The University of Warwick

THEORY OF COMPUTATION

REPORT NO. 61

REPLACEABILITY AND COMPUTATIONAL EQUIVALENCE IN FINITE DISTRIBUTIVE LATTICES

by

Meurig Beynon

REVISED NOVEMBER 1984

Department of Computer Science
University of Warwick
Coventry CV4 7DT
England

March 1984

Replaceability and computational equivalence in finite distributive lattices.

Meurig Beynon.

Dept. of Computer Science, University of Warwick.

ABSTRACT

Notions of replaceability and computational equivalence are defined in an abstract algebraic setting, and investigated in detail for finite distributive lattices. It is shown that when computing an element f of a finite distributive lattice D, the elements of D partition into classes of computationally equivalent elements, and define a quotient of D in which all intervals of the form $[t\wedge f, t\vee f]$ are boolean. This quotient is an abstract simplicial complex with respect to ordering by replaceability. Other results include generalisations and extensions of known theorems concerning replacement rules for monotone boolean networks.

Introduction.

The notion of replaceability has proved to be a useful concept in the study of monotone boolean function complexity. Research in this area has been concerned with the formulation of general replacement rules (e.g.[P] and [MG]), the use of replacement techniques in proving bounds on network size (e.g.[P], [MG], [D1] and [W]), and more recently, the investigation of closed forms for particular kinds of replacement ([D2]).

If f, g and h are monotone boolean functions, a replacement rule has the form " when computing f, replacement of g by h is universally valid ". From the algebraic perspective of this paper, f, g and h are viewed as elements of a free distributive lattice L; such a rule may then be reformulated " an expression for f in terms of g and a set of generators of L, still represents f if g is replaced by h ". In this way, replaceability modulo f defines a relation on the algebra L. It will be shown that this relation is well-defined not only when a general distributive lattice is substituted for L, but when L is a general algebra. Indeed, under very general hypotheses, replaceability modulo an element f defines a pre-order (a reflexive and transitive relation $\sqsubset_f$) on an algebra L, and the equivalence relation $\square_f$ derived by imposing anti-symmetry is an algebraic congruence called " computational equivalence modulo f ". The quotient algebra $L/\square_f$ is then ordered by $\sqsubset_f$.

Replaceability and computational equivalence in finite distributive lattices are the main subjects of this paper. Results include generalisations and extensions of known theorems concerning replacement rules for monotone boolean networks. Most of the proofs use lattice-theoretic arguments based upon finiteness and distributivity, and do not require the assumption of freeness.

The paper is divided into seven sections. §0 and §3 deal with generalities concerning computational equivalence and replaceability respectively. §'s 1 and 2 examine computational equivalence in the context of finite distributive lattices, and in particular describe how the quotient $L/\square_f$ can be determined up to isomorphism from the prime implicants and prime clauses of f (Theorem 1.2) when L is free. In a finite distributive lattice D, the element $\lambda(f)$ (resp $\mu(f)$), which is the largest (resp. smallest) element computationally equivalent to 0 (resp. 1) modulo f is significant, and $\square_f$ is the congruence defined on D by the relations $\lambda(f) = 0$, $\mu(f) = 1$ (Theorem 2.2). The element $\mu(f)$ is characterised as the largest element in D such that $[f , \mu(f)]$ is boolean, and dually (Cor.2.3).

§4 examines replaceability in finite distributive lattices, and includes new proofs and extensions of a recent result due to Dunne [D2], which in particular gives closed forms for z(f) (resp. u(f)), the largest (resp. smallest) element replaceable by 0 (resp. 1) when computing f in the free distributive lattice L (c.f. Cor.4.2). In conjunction, Theorems 1.2 and 4.1 show that in computing a monotone boolean function f, the computational role which a monotone boolean function g can play is completely determined by its relation to the prime implicants and prime clauses of f. Cor.4.5 characterises the set of computational equivalence classes, ordered by replaceability, as an abstract simplicial complex; an intriguing fact, in view of the categorical dualities

explored in [B1], [B2] and [B3], which indicate that abstract simplicial complexes can be viewed as geometric duals of finite distributive lattices.

There are many properties interrelating the elements $\mu(f)$, $\lambda(f)$, $u(f)$ and $z(f)$ which are sketched in §5. On any finite distributive lattice, the functions $z()$ and $u()$ define inverse bijections, which (as suggested by Dunne) may be helpful in classifying monotone boolean functions. The properties of the operators μ, λ, u and z are connected with computational equivalence relations (c.f. Theorem 2.2 and Lemma 5.1), and may be related to monotone boolean function complexity (c.f. Theorem 6.1, Cor.6.2).

The final section of the paper deals specifically with computation of monotone boolean functions. It includes a proof of a recent theorem of Dunne [D2], showing that when computing f using a monotone network in which the inputs are $x_1, x_2, \ldots, x_n$ and their negations, a negated input x' can be replaced by any monotone function h in the interval $[f|^{x=0}, f|^{x=1}]$. In this context, a "pseudo-complement" such as h can replace x' but cannot be computationally equivalent to x'. Theorem 6.1 and Cor.6.2 show in particular that if h can be chosen to lie in the interval $[\lambda(f)|^{x=0}, \mu(f)|^{x=1}]$, then h and x' are mutually replaceable in a restricted sense.

§0. Computational equivalence.

Suppose that A is an Ω-algebra, and that $F \subseteq A$. An equivalence relation $\sqsupset_F$ associated with F is defined by $g \sqsupset_F h$ if for all f in F:

" given an Ω-word w, and elements $a_1, a_2, \ldots, a_n$ in A:

$w(g, a_1, a_2, \ldots, a_n) = f$ iff $w(h, a_1, a_2, \ldots, a_n) = f$ ".

That is, for each f in F, an Ω-formula over A which represents f in terms of g still represents f when g is replaced by h, and vice versa. In effect, g and h are "computationally equivalent" for the purpose of computing the set of elements F using operations in Ω over A.

Note that an equivalent definition of $\sqsupset_F$ is obtained if the elements $a_1, a_2, \ldots, a_n$ are constrained to lie in a particular generating set for A. For this reason, it will be convenient in the sequel to suppose that $a_1, a_2, \ldots, a_n$ is a generating set for A, and let **a** denote $a_1, a_2, \ldots, a_n$. Intuitively, $\sqsupset_F$ defines computational equivalence modulo F "relative to an input set which generates A". If $F=\{f\}$, it will be convenient to write $\sqsupset_f$ for $\sqsupset_F$.

Lemma 0.1.

If $f \in F \subseteq A$, then $\sqsupset_f$ is an Ω-congruence on A, and $\sqsupset_F = \bigcap \{ \sqsupset_f \mid f \in F \}$.

Proof:

Suppose that $g \sqsupset_f h$, and that v is an Ω-word. Then

$$v(g, \mathbf{a}) \sqsupset_f v(h, \mathbf{a}) .$$

To see this, let w be an Ω-word, and let W be the Ω-word:

$$W(e,e_1,e_2,\ldots,e_n) \equiv w(v(e,e_1,e_2,\ldots,e_n),e_1,e_2,\ldots,e_n).$$

Then

$$w(v(g,\mathbf{a}),\mathbf{a}) = f \text{ iff } W(g,\mathbf{a}) = f$$
$$\text{iff } W(h,\mathbf{a}) = f \text{ since } g \,\square_f\, h$$
$$\text{iff } w(v(h,\mathbf{a}),\mathbf{a}) = f.$$

Thus if $\omega \in \Omega$ has arity k, and $g_i \,\square_f\, h_i$ for $1 \le i \le k$, an easy induction proves that

$$\omega(g_1, g_2, \ldots, g_k) \,\square_f\, \omega(h_1, h_2, \ldots, h_k) .$$

■

If α is an equivalence relation on a set S, and the equivalence class of s contains a single element, s will be called *solitary under* α, or simply *solitary* where the equivalence relation is clear from the context.

Lemma 0.2.

$\square_F$ is the unique maximal Ω-congruence on A such that each f in F is solitary.

Proof:

Define the Ω-word $w(e,e_1,e_2,\ldots,e_n) \equiv e$. Then $w(g,\mathbf{a}) = f$ only if g=f, and $\square_F$ has the stated property.

Let ϑ be an Ω-congruence on A such that f is solitary. By Lemma 0.1, it will suffice to show that $\square_f$ contains ϑ.

Suppose that $(g,h) \in \vartheta$. Given an Ω-word w:

$$w(g,\mathbf{a}) = f \text{ iff } (w(g,\mathbf{a}) , f) \in \vartheta$$
$$\text{iff } (w(h,\mathbf{a}) , f) \in \vartheta \text{ since } (g,h) \in \vartheta$$
$$\text{iff } w(h,\mathbf{a}) = f,$$

showing that $g \,\square_f\, h$.

■

Lemma 0.2 shows that computational equivalence is a trivial relation in the context of many choices of Ω. For instance, if A is a group or ring, a congruence class will be a coset of a subgroup containing 2 or more elements in a non-trivial case. In particular, if A is a Boolean algebra (where $\Omega = \{\wedge,\vee,'\}$), then $\square_f$ is trivial.

§1. Computational equivalence in distributive lattices.

A distributive lattice is defined by taking $\Omega = \{\wedge,\vee\}$, where $\wedge$ and $\vee$ are associative, commutative, and idempotent binary operators, and $\wedge$ distributes over $\vee$ (and vice versa). In this context, Ω-words are frequently described as "monotone boolean functions". The family of monotone boolean functions in literals $x_1,x_2,\ldots,x_n$, ordered by "implication", form the free distributive lattice on n generators, which will be denoted by FDL(n).

Distributive lattices form a class of algebras in which non-trivial computational equivalences can arise. As a simple example, let A=FDL(3), the distributive lattice freely generated by $\{x_1, x_2, x_3\}$ (see Fig.4), and let $f = x_1 \vee (x_2 \wedge x_3)$. If $t = x_1 \wedge (x_2 \vee x_3)$, then the $\{\wedge,\vee\}$-congruence defined by $g \equiv h$ iff $g \vee t = h \vee t$ is non-trivial, and is easily identified as $\Box_f$ using Lemma 0.2. It is important to observe that computational equivalence is not necessarily preserved when a quotient is taken; this in particular justifies consideration of general rather than simply free distributive lattices. As an illustration, let A and f be as in the example above. Then

$$x_2 \wedge x_3 \Box_f T_2^3 = (x_1 \wedge x_2) \vee (x_3 \wedge (x_1 \vee x_2)),$$

but there are quotients of A in which f is identified with T_2^3 but not with $x_2 \wedge x_3$.

The aim of this section is to show how computational equivalence relations on distributive lattices may be described and computed, and to explain how the isomorphism type of the resulting quotient may be determined. For instance, it will be shown that in a free distributive lattice, computational equivalence modulo a single element leads to a projective lattice which is 1-dimensional, in that the longest chain of meet-irreducible elements has length 2. Some preliminary results on finite distributive lattices are required, as summarised below. For details, see [G] or [B].

An element z in a lattice L is *meet-irreducible* if z is not the largest element of L, and z cannot be expressed as $a \wedge b$ where a and b are in $L \setminus \{z\}$. Dually, z is *join-irreducible* if z is not the smallest element of L, and cannot be expressed as $a \vee b$ where a and b are in $L \setminus \{z\}$.

Let D be a finite distributive lattice, and let **2** denote the lattice $\{0,1\}$, where $0 \leq 1$. In D, every element has a unique representation as a join of incomparable join-irreducibles and dually. If p is a join-irreducible of D, the map $\pi : D \to \mathbf{2}$ such that

$$\pi(z) = 1 \text{ iff } z \geq p$$

is a lattice homomorphism mapping D onto **2**, and all lattice homomorphisms mapping D onto **2** are of this type. By duality, the complement of $p\uparrow \equiv \{z \mid z \geq p\}$ has the form

$$\tilde{p}\downarrow \equiv \{z \mid z \leq \tilde{p}\},$$

where $\tilde{p}$ is a meet-irreducible. There is a 1-1 correspondence $p \leftrightarrow \tilde{p}$ between meet-irreducibles and join-irreducibles in D; via this correspondence, the subsets of meet-irreducibles and join-irreducibles are canonically isomorphic as posets under the ordering of D. If Q is the poset of meet-irreducibles of D, then D and the lattice $\mathbf{2}^Q$ comprising decreasing subsets of D (i.e. subsets which contain with d all elements $\leq$ d), ordered by inclusion, are canonically isomorphic. In particular, D is determined up to isomorphism by the poset Q. When the ordering on Q is trivial, D is complemented and will be referred to as a boolean lattice. Note that this term is used to refer to D as a $\{\wedge,\vee\}$-algebra, rather than a Boolean algebra.

Meet- and join-irreducibles are prominent throughout this paper, and some special notation is helpful. If X is a subset of the meet-irreducibles of D, and $g \in D$, then X[g] will be used to denote

$$\{q \mid q \in X \text{ and } q \geq g\},$$

and $\widetilde{X}$ the set of join-irreducibles of the form $\widetilde{q}$ where $q \in X$. Dually, if Y is a subset of the join-irreducibles of D, then Y[g] will be used to denote

$$\{p \mid p \in Y \text{ and } p \leq g\},$$

and $\widetilde{Y}$ the set of meet-irreducibles of the form $\widetilde{p}$ where $p \in Y$.

If $S \subseteq D$ the join of all elements in S will be denoted by $\bigvee S$, and dually.

For convenience, the term "congruence" will be used as a synonym for Ω-congruence, where $\Omega = \{\wedge, \vee\}$. If α is a lattice homomorphism, the *kernel* of α (denoted by Ker α), is the congruence defined by

$$(a,b) \in \text{Ker } \alpha \text{ iff } \alpha(a)=\alpha(b).$$

Congruences on finite distributive lattices are characterised by the following lemma:

Lemma 1.1.

Let D be a finite distributive lattice, and let Q be the poset of meet-irreducibles of D.

If $X \subseteq Q$, the equivalence relation defined by $g \equiv_X h$ if $X[g] = X[h]$ is a congruence on D, and

$$D / \equiv_X \cong 2^X.$$

where X is regarded as a partially ordered subset of D.

The correspondence $X \leftrightarrow \equiv_X$ defines an anti-isomorphism between the boolean lattice of subsets of Q, and the congruence lattice of D.

Proof:

Let σ be the map from D to 2^X which maps f in D to $\{ q \in X \mid q \not\geq f \}$. Given f_1 and f_2 in D, and q in X:

$$q \not\geq f_1 \vee f_2 \text{ iff } q \not\geq f_1 \text{ or } q \not\geq f_2,$$

and since q is meet-irreducible:

$$q \not\geq f_1 \wedge f_2 \text{ iff } q \not\geq f_1 \text{ and } q \not\geq f_2.$$

Thus σ is a lattice homomorphism, and Ker σ is $\equiv_X$. Moreover σ is onto: if S is a decreasing subset of X, then

$$\sigma(\bigwedge \{ q \notin S \}) = S.$$

Suppose that X and Y are subsets of Q. If $X \subseteq Y$ then $\equiv_Y \subseteq \equiv_X$. Moreover, if $z \in X \setminus Y$, and $y = \bigwedge Y[z]$, then $(y,z) \in \equiv_Y \setminus \equiv_X$. It follows that X=Y iff $\equiv_X = \equiv_Y$, and that $X \parallel Y$ iff $\equiv_X \parallel \equiv_Y$, so that the correspondence $X \leftrightarrow \equiv_X$ is an anti-isomorphism.

∎

Let D be a finite distributive lattice, and F a subset of D. In view of Lemma 0.1 and Lemma 1.1, a characterisation of $\Box_F$ can be obtained simply by identifying, for each f in F, the subset X(f) of meet-irreducibles such that $\Box_f = \equiv_{X(f)}$.

Theorem 1.2.

Let D and f be as above, and define:

P_f = set of maximal elements amongst join-irreducibles $\leq f$,

Q_f = set of minimal elements amongst meet-irreducibles $\geq f$.

Then $\square_f$ is the congruence $\equiv_X$ where $X = Q_f \cup \tilde{P}_f$.

Proof:

It suffices to show that $\equiv_X$ has the characteristic property of $\square_f$ stated in Lemma 0.2.

By definition, all elements of Q_f are $\geq f$, and all elements of P_f are $\leq f$. If $p \in P_f$, then $f \geq p$ iff $f \not\leq \tilde{p}$, so that $\{ q \in X \mid q \geq f \}$ characterises f uniquely. Thus f is solitary under $\equiv_X$.

Now suppose that g and h are inequivalent modulo $\equiv_X$. There is a meet-irreducible q in X such that $g \not\leq q$ and $h \leq q$. Suppose that $q = \tilde{p}$, where $p \in P_f$. Let u be the join of all elements in P_f except p, and (in the notation of Lemma 1) define $w(z,\mathbf{a}) \equiv u \vee (z \wedge p)$. Then $w(g,\mathbf{a}) = u \vee p = f$, whilst $w(h,\mathbf{a}) < f$, so that g and h are inequivalent modulo $\square_f$. A similar argument applies if $q \in Q_f$.

∎

Note that when D=FDL(n), the sets P_f and Q_f defined in Theorem 1.2 are the "prime implicants" and the "dual prime implicants" (or "prime clauses") of f respectively. In particular, if $f \in FDL[k] \subseteq FDL[n]$, then g and h in FDL[k] are computationally equivalent modulo f relative to FDL[k] iff they are computationally equivalent modulo f relative to FDL[n]. In general, if $f \in D \in K$, where D and K are finite distributive lattices, computational equivalence of elements of D modulo f relative to D and relative to K differ, since embedding D into K may alter the set of meet-irreducibles. For example, if K is the boolean closure of D, then $\square_f$ is trivial relative to K (c.f. Lemma 2.1).

Cor.1.3.

Let D be as in Theorem 1.2, and let F be a subset of D. In the notation of the Theorem, let $P = \bigcup \{ P_f \mid f \in F \}$, and $Q = \bigcup \{ Q_f \mid f \in F \}$.

If z is an element of D, then the congruence class of z modulo $\square_F$ is the interval $[z_0 , z_1]$, where

$$z_0 = \bigvee P[z] \vee \bigvee \tilde{Q}[z] \text{ and } z_1 = \bigwedge Q[z] \wedge \bigwedge \tilde{P}[z].$$

Proof:

An element y in the same class as z must be $\geq p$ for p in P[z], and $\not\leq q$ for q in Q\Q[z]. Thus $y \geq z_0$, since $y \not\leq q$ iff $y \geq \tilde{q}$. Similarly, $y \leq z_1$.

To complete the proof, it suffices to show that z and z_0 are in the same congruence class, or equivalently that

$$P[z] = P[z_0] \text{ and } Q[z] = Q[z_0].$$

(The proof that z and z_1 are in the same class uses a dual argument.)

Clearly, $z_0 \geq p$ for p in P[z], and since $y \geq \tilde{q}$ iff $y \not\leq q$, $z_0 \not\leq q$ for q in Q\Q[z]. If $p \in P \backslash P[z]$, then $p \not\leq z_0$, since $z_0 \leq z$. Finally, if $q \in Q[z]$, then $z_0 \leq z \leq q$.

∎

Suppose that F is a subset of the finite distributive lattice D. A problem similar to that of "computing all the elements of F" is that of "computing an element of F, irrespective of which". Computational equivalence in the context of such a problem is meaningful provided that F can be a congruence class for D i.e. provided that F is an interval $[f_0,f_1]$. The appropriate quotient of D is then obtained by identifying f_0 and f_1 in D and taking computational equivalence relative to the class of f_0 and f_1, and coincides with the quotient obtained by identifying f_0 and f_1 in $D/\Box_f$. If Q is the set of meet-irreducibles of D, this quotient is associated with the subset of

$$\cap\{\, Q[f] \mid f \in F \,\} \cup \cap\{\, Q \backslash Q[f] \mid f \in F \,\}$$

consisting of elements which are either minimal subject to $q \geq f$ or maximal subject to $q \not\geq f$ for some f in F viz. the set

$$Q_{f_1} \cup \tilde{P}_{f_0}.$$

§2. Computational equivalence with respect to one element.

Throughout this section, D will denote a finite distributive lattice, and f an element of D. A study of $\Box_f$ is of special interest in view of Lemma 0.1, and there are a number of simplifications in this case. In particular, there is a simple criterion for $\Box_f$ to be trivial, and the quotient $D/\Box_f$ is always a retract of D, whence projective if D is free.

The next results are further corollaries to Theorem 1.2:

Cor. 1.4.

Let D, f and X be as in Theorem 1.2.

The meet-irreducibles of $D/\Box_f$ form a poset isomorphic with X regarded as a poset of D, and the only possible order relations between elements of X are of the form $q \geq \tilde{p}$, where $p \in P_f$, $q \in Q_f$. In particular, the poset X is 1-dimensional i.e. the longest chain in X has length at most 2.

Proof:

In view of Lemma 1.1, it suffices to observe that if $q \in Q_f$ and $p \in P_f$, then $q \geq f \geq p$, whence $\tilde{p} \not\geq q$.

∎

Lemma 1.1, Theorem 1.2 and Cor. 1.4 are expressed in terms of meet-irreducibles, but may of course be dualised to join-irreducibles. The duality is based upon the fact that $q \leftrightarrow \tilde{q}$ defines an isomorphism between the posets of meet-irreducibles and join-irreducibles, and that $z \not\leq q$ iff $z \geq \tilde{q}$. This is illustrated in the next proof.

Cor.1.5.

If t is an element of $D/\Box_f$, then $[t\wedge f, t\vee f]$ is a boolean lattice.

Proof:

The lattice $D/\Box_f$ is canonically isomorphic with the lattice of decreasing subsets of its poset of join-irreducibles viz. $P_f \cup \tilde{Q}_f$. Under this isomorphism, the element t is associated with

$$P_f[t] \cup \tilde{Q}_f[t],$$

the set of join-irreducibles which it contains.

If $p \in P_f \backslash P_f[t]$, then $P_f[t\vee p] = P_f[t] \cup \{p\}$, whilst $\tilde{Q}_f[t] = \tilde{Q}_f[t\vee p]$. Similarly, if $q \in \tilde{Q}_f[t]$, then $P_f[t\wedge q] = P_f[t]$, whilst $\tilde{Q}_f[t\wedge q] = \tilde{Q}_f[t] \backslash \{\tilde{q}\}$.

An easy induction then shows that the interval $[t\wedge f, t\vee f]$ in $D/\Box_f$ is associated with the family of decreasing subsets of the form $X \cup Y$, where $P_f[t] \subseteq X \subseteq P_f$ and $Y \subseteq \tilde{Q}_f[t]$. It is thus a boolean lattice with $|P_f \backslash P_f[t]| + |\tilde{Q}_f[t]|$ atoms.

∎

Lemma 2.1.

The congruence $\Box_f$ on D is trivial iff both $f\uparrow$ and $f\downarrow$ are boolean.

Proof:

In view of Cor.1.5, it is enough to show that $\Box_f$ is trivial if both $f\uparrow$ and $f\downarrow$ are boolean. Suppose that (g,h) is a pair of distinct elements in D which are equivalent modulo $\Box_f$. Then one of the pairs $(f\wedge g, f\wedge h)$ and $(f\vee g, f\vee h)$ must also be distinct and equivalent modulo $\Box_f$. Thus if $\Box_f$ is non-trivial, it defines a non-trivial congruence on one of the boolean lattices $f\uparrow$ and $f\downarrow$. By Lemma 0.2, it is then enough to observe that in a boolean lattice every $(\wedge, \vee)$-congruence respects complements.

∎

If g is an element of D, there are sets P_g and Q_g associated with g as in Theorem 1.2. A map $\lambda : D \to D$ is defined by

$$\lambda(g) \equiv \bigvee \{p \wedge \tilde{p} \mid p \in P_g\}.$$

Dually, a map $\mu : D \to D$ is defined by

$$\mu(g) \equiv \bigwedge \{q \vee \tilde{q} \mid q \in Q_g\}.$$

Note that g lies in the interval $[\lambda(g), \mu(g)]$; in some sense, $\lambda(g)$ is the largest element $\leq g$ which contributes trivially towards a computation of g, and dually (c.f. §5).

Theorem 2.2.

Let D and f be as above, and define $e_f : D \to D$ by $e_f(z) \equiv (z \vee \lambda(f)) \wedge \mu(f)$.

The map e_f is a retract of D onto the interval $[\lambda(f), \mu(f)]$. The kernel of e_f is $\Box_f$, whence the image is isomorphic to $D/\Box_f$.

In particular, $\square_f$ is the quotient of D defined by the relations

$$\lambda(f) = 0 \, , \, \mu(f) = 1.$$

Proof:

That e_f is a retract onto $[\lambda(f),\mu(f)]$ is trivial.

To show that Ker $e_f \subseteq \square_f$ it is enough (by duality) to prove for z in D that $(z, z\vee\lambda(f)) \in \square_f$.

Given p in P_f, it follows from join-irreducibility that

$$\lambda(f) = \bigvee\{s\wedge\tilde{s} \mid s \in P_f\} \not\geq p,$$

so that $z\vee\lambda(f) \geq p$ iff $z \geq p$. Moreover, given q in Q_f:

$$q \geq f \geq \lambda(f), \text{ so that } q \geq z\vee\lambda(f) \text{ iff } q \geq z.$$

Thus $(z, z\vee\lambda(f)) \in \square_f$ by Theorem 1.2.

To complete the proof, it suffices to show that the interval $[f,\mu(f)]$ is boolean; by Lemma 2.1, and duality, there can then be no non-trivial congruence on $[\lambda(f),\mu(f)]$ in which f is solitary, proving that Ker $e_f = \square_f$.

Suppose that $X \subseteq Q_f$; then

$$f\vee\bigvee\tilde{X} = \bigwedge Q_f\vee\bigvee\tilde{X} = \bigwedge\{\, q\vee\bigvee\tilde{X} \mid q \in Q_f \,\}.$$

If q and t are distinct meet-irreducibles, then $q\vee\tilde{t} = q$, whence

$$f\vee\bigvee\tilde{X} = \bigwedge\mu(X)\wedge\bigwedge(Q_f\backslash X) = \mu(f)\wedge\bigwedge(Qf\backslash X)$$

Let $f\leq y\leq\mu(f)$ and $X=Q_f\backslash Q_f[y]$. It is evident that

$$f\vee\bigvee\tilde{X} \leq y \leq \bigwedge(Q_f\backslash X)\wedge\bigwedge\mu(X),$$

whence y has a canonical representation of the form

$$\bigwedge(Q_f[y])\wedge\bigwedge\mu(Q_f\backslash Q_f[y]).$$

It is then easy to deduce that $[f,\mu(f)]$ is boolean.

∎

Cor.2.3.

$\mu(f)$ is the largest element of D for which $[f,\mu(f)]$ is boolean, and dually.

Proof:

Suppose that $c\geq f$ in D, and that [f,c] is boolean. Then

$$f\leq c\wedge\mu(f)\leq c \text{ and } c\wedge\mu(f)\ \square_f\ c.$$

But since f is solitary under $\square_f$, the congruence $\square_f$ must be trivial on the boolean lattice [f,c], whence $c\leq\mu(f)$.

∎

A distributive lattice L is *projective* if, given distributive lattices A and B, and lattice homomorphisms

$$\alpha{:}A\to L \text{ and } \beta{:}B\to L$$

such that α is onto, there is a map $\rho{:}B\to A$ such that $\alpha\rho=\beta$. It is well-known (see [G] p.144) that a finite distributive lattice is projective iff it is a retract of FDL(n) for some n iff the join of any pair of meet-irreducible elements is either a meet-irreducible or the greatest element.

Theorem 2.2 shows directly that if $f \in FDL(n)$ then $FDL(n)/\sqsupset_f$ is projective. It follows that lattices of the form $FDL(n)/\sqsupset_f$ are a proper subclass of finite distributive lattices with a 1-dimensional poset of meet-irreducibles; for instance, the lattice $E=2^X$, where

$$X = \{a,b,c,d\} \text{ subject to } a \geq c,\ b \geq c,\ a \geq d,\ b \geq d$$

is not projective. It can also be seen that Theorem 2.2 does not generalise to $|F|>1$; if $D=FDL(6)$, and $F = \{\ x_1 \vee (x_2 \wedge x_3)\ ,\ x_4 \vee (x_5 \wedge x_6)\ \}$, then $FDL(6)/\sqsupset_f$ is isomorphic to $E \times E$, which is not projective, and cannot be a retract of FDL(6).

§3. Computational equivalence and replaceability.

Computational equivalence is closely related to a more traditional concept of "computational strength" which is usually expressed in terms of *replacement rules*. For monotone boolean functions, a complete description of all functional replacements which are valid when computing a fixed function f are described in [D2]. In this section, the preorder (i.e. reflexive, transitive) relation defined by " g is replaceable by h when computing f " is considered abstractly, and the results of [D2] are proved in greater generality.

Suppose that A is an Ω-algebra, and that $F \subseteq A$. A preorder relation $\sqsubset_F$ associated with F is defined by $h \sqsubset_F g$ (also written $g \sqsupset_F h$) if for all f in F:

" given an Ω-word w, and elements $a_1, a_2, \ldots, a_n$ in A:

if $w(g,a_1,a_2,\ldots,a_n) = f$ then $w(h,a_1,a_2,\ldots,a_n) = f$ ".

That is, for each f in F, an Ω-formula over A which represents f in terms of g still represents f when g is replaced by h.

It is clear that g and h are computationally equivalent modulo F iff

$$g \sqsupset_F h \text{ and } h \sqsupset_F g;$$

in particular, the relation $\sqsupset_F$ defines a partial order on the computational equivalence classes of $\sqsupset_F$.

As in the case of $\sqsupset_F$, an equivalent definition of $\sqsupset_F$ is obtained if the elements $a_1, a_2, \ldots, a_n$ are constrained to lie in a particular generating set for A, so that the conventions of §0 can be used. If $F=\{f\}$, it will be convenient to write $\sqsupset_f$ for $\sqsupset_F$.

The following lemmas are analogues of Lemmas 0.1 and 0.2:

Lemma 3.1.

If $f \in F \subseteq A$, then $\sqsupset_f$ respects the operations in Ω on A:

if $\omega \in \Omega$ has arity k, and $g_i \sqsubset_f h_i$ for $1 \leq i \leq k$, then

$$\omega(g_1, g_2, \ldots, g_k) \sqsubset_f \omega(h_1, h_2, \ldots, h_k),$$

and $\sqsubset_F = \bigcap \{\ \sqsubset_f \mid f \in F\ \}$.

Proof:

The proof is very similar to the proof of Lemma 0.1, and is left to the reader.

∎

Lemma 3.2.

$\sqsubset_F$ is the unique maximal preorder relation on A respecting the operations in Ω such that all elements in F are minimal (i.e: if $f \in F$ and $g \sqsubset_F f$, then g=f.)

Proof:

Define the Ω-word $w(e,e_1,e_2,\ldots,e_n) \equiv e$. Then $w(g,\mathbf{a}) = f$ only if g=f, and $\sqsubset_F$ has the stated property.

Let $\leqslant$ be a preorder on A with the stated properties. By Lemma 1, it will suffice to show that $\sqsubset_f$ contains $\leqslant$.

Suppose that $g \leqslant h$. Then $w(h,\mathbf{a}) = f$ iff $w(h,\mathbf{a}) \leqslant f$. But $w(g,\mathbf{a}) \leqslant w(h,\mathbf{a})$, since $g \leqslant h$ and $\leqslant$ respects Ω. Thus $w(h,\mathbf{a}) = f$ entails $w(g,\mathbf{a}) \leqslant w(h,\mathbf{a}) \leqslant f$, which proves that $w(g,\mathbf{a}) = f$.

∎

In many types of algebra, computational equivalence is a trivial notion, but the preorder by replaceability may still be of interest. For instance, in a boolean lattice B, it is easy to verify by Lemma 3.2 (c.f. Cor.4.4) that:

$$\text{given } f,g,h \in B\text{: } g \sqsubset_f h \text{ iff } g+f \leq h+f,$$

where '+' denotes boolean addition. Thus $\sqsubset_f$ is an order relation in this case, and $(B, \sqsubset_f)$ is a boolean lattice isomorphic to $(B,\leq)$. Replaceability as a relation on finite distributive lattices is considered below. The main result (Theorem 4.1) is based on [D2], but appears here in a more general context.

§4. Replaceability in distributive lattices.

Let D be a finite distributive lattice, and let $f \in D$. (Only replacement with respect to computing a single element is considered below, but the generalisation to a subset F is easy.) The sets P_f and Q_f are defined as in Theorem 1.2.

The following theorem generalises [D2] Theorems 2 and 3, which prove the result for D=FDL(n). It may be used to give an alternative proof of Cor.1.3.

Theorem 4.1. $g \sqsubset_f h$ iff $g \in [\bigvee P_f[h], \bigwedge Q_f[h]]$ iff $h \in [\bigvee \tilde{Q}_f[g], \bigwedge \tilde{P}_f[g]]$

Proof:

By Lemma 3.1, $\{\, g \mid g \sqsubset_f h \,\}$ is closed under $\wedge$ and $\vee$, and is necessarily an interval in D.

By duality, it suffices to show that $s = \bigvee P_f[h]$ is the least element of D such that $s \sqsubset_f h$.

Suppose then that $g \sqsubset_f h$. Certainly $f \geq h \wedge f \geq s$, so that

$$(h \wedge f) \vee \bigvee P_f \setminus P_f[h] = f,$$

and hence $(g\wedge f)\vee \bigvee P_f\backslash P_f[h] = f$. If now $p \in P_f[h]$, then $p\leq f$ but $p\not\leq \bigvee P_f\backslash P_f[h]$, whence $p\leq g\wedge f\leq g$ since p is join-irreducible. This proves that $g\geq s$.

Suppose that $w(h,\mathbf{a}) = f$. Then

$$f \leq w(s\vee h,\mathbf{a}\vee h) = w(s,\mathbf{a})\vee h,$$

and if $p \in P_f\backslash P_f[h]$, then $p\leq w(s,\mathbf{a})$ since p is join-irreducible. Also

$$w(s,\mathbf{a}) = w(s\wedge h,\mathbf{a}) \geq w(h,\mathbf{a})\wedge s = f\wedge s = s,$$

proving that

$$f= w(h,\mathbf{a}) \geq w(s,\mathbf{a}) \geq f.$$

To prove the second equivalence stated in the Theorem, note that

$$g \geq \bigvee P_f[h] \text{ iff } P_f[h] \subseteq P_f[g] \text{ iff } \tilde{P}_f[g] \subseteq \tilde{P}_f[h].$$

But for p in P_f:

$$\tilde{p} \in \tilde{P}_f[g] \text{ iff } p\not\leq g \text{ iff } g\leq\tilde{p},$$

so that $\tilde{P}_f[g] \subseteq \tilde{P}_f[h]$ iff $h\leq\bigwedge\tilde{P}_f[g]$.

A dual argument completes the proof. ∎

Cor.4.2.

If h is in D, then

$0 \sqsubset_f h$ iff $h \in [\ 0\ ,\ z(f)\ ]$, where $z(f) = \bigwedge \tilde{P}_f$,

and $1 \sqsubset_f h$ iff $h \in [\ u(f)\ ,\ 1\ ]$, where $u(f) = \bigvee \tilde{Q}_f$.

(These are generalisations of a replacement rule due to Mehlhorn c.f. [M] and [D2].)

The rest of this section deals with characterising the poset $(D/\Box_f\ ,\sqsubset_f)$. It is a familiar fact that in any computation of a monotone boolean function f, a function g is replaceable by any function between $g\wedge f$ and $g\vee f$. The next corollary to Theorem 4.1 shows that these are the only valid replacements in $D/\Box_f$.

Cor.4.3.

For a in $D/\Box_f$, let B(a) denote the interval $[a\wedge f, a\vee f]$ in $D/\Box_f$.

The map B is a 1-1 map from $D/\Box_f$ to intervals in $D/\Box_f$, and
given a,b in $D/\Box_f$: $a \sqsubset_f b$ iff $a \in B(b)$ iff $B(a) \subseteq B(b)$.

Proof:

In any distributive lattice, the element a is determined by $a\wedge f$ and $a\vee f$, whence B is 1-1.

To see that $a \sqsubset_f b$ iff $a \in B(b)$, it will suffice (by Theorem 4.1, and duality) to show that if h is a representative in D for the class b in $D/\Box_f$, then

$$s = \bigvee P_f[h] \sqsubset_f h\wedge f.$$

This follows from Theorem 1.2, since it is easy to verify that

$$P_f[s] = P_f[h\wedge f] = P_f[h] \text{ and } Q_f[s] = Q_f[h\wedge f] = Q_f.$$

∎

Cor.4.4.

If D is a boolean lattice, and f,g,h $\in$ D, then

$$g \sqsubset_f h \text{ iff } g+f \leq h+f.$$

Thus $(D, \sqsubset_f)$ is a boolean lattice isomorphic with $(D,\leq)$.

Proof:

Since D is boolean, D and $D/\square_f$ are isomorphic, and Cor.4.3 applies. It will suffice to show that

$$f+g \leq f+h \text{ iff } f\vee h \geq f\vee g \text{ and } f\wedge g \geq f\wedge h.$$

If $f\vee h \geq f\vee g$ and $f\wedge g \geq f\wedge h$, then

$$f+g = (f\vee g)\wedge(f\wedge g)' \leq (f\vee h)\wedge(f\wedge h)' = f+h.$$

Conversely, if $f+g \leq f+h$, then

$$f\vee h \geq f+h \geq f+g = (f\wedge g')\vee(f'\wedge g) \geq f'\wedge g.$$

Thus $f\vee h \geq (f'\wedge g)\vee(f\wedge g) = g$, proving that $f\vee h \geq f\vee g$. Since $f+g = f'+g'$, a dual argument shows that $f\wedge g \geq f\wedge h$.

The 1-1 correspondence $g \leftrightarrow f+g$ then defines an isomorphism between $(D,\leq)$ and $(D, \sqsubset_f)$.

∎

Cor.4.4 shows that the relation $\sqsubset_f$ is non-trivial on a boolean lattice B even though $\square_f$ is trivial (c.f. Lemma 2.1). Viewing B as a Boolean algebra, both $\square_f$ and $\sqsubset_f$ are trivial: if $\lessdot$ is an order on B respecting $\{\wedge,\vee,'\}$, and $g \lessdot h$, then

$$1 = g\vee g' \lessdot g\vee h' \lessdot h\vee h' = 1,$$

whence $h'\vee g = 1$; similarly $h'\wedge g = 0$, and $h=g$.

Cor.'s 1.5, 4.3 and 4.4 together show that $(D/\square_f, \sqsubset_f)$ is a decreasing subset of a boolean lattice, or "abstract simplicial complex." The maximal simplices in this complex are associated with elements g in $D/\square_f$ such that $[g\wedge f, g\vee f]$ is maximal amongst intervals of this type.

Since $\sqsubset_f$ respects $\wedge$ and $\vee$, it is easy to verify that if b lies between a and c in $(D/\square_f,\leq)$, and $a \sqsubset_f c$, then b also lies between a and c in $(D/\square_f, \sqsubset_f)$. In particular, there are simplices in the complex $(D/\square_f, \sqsubset_f)$ corresponding directly to the boolean intervals $f\uparrow$ and $f\downarrow$ in $(D/\square_f,\leq)$. It also follows that $\{y \mid y \sqsubset_f z(f)\}$ is a maximal simplex; if $g \geq z(f)$ then $g \sqsupset_f 0$, whence $0 \leq g \leq z(f)$, and $g \sqsubset_f z(f)$.

An alternative characterisation of the complex $(D/\square_f, \sqsubset_f)$ is provided by Cor.4.5.

Cor.4.5.

The simplicial complex $(D/\square_f, \sqsubset_f)$ is isomorphic with the family of trivially ordered subsets of $P_f \cup \tilde{Q}_f$ ordered by inclusion.

Proof:

The lattice $D/\Box_f$ is isomorphic with the family of decreasing subsets of $P_f \cup \tilde{Q}_f$ via the map which associates $P_f[g] \cup \tilde{Q}_f[g]$ with the element g in $D/\Box_f$ (c.f. Cor.1.5). Since the only possible order relations are of the form $\tilde{q} \geq p$, it follows that if X and Y are subsets of P_f and $\tilde{Q}_f$ respectively, then

$X \cup Y$ is trivially ordered iff $(P_f \backslash X) \cup Y$ is decreasing.

Let χ be the map which associates with g in $D/\Box_f$ the trivially ordered subset $\chi(g) = (P_f \backslash P_f[g]) \cup \tilde{Q}_f[g]$. As in the proof of Theorem 4.1,

$$g \sqsubset_f h \text{ iff } P_f[h] \subseteq P_f[g] \text{ and } \tilde{Q}_f[g] \subseteq \tilde{Q}_f[h] \text{ iff } \chi(g) \subseteq \chi(h).$$

The map χ thus defines the stated isomorphism.

■

§5. Properties of the maps μ, λ, z and u.

Given an element f in a finite distributive lattice D, the element $\mu(f)$ (resp. u(f)) is the smallest element of D computationally equivalent to (resp. replaceable by) 1 modulo f; the elements $\lambda(f)$ and z(f) are defined dually. Some simple properties of the maps λ, μ, z and u are described in this section. Details of proofs, and dualisation of results will be left to the reader.

If q is a meet-irreducible in D, then $\mu(q)$ is the element which covers q in D, viz. $q \prec \tilde{q}$. It is clear that if q_1 and q_2 are meet-irreducibles and $q_1 < q_2$, then $\mu(q_1) < \mu(q_2)$, whence $\mu(f) \equiv \wedge\mu(Q_f) = \wedge\mu(Q)$ for any set of meet-irreducibles Q containing Q_f. It is easy to deduce that μ is a $\wedge$-homomorphism $D \to D$; its image is then a closure lattice in D. In general, μ is not a $\vee$-homomorphism.

There is a relationship between μ and λ which can be most easily expressed as a Galois connection between D and D^*, the dual of D. For this purpose, λ and μ are considered as maps $D \to D^*$ and $D^* \to D$ respectively. If $d_1 \leq d_2$ in D, then $\lambda(d_1) \geq \lambda(d_2)$ in D^*. From the characterisation of μ and λ in Cor.2.3, it is clear that $\mu\lambda(d) \geq d$ for all d in D. By the standard theory of Galois connections $\mu\lambda$ is thus a closure operator on D, and $\lambda\mu\lambda \equiv \lambda$. Moreover, $\mu\lambda(D)$ and $\lambda\mu(D^*)$ are closure lattices in D and D^* respectively, and are dually isomorphic via the maps $\mu: \lambda\mu(D^*) \to \mu\lambda(D)$ and $\lambda: \mu\lambda(D) \to \lambda\mu(D^*)$.

There is also a relationship between the intervals of the form $[\lambda(f), \mu(f)]$ and the congruences of the form $\Box_f$, as expressed by the following lemma:

Lemma 5.1.

Using the notation of Theorem 2.2, the following are equivalent:

(i) $\Box_g \subseteq \Box_f$

(ii) f is solitary under $\Box_g$

(iii) $\lambda(f) \geq \lambda(g)$ and $\mu(f) \leq \mu(g)$

(iv) $e_f . e_g = e_f$.

Proof:

(i) and (ii) are equivalent by Lemma 0.2.

(ii) implies (iii): a necessary condition for f to be solitary under $\Box_g$ is that all elements of $[\lambda(f),\mu(f)]$ should be in distinct classes modulo $\Box_g$ (Lemma 2.1). By Theorem 2.2, this is only possible if $\lambda(f) \geq \lambda(g)$ and $\mu(f) \leq \mu(g)$.

(iii) implies (iv): Let

$$A = \lambda(g) \leq a = \lambda(f) \leq b = \mu(f) \leq B = \mu(g).$$

Then, by distributivity:

$$e_f.e_g(z) = (((z \vee A) \wedge B) \vee a) \wedge b = (z \vee a) \wedge b = e_f(z).$$

(iv) implies (i): if $y \Box_g z$, then $e_g(y) = e_g(z)$, whence

$$e_f(y) = e_f.e_g(y) = e_f.e_g(z) = e_f(z).$$

■

Some general relations between $\lambda(f)$, $\mu(f)$, $z(f)$ and $u(f)$ will now be established; these are summarised in Fig's.1a and 1b.

If $X \subseteq Q_f$, then (as in the proof of Theorem 2.2) $f \vee \bigvee \tilde{X} = \bigwedge(Q_f \backslash X) \wedge \bigwedge \mu(X)$. This proves in particular that $\mu(f) = f \vee \bigvee \tilde{Q}_f = f \vee u(f)$. Since $\mu(f) \Box_f 1$, the relation $f \vee \bigvee \tilde{X} \Box_f \bigwedge(Q_f \backslash X)$ is another consequence.

The map u is such that if Q is a trivially ordered subset of meet-irreducibles, then $u(\bigwedge(Q)) = \bigvee(u(Q))$. If q_1 and q_2 are meet-irreducibles, then $q_1 \geq q_2$ iff $\tilde{q}_1 \geq \tilde{q}_2$, whence Q is trivially ordered iff $\tilde{Q}$ is trivially ordered. Duality shows at once that u and z are inverse bijections.

From the relation $f \vee u(f) = \mu(f)$ proved above, it follows that by duality that $\lambda u(f) = u(f) \wedge z u(f) = u(f) \wedge f$. Since λ is a $\vee$-homomorphism, $\lambda(f) \vee \lambda u(f) = \lambda\mu(f)$, whence $\lambda\mu(f) \Box_f \lambda u(f)$.

Consider the map $u\lambda$. For general f in D:

$$u\lambda(f) = u(\bigwedge \tilde{P}_f \wedge \bigwedge Q_f) = u(\bigwedge \tilde{P}_f) \vee u(\bigwedge(Q_f \backslash Q_f[z(f)])) = f \vee \bigvee \tilde{Q}_f[z(f)],$$

since $Q_f \backslash Q_f[z(f)] = \{\, q \in Q_f \mid q \not\geq \tilde{p} \text{ for any } p \text{ in } P_f \,\}$. In the particular case in which $D/\Box_f$ is boolean, $u\lambda = \mu$. Indeed, the condition is necessary and sufficient, since $u\lambda(f) = \mu(f)$ entails $\mu\lambda(f) = u\lambda(f) \vee \lambda(f) = \mu(f)$, proving $[\lambda(f), \mu\lambda(f) = \mu(f)]$ boolean.

It will be convenient to denote the equivalence classes of $\lambda(f)$, $\mu(f)$, $z(f)$ and $u(f)$ in $D/\Box_f$ by λ_f, μ_f, z_f and u_f respectively. There is a distinction between relations between computational equivalence classes modulo f, and relations in D. For instance, if D = FDL(5), and $f = (x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge x_4 \wedge x_5)$, then $z(f) \not\leq \mu(f)$, and $\mu\lambda(f) < \mu z(f)$. General relations between classes analogous to the relations between elements in Fig.'s 1a and 1b are summarised in Fig.2.

Relationships in $D/\Box_f$ can be most easily understood by representing $D/\Box_f$ as the set of decreasing subsets of the poset $P \equiv P_f \cup \tilde{Q}_f$ (c.f. Cor.1.5). In this representation, z_f is the largest decreasing subset which does not contain an element of P_f viz. the decreasing subset whose maximal elements are those elements of $\tilde{Q}_f$ which are minimal in P. Since u_f is the decreasing subset generated by $\tilde{Q}_f$, the relation $z_f \leq u_f$ holds in $D/\Box_f$.

From the representation, it is obvious that $z_f = u_f$ iff $D/\Box_f$ is boolean. Since u(f) and z(f) are respectively greatest and least representatives in D for their

respective computational equivalence classes, $z(f) \geq u(f)$ iff $D/\Box_f$ is boolean. The subcase $u(f)=z(f)$ is interesting. In this case:

$$Q_{z(f)} = \tilde{P}_f \text{ and } Q_f = \tilde{P}_{u(f)} = \tilde{P}_{z(f)},$$

so that by Theorem 4.1: $g \sqsubset_f h$ iff $h \sqsubset_{z(f)} g$. Thus $\Box_f = \Box_{z(f)}$, but the orderings on the equivalence complexes associated with f and z(f) are dual. As an example, let $f=(x_1 \wedge x_2) \vee (x_2 \wedge x_3) \vee (x_3 \wedge x_4)$ in FDL(4).

Another special case occurs if z_f is the least element of $D/\Box_f$; this arises iff no element of $\tilde{Q}_f$ is minimal in P. Because $f \wedge z(f) = \lambda(f)$, and $\lambda(f)$ is the maximal representative in D for the least element of $D/\Box_f$, an equivalent condition is $f \geq z(f)$. This is also equivalent to $f = \mu\lambda(f)$; the condition for f to be "closed" under $\mu\lambda$.

For obvious reasons, the study of free distributive lattices, or equivalently monotone boolean functions, has a special interest. The fact that most of the results and proofs concerning computational equivalence and replacement rules do not require the assumption of freeness may indicate that a deeper understanding of the particular structure of free distributive lattices is important.

The structure of the semi-lattice $\mu(FDL(n))$ seems to be difficult to analyse completely. It may be regarded as a closure lattice in FDL(n); the case n=4 is depicted in Fig.3. As Fig.3 illustrates, the closure lattice is in general non-modular, but has some curious properties. For instance, the sublattice K generated by the n-1 elements

$$\mu(x_1), \mu(x_2), \ldots, \mu(x_{n-1})$$

is isomorphic with FDL(n-1). To see this, consider the homomorphism from FDL(n-1) onto K which maps x_i to $\mu(x_i)$ for each i, and observe that the map $K \to FDL(n-1)$ mapping w to $w|^{x_n=0}$ is its inverse.

When n=4, the lattice $\mu(FDL(n))$ also has the property that each element $\mu(t)$ is contained in one of the n distributive sublattices analogous to K, but this is not the case in general. For example, take n=6, and define

$$t = (x_1 \vee x_2 \vee x_3) \wedge (x_4 \vee x_5 \vee x_6) \wedge (x_2 \vee x_5) \wedge (x_1 \vee x_3 \vee x_5 \vee x_6).$$

The closure lattice $\mu(FDL(n))$ is also self-dual: to see this, define a map β: $\mu(FDL(n)) \to \mu(FDL(n))$ via

$$\beta(\mu(f)) \equiv \mu\lambda(f^*),$$

where f^* is the dual of f in FDL(n). Certainly β is well-defined, since $\lambda(f^*) = (\mu(f))^*$; moreover, if $\beta(\mu(f)) = \beta(\mu(g))$, then

$$\lambda(f^*) = \lambda\mu\lambda(f^*) = \lambda\mu\lambda(g^*) = \lambda(g^*),$$

whence $\mu(f) = \mu(g)$.

In the above context, it may be worth remarking that the algebraic properties of monotone boolean functions in n variables viewed as degenerate functions of n+1 variables are considerably simpler than those of non-degenerate functions. For such functions, computational equivalence always leads to a boolean quotient, in view of Theorem 1.2, and accordingly the relations $u\lambda = \mu$ and $z\mu = \lambda$ apply. As noted above, the closure lattices defined by λ and μ on this subclass are free distributive lattices, whose structure may

prove to be more tractable.

§6. Complements and monotone v non-monotone networks.

Recent work of Berkowitz, Wegener [W] and Dunne [D2] has shown that there are sometimes useful ways of simulating non-monotone networks for computing a monotone function without using negation.

In this section, this problem is studied using an algebraic approach, and new proofs of results of [D2] and [W] are given.

Suppose that f is a monotone boolean function in n variables i.e. an element of L=FDL(n). The lattice L, freely generated by $x_1,x_2,\ldots,x_n$, can be embedded into FDL(2n), freely generated by $x_1,x_2,\ldots,x_n,y_1,y_2,\ldots,y_n$, and into the free boolean algebra FBA(n) freely generated by $x_1,x_2,\ldots,x_n$. There is then a projection π : FDL(2n)→FBA(n) which maps y_i to x_i' for each i, and acts as the identity on L.

A monotone network for computing f in which the inputs are $x_1,x_2,\ldots,x_n$ and their negations is associated with an element v in FDL(2n) such that $\pi(v) = f$. If V is the set of such elements v (that is, the inverse image of f under π), an element h_i in FDL(2n) is a *pseudo-complement* of x_i (see [D2]) if y_i is replaceable by h_i for purposes of computing an element of V, irrespective of which. (This definition differs from that of [D2], in that h_i is not required to lie in L.)

As explained in §2, the relevant notion of computational equivalence in FDL(2n) in this context corresponds to first identifying the elements of V to form a class {V}, then evaluating computational equivalence relative to {V} in this quotient. By Lemma 0.2, it is evident that the projection π defines the required quotient; all the elements of V are identified under π, and no further identification of elements in the boolean image FBA(n) can leave {V} solitary.

By Cor.4.3, the pseudo-complements of x_1 in FDL(2n) are the inverse images under π of elements in the interval $[y_1\wedge f, y_1\vee f]$ of FBA(n). Since π acts as the identity on L, there is at most one pre-image in L under π for each element in FBA(n). But $\pi(y_1\wedge f) = f|^{x_1=0} = \pi(f|^{x_1=0})$, and similarly $\pi(y_1\vee f) = \pi(f|^{x_1=1})$, proving Theorem 6 in [D2].

To characterise pseudo-complements of x_1 in FDL(2n) rather than in L, the principles explained in §2 will be used. The elements of V define an interval $[f_0,f_1]$. Since Ker π is the smallest congruence containing all pairs of the form $(x_i\vee y_i,1)$ and $(x_i\wedge y_i,0)$, it follows that $f_0 = f\wedge\bigvee_1^n(x_i\vee y_i)$ and $f_1 = f\vee\bigwedge_1^n(x_i\wedge y_i)$. Hence the set P (resp. Q) of prime implicants (resp. prime clauses) of f_0 (resp. f_1) are the terms in the non-monotone DNF (resp. CNF) of f with y_i substituted for x_i' for each i. (Via the correspondence of Lemma 1.1, Ker π is associated with the subset $Q\cup\tilde{P}$ of the meet-irreducibles of FDL(2n), which of course - being the set of clauses of the form $e_1+e_2+\cdots+e_n$, where $e_i = x_i$ or y_i - is independent of f, but P and Q are semantically useful.)

By Theorem 4.1, the pseudo-complements of x_1 define the interval $[\vee P[f_0],\wedge Q[f_1]]$, which is easily identified as $[f|^{x_1=0}\wedge y_1, f|^{x_1=1}\vee y_1]$. Since $\bigwedge_1^n x_i$ is in $P\backslash P[y_1]$, it is also clear that there can be no element computationally equivalent

to y_1 in L.

The above discussion indicates that there are many monotone functions which can replace a negated input in a monotone network computing a monotone function f from the inputs $x_1,x_2,\ldots,x_n$ and their negations, but it is never possible to find a monotone function h_1 which simulates a negated input x_1' so precisely that a monotone network computing f from the inputs $x_1,x_2,\ldots,x_n,h_1,x_2',\ldots,x_n'$ still computes f when x_1' replaces h_1. Even so, it will be shown that for certain functions f there may be pseudo-complements h_1 for x_1 for which the replacement of h_1 by x_1' in such a context still "very nearly" computes f. This result is proved as a corollary to a more general theorem:

Theorem 6.1.

In the notation introduced above, the boolean closure of $L/\Box_f$ and $FBA(n)/\{\lambda(f)=0,\mu(f)=1\}$ are isomorphic.

If $V(e_1,e_2,\ldots,e_n)$ is an arbitrary boolean expression such that $V(x_1,x_2,\ldots,x_n)$ is well-defined in $L/\Box_f$ and evaluates to f, then

$$f = (V(x_1,x_2,\ldots,x_n) \vee \lambda(f)) \wedge \mu(f)$$

in the free boolean algebra FBA(n).

Proof:

Let P_f and Q_f be the set of prime implicants and the set of prime clauses of f respectively, and let P and Q be as defined above. If S^* denotes the set of possible conjunctions of literals in a set S, define

$$\alpha:\{x_1,x_2,\ldots,x_n\}^* \to \{x_1,x_2,\ldots,x_n,y_1,y_2,\ldots,y_n\}^* \text{ by } \alpha(\bigwedge_{i\in I} x_i) = \bigwedge_{i\in I} x_i \wedge \bigwedge_{i\notin I} y_i.$$

Then α is 1-1, and identifies P_f with a subset P_0 of P. The set Q_f can be identified with a subset Q_0 of Q via a map β defined in a dual manner.

Since $P\backslash P_0 = \alpha(P_{\lambda(f)})$ and $Q\backslash Q_0 = \beta(Q_{\mu(f)})$, the quotient of FDL(2n) which corresponds (c.f. Lemma 1.1) to the set of meet-irreducibles $P_0 \cup \tilde{Q}_0 \subseteq P \cup \tilde{Q}$ is a quotient of FBA(n), which can be readily identified as $FBA(n)/\{\lambda(f)=0,\mu(f)=1\}$. By Theorem 1.2, the elements g and h in L are equivalent under $\Box_f$ relative to L iff $P_f[g] = P_f[h]$ and $Q_f[g] = Q_f[h]$. But for g in L:

$$\alpha(P_f[g]) = P_0[g] \text{ and } \beta(Q_f[g]) = Q_0[g].$$

Thus the projection of FDL(2n) onto $FBA(n)/\{\lambda(f)=0,\mu(f)=1\}$ associated with the set of meet-irreducible's $P_0 \cup \tilde{Q}_0$ induces an embedding ρ of $L/\Box_f$ into the image. It follows that $FBA(n)/\{\lambda(f)=0,\mu(f)=1\}$ is the boolean closure of $L/\Box_f$, since both lattices have the same number of meet-irreducibles.

Suppose that $V(e_1,e_2,\ldots,e_n)$ is a boolean word, and that $V(x_1,x_2,\ldots,x_n)$ is well-defined in $L/\Box_f$ and evaluates to f. As above, let π denote the projection of FDL(2n) onto FBA(n) which maps x_i to x_i and y_i to x_i'. In view of the embedding ρ described above, the function $v=V(x_1,x_2,\ldots,x_n)$ in FBA(n) will satisfy $v[\pi(P_0)] = f[\pi(P_0)]$ and $v[\pi(Q_0)] = f[\pi(Q_0)]$. But

$$\mu(f) \geq \lambda(f) \geq p \text{ for all } p \text{ in } P\backslash P_0$$

and $q \geq \mu(f) \geq \lambda(f)$ for all q in $Q\backslash Q_0$, whence

$$f = \pi(f_0) = \bigvee \pi(P) \leq (v \vee \lambda(f)) \wedge \mu(f) \leq \bigwedge \pi(Q) = \pi(f_1) = f.$$

■

In the theorem, the condition for $V(x_1,x_2, \ldots, x_n)$ to be well-defined is that all necessary complements of sub-expressions of V exist in $L/\Box_f$; this condition is redundant if $L/\Box_f$ is boolean, that is if each x_i has a complement in $L/\Box_f$.

Let x denote one of the free generators of FDL(n). The element h in L serves as a complement for x in $L/\Box_f$ iff $x \vee h \geq \mu(f)$ and $x \wedge h \leq \lambda(f)$.

Lemma 6.2.

If a and b are arbitrary elements of L, then the inequalities

$$x \vee h \geq a \text{ and } x \wedge h \leq b$$

can be satisfied simultaneously by some h iff $a|^{x=0} \leq b|^{x=1}$. When this condition is satisfied, the solution set is the interval $[\, a|^{x=0}, b|^{x=1} \,]$. In particular:

$$x \text{ is complemented in L iff } \mu(f)|^{x=0} \leq \lambda(f)|^{x=1} \text{ iff } u(f)|^{x=0} \leq z(f)|^{x=1}.$$

Proof:

If $x \vee h \geq a$ and $x \wedge h \leq b$, then $b|^{x=1} \geq h|^{x=1} \geq h|^{x=0} \geq a|^{x=0}$. Moreover $x \vee a|^{x=0} \geq a$, and $x \wedge b|^{x=1} \leq b$.

Taking $a=\mu(f)$ and $b=\lambda(f)$ proves that

$$x \text{ is complemented in L iff } \mu(f)|^{x=0} \leq \lambda(f)|^{x=1}.$$

The latter condition entails $u(f)|^{x=0} \leq z(f)|^{x=1}$, since

$$u(f)|^{x=0} \leq \mu(f)|^{x=0} \leq \lambda(f)|^{x=1} \leq z(f)|^{x=1}.$$

For the converse, since $\lambda(f) = f \wedge z(f)$ and $\mu(f) = f \vee u(f)$, it suffices (by duality) to prove that

$$z(f)|^{x=1} \geq f|^{x=0}.$$

Now $z(f)|^{x=1} = \bigwedge \widetilde{S}$ and $f|^{x=0} = \bigvee T$, where $\widetilde{S} = \widetilde{P}_f \backslash \widetilde{P}_f[x]$ and $T = P_f \backslash P_f[x]$. If p is meet-irreducible, $p \leq x$ iff $\tilde{p} \not\geq x$, whence P_f is the disjoint union of S and T. But if $s \in S$ and $t \in T$, then $t \not\geq s$ so that $\tilde{s} \geq t$.

■

The following corollary follows directly from Theorem 6.1 and Lemma 6.2:

Cor.6.3.

Let f and L be as above.

If x_1 has a complement in $L/\Box_f$, and h_1 is a representative in L for x_1' in $L/\Box_f$, then h_1 is a monotone pseudo-complement for x_1.

Moreover, if w is a monotone boolean expression such that $w(x_1,x_2, \ldots, x_n,h_1) = f$ in L, then $f = (w(x_1,x_2, \ldots, x_n,x_1') \vee \lambda(f)) \wedge \mu(f)$.

Acknowledgement.

I am indebted to Paul Dunne for a number of useful discussions, and for introducing me to the theorems from reference [D2] which appear here in a modified form.

References.

[B1] Beynon, W.M.

Geometric aspects of partially-ordered systems,
Ph.D. thesis, King's College, Univ. of London, 1973.

[B2] Beynon, W.M.

Duality theorems for finitely-generated vector lattices,
Proc.Lond.Math.Soc. (3) 31, 114-128, 1975.

[B3] Beynon, W.M.

Vector lattices freely generated by distributive lattices,
Math.Proc.Camb.Phil.Soc. (81), 193-200, 1977.

[B] Birkhoff, G.A.

Lattice Theory, 3rd ed.
AMS Colloquium Publications, Vol.XXV, 1967.

[D1] Dunne, P.E.

A 2.5n lower bound on the monotone network complexity of T_3^n,
Theory of Computation Report 62, Univ. of Warwick, 1984.

[D2] Dunne, P.E.

Some results on replacement rules in monotone boolean networks,
Theory of Computation Report 64, Univ. of Warwick, 1984.

[G] Grätzer, G.

Lattice Theory: first concepts and distributive lattices,
W.H.Freeman and Co., San Francisco, 1971.

[M] Mehlhorn, K. & Galil, Z.

Monotone switching networks and boolean matrix product,
Computing (16), 99-111, 1976.

[P] Paterson, M.S.

Complexity of monotone networks for boolean matrix product,
Theoretical Computer Science (1), 13-20, 1975.

[W] Wegener, I

On the complexity of slice-functions,
Internal Report, Univ. Of Frankfurt, July 1983.

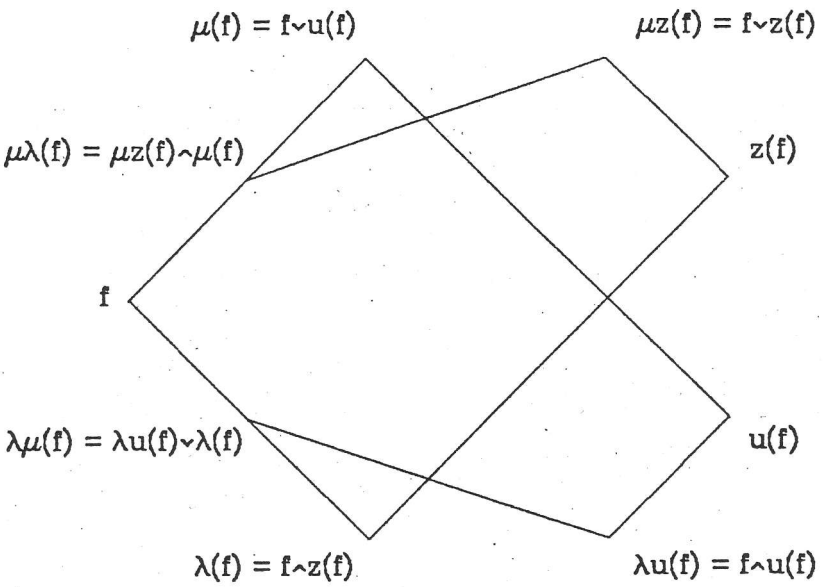

Fig.1a: The general case.

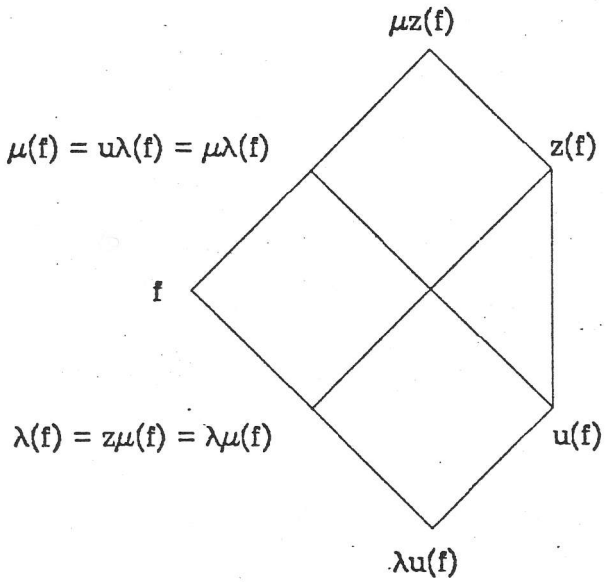

Fig.1b: $D/\Box_f$ is boolean.

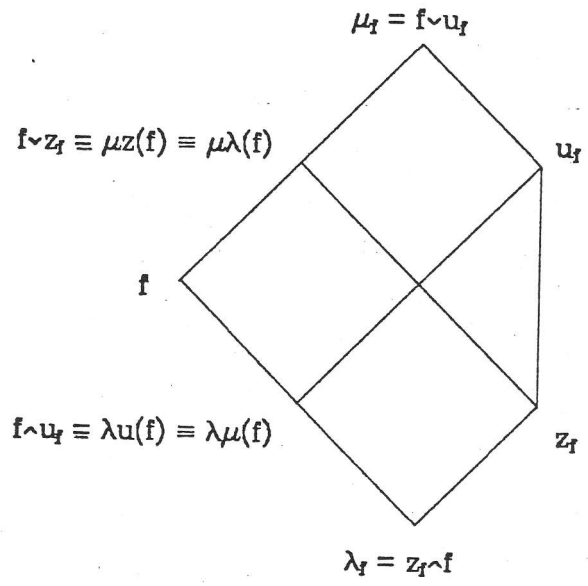

Fig.2: Relations in $D/\Box_f$.

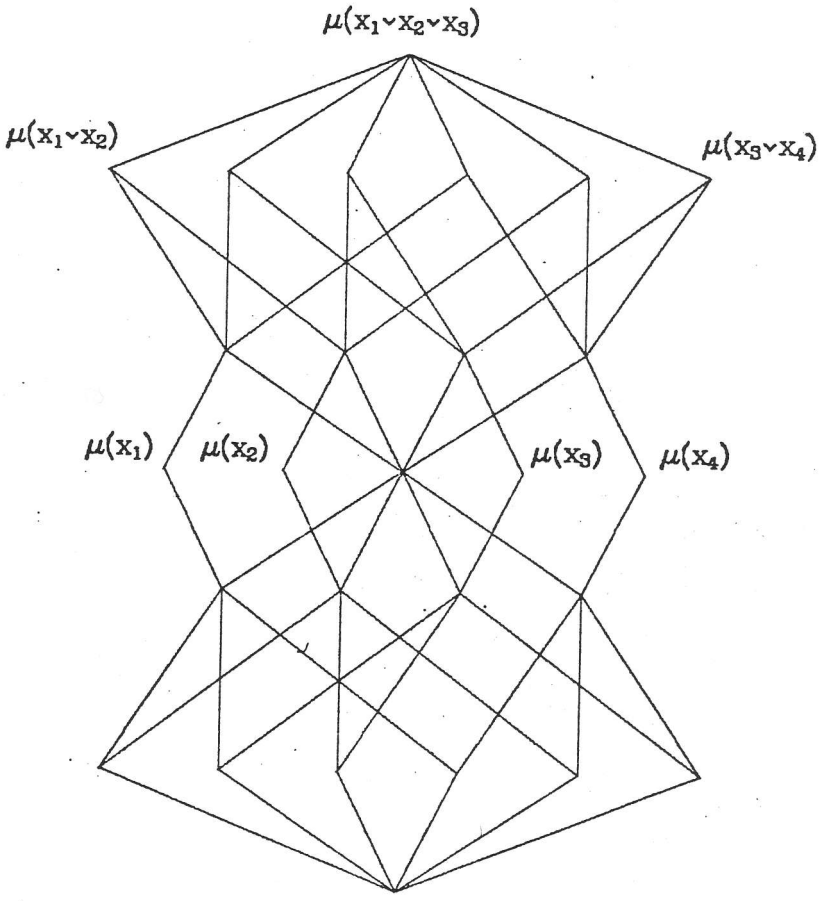

Fig.3: The closure lattice $\mu(\mathrm{FDL}(4))$.

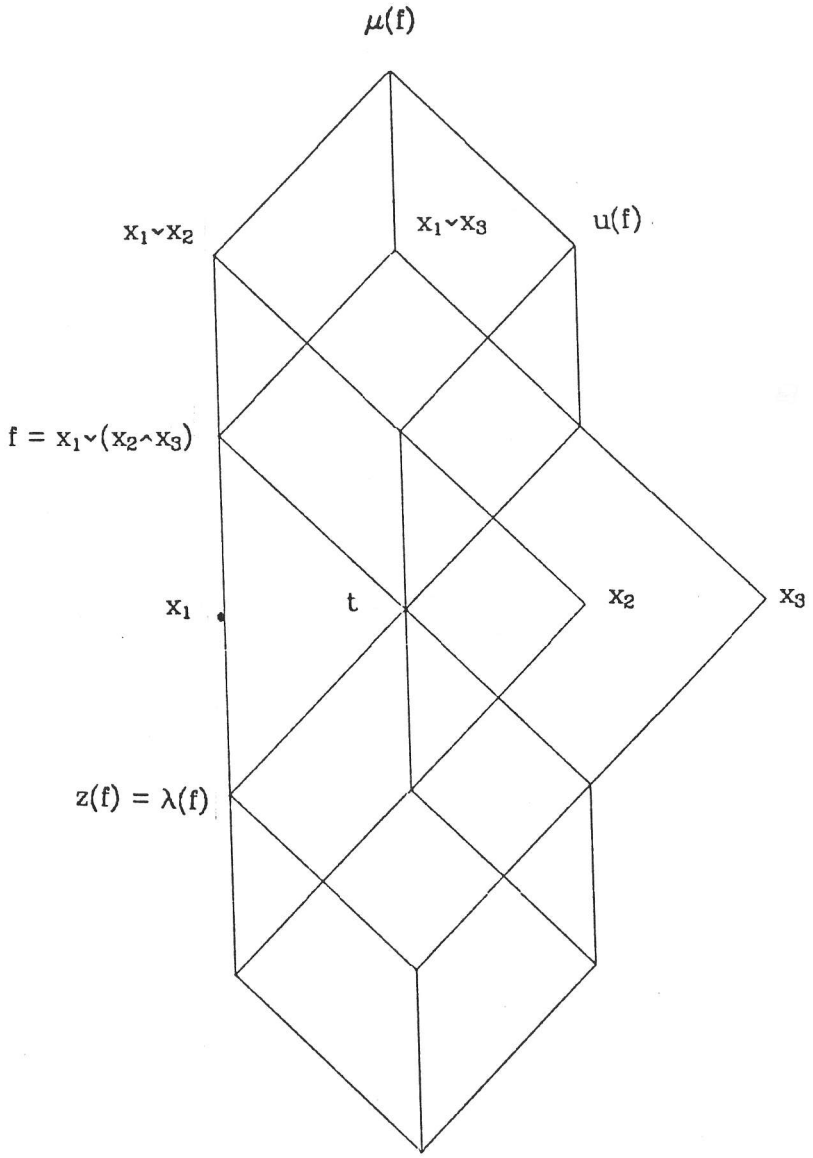

Fig 4a: $f = x_1 \vee (x_2 \wedge x_3)$ in FDL(3).

FDL(3)/ $\square_f$ is isomorphic with the interval $[\lambda(f), \mu(f)]$.

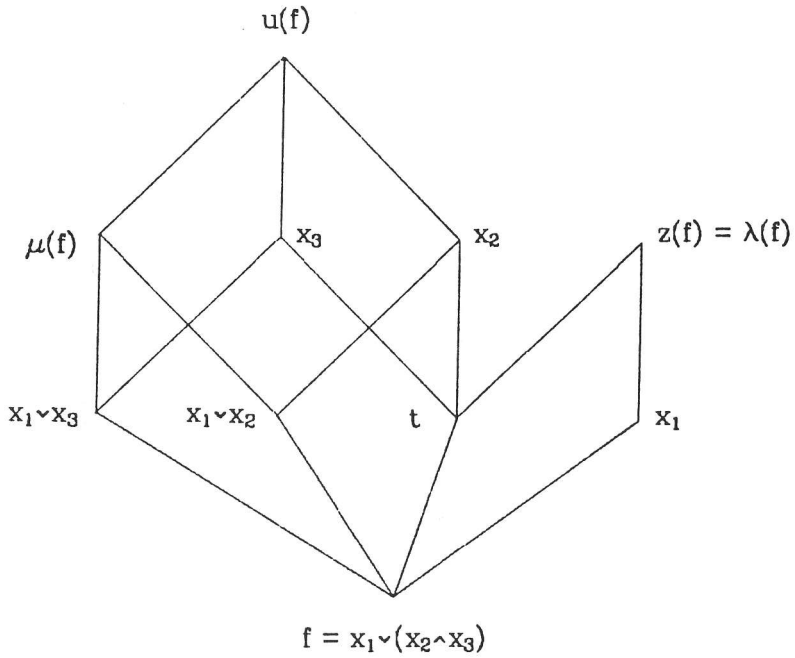

Fig 4b: The complex (FDL(3)/ $\square_f$, $\sqsubset_f$) with nodes labelled by representatives of the equivalence classes.