All Terminal Bubbles Programs Yield the Elementary Symmetric Polynomials

By R. P. KURSHAN

(Manuscript received May 18, 1970)

R. L. Graham has discussed various combinatorial aspects of the behavior of magnetic domains or "bubbles". Representing the initial state of a configuration of $n$ magnetic domains by the $n$-tuple of indeterminates $B = (X_1, \ldots, X_n)$, he showed that subsequent configurations of magnetic domains obtainable (within the constraints of the problem) correspond exactly to subsequent $n$-tuples of Boolean expressions in the $X_i$'s* obtainable from $B$ through an application to $B$ of a product of transformations ("commands" in Ref. 1) of the form $T_{ij}(1 \leq i < j \leq n)$ where if $P = (P_1, \ldots, P_n)$ is an $n$-tuple of Boolean expressions in the $X_i$'s, then $T_{ij}(P) = (Q_1, \ldots, Q_n)$,

$$Q_k = \begin{cases} P_i \cup P_j & \text{if } \ k = i \\ P_i \cap P_j & \text{if } \ k = j \\ P_k & \text{otherwise} \end{cases}, \quad k = 1, \ldots, n.$$  

Furthermore, he showed that

if $3$ is an (2)-fold product of such transformations

and if $T$ is any other, then $(T \circ 3)(B) = 3(B)$. (*)

This provides a limitation on the number of distinct $n$-tuples of the form $\mathcal{U}(B) = (P_1, \ldots, P_n)$ where $\mathcal{U}$ is a product of transformations, and hence provides a limitation on the number of distinct $P_i$'s thus obtainable from various $\mathcal{U}$'s. Graham showed that for $n = 11$, this limitation implies that not all Boolean expressions in the $X_i$'s are realizable as a $P_i$.

This led to an (as yet unsuccessful) attempt to characterize those expressions which are realizable. The purpose of this note is to observe a fragmentary result in this direction: that if $3$ is as above, then $3(3(B)) =$

*A Boolean expression in the $X_i$'s is either a term of the form $X_i \ (1 \leq i \leq n)$, a term of the form $P \cup Q$ or a term of the form $P \cap Q$, where both $P$ and $Q$ are Boolean expressions in the $X_i$'s; expressions may be reduced as if the $X_i$'s were sets.
(S_1, \ldots, S_n) where S_i is the elementary symmetric polynomial in X_1, \ldots, X_n of degree i (here interpreting \bigcup as + and \bigcap as -). The situation will be rephrased in terms of a semiring.

For a fixed n let R be the (Boolean) commutative semiring generated by X_1, \ldots, X_n subject to the relations:

for i = 1, \ldots, n, \quad (1) \quad X_i^2 = X_i,

(2) fX_i + f = f \quad \text{for all } f \in R.

It follows that 2X_i = X_i(i = 1, \ldots, n) and hence, each f \in R is a Boolean polynomial in the indeterminates X_1, \ldots, X_n (that is, the X_i's behave like sets with respect to + and \cdot interpreted as \bigcup and \bigcap respectively).

Throughout, if x \in R^n (the set of n-tuples of elements of R), then for 1 \leq k \leq n, x_k will denote the kth coordinate of x, that is, x = (x_1, \ldots, x_k, \ldots, x_n). Let T (or T_n) be the set of transpositions of \{1, \ldots, n\} and for t \in T—say t = (i, j), i < j—define t : R^n \to R^n by

\[ (tf)_k = \begin{cases} f_i + f_j & \text{if } k = i \\ f_i \cdot f_j & \text{if } k = j \\ f_k & \text{otherwise} \end{cases} \]

Let B = B_n = (X_1, \ldots, X_n) \in R^n and set C_n = \bigcup_{k=0}^n T^k(B) where m = (\binom{n}{2})^* and T^k = \{t_1t_2 \cdots t_k | t_1, t_2, \ldots, t_k \in T\}. A point C \in C_n is said to be terminal if t(C) = C for all t \in T. It is not hard to see that (S_1, \ldots, S_n) is a terminal element of C_n where S_i(1 \leq i \leq n) is the elementary symmetric polynomial in X_1, \ldots, X_n of degree i; in what follows it will be shown that this characterizes the terminal elements of C_n.

The elements of R may be partially ordered by f \leq g \iff f + g = g. For D \in R^n, 1 \leq j \leq n, define D^j \in R^n by D^j = D_s(X_1, \ldots, X_{i-1}, 0, X_{i+1}, \ldots, X_n), 1 \leq i \leq n.

**Lemma 1:** C is terminal \iff C_1 \geq C_2 \geq \cdots \geq C_n.

**Proof:** Obvious.

* By (1), C_n = \bigcup_{k=0}^n T^k(B); on the other hand C_n = \bigcup_{k=0}^n T^k(B) \Rightarrow r \geq m: using notation developed below, this can be proved by induction on n as follows. If n = 1 it is clear; assuming it is true for a given n, identify C_n with \{D \in C_{n+1}^+ | D \subseteq C_{n+1}\} (see remark following Lemma 3). Using the theorem below and the induction hypothesis, there is a \beta such that \beta(B_{n+1}) = (S_1^{n+1}, S_2^{n+1}, \ldots, S_n^{n+1}, X_{n+1}), and \beta is a product of at least \binom{n+1}{2} transpositions. Let \beta' = (1 2)(2 3) \cdots (n n + 1)\beta; then \beta'(B_{n+1}) = (S_1, \ldots, S_{n+1}), \beta' is a product of \binom{n}{2} + n = \binom{n+1}{2} transpositions and if for some \mu (\mu \beta)(B_{n+1}) = \beta'(B_{n+1}) then \mu must be a product of at least n transpositions.
Lemma 2: If \( f, g \in R \) are such that \( X_i \) divides no summand of either, then \( f + X_i h_1 = g + X_i h_2 \Rightarrow f = g \).

Proof: Writing \( f + X_i h_1 \) as a sum of products of \( X_m \)'s, both \( f \) and \( g \) are precisely the sum of those products which are not divisible by \( X_i \).

Lemma 3: If \( D \in C_n \), then for each \( j = 1, \ldots, n \) there exists \( i \) such that \( D_i = 0 \).

Proof: Assume \( D \in C_n \) and \( 1 \leq j \leq n \). Find \( t_1, \ldots, t_r \in T \) such that \( tB = D \) where \( t = t_1 t_{r-1} \cdots t_1 \). If \( r = 1 \), say \( t = (\alpha, \beta) \), \( \alpha < \beta \); if \( j \neq \alpha \) then \( D_i^j = 0 \) and if \( j = \alpha \) then \( D_i^j = 0 \). Now assume the assertion is true whenever \( r < u \), and \( D = t_u \cdots t_1 B \). Find \( i \) such that \( (t_{u-1} \cdots t_1 B)_i = 0 \) and let \( t_u = (\alpha, \beta) \), \( \alpha < \beta \). As above, if \( i \neq \alpha \) then \( D_i = 0 \) and if \( i = \alpha \) then \( D_i^j = 0 \). Induction on \( r \) completes the proof.

Given \( D \in C_n \), Lemma 3 provides the machinery for associating \( D^i \) in a natural way with an element \( \bar{D}^i \) of \( C_{n-1} \): making the initial association \( X_i \rightarrow X_{i-1} \) in \( B_n \) and \( i \rightarrow i-1 \) in \( T_n \) for \( i > j \), define \( \bar{D}^i = t'_1 \cdots t'_m B_{n-1} \) where if \( t_m = (\alpha, \beta) \), \( \alpha < \beta \) then
\[
t'_m = \begin{cases} t_m & \text{if } (t_{m-1} \cdots t_1 B)_i \neq 0 \text{ for } i = \alpha, \beta \\ \text{identity otherwise} & \end{cases}
\]
for \( 1 \leq m \leq r \). It is clear that \( \bar{D}^i \) represents a collapsing of \( D \) at a coordinate \( i \) where \( D_i^j = 0 \) plus a permutation \( \pi \) of the other \( D^i \)'s:
\[
\bar{D}^i = (D^i(x_{1(1)}), D^i(x_{2(1)}), \ldots) \in R^{n-1}.
\]
However, the extent of possible permuting is limited by the completeness of the order \( \leq \) on the \( D^i \)'s as is demonstrated in the next two lemmas which apply for \( 1 \leq i, j, k \leq n \).

Lemma 4: \( D \in C_n, D_i \leq D_j \Rightarrow j \leq i \).

Proof: It suffices to note that an application of a transposition to a member of \( C_n \) preserves the order of the indices.

Lemma 5: \( D_i \leq D_k \Rightarrow D_i^j \leq D_k^j \).

Proof: Writing \( D_i = D_i^j + X_i g \) and \( D_k = D_k^j + X_i h \), obtain \( D_i^j + X_i h = D_k = D_i + D_k = D_i^j + D_i^j + X_i(g + h) \) which by Lemma 2 implies that \( D_k^j = D_i^j + D_i^j \), that is, \( D_i^j \leq D_k^j \).

It follows from Lemmas 1, 3, 4 and 5 that if \( C \in C_n \) is terminal, then \( C' = (\bar{C}_1, \bar{C}_2, \ldots, \bar{C}_{n-1}, 0) \) and \( \bar{C}^i \) is terminal in \( C_{n-1} \) for \( 1 \leq j \leq n \).

Theorem: \( C \in C_n \) is terminal if and only if \( C_i = S_i \), \( (1 \leq i \leq n) \).
Proof: $\Leftarrow$. This direction is clear.

$\Rightarrow$. By induction on $n$—if $n = 1$ then $c = \{B\}$ and $B = (X_1)$ so the assertion holds. Now assume the assertion holds for $n < k$, and let $C \subseteq c_k$ be terminal. Then each $C_i$ is terminal in $c_{k-1}$ and hence by the induction hypothesis each $C_i = S_i(i = 1, \ldots, k - 1; j = 1, \ldots, k)$.

In particular then $C_i \neq X_1X_2\cdots X_k$ for $i = 1, \ldots, k - 1$. Furthermore, each $C_i$ can be expressed as $C_i = P_1 + \cdots + P_r$ where each $P_m$ is a product of some but not all of the $X_i$'s. It follows for $i < k$ that

$$C_i = \sum_{P_m} P_m,$$

and consequently $C_* = \sum_{i=1}^{k} C_i = \sum_{i=1}^{k} S_i = S_i$.

It is left to the reader to show that $C_* = S_*$ and thus complete the induction argument.

REFERENCE