, $\theta(x)$ is a congruence on $\mathbf{T}(x)$.

  For $u \in \mathscr{F}^*$, we have $\langle w_1 u, w_2 u\rangle \in \theta$. Hence, $\theta(x)$ is fully invariant.

Acceptance by f.s.a.'s and Finite Index

Lemma

If L is a language of type $\mathscr{F}$ accepted by some f.s.a., then there is a $\theta \in \mathrm{Con}\langle \mathscr{F}^*, \cdot, 1\rangle$, such that θ is of finite index (i.e., $\langle \mathscr{F}^*, \cdot, 1\rangle/\theta$ is finite) and $L^\theta = L$, i.e., L is a union of cosets of θ.

- Choose $\mathbf{A}$ an f.s.a. of type $\mathscr{F}$, such that $\mathscr{L}(\mathbf{A}) = L$. Let $\mathbf{F}_A(\overline{x})$ be the free algebra freely generated by $\overline{x}$ in the variety $V(\langle A, F\rangle)$. Let $\alpha : \mathbf{T}(x) \to \mathbf{F}_A(\overline{x})$ be the natural homomorphism defined by $\alpha(x) = \overline{x}$, and let $\beta : \mathbf{F}_A(\overline{x}) \to \langle A, F\rangle$ be the homomorphism defined by $\beta(\overline{x}) = a_0$. Then, with $L(x) = \{w(x) : w \in L\}$,

$$L(x) = \alpha^{-1}(\beta^{-1}(A_0)) = \bigcup_{p \in \beta^{-1}(A_0)} p/\ker\alpha.$$

  Hence, $L(x) = L(x)^{\ker\alpha}$. But $\ker\alpha$ is a fully invariant congruence on $\mathbf{T}(x)$. Thus, $\ker\alpha = \theta(x)$, for some $\theta \in \mathrm{Con}\langle \mathscr{F}^*, \cdot, 1\rangle$. Hence, $L(x) = L(x)^{\theta(x)}$ and $L = L^\theta$. We know $\ker\alpha$ is of finite index. Thus, θ is also of finite index.

Myhill's Theorem

Theorem (Myhill)

Let L be a language of type $\mathscr{F}$. Then L is the language of some f.s.a. iff there is a $\theta \in \mathrm{Con}\langle\mathscr{F}^*,\cdot,1\rangle$ of finite index such that $L^\theta = L$.

($\Rightarrow$) This was proved by the preceding lemma.

($\Leftarrow$) Suppose θ is a congruence of finite index on $\mathscr{F}^*$, such that $L^\theta = L$. Let

$$\begin{array}{ll} A = \{w/\theta : w \in \mathscr{F}^*\}, & f(w/\theta) = fw/\theta, \text{ for } f \in \mathscr{F}, \\ a_0 = 1/\theta, & A_0 = \{w/\theta : w \in L\}. \end{array}$$

We have

$$\begin{array}{lll} \langle A, F, a_0, A_0\rangle \text{ accepts } w & \text{iff} & w(1/\theta) \in A_0 \\ & \text{iff} & w/\theta \in A_0 \\ & \text{iff} & w/\theta = u/\theta \text{ for some } u \in L \\ & \text{iff} & w \in L. \end{array}$$

Equivalence of Words Modulo a Language

Definition

Given a language L of type $\mathscr{F}$, define the binary relation $\equiv_L$ on $\mathscr{F}^*$ by

$$w_1 \equiv_L w_2 \quad \text{iff} \quad (uw_1v \in L \Leftrightarrow uw_2v \in L, \text{ for } u, v \in \mathscr{F}^*).$$

Lemma

If we are given L, a language of type $\mathscr{F}$, then $\equiv_L$ is the largest congruence θ on $\langle \mathscr{F}^*, \cdot, 1\rangle$, such that $L^\theta = L$.

- $\equiv_L$ is an equivalence relation on $\mathscr{F}^*$. If $w_1 \equiv_L w_2$ and $t_1 \equiv_L t_2$, then for $u, v \in \mathscr{F}^*$, $uw_1t_1v \in L$ iff $uw_1t_2v \in L$ iff $uw_2t_2v \in L$. Hence, $w_1t_1 \equiv_L w_2t_2$ and $\equiv_L$ is a congruence on $\langle \mathscr{F}^*, \cdot, 1\rangle$.
  Suppose $w \in L$ and $w \equiv_L t$. Then $1 \cdot w \cdot 1 \in L \Leftrightarrow 1 \cdot t \cdot 1 \in L$ implies $t \in L$. Hence, $w/\equiv_L \subseteq L$. Thus, $L^{\equiv_L} = L$.
  Finally, suppose $L^\theta = L$. Then, for $\langle w_1, w_2\rangle \in \theta$ and $u, v \in \mathscr{F}^*$, $\langle uw_1v, uw_2v\rangle \in \theta$, whence, since $uw_1v/\theta = uw_2v/\theta$, we obtain $uw_1v \in L \Leftrightarrow uw_2v \in L$. So $w_1 \equiv_L w_2$. Hence, $\theta \subseteq \equiv_L$.

The Syntactic Monoid and Regular Languages

Definition

If we are given a language L of type $\mathscr{F}$, then the **syntactic monoid M_L of L** is defined by

$$M_L = \langle \mathscr{F}^*, \cdot, 1 \rangle / \equiv_L.$$

Theorem

A language L is accepted by some f.s.a. iff M_L is finite.

- Lis accepted by some f.s.a. iff, by Myhill's Theorem, there exists $\theta \in \mathrm{Con}\langle \mathscr{F}^*, \cdot, 1 \rangle$ of finite index, such that $L^\theta = L$, iff, by the preceding lemma, $L^{\equiv_L}$ has finite index iff $M_L = \langle \mathscr{F}^*, \cdot, 1 \rangle / \equiv_L$ is finite.