B.S.T.J. BRIEF

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".[1] Representing the initial state of a configuration of n magnetic domains by the n-tuple of indeterminates $B = (X_1, \cdots, X_n)$, 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 $T_{ij}(1 \leqq i < j \leqq n)$ where if $P = (P_1, \cdots, P_n)$ is an n-tuple of Boolean expressions in the X_i's, then $T_{ij}(P) = (Q_1, \cdots, Q_n)$,

$$Q_k = \begin{Bmatrix} P_i \bigcup P_j & \text{if} \quad k = i \\ P_i \bigcap P_j & \text{if} \quad k = j \\ P_k & \text{otherwise} \end{Bmatrix}, \qquad k = 1, \cdots, n.$$

Furthermore, he showed that

if $\mathfrak{J}$ is an $\binom{n}{2}$-fold product of such transformations and if T is any other, then $(T \circ \mathfrak{J})(B) = \mathfrak{J}(B)$. (†)

This provides a limitation on the number of distinct n-tuples of the form $\mathfrak{U}(B) = (P_1, \cdots, P_n)$ where $\mathfrak{U}$ is a product of transformations, and hence provides a limitation on the number of distinct P_i's thus obtainable from various $\mathfrak{U}$'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 $\mathfrak{J}$ is as above, then $\mathfrak{J}(B) =$

* A Boolean expression in the X_i's is either a term of the form X_i $(1 \leqq i \leqq n)$, 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.

$(S_1, \cdots, S_n)$ where S_i is the elementary symmetric polynomial in $X_1, \cdots, X_n$ of degree i (here interpreting $\cup$ as $+$ and $\cap$ as $\cdot$). The situation will be rephrased in terms of a semiring.

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

$$\text{for} \quad i = 1, \cdots, n, \quad (1)\ X_i^2 = X_i,$$
$$(2)\ fX_i + f = f \quad \text{for all} \quad f \in R.$$

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

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

$$(tf)_k = \begin{cases} f_i + f_j & \text{if} \quad k = i \\ f_i \cdot f_j & \text{if} \quad k = j \\ f_k & \text{otherwise} \end{cases}. \quad \text{Let } B = B_n = (X_1, \cdots, X_n) \in R^n$$

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

The elements of R may be partially ordered by $f \leqq g \Leftrightarrow f + g = g$. For $D \in R^n$, $1 \leqq j \leqq n$, define $D^j \in R^n$ by $D_i^j = D_i(X_1, \cdots, X_{j-1}, 0, X_{j+1}, \cdots, X_n)$, $1 \leqq i \leqq n$.

Lemma 1: C is terminal $\Leftrightarrow C_1 \geqq C_2 \geqq \cdots \geqq C_n$.

Proof: Obvious.

---

* By (†), $\mathcal{C}_n = \bigcup_{k=0}^{\infty} T^k(B)$; on the other hand $\mathcal{C}_n = \bigcup_{k=0}^{r} T^k(B) \Rightarrow r \geqq m$: 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 $\mathcal{C}_n$ with $\{D^{n+1} \mid D \in \mathcal{C}_{n+1}\} \subset \mathcal{C}_{n+1}$ (see remark following Lemma 3). Using the theorem below and the induction hypothesis, there is a $\mathcal{G}$ such that $\mathcal{G}(B_{n+1}) = (S_1^{n+1}, S_2^{n+1}, \cdots, S_n^{n+1}, X_{n+1})$, and $\mathcal{G}$ is a product of at least $\binom{n}{2}$ transpositions. Let $\mathcal{G}' = (1\ 2)(2\ 3) \cdots (n\ n+1)\mathcal{G}$; then $\mathcal{G}'(B_{n+1}) = (S_1, \cdots, S_{n+1})$, $\mathcal{G}'$ is a product of $\binom{n}{2} + n = \binom{n+1}{2}$ transpositions and if for some $\mathcal{U}$ $(\mathcal{U}\mathcal{G})(B_{n+1}) = \mathcal{G}'(B_{n+1})$ then $\mathcal{U}$ 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 $D \in \mathcal{C}_n$, then for each $j = 1, \cdots, n$ there exists i such that $D_i^j = 0$.

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

Given $D \in \mathcal{C}_n$, Lemma 3 provides the machinery for associating D^j in a natural way with an element $\tilde{D}^j$ of $\mathcal{C}_{n-1}$: 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 $\tilde{D}^j = t_r' \cdots t_1' B_{n-1}$ where if $t_m = (\alpha, \beta), \alpha < \beta$ then

$$t_m' = \begin{cases} t_m & \text{if } \quad (t_{m-1} \cdots t_1 B_n)_i^j \neq 0 \quad \text{for} \quad i = \alpha, \beta \\ \textit{identity} & \text{otherwise} \end{cases}$$

for $1 \leqq m \leqq r$. It is clear that $\tilde{D}^j$ represents a collapsing of D at a coordinate i where $D_i^j = 0$ plus a permutation π of the other D_i^j's: $\tilde{D}^j = (D_{\pi(1)}^j, D_{\pi(2)}^j, \cdots) \in R^{n-1}$.

However, the extent of possible permuting is limited by the completeness of the order $\leqq$ on the D_i^j's as is demonstrated in the next two lemmas which apply for $1 \leqq i, j, k \leqq n$.

Lemma 4: $D \in \mathcal{C}_n$, $D_i \leqq D_j \Rightarrow j \leqq i$.

Proof: It suffices to note that an application of a transposition to a member of $\mathcal{C}_n$ preserves the order of the indices.

Lemma 5: $D_i \leqq D_k \Rightarrow D_i^j \leqq D_k^j$.

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

It follows from Lemmas 1, 3, 4 and 5 that if $C \in \mathcal{C}_n$ is terminal, then $C^j = (\tilde{C}_1^j, \tilde{C}_2^j, \cdots, \tilde{C}_{n-1}^j, 0)$ and $\tilde{C}^j$ is terminal in $\mathcal{C}_{n-1}$ for $1 \leqq j \leqq n$.

Theorem: $C \in \mathcal{C}_n$ is terminal $\Leftrightarrow C_i = S_i$, $(1 \leqq i \leqq n)$.

Proof: $\Leftarrow$. This direction is clear.

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

In particular then $C_i \neq X_1 X_2 \cdots X_k$ for $i = 1, \cdots, k - 1$. 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

$$C_i^j = \sum_{X_j \nmid P_m} P_m, \quad \text{and consequently } C_i = \sum_{j=1}^{k} C_i^j = \sum_{j=1}^{k} S_i^j = S_i.$$

It is left to the reader to show that $C_k = S_k$ and thus complete the induction argument.

REFERENCE

1. Graham, R. L., "A Mathematical Study of a Model of Magnetic Domain Interactions," B.S.T.J., this issue, pp. 1627–1644.