MIT/LCS/TM-138

DYNAMIC ALGEBRAS:

EXAMPLES, CONSTRUCTIONS, APPLICATIONS

Vaughan R. Pratt

July 1979

Dynamic Algebras: Examples, Constructions, Applications

Vaughan R. Pratt

Abstract

Dynamic algebras combine the classes of Boolean (B ∨ ′ 0) and regular (R ∪ ; *) algebras into a single finitely axiomatized variety ($\mathscr{B}$ $\mathscr{R}$ ◇) resembling an R-module with "scalar" multiplication ◇. The basic result is that * is reflexive transitive closure, contrary to the intuition that this concept should require quantifiers for its definition. Using this result we give several examples of dynamic algebras arising naturally in connection with additive functions, binary relations, state trajectories, languages, and flowcharts. The main result is that free separable dynamic algebras are residually separable-and-finite, important because finite separable dynamic algebras are isomorphic to Kripke structures. Applications include a new completeness proof for the Segerberg axiomatization of propositional dynamic logic, and yet another notion of regular algebra.

Key words

Dynamic algebra, logic, program verification, regular algebra.

This research was supported by the National Science Foundation under NSF grant no. MCS78-04338.

Dynamic Algebras: Examples, Constructions, Applications

Vaughan R. Pratt

1. INTRODUCTION

We propose, with Kozen [17], the notion of a *dynamic algebra*, which integrates an abstract notion of *proposition* with an equally abstract notion of *action*. Just as propositions tend to band together to form *Boolean* algebras, as Halmos [12] puts it, with operations $\vee$ and $'$, so do actions organize themselves into *regular* algebras, with operations $\cup$; $*$. Analogously to the proposition $p \vee q$ being the *disjunction* of propositions p and q, and p' the *complement* of p, the action $a \cup b$ is the *choice* of actions a or b, a;b, or just ab, is the *sequence* a followed by b, and a^* is the *iteration* of a indefinitely often.

Just as $\vee$ and $'$ have a natural set theoretic interpretation, so do $\cup$, ; and $*$ have natural interpretations on additive functions, binary relations, trajectory sets, languages, and matrices over regular algebras, to name those regular algebras that are suited to dynamic algebra. The section below on examples illustrates this.

It is natural to think of an action as being able to bring about a proposition. We write $\langle a \rangle p$, or just ap, pronounced "a *enables* p," as the proposition that action a can bring about proposition p. A *dynamic algebra* then is a Boolean algebra $(B \vee ' 0)$, a regular algebra $(R \cup ; *)$, and the *enables* operation $\diamond : R \times B \to B$.

Motivation. An important problem in computer science is how to reason about computer programs. The proposals of [10,14,29,8,6,21] are representative of a class of methods (by no means the only class) that may be exemplified by the following.

Let $x:=5$ denote the program for setting the value of the program variable x to 5. Then $\langle x:=5 \rangle x=5$ asserts that setting x to 5 can make x equal to 5, which is necessarily true and so is the same (abstract) proposition as the unit 1 of the Boolean algebra of all such propositions. Thus we would write $\langle x:=5 \rangle x=5 = 1$. On the other hand $\langle x:=x+1 \rangle x=5$, again viewed abstractly,

is not 1 but rather is the same abstract proposition as x=4. (The "1" in "x+1" is numeric 1, distinguished by context from Boolean 1.) And $\langle x:=x-1^*\rangle x=0$ must be $x\geqslant 0$, as it is not possible to make an initially negative variable zero by decrementing it indefinitely.

These observations about x:=5, x:=x+1, etcetera, depend on the nature of program variables, numbers, arithmetic, assignment, and so on. However there are also more universal observations one can make, at a level that knows nothing about programs that manipulate variables and numbers. For example no program can bring about the truth of *false*; that is, $a0=0$. Moreover, a program can bring about $p\vee q$ just when it can bring about p or it can bring about q, i.e. $a(p\vee q) = ap\vee aq$. One of a or b can bring about p just when either a can bring about p or b can, i.e. $(a\cup b)p = ap\vee bp$. And ab can bring about p just when a can bring about a situation from which b can bring about p, i.e. $(ab)p = a(bp)$. (In full, $\langle a;b\rangle p = \langle a\rangle(\langle b\rangle p)$. We rely on context to indicate where to insert ; and $\Diamond$.)

Suppose now that either p holds, or a can bring about a situation from which a can *eventually* (by being iterated) bring about p. Then a can eventually bring about p. That is, $p\vee aa^*p \leqslant a^*p$. (We write $p\leqslant q$ to indicate that p implies q, defined as $p\vee q = q$.) In turn, if a can eventually bring about p, then either p is already the case or a can eventually bring about a situation in which p is not the case but one further iteration of a will bring about p. That is, $a^*p \leqslant p\vee a^*(p'\wedge ap)$. This is the principle of induction, in a simple Boolean disguise as can be seen by forming the contrapositive and replacing p' by q to yield $q \wedge [a^*](q\supset[a]q) \leqslant [a^*]q$, where $[a]p, p\supset q$ abbreviate $(ap')', p'\vee q$ respectively. [a] is the *dual* of $\langle a\rangle$, and [a]p asserts that whatever a does, p will hold if and when a halts.

The notion of a *test* program p? is also useful. A test cannot bring about a different situation; moreover p? cannot bring about even the present situation unless p already holds. Thus $(p?)q = p\wedge q$. Tests are of use in defining certain well-known programming constructs such as *if* p *then* a *else* b = $(p?a)\cup(p'?b)$, and *while* p *do* a = $(p?a)^*p'?$. We will have little to say about tests in this paper.

Outline. The remainder of the paper is as follows. Section 2 supplies the main definitions. Section 3 gives the basic result, that the regular operation * of a dynamic algebra is reflexive transitive closure, or quasiclosure to be precise. Section 4 illustrates the abstract concept of dynamic algebra with five concrete examples of dynamic algebras that arise in practice, and also gives some counterexamples. Section 5 gives the main results, that free dynamic algebras are residually (separable-and-finite)-or-Boolean-trivial (isomorphic to a subdirect product of dynamic algebras each of which is either

separable and finite or has a one-element Boolean component), and that free separable dynamic algebras exist and are residually separable-and-finite.

Section 6 gives several applications of these results. Using the fact that every finite separable dynamic algebra is isomorphic to a Kripke structure we apply the first part of the main result to show the completeness of the Segerberg axiomatization of propositional dynamic logic [30], which we state in algebraic form as the equality of two varieties. Using the second part of the main result we show that separable dynamic algebras and Kripke structures generate the same variety and so have the same equational theory, both Boolean and regular. Finally we explore a new definition of the notion of regular algebra, a surprisingly controversial class given the importance of some of its instances. Section 7 tidies up some loose ends. Section 8 supplies some algebraic prerequisites as a convenient reference for the reader who may need prompting on some of the definitions; in the text we refer thus[8] to this section.

For us the most interesting parts of the paper are Theorems 3.4 (* is reflexive transitive closure) and 5.3 (existence of filtrations). We find it surprising that an equational system can define reflexive transitive quasiclosure exactly, that is, with no nonstandard models. While it may not come as a surprise to those familiar with the Fischer-Ladner filtration result [9] that it can be obtained in an algebraic form, those familiar with the various efforts to obtain the completeness result may find it of interest that the filtration result itself need be the only subtle part. Lemma 3.1 is the key to the rest of the paper, filtration included, but it is not a difficult lemma.

2. DEFINITIONS

Syntax. We define the following classes of algebras.

Class	*Symbol*	*Similarity Type*
Boolean algebras	$\mathscr{B}$	(B ∨ ′ 0)
Regular algebras	$\mathscr{R}$	(R ∪ ; *)
Dynamic algebras	$\mathscr{D}$	($\mathscr{B}$ $\mathscr{R}$ ◇)
Test algebras	$\mathscr{E}$	($\mathscr{D}$?)

The types are: ∨:B×B→B, ′:B→B, 0:B, ∪:R×R→R, ;:R×R→R, *:R→R, ◇:R×B→B, ?:B→R. We write p∧q for (p′∨q′)′, 1 for 0′, [a]p for (ap′)′, p≤q for p∨q=q, a≤b for ∀p(ap≤bp).

Semantics. A Boolean algebra is a complemented distributive lattice, these all being properties definable equationally. A dynamic algebra ($\mathscr{B}$ $\mathscr{R}$ $\Diamond$) satisfies the following equations.

1.	$\mathscr{B}$ is a Boolean algebra.	3.	$(a \cup b)p = ap \vee bp$
2a.	$a0 = 0$	4.	$(ab)p = a(bp)$
2b.	$a(p \vee q) = ap \vee aq$	5a,b.	$p \vee aa^*p \leqslant a^*p \leqslant p \vee a^*(p' \wedge ap)$.

These axioms are obtained from the Hilbert-style Segerberg axioms [30] for propositional dynamic logic [9] in the same way one may obtain Boolean identities from a Hilbert-style axiomatization of propositional calculus. Note that axiom 2a is obtained from the modal logic inference rule of Necessitation, namely from p infer [a]p. We have discussed the motivation for all of these axioms in the previous section.

A test algebra satisfies:

6. $(p?)q = p \wedge q$.

We will not prove anything about test algebras in this paper. Although they introduce a little complication into some of the arguments, the reader should find it straightforward to extend most of the results below about dynamic algebras to test algebras. We mention *converse* among the open problems of Section 7.

Predynamic Algebras. A *predynamic* algebra is any algebra similar to (having the same similarity type as, but not necessarily satisfying the equations for) a dynamic algebra. Free predynamic algebras are used in this paper for the notion of an FL-set.

Separability. If $ap=bp$ for all p we call a and b *inseparable*, an equivalence relation which we shall later show to be a congruence relation on dynamic algebras. Following Kozen [17] we call *separable* any dynamic algebra in which inseparability is the identity relation. We let S denote the class of separable dynamic algebras.

Separability can be expressed with the first-order sentence $\forall a \forall b \exists p(ap=bp \rightarrow a=b)$. (Taking the contrapositive of the quantifier-free part makes this more understandable.) This being a Horn sentence [5, p. 235], it follows that S is closed under direct products [15]. Example 7 shows that S is closed under neither homomorphisms nor subalgebras.

3. BASIC RESULT

In this section we prove the fundamental theorem of dynamic algebra. We present this result before giving the examples, partly because it helps somewhat in understanding the examples, partly because its proof does not deserve to be buried deeper in the paper.

Actions as Functions. Although we have taken the type of $\Diamond$ to be $\Diamond: R \times B \to B$ we could equivalently have taken it as $\Diamond: R \to (B \to B)$; the reason for the former was so that it would be clear that we were defining an ordinary algebra. The latter type is consistent with our use of the notation $\langle a \rangle p$ - we may think of $\langle a \rangle$ as a function on B. Our use of the alternative notation ap is to suggest that we may think of a itself as a function on B. All that is lacking is *extensionality*; that is, we may have ap = bp for all $p \in B$ yet not have a=b. The lack of extensionality does not prevent us from appearing to be able to define operations such as composition by saying that (ab)p = a(bp) for all p.

Accordingly we shall think of the elements of R as *quasifunctions*, having all the attributes of functions save extensionality. In a separable dynamic algebra they become functions.

Recall that $a \leqslant b$ means that $ap \leqslant bp$ for all p. It follows that $\leqslant$ on quasifunctions is reflexive and transitive but not antisymmetric, and so is a quasiorder. In a separable dynamic algebra it becomes a partial order.

The content of axioms 2a,b is now clear. Axiom 2a says that all quasifunctions are *strict* (0-preserving), and axiom 2b that they are *finitely additive* (preserving joins of finite non-empty sets).

Continuing in this vein, axioms 3 and 4 leave no doubt that $\cup$ is pointwise disjunction and ; is composition. In the absence of extensionality we must consider these apparent functionals to be be *quasifunctionals*, which are operations on quasifunctions with which the relation of inseparability is compatible ($a \equiv a'$ and $b \equiv b'$ implies $a \cup b \equiv a' \cup b'$ etc.), easily seen from axioms 3 and 4 to be the case for $\cup$ and ;.

Axiom 5 however is nothing short of inscrutable. It may be made a little more symmetric by rephrasing it as $p \vee (p' \wedge aa^*p) \leqslant a^*p \leqslant p \vee a^*(p' \wedge ap)$, using Boolean manipulation on 5a. This can then be broken up into $p \leqslant a^*p$ together with the even more symmetric $p' \wedge aa^*p \leqslant p' \wedge a^*p \leqslant a^*(p' \wedge ap)$. The lower and upper bounds on $p' \wedge a^*p$ seem to be referring to the start and end of the "interval" during which p remains false, an interval which must exist when $p' \wedge a^*p$ holds. This intuitive analysis, while suggestive, is however not a

characterization of *. The following supplies a more satisfactory formal analysis.

Let $a!p = \{q | p \vee aq \leqslant q\}$. Let min S be the least element of the partially ordered set S when it exists, and undefined otherwise. (This is in contrast to $\wedge S$, the meet of S, which may exist but not be in S.)

We propose the following alternative to 5a,b.

$$5'. \qquad a^*p = \min(a!p).$$

Axiom 5′ is not an acceptable equational identity for the purpose of defining a variety because of its use of min and !. However it provides an excellent metamathematical characterization of *, as the following lemma shows.

Lemma 3.1. 5a,b and 5′ are interchangeable as axioms.

Proof. (→). Assume 5a,b. 5a asserts that $a^*p \in a!p$. Now consider arbitrary $q \in a!p$. We show that $a^*p \leqslant q$. We have:

	$p \leqslant q$	$(p \vee aq \leqslant q)$
Hence	$a^*p \leqslant a^*q$	(2b - expand definition of $\leqslant$)
	$\leqslant q \vee a^*(q' \wedge aq)$	(5b)
	$= q \vee a^*0$	$(p \vee aq \leqslant q)$
	$= q.$	(2a,1)

(←). Assume $a^*p = \min(a!p)$. Then $a^*p \in a!p$, so 5a holds. For 5b it suffices to show that $p \vee a^*(p' \wedge ap) \in a!p$, since $a^*p \leqslant q$ for any $q \in a!p$.

$p \vee a(p \vee a^*(p' \wedge ap))$	$= p \vee (p' \wedge a(p \vee a^*(p' \wedge ap)))$	(1)
	$= p \vee (p' \wedge (ap \vee aa^*(p' \wedge ap)))$	(2b)
	$\leqslant p \vee (p' \wedge ap \vee aa^*(p' \wedge ap))$	(1)
	$\leqslant p \vee a^*(p' \wedge ap)$	$(5' \rightarrow 5a)$ ∎

Notice that we used only isotonicity of a ($p \leqslant q \rightarrow ap \leqslant aq$) in the → direction. If we relax axiom 2b to require only isotonicity we get *isodynamic algebras*, which we shall consider in Section 6 in discussing regular algebras. In Section 6 we show that isotonicity is inadequate for the ← direction.

From Lemma 3.1 we infer that * is a quasifunctional, since if $a \equiv a'$ then $a^*p = \min(a!p) \equiv \min(a'!p) = a'^*p$, so $a^* \equiv a'^*$. Thus ≡ is a congruence relation. We now address the question of characterizing which quasifunctional * is. We define a quasiclosure operator to be as for a closure operator[8],

except that idempotence is replaced by *quasi-idempotence*, $fx \leqslant ffx$ and $ffx \leqslant fx$, which for regular elements means $fa \equiv ffa$ where $\equiv$ is inseparability.

Lemma 3.2. $*$ is a quasiclosure operator.

Proof.
(Isotonicity.) If $a \leqslant b$ then for all p, $b!p \subseteq a!p$, whence $\min(a!p) \leqslant \min(b!p)$, thus $a*p \leqslant b*p$, whence $a* \leqslant b*$.
(Reflexivity.) $p \leqslant a*p$, so $ap \leqslant aa*p \leqslant a*p$, for all p, whence $a \leqslant a*$.
(Quasi-idempotence.) $a*p = \min(a!a*p) = a*a*p$, so $a*p \in a*!p$. But if $q \in a*!p$, $p \leqslant q$, so $a*p \leqslant a*q \leqslant q$, whence $a*p = \min(a*!p) = a**p$. ∎

We call the quasiclosure system associated with $*$ the *system of asterates*, the word "asterate" being Conway's [7,p.25]. By the definition of a closure system[8], an asterate is a fixed point of $*$.

There are of course many quasiclosure operators, and merely being one is not a remarkable thing in a variety. So which quasiclosure operator is $*$? We say that the quasifunction a is *reflexive* when $p \leqslant ap$ for all p, and *transitive* when $aa \leqslant a$. Thus a is reflexive and transitive when for all p, $p \vee aap \leqslant ap$, i.e. $ap \in a!p$, the characterization we use in the next proof.

Lemma 3.3. a is an asterate iff a is reflexive and transitive.

Proof. ($\rightarrow$) $ap = a*p \in a!p$.
($\leftarrow$) $a*p = \min(a!p) \leqslant ap$, and $ap \leqslant a*p$, so $a*p = ap$. ∎

Thus the system of asterates coincides with the set of reflexive transitive quasifunctions, making $*$ reflexive transitive quasiclosure. From all this we infer the following "representation theorem" for dynamic algebras.

Theorem 3.4. Every dynamic algebra is a Boolean algebra $\mathscr{B}$ together with a set of strict finitely additive quasifunctions on $\mathscr{B}$ closed under the quasifunctionals of pointwise disjunction, composition, and reflexive transitive quasiclosure.

Note that when a is reflexive, $aap = ap$ iff $a*p = ap$, for all p.

This theorem is very helpful in reasoning about dynamic algebras. It does not however make as satisfactory a connection as does Theorem 6.2 with the intuitions of computer scientists, which tend to be oriented towards the notion of *state* as providing a "place" for predicates to hold in, and for programs to travel between. Example 2 below, Kripke structures, amplifies this intuition.

4. EXAMPLES

This section is meant to be suggestive rather than encyclopedic, and is kept short by omitting proofs and lengthy explanations. The reader will however find the following lemmas helpful in understanding Example 1.

Lemma 4.1. The set a!p is closed under arbitrary meets when they exist.

Proof. Let $S \subseteq a!p$, and suppose $\wedge S$ exists. Then for any $r \in S$, $\wedge S \leqslant r$ so $p \vee a(\wedge S) \leqslant p \vee ar \leqslant r$. Hence $p \vee a(\wedge S) \leqslant \wedge S$ ($\wedge S$ is the *greatest* lower bound on S), so $\wedge S \in a!p$. ∎

Corollary 4.2. In a complete lattice (hence in a complete Boolean algebra) min(a!p) always exists and is $\wedge(a!p)$.

Let X be a set of subsets of a lattice $\mathscr{B}$, and write aS for $\{as|s \in S\}$ for any S in X. We call the quasifunction a *X-additive* when $a(\vee S) = \vee(aS)$ for all S in X for which $\vee S$ exists. We call a respectively *strict*, *isotonic*, *finitely additive*, *continuous*, and *completely additive*, when a is X-additive for X respectively $\{\varphi\}$, the set of nonempty finite chains of $\mathscr{B}$, the set of nonempty finite subsets of $\mathscr{B}$, the set of directed sets of $\mathscr{B}$, and the power set $2^{\mathscr{B}}$ of all subsets of $\mathscr{B}$.

Lemma 4.3. The quasifunctionals $\cup$; * on quasifunctions on a complete lattice preserve X-additivity for any X.

Proof. Let $S \in X$. For $\cup$ we have $(a \cup b)(\vee S) = a(\vee S) \vee b(\vee S) = \vee(aS) \vee \vee(bS) = \vee((a \cup b)S)$. For ; we have $(ab)(\vee S) = a(b(\vee S)) = a(\vee(bS)) = \vee(a(bS)) = \vee((ab)S)$. For * we have $(\vee S) \vee a(\vee(a^*S)) = (\vee S) \vee (\vee(aa^*S)) = \vee(S \cup aa^*S) \leqslant \vee(a^*S)$, so $\vee(a^*S) \in a!(\vee S)$. For any $r \in a!(\vee S)$ we argue as follows. Let $s \in S$, so $s \leqslant \vee S$, so $a!(\vee S) \subseteq a!s$, whence $a^*s = \min(a!s) \leqslant r$ (min(a!s) exists by Corollary 4.2). So $\vee(a^*S) \leqslant r$. Hence $\vee(a^*S) = \min(a!(\vee S)) = a^*(\vee S)$. ∎

Thus if a and b are strict, so are $a \cup b$, ab, and a^*. The same holds with "strict" replaced by "isotonic," "finitely additive," "continuous," or "completely additive."

Example 1: Full dynamic algebras. Given a complete Boolean algebra $\mathscr{B} = (B \vee ' 0)$, let $\vec{R}$ be the set of all strict finitely (resp. completely) additive functions on B and let $\Diamond : R \times B \to B$ be application of elements of R to elements of B. By Lemma 4.3, R is closed under $\cup$; * when assigned the interpretations of Theorem 3.4. Hence by that theorem $(\mathscr{B}\ (R\ \cup\ ;\ *)\ \Diamond)$ is a dynamic algebra. We call it the full (resp. completely full) dynamic algebra

on $\mathcal{B}$. Note that the completely full algebra has fewer functions than the full one. Both are of course separable.

The class of full dynamic algebras contains some pathological cases, as Example 6 will show. Examples 2-5 however give algebras encountered in ordinary practice.

Example 2: Kripke structures. Given a set W (the set of *possible worlds*, or *states*), let $\mathcal{B}$ be the power set algebra on W. Then the *full Kripke structure on* W is the completely full dynamic algebra on $\mathcal{B}$, a separable dynamic algebra. A *Kripke structure on* W is a subalgebra of the full Kripke structure on W. The class K consists of all Kripke structures. The class of dynamic algebras, being a variety, is closed under taking subalgebras, whence Kripke structures are dynamic algebras. They are not however necessarily separable ones since S is not closed under subalgebras, as Example 7 will show.

Completely additive functions on the complete Boolean algebra of subsets of W correspond to binary relations on W. This is because the set of functions $f:W\to 2^W$ (binary relations) naturally corresponds to the completely additive subset of the set of functions $f:2^W\to 2^W$. The correspondence is as follows. If $f:W\to 2^W$ is a binary relation, the corresponding $g:2^W\to 2^W$ satisfies $g(U) = \cup\{f(u)|u\in U\}$. Conversely, any completely additive $g:2^W\to 2^W$ must satisfy $g(U) = \cup\{g(\{u\})|u\in U\}$, by complete additivity, so the restriction of g to the atoms of 2^W corresponds naturally to a function $f:W\to 2^W$.

From this it should be clear that the operations of pointwise disjunction and composition correspond exactly to those of union and composition for binary relations. Reflexive transitive closure for functions on lattices similarly corresponds to reflexive transitive closure for binary relations since the definition of reflexive transitive closure depends only on $\cup$ and ; and these have already been shown to correspond. Note that we need to start from the full power set algebra to avoid omitting any closures and getting the wrong reflexive transitive closure; "smaller" Kripke structures are obtained as subalgebras *after* * is defined.

Because of this correspondence we will *define* binary relations on W to be completely additive functions on 2^W.

Kripke structures supply quite satisfactory models of programs. The elements of the sets constituting the Boolean part of a Kripke structure model the states of one or more computers. Each Boolean element is then a predicate on states; for example the formula $x\geq 0$ denotes the set of states in which the variable x is non-negative. The regular elements correspond to binary relations on the set of states. The relations in turn correspond to the edges

of a graph whose vertices are the states. Each edge is labelled with a program. The whole graph then presents a picture of all the possible states of a system together with all the possible state transitions, each labelled with its agent.

The graph enjoys certain closure properties. For example there exists between two states a transition labelled either a or b just when there exists between those states a transition labelled a∪b. There exists a path between two states consisting of transition a (to some state) followed by transition b just when there exists a transition ab between those two states. There exists a (possibly trivial) finite path of a's between two states just when there exists a transition a^* between those states (whence for every state and every program a there is a transition a^* leaving and returning to that state).

Because of the importance of Kripke structures in computer science, the question arises as to whether the equational theory of dynamic algebras does justice to Kripke structures. The next section lays the groundwork for showing in the section after it that the classes K and S (Kripke structures and separable dynamic algebras) generate the same variety and so have the same equational theory. Both the Boolean and regular theory are of considerable importance in reasoning about programs, the former dealing with program correctness and termination, the latter with program equivalence.

Example 3: Trajectory algebras. These constitute a variation on Kripke structures in which $\mathscr{B}$ is as before, while the completely additive functions in R are replaced by sets of non-empty strings over the set W of states. The regular operations are as follows. ∪ is set union, ; is "fusion product," in which $ab = \{u\ldots v\ldots w | u\ldots v \in a \text{ and } v\ldots w \in b\}$, and $a^* = W \cup a \cup aa \cup aaa \cup \ldots$ (Fusion product differs from concatenation in that there is a requirement of "compatibility" between the strings being "fused." Thus the fusion product of {ab,cd} with {de,bc} is {abc,cde}, while the concatenation is {abde,abbc,cdde,cdbc}.) Finally $ap = \{u | u\ldots v \in a \text{ and } v \in p\}$.

In a Kripke structure a program can be considered a set of pairs of states, each pair having an initial and a final state. In a trajectory algebra a program is a set of state trajectories, each trajectory having an initial state, intermediate states, and a final state.

Trajectory algebras supply a natural example of a nonseparable dynamic algebra. This is because two sets of trajectories may differ only in their intermediate states, and hence exhibit the same functional behavior on $\mathscr{B}$.

Other modalities besides $\Diamond$ suggest themselves for trajectory algebras, such "throughout" and "sometime during." A complete axiomatization of such modalities appears in [24].

Example 4: Linguistic Algebras. Let Σ^* denote the set of finite strings over some alphabet Σ. A *language* is a subset of Σ^*. Recall that a field of sets is a set of sets closed under union and complementation relative to its union. We define a *regular algebra of languages* to be a set of languages closed under union, concatenation, and reflexive transitive closure. A *finitary-linguistic dynamic algebra* over a given alphabet is an algebra consisting of a field of languages (with complementation being relative to Σ^*), a regular algebra of languages, and the operation of concatenation, all languages being over the given alphabet. Every finitary-linguistic dynamic algebra is a dynamic algebra.

In connection with programs Σ may be considered to be the vocabulary of commands the computer can issue. A program is then a set of command sequences. There seems to be no natural interpretation of propositions in this setting.

Σ^ω denotes the set of infinite-to-the-right strings over Σ. A *linguistic dynamic algebra* differs from a finitary one in that B,R are sets of *infinitary* languages (subsets of $\Sigma^* \cup \Sigma^\omega$). Every linguistic dynamic algebra is a dynamic algebra.

With some thought the reader may verify that $a^*(ap \wedge ap')' = 1$ is an identity of finitary-linguistic dynamic algebras but not of linguistic dynamic algebras, and hence not of dynamic algebras.

Every finite Kripke structure is a homomorphic image of a linguistic dynamic algebra (see [25] for a proof). It follows from this and the results below that the Boolean equational theory of linguistic dynamic algebras coincides with that of dynamic algebras.

An application of linguistic dynamic algebras is to Pnueli's tense-logic treatment of non-terminating processes [19]. Though no semantics is proposed in [19], Pnueli has suggested elsewhere [20] that the semantics of propositions be a set of sequences, with ; being defined as concatenation.

Example 5: Flowchart Algebras. Let $\mathscr{D} = (\mathscr{B}\ \mathscr{R}\ \Diamond)$ be a separable dynamic algebra, and let V be a finite set of *dimensions*. Take $\mathscr{B}'$ to be the direct power $\mathscr{B}^V$, whose elements are Boolean vectors that combine pointwise under $\vee$ and $'$, using the corresponding operations of $\mathscr{B}$.

A *regular matrix* is a function $a:V^2 \to R$. Regular matrices combine pointwise under $\cup$ using the corresponding operation of $\mathscr{R}$. They are multiplied in the usual way for matrices, taking $\cup$ and ; from $\mathscr{R}$ as the exterior and interior operations respectively. When a is a 1×1 matrix ($|V| = 1$) with sole element $b \in R$, a^* is the 1×1 matrix with sole element b^*. When V can be partitioned into two non-empty subsets V_1, V_2, inducing a corresponding partition of a as the block matrix

$$\begin{pmatrix} A & B \\ D & C \end{pmatrix}$$

then, following Conway [7], a^* is taken to be the matrix

$$\begin{pmatrix} (A^*BC^*D)^*A^* & (A^*BC^*D)^*A^*BC^* \\ (C^*DA^*B)^*C^*DA^* & (C^*DA^*B)^*C^* \end{pmatrix}$$

Separability is used to ensure that this definition of a^* does not depend on the choice of partition of V.

A set of such matrices closed under these three operations forms an algebra $\mathscr{R}'$. The operation $\diamond'$ multiplies matrices by vectors in the usual way, with the $\vee$ of $\mathscr{B}$ as the exterior operation and the ; of $\mathscr{R}$ as the interior. The algebra $(\mathscr{B}'\ \mathscr{R}'\ \diamond')$ we call a *flowchart algebra.*

Every flowchart algebra is a dynamic algebra.

Flowchart algebras supply a natural solution to the problem of treating programs algebraically. The traditional method is via "elimination of goto's," using various program transformations that non-trivially manipulate the structure of the original program. Flowchart algebras permit an algebraic treatment of the original "goto-laden" program. The set V supplies vertices for a graph; each Boolean vector gives a possible labelling of the vertices with facts from $\mathscr{B}$, while each matrix defines a labelling of the edges of the graph with programs from $\mathscr{R}$.

In this formulation the vertex labels are the complements of the formulas used in the programming milieu to annotate flowcharts as described in [10], the complement being attributable to our use of $\diamond$ as "possible" where programming custom calls for the dual "necessary." Axiom 5b in this setting amounts to the so-called "Floyd induction" principle; the reader familiar with [10] will find the axiom more recognizable if the contrapositive is taken and p replaced by p' (as just mentioned) to yield $p \wedge [a^*](p \supset [a]p) \leqslant [a^*]p$, where $[a]p$ abbreviates $(ap')'$ and $p \supset q$ abbreviates $p' \vee q$.

Example 6: A non-standard dynamic algebra. This example shows that there exist dynamic algebras in which $a^*p = \vee\{a^i p | i \geq 0\}$ fails. Let $\mathscr{B}$ be the power set algebra of $N \cup \{\infty\} = \{0,1,2,\ldots,\infty\}$ and let $\mathscr{D}$ be the full dynamic algebra on $\mathscr{B}$, a specialization of Example 1. Now let a be the function mapping $p \subseteq N \cup \{\infty\}$ to $\{n+1 | n \in p\} \cup \{\infty | p \text{ is infinite}\}$. That is, a(p) forms the set of successors of the elements of p (with $\infty+1$ defined as ∞) together with ∞ when p is infinite. Observe that a is strict and finitely additive but not continuous and so not completely additive. Then $\vee\{a^i\{0\} | i \geq 0\} = N$, while $\min(a^!\{0\}) = N \cup \{\infty\}$.

Kozen [17] calls a dynamic algebra **-continuous* when it satisfies $a^*p = \vee\{a^i p | i \geq 0\}$. His definition of a dynamic algebra includes *-continuity as a requirement, along with conditions on $\mathscr{R}$ axiomatizing it as a regular *-continuous algebra, in place of Segerberg's 5a,b (which then becomes a theorem). Let us call this class *C (for *-continuous). Example 6 contradicts $S \subseteq {}^*C$.

It can be shown that $K \subseteq {}^*C$, whence not all dynamic algebras are isomorphic to Kripke structures. Kozen has asked whether every *-continuous dynamic algebra is isomorphic to a Kripke structure.

One might ask whether *C forms a variety. Now $S \subseteq VK$ (the variety generated[8] by K), as we show later. But since $K \subseteq {}^*C$, $VK \subseteq V{}^*C$, whence $S \subseteq V{}^*C$. Example 6 is in S but not in *C, whence *C is not a variety.

The last two examples are not examples of dynamic algebras so much as examples of their behavior under various operations.

Example 7: Loss of separability under homomorphisms and subalgebras. Let $\mathscr{D} = ((\{0,P,P',1\} \vee {}' 0) (\{A,B\} \cup ; *) \Diamond)$ such that $BP = 1$, $Ap = Bp = p$ otherwise, and such that $\mathscr{D}$ is a dynamic algebra (whence $\cup$; * are determined.) Let $h: \mathscr{D} \to \mathscr{D}$ satisfy $h(P') = h(0) = 0$, $h(P) = h(1) = 1$, $h(A) = A$, $h(B) = B$, a homomorphism as the reader may verify. The homomorphic image $h(\mathscr{D})$ is not separable. Furthermore $h(\mathscr{D})$ is also a subalgebra of $\mathscr{D}$. Hence S is closed under neither homomorphisms nor subalgebras. That separability is expressible with a Horn sentence ensures that S is closed under direct products.

Example 8: Effect of homomorphisms on the regular component of a separable dynamic algebra. It may have occurred to the reader that the class of regular components of separable dynamic algebras might make a good candidate for the class of regular algebras, whatever they might be. This is discussed in more detail in the section on applications. Here we show non-preservation of this class under homomorphisms.

Let $\mathscr{B}$ be the power set algebra on the set of all finite strings on an arbitrary alphabet. Let $\mathscr{R}$ consist of those elements of B containing λ (the empty string), with $\cup$; * having their standard interpretations on languages. Let $\diamond$ be concatenation. Then $(\mathscr{B}\ \mathscr{R}\ \diamond)$ is a dynamic algebra, separable because $\{\lambda\} \in B$. Let $\mathscr{R}'$ be $(\{I,A,A^*\} \cup ; *)$ with $I \leqslant A \leqslant A^*$, asterates I,A*, I acting as multiplicative identity, AA = A, all remaining products equal to A*. This is not the regular component of any dynamic algebra because A is reflexive and transitive but not an asterate, contradicting Lemma 3.3. Define $h:\mathscr{R}\to\mathscr{R}'$ so that $\{\lambda\}$ goes to I, infinite sets to A*, finite sets to A, visibly a homomorphism. This establishes that the class of regular components of separable dynamic algebras is not preserved under homomorphisms. The example is Conway's [7,p.102], minus the element 0.

5. MAIN RESULT

The main result has two parts. The first part states that every free dynamic algebra is residually (separable-and-finite)-or-Boolean-trivial. The second part states that every free separable dynamic algebra is residually separable-and-finite. The first part is adequate for showing completeness of the Segerberg axiomatization of propositional dynamic logic, and the reader wishing to see only that result may skip the second part. The first part is however inadequate for the next application, that every free separable dynamic algebra is residually K (isomorphic to a subdirect product of Kripke structures), whence every separable dynamic algebra is a homomorphic image of such a subdirect product. This is a useful representation theorem for dynamic algebras, though not as strong as showing that every dynamic algebra is isomorphic to a Kripke structure, which Example 6 showed to be false for our notion of dynamic algebra.

We approach the main result via an abstract version of the modal logic technique of *filtration*, which in a Kripke structure setting is the process of dividing a Kripke model of a given formula p by an equivalence relation on its worlds to yield a finite Kripke model of p. Fischer and Ladner [9] showed that filtration could be made to work for propositional dynamic logic just as well as for modal logic. We extend their result to show that filtration does not depend on any special properties of Kripke structures but works for all dynamic algebras, even ones that are not *-continuous in Kozen's sense [17]. Our proof is little more than the abstract version of that of [9]. We attend first to some prerequisites.

The reader may wish to look at the account of generator sets and free algebras in Section 8. We let P,Q,...,A,B,...,X,Y,... range over the set of generators in B,R,BUR respectively, and write B_0,R_0,D_0 for the respective generator sets.

Lemma 5.1. The regular component of any subalgebra of a dynamic algebra $\mathscr{D} = (\mathscr{B}\ \mathscr{R}\ \Diamond)$ containing the regular generators of a generator set of $\mathscr{D}$ coincides with $\mathscr{R}$.

Proof. Left to the reader. ∎

The Boolean analogue of this Lemma is false; the Boolean generators generate only part of the Boolean component (consider AP etc.).

FL-sets. An FL-set is a Boolean subset F of a predynamic algebra such that

$$\begin{array}{llll} pvq & \in F & \to p,q & \in F \\ p' & \in F & \to p & \in F \\ ap & \in F & \to p & \in F \\ (a\cup b)p & \in F & \to ap, bp & \in F \\ (ab)p & \in F & \to a(bp) & \in F \\ a^*p & \in F & \to p, aa^*p & \in F. \end{array}$$

These rules form a generative system with source set[8] the Boolean elements of a free predynamic algebra; we call the associated closure operator *FL-closure*, FL(X).

Lemma 5.2. (Fischer-Ladner [9].) The FL-closure of a finite Boolean subset of a free predynamic algebra is finite.

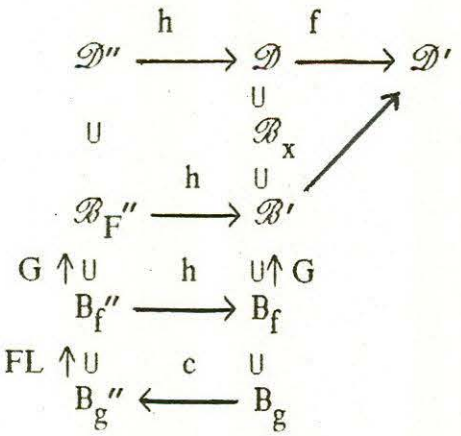
See [9] for a proof.

Filtration. We are now in a position to state and prove the central theorem of this paper, which asserts the existence of filtrations.

Theorem 5.3. Given an S-free[8] dynamic algebra $\mathscr{D} = (\mathscr{B}\ \mathscr{R}\ \Diamond)$ and a finite subset B_g of B, there exists a dynamic algebra $\mathscr{D}'$ and a homomorphism $f:\mathscr{D}\to\mathscr{D}'$ injective on B_g, with $f(\mathscr{D})$ separable and finite.

We call f a *filtration*, and $f(\mathscr{D})$ a *filtrate*, of B_g.

Proof. Our construction of $\mathscr{D}'$ and f from $\mathscr{D}$ and B_g proceeds via a series of steps given by the following diagram.



The components of the diagram are as follows. The arrows trace the order of construction, except for the top two arrows which represent homomorphisms. $\mathscr{D}$ and B_g are given. $\mathscr{D}''$ is a free predynamic algebra generated by the generators of $\mathscr{D}$ and $h:\mathscr{D}''\to\mathscr{D}$ is the homomorphism fixing those generators (whence h is onto). B_g'' is $c(B_g)$ where $c:B\to B''$ is a choice function satisfying $hc(p) = p$; c exists by the Axiom of Choice and because h is onto. (This use of ACh can be eliminated at the cost of a little more complication.) $B_f'' = FL(B_g'')$, finite by Lemma 5.2, and $\mathscr{B}_F'' = G(B_f'')$, the subalgebra generated by B_f''. $B_f = h(B_f'')$, finite because B_f'' is, and $\mathscr{B}' = h(\mathscr{B}_F'') = h(G(B_f'')) =^8 G(h(B_f''))$, finite because finitely generated Boolean algebras are finite. $\mathscr{D}'$ is the full, hence completely full, dynamic algebra on $\mathscr{B}'$ (see Example 1 above; thus $\mathscr{D}'$ is separable and finite). Since $\mathscr{B}'$ is a finite and hence complete sublattice of $\mathscr{B}$ it defines a closure operator[8] J on $\mathscr{B}$. The homomorphism f agrees with J on B_0 (the Boolean generators of $\mathscr{D}$) and maps each regular generator A to "JA", the function on B′ that takes p to J(Ap), which the reader may verify is strict and finitely additive and so in R′. Such an f exists since $\mathscr{D}$ is S-free. $\mathscr{B}_x$ is the set of all fixed points of f, a Boolean subalgebra of $\mathscr{B}$ as it happens.

The one inclusion shown in the diagram that requires verification is $\mathscr{B}' \subseteq \mathscr{B}_x$.

Claim (i). For all $a \in R''$ and $p \in B'$, $fh(a)p \geqslant h(a)p$.
Claim (ii). For all $ar \in B_F''$, $fh(a)h(r) = h(a)h(r)$.

We prove these claims by induction on R″, proving (i) explicitly. For (ii) replace $\geqslant$ by = and p by h(r) uniformly in the proof of (i). (We need h(r) rather than p in (ii) to make use of B_F'' being an FL-set.) We write α,β for h(a),h(b). Superscripts on = and $\geqslant$ refer to notes below; the notes

specify whether they are for Claim (i) or (ii) or both. Lemma 5.1 justifies confining the induction to R".

$fh(A)p = \wedge\{q \in B' | q \geqslant h(A)p\} \geqslant h(A)p.$
$fh(a \cup b)p = (f(\alpha) \cup f(\beta))p = f(\alpha)p \vee f(\beta)p \geqslant^1 \alpha p \vee \beta p = h(a \cup b)p.$
$fh(ab)p = f(\alpha)f(\beta)p \geqslant^2 \alpha\beta p = h(ab)p.$
$fh(a^*)p = f(\alpha)^*p = \min(f(\alpha)!_{B'}p) \geqslant^3 \min(\alpha!_{B'}p) \geqslant^4 \min(\alpha!_B p) = h(a^*)p.$

Notes.
1. (ii) $(a \cup b)r \in B_F'' \to ar, br \in B_F''$, B_F'' being FL-closed.
2. (ii) Similarly $(ab)r \in B_F'' \to a(br), br \in B_F''$.
3. (i) Since $f(\alpha)q \geqslant \alpha q$ for all q by induction, $f(\alpha)!_{B'}p \subseteq \alpha!_{B'}p$.
   (ii) $a^*r \in B_F'' \to a(a^*r) \in B_F''$, so $f(\alpha)\alpha^*p = \alpha\alpha^*p$ by induction, so
   $\alpha^*p \in f(\alpha)!_{B'}p$, so $\min(f(\alpha)!_{B'}p) \leqslant \alpha^*p = \min(\alpha!_{B'}p)$, so
   = by 3(i).
4. (i) Since $B' \subseteq B$, $\alpha!_{B'}p \subseteq \alpha!_B p$.
   (ii) Since $\alpha^*p \in B'$, $\alpha^*p \in \alpha!_{B'}p$, so $\min(\alpha!_{B'}p) \leqslant \alpha^*p = \min(\alpha!_B p)$.

Claim (iii). For all $r \in B_F''$, $fh(r) = h(r)$.

We proceed by structural induction on B_F''.

$fh(P) = h(P)$ (construction of f on generators, $P \in B_F''$, h preserves generators).
$fh(p \vee q) = fh(p) \vee fh(q) = h(p) \vee h(q) = h(p \vee q).$
$fh(p') = fh(p)' = h(p)' = h(p').$
$fh(ap) = fh(a)fh(p) = fh(a)h(p) = h(a)h(p)$ (by (ii)) $= h(ap).$

We infer that $\mathscr{B}' = h(\mathscr{B}_F'') \subseteq \mathscr{B}_X$. This completes the defense of the diagram, establishing that $\mathscr{D}'$ is finite and separable, and f fixes B_g. Clearly $f(\mathscr{D})$ is finite. To see that $f(\mathscr{D})$ is separable it suffices to observe that the Boolean component of $f(\mathscr{D})$ is $\mathscr{B}'$ since $\mathscr{B}' \subseteq \mathscr{B}_X$; in fact $\mathscr{B}' = \mathscr{B}_X$ as it happens. The regular component of $f(\mathscr{D})$ may be smaller than that of $\mathscr{D}'$, but that will not compromise separability. ∎

We now give the first part of the main result.

Theorem 5.4. (Main result, first part.) Every free dynamic algebra $\mathscr{D}$ is residually (separable-and-finite)-or-Boolean-trivial.

Proof. Take the separating set of congruences to consist of the kernels of the filtrations of the doubletons of $\mathscr{D}$, together with the congruence relation that is the complete relation on the Booleans and the identity relation on the regular elements. The filtration kernels separate the Booleans while the other relation separates the regular elements, so this is a separating set of

congruences. The corresponding quotients are either separable and finite (Theorem 5.3) or Boolean-trivial in the case of the congruence that is the complete relation on the Booleans. ∎

It can be shown that every full dynamic algebra is *simple*, that is, admits only the identity congruence and the complete congruence. Kozen has pointed out to us that this implies that Theorem 5.4 cannot be strengthened by omitting "free," simplicity being an even stronger condition than that of being subdirectly irreducible.

The reader may at this point wish to skip the second part of the main result and go the next section, where the Segerberg completeness result is proved without depending on the second part. The second part is of interest in that it supplies a situation when the Boolean-trivial factor of the first part may be omitted.

Theorem 5.5. (Main result, second part.) Every free separable dynamic algebra is residually separable-and-finite.

Proof. Take the kernels of the filtrations of the doubletons of $\mathscr{D}$ as for Theorem 5.4, possible because free separable dynamic algebras are S-free. This set separates the Booleans. It also separates $a \neq b$, since by separability there exists p such that $ap \neq bp$, whence $ap \not\equiv bp$ for some congruence, so $a \not\equiv b$ for that congruence. Hence the kernels form a separating set. The corresponding quotients are separable and finite by Theorem 5.3. ∎

For this theorem to be of any use, free separable dynamic algebras must exist. As Example 7 shows, S is not a variety and hence not a guaranteed source of free algebras. However VS, the variety generated by S, does have free algebras, which we can show supply the necessary free separable dynamic algebras.

Lemma 5.6. Every free VS-algebra having at least one Boolean generator is separable.

Proof. Let $\mathscr{D}$ be a free VS-algebra. If $a \neq b$ in $\mathscr{D}$ then there exists $\mathscr{D}'$ in S and a homomorphism $h:\mathscr{D}\to\mathscr{D}'$ which maps a,b to distinct elements[8]. Since $\mathscr{D}'$ is separable there must exist $p \in B'$ such that $h(a)p \neq h(b)p$. If we take $g:\mathscr{D}\to\mathscr{D}'$ to be a homomorphism agreeing with h on the generators of $\mathscr{K}$ and satisfying $g(P) = p$, we have $g(aP) = g(a)g(P) = h(a)p \neq h(b)p = g(b)g(P) = g(bP)$, whence $aP \neq bP$. Hence $\mathscr{D}$ is separable. ∎

We do not know whether this Lemma holds when there are no Boolean generators. Fortunately for our application all we need are free algebras with *at least* a given number of generators.

6. APPLICATIONS

The first application uses the first part of the main result to show the completeness of the Segerberg axiomatization of propositional dynamic logic. Completeness of this system, as with other modal logics, is traditionally measured with respect to Kripke structures. In the program logic application this is because of the satisfactory way in which Kripke structures model computation, as discussed in Example 2. We first prove an easy result about finite Kripke structures.

Theorem 6.1. Every finite separable dynamic algebra is isomorphic to a (finite) Kripke structure.

Proof. Let $\mathscr{D} = (\mathscr{B}\ \mathscr{R}\ \Diamond)$ be a separable finite dynamic algebra. Then by the fact that every finite Boolean algebra is isomorphic to the power set algebra of its atoms, and by separability, $\mathscr{D}$ is isomorphic to a subalgebra of the full (hence completely full by finiteness of $\mathscr{B}$) dynamic algebra on the power set algebra of the atoms of $\mathscr{B}$, which is by definition a Kripke structure. ∎

Let K^+ be the class of Kripke structures together with the class of Boolean-trivial dynamic algebras, that is, dynamic algebras with one Boolean element, and let Da be the class of dynamic algebras. Recall that VC is the variety generated[8] by class C.

Theorem 6.2. $Da = VK^+$.

Proof. Certainly $K \subseteq Da$, and trivially the Boolean-trivial algebras are too, so since Da is a variety, $VK^+ \subseteq Da$. Conversely, by Theorems 5.4 and 6.1 every free dynamic algebra is in VK^+, whence so is every dynamic algebra, being a homomorphic image of some free dynamic algebra. ∎

Although K^+ is a bigger class than K its Boolean theory cannot be decreased since the Boolean theory of Boolean-trivial algebras must include all Boolean identities holding in K. Thus Theorem 6.2 supplies an algebraic form of the Segerberg-Parikh completeness result for propositional dynamic logic. The connection with the Hilbert-style form of Segerberg's axiom system is easily made along the lines one would use to translate identities of Boolean algebra into their corresponding Hilbert-style axioms.

There are two unsatisfactory aspects to Theorem 6.2. First, K^+ is somewhat artificial compared with K. Second, the regular theory of K^+ is trivial (has only identities x=x) since the regular theory of Boolean-trivial dynamic algebras is trivial, whereas the regular theory of K is quite rich. The following shows just how rich it is.

Theorem 6.3. The projection of K on its regular coordinate (i.e. the class of regular components of Kripke structures) is the class of regular algebras of binary relations.

Proof. The former is certainly included in the latter. Conversely, any regular algebra of binary relations on a set W is the regular component of a subalgebra of the full dynamic algebra on W, a Kripke structure. ∎

Hence the regular theory of K is the theory of regular algebras of binary relations. Thus a connection with K would be much more rewarding than the connection with K^+. The axiom of separability supplies exactly that connection inasmuch as it supplies the missing regular theory, as the following shows.

Theorem 6.4. VS = VK.

Proof. Since K is the closure under subalgebras of full Kripke structures, which are separable, we have VK ⊆ VS. Since free algebras in S are residually separable-and-finite, they are residually K by Theorem 6.1. Furthermore every separable dynamic algebra is a homomorphic image of some free separable dynamic algebra by Lemma 5.6, so VS ⊆ VK. ∎

Combining Theorems 6.2 and 6.4 we infer that VS may be defined axiomatically by the dynamic algebra axioms together with an appropriate set of axioms for binary relations. There is unfortunately no finite equational axiomatization of the latter [26], though the dynamic algebra axioms plus the axiom of separability comes to within a quantifier of one. The system of Salomaa [27] comes similarly close, to within a nonstandard inference rule.

Regular Algebras. Is there such a thing as a regular algebra? Unlike such satisfactorily defined classes as groups, rings, lattices, Boolean algebras, and even dynamic algebras, regular algebras have an identity problem: there is no agreed-on definition of a regular algebra. Moreover, a monograph by J.H. Conway [7] gives some insight as to why.

Conway exhibits five classes of algebras of type (R ∪ ; * 0 1), called *X-Kleene algebras* for X ranging over S,N,R,C,A, in order of strictly increasing size. We immediately rename S to T to avoid conflict with our S;

his S stood for Standard. T appears to consist of complete lattices under U in which ; is associative and distributes over all joins, and $a^* = \vee\{a^i|i\geq 0\}$. Furthermore, 0 and 1 are additive and multiplicative identities respectively. N (Normal) is HT and R (Regular) is VT, where HT is the hereditary closure (closure under subalgebras) of T and VT is the variety generated by T (closure under subalgebras and homomorphisms - T is already closed under direct products). C is a variety strictly larger than VT axiomatized by a finite set of axioms together with $a^* = (a^n)^*a^{<n}$, essentially Kleene's axiom schema (11) of 7.2 [16]. A (Acyclic) is a finitely axiomatized variety whose significance is not apparent to us; it is Kleene's system less the infinite schema.

Kozen [17] has proposed a definition of regular algebra, of the same similarity type as Conway's, as a semilattice under U in which ; is associative and distributes over finite joins and over $\vee\{a^i|i\geq 0\}$, the latter, defined as a^*, being the only infinite join required to exist. Let us call this the class Z.

Theorem 6.4 suggests that the regular components of separable dynamic algebras might constitute an interesting class of regular algebras. Let $\mathscr{R}$ = ($\{0,2,1\}$ U ; *) where $0 \leqslant 2 \leqslant 1$ (defining U), 1 is the only asterate, and ; is integer multiplication modulo 4 (so 2;2 = 0). This is Conway's third example of a T-algebra on p. 101 of [7]. However Kozen has pointed out to us that in any separable dynamic algebra, if $a \leqslant I$ (where Ip = p for all p), aa = a. Thus $\mathscr{R}$ is not the regular component of any separable dynamic algebra.

It is the case that every regular algebra of binary relations is the regular component of a separable dynamic algebra, namely a subalgebra of a full Kripke structure where all the Boolean elements are retained (to maintain separability). Furthermore every regular algebra of languages on the alphabet Σ is isomorphic to a regular algebra of binary relations; the isomorphism maps the language L to $\{(u,uv)|u\in\Sigma^*, v\in L\}$. Hence the regular components of separable dynamic algebras include all regular algebras of binary relations and of languages. Since these are of central importance in the theory of regular algebras we might be forgiven for excluding apparent oddities such as the example immediately above.

To do so however would be to exclude some well-motivated algebras. Kozen has pointed out to us that (N min + K0) is such an algebra, where N = $\{0,1,2,\ldots\}$, min(9,5) = 5 etc., and K0 is the constantly zero function. This algebra is of central importance in the computation of minimal cost routes in networks; given a *choice* of routes one wants the cheaper of the two, whence min; the cost of a *sequence* of two routes is the sum of their costs, whence +; and the cheapest way to travel a route an arbitrary number of times is not to venture forth even once, whence K0.

To avoid excluding such algebras we propose to relax axiom 2b of the dynamic algebra conditions to:

2i. $ap \leqslant a(p \vee q)$.

We call such algebras *isodynamic*; every dynamic algebra is an isodynamic algebra as is easily verified. To see that the converse does not hold, let $\mathscr{B}$ have elements $0,P,P',1$ and let A be the function on B mapping P' to P and fixing everything else. A is isotonic but not finitely additive. Take $\mathscr{R}$ to be $(\{A,A^*\} \cup ; *)$ where A^* maps P' to 1 and fixes everything else, with $\cup$ pointwise disjunction and ; composition. Take $\diamond$ to be application. Then $(\mathscr{B}\ \mathscr{R}\ \diamond)$ is an isodynamic algebra, as may be verified by calculation.

A more interesting example takes $\mathscr{B}$ to be the power set algebra on N and $\mathscr{R}$ to contain for each $i \geqslant 0$ the function A^i on 2^N that removes the least i elements from its argument. These functions can be seen to be isotonic but not finitely additive. Define $A^i \cup A^j = A^{\min(i,j)}$, $A^i;A^j = A^{i+j}$, and $A^{i*} = A^0$. Taking $\diamond$ to be application, it can be verified that $(\mathscr{B}\ \mathscr{R}\ \diamond)$ is a separable isodynamic algebra whose regular component is isomorphic to the above-mentioned (N min + K0) algebra.

One would hope that Example 1 generalizes in the obvious way to isodynamic algebras. Suppose it did. Consider the full isodynamic algebra on $\{0,1,2\}$, with of course $a^*p = \min(a!p)$. Lemma 4.3 works for isotonic functions so there is no question about $\cup$; and * being defined. Now let us write p as $\Sigma_{i \in p} 2^i$, e.g. $\{1,2\}$ is written as 6. Let A be some isotonic function such that $A1 = A2 = 2$, $A3 = A5 = 7$. Then $A!1 = \{7\}$ and $2 \in A!2$, so $A^*1 = \min(A!1) = 7$ and $A^*2 = \min(A!2) = 2$. But $1 \vee A^*(1' \wedge A1) = 1 \vee A^*(6 \wedge 2) = 1 \vee A^*2 = 1 \vee 2 = 3$, contradicting axiom 5b. Thus "full isodynamic algebras" are not isodynamic and so Example 1 does not generalize. Incidentally this shows why isotonicity is inadequate for the $\leftarrow$ direction of Lemma 3.1; if this direction worked with isotonicity the remaining arguments leading up to Example 1 would all go through for full isodynamic algebras. We do not at present have any nice characterization of which isotonic functions on a complete Boolean algebra satisfy axiom 5b under the min(a!p) interpretation of a^*p.

We now exhibit a regular component of a separable isodynamic algebra which is not in VT. Let P generate a four element Boolean algebra $\mathscr{B}$, and take A to be the function on B mapping P to P' and fixing the rest of B. Take I to be the identity function on B. Then $A(A \cup I)P = 1$ but $AAP = AIP = P'$ so $A(A \cup I)P \neq (AA \cup AI)P$. Hence $A(A \cup I) \neq AA \cup AI$, contradicting a law of VT. The closest we can come to this law is $ab \cup ac \leqslant a(b \cup c)$. However $(a \cup b)c = ac \cup bc$ holds. Note also that Theorem 3.4 holds, so * is reflexive transitive closure in a separable isodynamic algebra.

With the above in mind we identify the class of regular components of separable isodynamic algebras as an interesting class of regular algebras.

7. LOOSE ENDS

Complexity. The set of valid formulas of propositional dynamic logic has been shown to be complete in deterministic exponential time, the lower bound appearing in [9], the upper bound in [22]. (A simpler proof of the upper bound appears in [25].) The intimate connection between that theory and the equational theory of dynamic algebras establishes the same complexity result for the latter. The theory of separable dynamic algebras has the same complexity since its theorems are those of dynamic algebras together with a=b if and only if aP=bP (P any propositional variable) is a theorem.

Origin. The origin of dynamic algebra is in dynamic logic ([21], see also [23]), whose origin is in turn in modal logic. It is rather surprising that the calculus of binary relations was not incorporated into the Kripke semantics of modal logic earlier. As pointed out at the end of [9], the classical modal logics K, T, S3, S4, and S5 are all special cases of dynamic logic (S5 requires converse), so that decidability of satisfiability for each of these logics follows from the procedure given in [9] for propositional dynamic logic. Closely related logics, all addressed specifically at programming, are those of Hoare [14], Salwicki [29], Dijkstra [8], and Constable [6]. Example 4 makes a connection with the logic of Floyd [10].

Terminology. We had originally called dynamic algebras Hoare algebras, after [14], which contains a Gentzen-like form of the dynamic logic theorems given in [21] and extended by Segerberg to a propositionally complete system. We adopted Kozen's term "dynamic algebra" after seeing [17]. Some time later we realized that Kozen's definition of a dynamic algebra was strictly stronger than ours because of its assumptions about continuity; we have yet to resolve this terminological conflict. The term "separable" is also Kozen's, as is the analogy of dynamic algebras to modules with regular elements acting as "scalars."

There is a close similarity between the axioms for dynamic algebras and those for modules. One might call a dynamic algebra a *Boolean semimodule with* * (cf. [28] which employs a concept of semimodule, though neither Boolean nor having *).

Open Problems. We mention again Kozen's problem, is every *-continuous dynamic algebra isomorphic to a Kripke structure?

We have treated neither tests, p?, nor converse, a^-. Converse formalizes the idea of running a program in reverse, and was studied in this context in [1]. See [18] for a complete axiomatization of converse (essentially $a(a^-p)' \wedge p = 0$ and $a^-(ap)' \wedge p = 0$). Is there an algebraic analogue of our Lemma 3.1 for converse?

What is the axiom rank and base rank [5,p.173] for dynamic algebras? The axiom rank is at most 3 since the Segerberg axiomatization only requires 3 variables in each axiom.

What reasonable axioms are there for regular $'$ in dynamic algebra? We propose the term "complemented dynamic algebra" for a dynamic algebra expanded by adding regular complement.

A related question that the reader may find better defined deals with the problem of recognizing identities for the complemented linguistic dynamic algebras $((2^L \vee ')\ (2^L \cup\ ;\ *\ ')\ \Diamond)$ where $L = S^* \cup S^\omega$ and S is an arbitrary alphabet. Is this problem even decidable?

8. BACKGROUND

A grasp of the ideas in one of [3,5,11] is more than sufficient preparation for this paper. The following first aid may prove convenient for the reader comfortable with the definitions of subalgebra, homomorphism, direct product, lattice, and Boolean algebra.

Minor Points. We use *poset* for partially ordered set and *join* and *meet* for least upper bound $\vee S$ and greatest lower bound $\wedge S$ of a subset S of a poset. Note that $\vee\varphi$ exists just when $\mathcal{B}$ contains a least element, as it does when it is a Boolean algebra. A directed set is a non-empty set which contains upper bounds on each of its finite subsets. A *complete sublattice* of a poset P contains all its meets and joins as defined in P. The *power set algebra* on the set X is a complete Boolean algebra consisting of all subsets of the set X. A *field of sets* is any subalgebra of a power set algebra, necessarily Boolean, not necessarily complete or atomic; conversely every Boolean algebra is isomorphic to a field of sets [31]. Being complete and being atomic are independent for infinite Boolean algebras and both true for finite ones.

Heterogeneous Algebras. As is shown in [4], all of the following carries through for heterogeneous algebras of the sort used here, in our case having up to two carriers B and R and up to eight operations, $\vee\ '\ 0\ \cup\ ;\ *\ \Diamond\ ?$, of various types. Direct products and homomorphisms respect type in the heterogeneous case; one would not find a Boolean element paired with a regular in a direct product, nor a homomorphism mapping a Boolean element to a regular.

Closure Operators. A *closure operator* on a poset P is an isotonic reflexive idempotent function f on P; that is, $x \leqslant y$ implies $fx \leqslant fy$, $x \leqslant fx$, and $ffx = fx$. A *closure system* on a poset is the set of fixed points of some closure operator. Every complete sublattice L of a poset P is a closure system with associated closure operator $J(x) = \wedge\{y \in L | x \leqslant y\}$. P itself need not form a complete lattice, though it must have a greatest element, which will appear in every complete sublattice as $\wedge\varphi$. When P *is* a complete lattice, every closure system of P is a complete sublattice of P.

Generative Systems. A system of rules of the form, "if u is in the set then so are v,w,...," is called a *generative system.* The set of all subsets of a given *source set* each meeting all the rules is clearly closed under intersection and so forms a closure system. Hence associated with any generative system and source set is a closure operator on the power set of the source set.

Generator Sets. The set of subalgebras of an algebra $\mathscr{A}$ is closed under intersection and so forms a closure system. The associated closure operator G yields for each subset X of A the subalgebra G(X) *generated by* X. X is called a *generating set* of G(X), and the elements of X are called *generators.* A useful property of G is that it commutes with homomorphisms; $h(G(X)) = G(h(X))$ for any subset X of A and homomorphism h from $\mathscr{A}$.

Free Algebras. Given a class C of similar algebras, an algebra $\mathscr{A}$ of the same similarity type, not necessarily in C, is *C-free* when it contains a generating set A_0 such that any function from A_0 to an algebra in C extends to a homomorphism, necessarily uniquely by the previous paragraphs. When such an $\mathscr{A}$ is in C we call $\mathscr{A}$ a *free C-algebra.* (The standard notion of "free" is the latter; we need the former, C-free, for Theorem 5.3.)

Any non-trivial class closed under subalgebras and direct products has free algebras [5,p.138].

Varieties. A class of similar algebras closed under subalgebras, direct products, and homomorphisms is called a *variety*; equivalently [2], a variety is any class defined by a (possibly infinite) set of equational identities. Thus Boolean and dynamic algebras form varieties, being defined purely by equational identities.

The class of all varieties of a similarity type is closed under arbitrary intersection (take the variety defined by the union of their theories) and so form a closure system, so that the variety generated by any class of similar algebras always exists. We write VC for the variety generated by class C. If $a \neq b$ in any free algebra $\mathscr{A}$ of VC then there exists an algebra

$\mathcal{A}'$ of C and a homomorphism $h:\mathcal{A}\to\mathcal{A}'$ for which $h(a) \neq h(b)$. (This is because any law of C algebras must be a law of VC algebras.)

A set of congruences on an algebra $\mathcal{A}$ is called *separating* when no two elements of $\mathcal{A}$ are related in every congruence. $\mathcal{A}$ is *residually P*, P being some property of algebras, when $\mathcal{A}/\equiv$ is P for each congruence $\equiv$ in some separating set of congruences on $\mathcal{A}$.

If $\mathcal{A}$ is residually P then $\mathcal{A}$ is isomorphic to a substructure of a direct product of P algebras, which themselves are homomorphic images of $\mathcal{A}$ (the natural homomorphism onto the quotient). Substructures of direct products obtained in this way from separating sets of congruences are called *subdirect products*. Thus given a class C of residually P algebras it follows easily that $VC = V(P \cap HC)$ where VC is the variety generated by C and $HC \subseteq VC$ is the class of homomorphic images of C.

As varieties are closed under subalgebras and direct products they have free algebras. Lemma 5.8 shows that free separable dynamic algebras with at least one Boolean generator exist.

Letting S denote the class of separable dynamic algebras, we point out that both free dynamic algebras and free separable dynamic algebras are S-free, an essential aspect of Theorem 5.3. Note that there are no non-trivial separable free dynamic algebras; the adjectives do not commute!

Deductive Systems. It is a well-publicized fact that the pure predicate calculus has a deductive system that is complete in the sense that it can be used to prove from a set Γ of first-order formulas, the *non-logical axioms*, any first-order formula valid in the axiomatic class consisting of all models of Γ. Less well-publicized is the fact that the rules permitted for manipulating equations in high school algebra is complete in the same sense, with pure equations in place of first-order formulae and varieties in place of axiomatic classes. The rules invariably include implicitly those in the following system, whose only logical axiom is X=X for some variable X.

Symmetry: $x=y \to y=x$.
Transitivity: $x=y, y=z \to x=z$.
Replacement $x_1=y_1, \ldots, x_n=y_n \to f(x_1,\ldots,x_n)=f(y_1,\ldots,y_n)$ for any n-ary f.
Substitution $(s(X)=t(X) \to s(y)=t(y)$ for any variable X and term y).

These rules form a generative system with source set pairs of elements of a word algebra, and the associated closure operator is called deductive closure. The system is complete in the sense that the deductive closure of a set of axioms coincides with the set of equations holding identically in the

variety defined by the axioms. The proof is easier than for the first-order case, see e.g. [13].

The significance of this fact for us is that we need not get involved in the details of deductive closure since this is now all taken care of for us. Our only obligation is to ensure that any given system of axioms really does define the same variety as that generated by the class of models we are interested in.

Acknowledgments. D. Kozen was a most helpful source of ideas and pointers into the literature. J. Halpern provided many helpful comments on an early draft of the paper.

9. BIBLIOGRAPHY

[1] de Bakker, J.W., and W.P. de Roever., A calculus for recursive program schemes, In *Automata, Languages and Programming* (ed. Nivat), 167-196 North Holland, 1972.

[2] Birkhoff, G., On the Structure of Abstract Algebras, Proc. Camb. Phil. Soc. *31*, 433-454, 1935.

[3] Birkhoff, G., *Lattice Theory*, AMS Coll. Pub. *25* (Am. Math. Soc., Providence, RI), 1948.

[4] Birkhoff, G. and J.D. Lipson, Heterogeneous Algebras, J. of Combinatorial Theory, *8*, 115-133, 1970.

[5] Cohn, P.M., *Universal Algebra*, Harper and Row, New York, 1965.

[6] Constable, R.L., On the Theory of Programming Logics, Proc. 9th Ann. ACM Symp. on Theory of Computing, 269-285, Boulder, Col., May 1977.

[7] Conway, J.H., *Regular Algebra and Finite Machines*, Chapman and Hall, London, 1971.

[8] Dijkstra, E.W., *A Discipline of Programming*. Prentice-Hall. 1976

[9] Fischer, M.J. and R.E. Ladner., Propositional Modal Logic of Programs, Proc. 9th Ann. ACM Symp. on Theory of Computing, 286-294, Boulder, Col., May 1977.

[10] Floyd, R.W., *Assigning Meanings to Programs*, In *Mathematical Aspects of Computer Science* (ed. J.T. Schwartz), 19-32, 1967.

[11] Graetzer, *Universal Algebra*, Van Nostrand, Princeton, NJ, 1968.

[12] Halmos, P.R., *Algebraic Logic*, Chelsea, New York, 1962.

[13] Henkin, L., The Logic of Equality, AMM *84*, 8, 597-612, Oct. 1977.

[14] Hoare, C.A.R., An Axiomatic Basis for Computer Programming, Comm. of the ACM *12*, 576-580, 1969.

[15] Horn, A., On Sentences which are True of Direct Unions of Algebras, JSL *16*, 14-21.

[16] Kleene, S.C., Representation of Events in Nerve Nets, in *Automata Studies*, (eds. Shannon, C.E. and J. McCarthy), 3-40, Princeton University Press, Princeton, NJ, 1956.

[17] Kozen, D. A Representation Theorem for Models of *-free PDL, Manuscript, May 1979.

[18] Parikh, R., A Completeness Result for PDL, Symposium on Mathematical Foundations of Computer Science, Zakopane, Warsaw, Sept. 1978.

[19] Pnueli, A., The Temporal Logic of Programs, 18th IEEE Symposium on Foundations of Computer Science, 46-57. Oct. 1977.

[20] Pnueli, A., Correctness of Concurrent Programs: The Temporal Logic Approach, Unpublished talk, NSF-CBMS Conference on the Logic of Computer Programming, Troy, NY. June 1978.

[21] Pratt, V.R., Semantical Considerations on Floyd-Hoare Logic, Proc. 17th Ann. IEEE Symp. on Foundations of Comp. Sci., 109-121. Oct. 1976.

[22] Pratt, V.R., A Near Optimal Method for Reasoning About Action, MIT/LCS/TM-113, M.I.T., Sept. 1978.

[23] Pratt, V.R., Applications of Modal Logic to Programming, to appear in *Studia Logica.*

[24] Pratt, V.R., Process Logic, Proc. 6th Ann. ACM Symp. on Principles of Programming Languages, Jan. 1979.

[25] Pratt, V.R., Models of Program Logics, Proc. 20th IEEE Conference on Foundations of Computer Science, Oct. 1979.

[26] Redko, V.N., On Defining Relations for the Algebra of Regular Events, (Russian), Ukrain. Mat. Z., *16*, 120-126, 1964.

[27] Salomaa, A., Two Complete Axiom Systems for the Algebra of Regular Events, J. of the ACM *13*, 158-169, 1966.

[28] Salomaa, A., and M. Soittola, *Automata-Theoretic Aspects of Formal Power Series*, Springer-Verlag, New York, 1978.

[29] Salwicki, A., Formalized Algorithmic Languages, Bull. Acad. Pol. Sci., Ser. Sci. Math. Astr. Phys. Vol. 18. No. 5. 1970.

[30] Segerberg, K., A Completeness Theorem in the Modal Logic of Programs, Preliminary report. Notices of the AMS, *24*, 6, A-552. Oct. 1977.

[31] Stone, M.H., The Theory of Representations for Boolean Algebras, Trans. of the Am. Math. Soc. *40*, 37-111, 1936.