Maximally Independent Sets, Minimal Generating Sets, and Irreducibles

by

BERNARD P. ZEIGLER*

Department of Computer and Communication Sciences
University of Michigan
Ann Arbor, Michigan 48104

1. Introduction. Cohn [2, p. 253] characterizes precisely the algebraic closure operators which give rise to transitive dependence relations as those enjoying the exchange property. His Lemma 2.2 shows that for such closure operators, maximally independent sets and minimal generating sets are the same concepts. (Using Zorn's Lemma, Theorem 2.4 states the consequence that bases exist and are all of the same cardinality.)

Cohn leaves unanswered the question for arbitrary closure operators as to the relation between minimal generating sets and maximally independent sets. This note answers this question by showing that a minimal generating set is maximally independent but provides a counterexample to show that maximally independent sets are not necessarily minimal generating sets. This result justifies the use of the exchange property to enforce the equivalence of the two concepts.

The motivation for considering this question arose by noticing a hole in a theorem by Wymore [5] concerning generating sets of inputs for dynamic systems. This problem is discussed in the last section of this note.

Another concept which appears often in algebraic theories (cf. especially the Krohn and Rhodes theory in [1, p. 41]) is that of irreducible elements. The connection between irreducible elements and generators seems not to have been made explicit. Here we also establish such a connection.

2. Generating Sets and Dependence Relations. I shall briefly review the key concepts given in Cohn [2].

A *closure operator* on a set S is a mapping $J: 2^S \to 2^S$ (2^S being the set of all subsets of S) which satisfies

(J.1) $X \subseteq Y \Rightarrow J(X) \subseteq J(Y)$
(J.2) $X \subseteq J(X)$
(J.3) $J \cdot J(X) = J(X)$

We shall say that X *generates* Y whenever $Y \subseteq J(X)$. We write X generates y (for $y \in S$) to mean X generates $\{y\}$.

* Work supported by National Science Foundation Grant No. GJ-29989X.

MATHEMATICAL SYSTEMS THEORY, Vol. 8, No. 2.

J is said to be *algebraic* if whenever y is generated by X it is in fact generated by a finite subset of X.

Algebraic closure operators arise precisely by closing a set under the operations of an algebra ([2], Theorem 5.2, p. 81). A familiar example of such an algebra is a group with its binary operation.

A subset G of S is called a *generating* set if G generates S. Such a set is *minimal* if in addition whenever $H \subseteq G$ and H generates S we have $H = G$.

Let a family $\mathscr{D}$ of subsets of S be such that X is in $\mathscr{D}$ if, and only if, some finite nonempty subset of X is in $\mathscr{D}$. $\mathscr{D}$ is a family of *dependent* sets; its complement in 2^S contains exactly the *independent* sets. The linearly dependent subsets of a vector space are a familiar example.

An element $a \in S$ *depends* on X if $a \in X$ or if there is an independent subset X' of X such that $X' \cup \{a\}$ (written $X' \cup a$) is dependent. $\langle X \rangle = \{a | a \text{ depends on } X\}$ is called the *span* of X. X *spans* S if $\langle X \rangle = S$; a *basis* is an independent spanning set. The dependence relation $\mathscr{D}$ is *transitive* if $\langle\langle X \rangle\rangle = \langle X \rangle$.

Given an algebraic closure operator J: $2^S \to 2^S$ we can associate with it a dependence relation as follows:

A subset X of S is *dependent* if there is an $x \in X$ such that $X - \{x\}$ (written $X - x$) generates x. $X \in 2^S$ is *independent* if it is not dependent. Thus a set is independent if none of its members can be generated by the others. Obviously $\varnothing$ is independent. An independent set is *maximally* independent if it is not properly contained in any independent set.

J is said to possess the *exchange* property if whenever y is not generated by X but is generated by $X \cup z$ we also have that z is generated by $X \cup y$ ($X \subseteq S$, $y \in S$, $z \in S$).

Cohn's Proposition 2.1 states that for an operator J enjoying the exchange property, the dependence relation associated with J is transitive; moreover, from the proof we see that $\langle X \rangle = J(X)$, hence that X is a generating set, just in case X is a spanning set, just in case X is maximally independent (Lemma 2.2). As mentioned above, the existence of cardinality invariant bases necessarily follows for such operators.

Let us then consider what can be said if J does not enjoy the exchange property.

First we note that *generates* can be viewed equivalently as a binary relation on 2^S which satisfies

(G.1) Transitivity

(G.2) For any family of sets $\mathscr{F}$, $(\forall y \in \mathscr{F})$ (X *generates* Y) $\Leftrightarrow$ X *generates* $\bigcup \{Y | Y \in \mathscr{F}\}$

(G.3) $X \supseteq Y \Rightarrow X$ *generates* Y.

As a consequence of (G.3) we also have that *generates* is reflexive.

The equivalence is stated as

THEOREM 1. *Given a closure operator J, the associated* generates *relation* (X *generates* $Y \Leftrightarrow Y \subseteq J(X)$) *satisfies the axioms (G.1)–(G.3). Conversely, to every relation on 2^S satisfying (G.1)–(G.3) there corresponds a closure operator, and moreover this correspondence is bijective.*

Proof. ($\Rightarrow$) That the axioms are satisfied is easily shown by noting that (G.1) follows from (J.1) aod (J.3), (G.2) is a consequence of the definition and (G.3) follows from (J.2).

($\Leftarrow$) Let R be a relation on 2^S satisfying (G.1)–(G.3). Define J_R: $2^S \to 2^S$ by $J_R(X) = \bigcup \{Z|XRZ\}$. Then J_R is a closure operator as follows:

(a) Let $X \subseteq Y$. By (G.3), YRX. Thus by transitivity $XRZ \Rightarrow YRZ$ and $\{Z|XRZ\} \subseteq \{Z|YRZ\}$, so $J_R(X) \subseteq J_R(Y)$.

(b) Since R is reflexive (G.3), $X \in \{Z|XRZ\}$, thus $X \subseteq J_R(X)$.

(c) From (b) $J_R(X) \subseteq J_R(J_R(X))$. From (G.2), $XRJ_R(X)$ and $J_R(X)$ $RJ_R(J_R(X))$, so by transitivity (G.1) $XRJ_R(J_R(X))$ and thus $J_R(X) \supseteq J_R(J_R(X))$. Thus $J_R(X) = J_R \cdot J_R(X)$.

Now, let R and R' satisfy (G.1)–(G.3) and suppose $J_R = J_{R'}$. Then $XRY \Rightarrow Y \subseteq J_R(X) \Rightarrow Y \subseteq J_{R'}(X)$. By (G.3), $J_{R'}(X)R'Y$. But $XR'J_{R'}(X)$, so by transitivity $XR'Y$. By symmetry we have that $XRY \Leftrightarrow XR'Y$ so $R = R'$ and the mapping $R \to J_R$ is one-to-one. This mapping is also onto since, given a closure operator J, it is easily seen that $J_{generates} = J$.

We use this reformulation to prove

THEOREM 2. *Let G be a generating set. G is a minimal generating set if and only if G is maximally independent.*

Proof. ($\Rightarrow$) Suppose G is not independent. Then there is an $x \in G$ such that $G-x$ generates x. By reflexivity, $G-x$ generates $G-x$ and by (G.2), $G-x$ generates G. Since G generates S we have by transitivity that $G-x$ generates S so that G is not a minimal generating set. Thus G is independent.

Now if G were not maximally independent there would be an $x \in G$ such that $G \cup x$ is independent. But this contradicts the fact that G generates x.

($\Leftarrow$) Let G be a non-minimal generating set. There is an $H \subset G$ such that H generates S and an $x \in G-H$ such that H generates x. By axiom (G.3) and transitivity, $G-x$ generates x, so that G is not independent.

The central point of this note is that a maximally independent set is not necessarily a generating set. To see this let R be a reflexive transitive relation on S. Let $\tilde{R}$ be the extension of R to 2^S, i.e.,

$$X\tilde{R}Y \Leftrightarrow (\forall y \in Y)\,(\exists x \in X)\,(xRy).$$

One verifies readily that $\tilde{R}$ is a generates relation on 2^S. In this class of models, X is dependent if there are distinct $x, y \in X$ such that xRy.

In particular let $S = \{1, 2, 3\}$ with $R = \{(1, 1), (2, 2), (3, 3), (1, 2), (1, 3)\}$ as in the graph in Figure 1.

Now $\{2, 3\}$ is independent; also $\{2, 3\}$ is maximally independent since $\{1, 2, 3\}$ is dependent ($\{1\}$ generates $\{2, 3\}$). But $\{2, 3\}$ is not a generating set since 1 is not generated by $\{2, 3\}$. *Thus it is not true that a maximally independent set is necessarily a generating set.* (Note however that in agreement with Theorem 1, $\{1\}$ is both a minimal generating set and a maximally independent set.)

We see also that *generates* does not satisfy the exchange property since 3 is not generated by 2 and $\{1, 2\}$ generates 3 but 1 is not generated by $\{2, 3\}$.

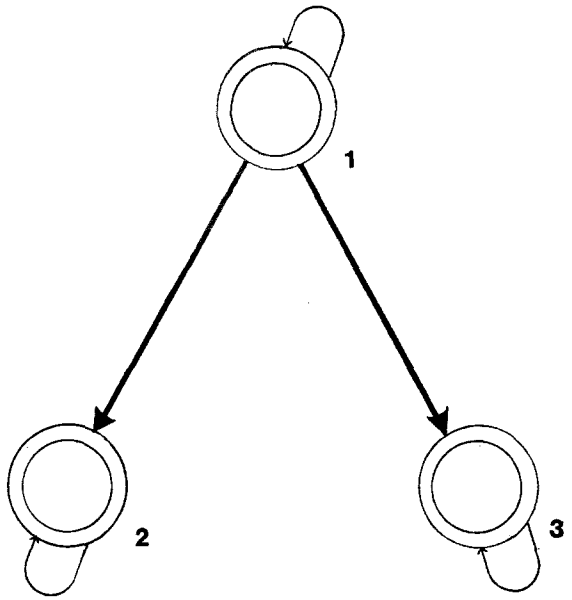

Figure 1.

From Cohn's Lemma 2.2 we know that if J satisfies the exchange property, then G is a generating set if, and only if, G is maximally independent. The above justifies the use of the exchange property as an hypothesis. For completeness sake we provide a direct proof of this result.

THEOREM 3. *A maximally independent set is a minimal generating set if* generates *satisfies the exchange property.*

Proof. Suppose that G is maximally independent but not a generating set. Then there is an $x \notin G$ which is not generated by G. Now $G \cup x$ is dependent (since G is maximally independent) so there is a $z \in G \cup x$ such that $G \cup x - z$ generates z. If $z = x$ then $G \cup x - x$ generates x, a contradiction. So $z \in G$. Since G is independent, z is not generated by $G - z$. Since $G - z \cup x$ generates z we have by the exchange property $G - z \cup z$ generates x, again a contradiction.

Thus, G is maximally independent implies G is a generating set and by Theorem 2, G is a minimal generating set.

We remark that in the case of reflexive and symmetric relations R the exchange property is always satisfied for the relational extension $\tilde{R}$, this being the basis for matroid theory. (Symmetry is also necessary as can be seen by setting $X = \varnothing$ in the statement of the exchange property.)

3. Irreducibles. An element $x \in S$ is *irreducible* with respect to a closure operator J if whenever x is generated by X then necessarily $x \in X$. We see immediately that the set of irreducibles, I, is included in every (minimal) generating set. Thus if I is a generating set it is also the unique minimal generating set. However, I need not be a generating set as the following example shows.

Let $S = \{1, 2\}$, $R = S^2$ and let *generates* be interpreted as $\tilde{R}$ as before.

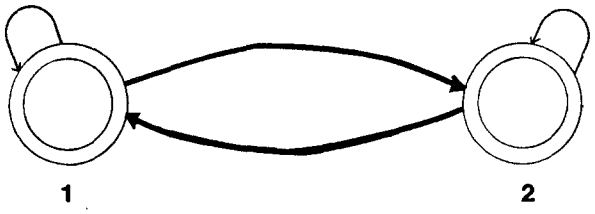

Figure 2.

Graphically, it is clear from Figure 2 that there are no irreducibles ($I = \varnothing$), yet both $\{1\}$ and $\{2\}$ are minimal generating sets.

However, we can show that the only generating set which is included in every generating set is the irreducibles I.

THEOREM 4. *If a generating set G is included in every generating set then $G = I$, the irreducible set.*

Proof. Let G be a generating set which is included in every generating set. For $x \in G$ suppose that X generates x. We will show that $x \in X$. It then follows that $G \subseteq I$, hence $G = I$. Using axioms (J.1), (J.2) and (J.3) we have $J(G-x \cup X) \supseteq J(G-x) \cup J(X) \supseteq G-x \cup x \supseteq G$. Thus $J(G-x \cup X) = J \cdot J(G-x \cup X) \supseteq J(G) \supseteq S$. Hence $G-x \cup X$ is a generating set. Since G is included in it, we have $x \in G-x \cup X$, hence that $x \in X$, as required.

4. Application to the Wymore Case. Let S be the set of functions from the reals to the reals. To each real number there is associated a unary operator operator t_r called *translation by r* such that $t_r(f)\,(x) = f(r+x)$. There is also a binary *segmentation* operator | such that

$$f|g(x) = \begin{cases} f(x) & \text{for } x < 0 \\ g(x) & \text{for } x \geq 0. \end{cases}$$

It is well known that to an algebra such as this, there corresponds a canonical closure operator $J\colon 2^S \to 2^S$, where $J(X)$ is the least set of functions in S containing X and closed under the translation operators t_r and segmentation.[1]

Wymore's Theorem 4.8 [5] asserts the existence of minimal generating sets (called input bases) for the J-closed subsets (called admissible sets). The proof actually demonstrates the existence of maximally independent sets. However, the identification of the maximally independent sets with minimal generating sets is unjustified since as we now demonstrate, the above closure operator does not possess the exchange property.

To see this, let x and z be two distinct constant functions on the reals, and let $y = x|z$. Now while y cannot be generated from x alone and y is generated from both x and z, it is not the case that z can be generated from x and y.

Proof. Say that a function f has a c-tail if there is a t such that $f(x) = c$ for $x \leq t$. Note that both x and $x|z$ have a c-tail where c is the constant value of

[1] The details for this special case are carried out by Cornacchio [3], where a closure operator is called a Hammer closure operator (Hammer [4]).

x. It is easy to show by induction that any function generated by (in the J-closure of) x and $x|z$ must have a c-tail and hence must be distinct from z which by assumption has a c'-tail for $c' \neq c$.

Of course this does not preclude the existence of minimal generating sets for the J-closed sets. Having tried a number of approaches, I have failed to establish Wymore's Theorem or find a counterexample. However, Professor David Muller has found a counterexample [6].

REFERENCES

[1] M. A. ARBIB, editor, *Algebraic Theory of Machines, Languages and Semigroups*, Academic Press, New York, 1968.

[2] P. M. COHN, *Universal Algebra*, Harper and Row, London, 1965.

[3] J. CORNACCHIO, Topological concepts in the mathematical theory of general systems, in *Trends in General Systems Theory*, G. J. Klir, editor, John Wiley, New York, 1972.

[4] P. C. HAMMER, *Advances in Mathematical Systems Theory*, Pennsylvania State University Press, 1969.

[5] A. W. WYMORE, *A Mathematical Theory of Systems Engineering: The Elements*, John Wiley, New York, 1967.

[6] D. E. MULLER, Functions generated using translation and segmentation operators, *Math. Systems Theory* (to appear).

(*Received 6 August 1973*)