# *On the decomposition of Boolean polynomials*

Dedicated to Professor Y. Kawada on his 60th birthday

By Curtis GREENE* and Gaisi TAKEUTI**

## 1. Introduction.

In this paper, we will prove the following theorem:

THEOREM 1. *Let $M=(m_{ij})$ be a rectangular matrix with entries in a set $X$, satisfying:*

(i) *If $i\neq i'$ and $j\neq j'$, and $m_{ij}=m_{i'j'}=z$, then $m_{ij'}=m_{i'j}=z$.*

(ii) *If $S\subseteqq X$ and $S$ meets every row of $M$, then $S$ contains a column of $M$.*

(iii) *If $S\subseteqq X$ and $S$ meets every column of $M$, then $S$ contains a row of $M$.*

(iv) *$M$ contains at least two distinct entries.*

*Then $M$ can be partitioned into two disjoint nonempty rectangular submatrices.*

Condition (i) says that the elements of $X$ form rectangular submatrices of $M$. It can be shown without great difficulty that (ii) and (iii) are equivalent (see Lemma 2.6).

Aside from its own interest as a combinatorial result, Theorem 1 has application to other areas, and in fact arose in connection with the following situation. Let $p(x_1, x_2, \cdots, x_n)$ be a Boolean polynomial which involves the variables $x_1, x_2, \cdots, x_n$ and the symbols $\vee$ and $\wedge$ (but no negations). We ask: *when can $p$ be expressed in a form in which each variable occurs only once*? Polynomials with this property will be called *completely decomposable.* For example, if $p_1=(x\vee z)\wedge(y\vee z)\wedge w$, then $p_1$ is completely decomposable, since we can write $p_1=((x\wedge y)\vee z)\wedge w$. On the other hand, if $p_2=(x\vee y)\wedge(x\vee z)\wedge(y\vee z)$, then $p_2$ cannot be expressed without multiple occurrences of variables, and hence is not completely decomposable.

We will answer this question by restating it in a purely combinatorial fashion, making use of the canonical conjunctive and disjunctive forms for polynomials $p$ of the type considered here (i.e. without negations). This leads to a purely set-theoretic problem, which can in turn be solved by proving Theorem 1.

If $p(x_1, x_2, \cdots, x_n)$ is a Boolean polynomial without negations, we can write

$$p=\bigwedge_i(\bigvee_{x\in A_i}x)$$

* Supported in part by ONR N00014-67-A-0204-0063.
** Supported in part by NSF MPS 74-07499.

and

$$p=\bigvee_i(\bigwedge_{x\in B_i}x)$$

for suitable families $\{A_i\}$ and $\{B_i\}$ of subsets of variables. If we assume that both expressions are minimal, in the sense that $A_i \not\supset A_j$ and $B_i \not\supset B_j$ for $i\neq j$, then this correspondence uniquely associates polynomials with pairs of families of sets. Our main result about polynomials can be stated as follows:

THEOREM 2. *Let $p$ be a Boolean polynomial, and let $\{A_i\}$ and $\{B_i\}$ be the families of sets determined from $p$ as above. Then $p$ is completely decomposable if and only if $|A_i\cap B_j|=1$ for all $i$, $j$.*

For example, consider the polynomials $p_1$ and $p_2$ defined earlier. We have

$$p_1=(x\wedge y\wedge w)\vee(z\wedge w)=(x\vee z)\wedge(y\vee z)\wedge w$$

$$p_2=(x\wedge y)\vee(y\wedge z)\vee(x\wedge z)=(x\vee y)\wedge(y\vee z)\wedge(x\vee z)\,.$$

Then $p_1$ satisfies the conditions of Theorem 1, while $p_2$ does not.

REMARK. For an arbitrary polynomial $p$, it is always true that $|A_i\cap B_j|\geqq 1$, for all $i$, $j$. Thus Theorem 2 is a characterization of the extreme cases of this inequality.

## 2. Notation: Systems of choice sets.

In this section, we will develop the notation required to treat the problems described in section 1 from a purely set-theoretic point of view. Most of the ideas introduced here are elementary or well-known, and almost no proofs have been included. Although we will ultimately be concerned with finite sets exclusively, no finiteness assumptions are made at the outset.

DEFINITION 2.1. *Let $\mathcal{A}$ be a family of subsets of $X$, and let $U\subseteqq X$. We say that $U$ is a choice set for $\mathcal{A}$ if $U\cap A\neq\Phi$ for all $A\in\mathcal{A}$.*

DEFINITION 2.2. *Let $\mathcal{A}$ and $\mathcal{B}$ be families of subsets of $X$. The triple $\langle\mathcal{A},\mathcal{B},X\rangle$ is said to be a mutual choice system (abbreviated MCS) if the following conditions hold:*

(i) *$\mathcal{A}$ consists of all minimal choice sets for $\mathcal{B}$.*
(ii) *$\mathcal{B}$ consists of all minimal choice sets for $\mathcal{A}$.*
(iii) $\cup\mathcal{A}=\cup\mathcal{B}=X$.

Clearly, this definition implies that each of the families $\mathcal{A}$ and $\mathcal{B}$ must be an antichain (i. e. $A\not\supset A'$ for all $A$, $A'\in\mathcal{A}$, and similarly for $\mathcal{B}$).

LEMMA 2.3. *When $X$ is finite, each of the conditions* (i) *and* (ii) *in Definition* 2.2 *implies the other.*

A direct proof can be constructed without difficulty, but we will not do so. The lemma follows immediately from the fact that, when $X$ is finite, $\mathscr{A}$ and $\mathscr{B}$ correspond to the families induced by the dual canonical forms of a Boolean polynomial. In the notation of section 1, if $\mathscr{A}=\{A_i\}$, then $\mathscr{B}=\{B_i\}$, and conversely.

DEFINITION 2.4. *An MCS* $\langle\mathscr{A}, \mathscr{B}, X\rangle$ *is said to be unitary if* $|A\cap B|=1$ *for all* $A\in\mathscr{A}$, $B\in\mathscr{B}$.

Given a unitary MCS $\langle\mathscr{A}, \mathscr{B}, X\rangle$ we define its *intersection matrix* to be the array $M=(m_{ij})$ of elements of $X$ defined as follows: if $\mathscr{A}=\{A_i\}$ and $\mathscr{B}=\{B_i\}$ then $m_{ij}$ is the unique element of $A_i\cap B_j$. The rows of $M$ represent the $A_i$'s (with possible repetitions) and the columns represent the $B_j$'s. The following lemma follows immediately from the definition of $M$ and the properties of an MCS.

LEMMA 2.5. *The intersection matrix $M$ of a unitary MCS satisfies*:

(i) *If* $i\neq i'$ *and* $j\neq j'$, *and* $m_{ij}=m_{i'j'}=z$, *then* $m_{ij'}=m_{i'j}=z$.

(ii) *If a collection of entries meets every row of $M$, then it contains a column of $M$.*

(iii) *If a collection of entries meets every column of $M$, then it contains a row of $M$.*

*Conversely, if $M$ is any matrix which satisfies* (i)-(iii), *then the rows and columns of $M$ form a unitary MCS.*

We have immediately the following analog of Lemma 2.3 for intersection matrices:

LEMMA 2.6. *If $M$ is any matrix such that condition* (ii) *of Lemma* 2.5 *holds, then condition* (iii) *also holds, and conversely.*

(We omit the proof. Interestingly, it is not necessary to assume that (i) holds.)

By a *subrectangle* of $M$ we mean any rectangular submatrix of $M$. Two subrectangles are said to be *disjoint* if no element of $X$ appears in both.

DEFINITION 2.7. *A unitary MCS is said to be separable if its intersection matrix can be partitioned into two disjoint subrectangles.*

Our main theorem (expressed in set-theoretic language) is the following:

THEOREM 3. *If* $\langle\mathscr{A}, \mathscr{B}, X\rangle$ *is a unitary MCS such that* $1<|X|<\infty$, *then* $\langle\mathscr{A}, \mathscr{B}, X\rangle$ *is separable.*

We will give a proof of Theorem 3 in the next section. First, however, we indicate how our characterization theorem for Boolean polynomials (Theorem 2) follows as a corollary.

Suppose that $\langle \mathcal{A}, \mathcal{B}, X\rangle$ is a unitary MCS, whose intersection matrix $M$ can be separated into subrectangles $M_1$ and $M_2$. We may suppose that $M_1$ and $M_2$ consist of disjoint sets of columns of $M$, whose entries partition $X$ into two disjoint subsets $X_1$ and $X_2$. It is easy to see that $M_1$ and $M_2$ each satisfy conditions (i) and (ii) of Lemma 2.5, and hence, by Lemma 2.6, also condition (iii). Thus $M_1$ and $M_2$ determine systems $\langle \mathcal{A}_1, \mathcal{B}_1, X_1\rangle$ and $\langle \mathcal{A}_2, \mathcal{B}_2, X_2\rangle$, each of which is a unitary MCS.

Clearly the process of separating a unitary MCS into two disjoint parts corresponds to decomposing the corresponding Boolean polynomial $p$ as $p=p_1\vee p_2$ or $p=p_1\wedge p_2$, where $p_1$ and $p_2$ involve disjoint sets of variables. The above remarks show that this process can be repeated, until $p$ has been decomposed into singleton sets. Thus $p$ is completely decomposable if the corresponding MCS is unitary. The converse is easy to verify by induction, and this completes the proof of Theorem 2.

## 3. Proof of Theorem 3.

DEFINITION 3.1. *A homomorphism of a unitary MCS* $\langle \mathcal{A}, \mathcal{B}, X\rangle$ *is a map* $\phi: X\to X'$ *such that* $\langle \phi[\mathcal{A}], \phi[\mathcal{B}], \phi[X]\rangle$ *is a unitary MCS. A homomorphism* $\varphi$ *is proper if* $1<|\varphi[X]|<|X|$.

LEMMA 3.2. *If* $\langle \mathcal{A}, \mathcal{B}, X\rangle$ *is a unitary MCS with intersection matrix* $M$, *then a map* $\phi: X\to X'$ *is a homomorphism if and only if for every* $y\in\phi[X]$, $\phi^{-1}[y]$ *is a subrectangle of* $M$.

The proof of Lemma 3.2 is straightforward and left to the reader. The main step in the proof of Theorem 2 is contained in the next lemma:

LEMMA 3.3. *Every finite unitary MCS* $(\mathcal{A}, \mathcal{B}, X)$ *with* $|X|>2$ *possesses a proper homomorphic image.*

PROOF. By Lemma 3.2, it will be sufficient to show that if $M$ is the intersection matrix of $(\mathcal{A}, \mathcal{B}, X)$, then there exists a subset $U\subseteqq X$ satisfying $1<|U|<|X|$ whose elements form a subrectangle of $M$. Identifying the elements of $U$ provides the desired homomorphic image. We construct such a subrectangle as follows:

Assume that the first two rows of $M$ agree in the largest number of columns, among all pairs of rows in $M$. Denote these rows by $A_1$ and $A_2$. (We may identify rows with sets in $\mathcal{A}$, and columns with sets in $\mathcal{B}$.) Also denote the columns in which $A_1$ and $A_2$ agree by $B_1, B_2, \cdots, B_m$ and those in which they disagree by $B_{m+1}, B_{m+2}, \cdots$. We write $B_i\cap A_1=B_i\cap A_2=\{c_i\}$, $i=1, 2, \cdots, m$, and define $C=\{c_1, c_2, \cdots, c_m\}$. Let $A_1, A_2, \cdots, A_k$ denote the list of all rows containing $C$, and let $U=\bigcup_1^k(A_i-C)$. Note that the sets $A_i-C$ are pairwise disjoint, by the maximality of $m$.

We claim that the elements of $U$ determine a subrectangle of $M$ (which is obviously nontrivial). Suppose that this is not the case. Then there exist elements $a_1$ and $a_2 \in U$ and $p \notin U$, together with appropriate rows and columns of $M$ whose intersections have the form

$$\begin{array}{c|ccccc|} & & B_i & & B_j & \\ \hline & & \vdots & & \vdots & \\ A_1' & \cdots\cdots & a_1 & \cdots\cdots\cdots\cdots & q & \cdots\cdots \\ & & \vdots & & \vdots & \\ A_2' & \cdots\cdots & p & \cdots\cdots\cdots\cdots & a_2 & \cdots\cdots \\ & & \vdots & & \vdots & \\ \hline \end{array}$$

(Here $q$ is unrestricted). After suitable renumbering of rows, we may assume that $a_1$ occurs in $A_1$ and $a_2$ occurs in $A_2$ (if both occur in the same row, choose a different $a_1$). Furthermore, we may assume that $A_1 = A_1'$, since $A_1$ has the same properties as $A_1'$. Finally, since $a_1, a_2 \notin C$ we may assume that $B_i = B_{m+1}$ and $B_j = B_{m+2}$. In other words, we have

$$B_{m+1} \cap A_1 = \{a_1\} \qquad B_{m+2} \cap A_1 = \{q\}$$

$$B_{m+1} \cap A_2' = \{p\} \qquad B_{m+2} \cap A_2' = B_{m+2} \cap A_2 = \{a_2\}$$

Next define $B_i \cap A_2' = \{\tilde{c}_i\}$, $i = 1, 2, \cdots, m$, and let $\tilde{C} = \{\tilde{c}_1, \tilde{c}_2, \cdots, \tilde{c}_m\}$.

Consider the set $A = \tilde{C} \cup (A_1 - C)$. Clearly $A$ meets every column, since $\tilde{C}$ meets columns $1, 2, \cdots, m$ and $A_1 - C$ meets columns $m+1, m+2, \cdots$. Hence, by Lemma 2.5 (ii), there exists a row $A_0 \subseteqq A$. Our next step will be to show that $A_0 = A$. This will be done by computing the intersection of $A_0$ with each column of $M$. We define $A_0 \cap B_i = \{\alpha_i\}$, $i = 1, 2, \cdots$.

(1) First, we have $\alpha_i = \tilde{c}_i$ for $i = 1, 2, \cdots, m$. For if $\alpha_i \in \tilde{C}$, then this follows from Lemma 2.5 (i). On the other hand, if $\alpha_i = a \in A_1 - C$, then $a \in B_i \cap A_1 \subseteqq C$, which is a contradiction.

(2) Next, we have $\alpha_{m+1} = a_1$. For if $\alpha_{m+1} \in A_1 - C$, this follows from Lemma 2.5 (i). On the other hand, if $\alpha_{m+1} \in \tilde{C}$, then $\alpha_{m+1} = p$ by a similar argument. But this implies that $A_0$ and $A_2'$ agree in columns $1, 2, \cdots, m+1$. By the maximality of $m$, we must have $A_0 = A_2'$. But this is impossible, since $a_2 \in A_2'$ but $a_2 \notin A_1 - C$ and $a_2 \notin \tilde{C}$. (This last statement follows from Lemma 2.5 (i) and the fact that $a_2 \in A_2 - C$.)

(3) Finally, we have $\{\alpha_j\} = A_1 \cap B_j$ for $j > m+1$. This follows from Lemma 2.5 (i) if $\alpha_j \in A_1 - C$. On the other hand, if $\alpha_j = \tilde{c} \in \tilde{C}$, then $A_2' \cap B_j = \{\tilde{c}\}$, which means that $A_0$ and $A_2'$ agree in columns $1, 2, \cdots, m$ and $j$ but not $m+1$. (We have already shown that $\alpha_{m+1} = a_1 \neq p$.) This contradicts the maximality of $m$.

Thus every element of $\tilde{C} \cup (A_1 - C)$ appears as some $\alpha_i$, and we have proved that $A_0=\tilde{C}\cup(A_1-C)$.

Now let $A'=\tilde{C}\cup(A_2-C)$. Clearly $A'$ meets every column of $M$, and hence must contain a row $A'_0$. Again we will show that $A'_0=A'$, by calculating $A'_0\cap B_i=\{\alpha'_i\}$ for all $i$.

An argument identical to (1) above shows that $\alpha'_i=\tilde{c}_i$ for $i=1, 2, \cdots, m$. When $i>m$, we have $\{\alpha'_i\}=A_2\cap B_i$ as long as $\alpha'_i\in A_2-C$, by Lemma 2.5 (i). On the other hand, if $\alpha'_i=\tilde{c}\in\tilde{C}$, $i>m$, then comparing $A'_0$ with $A_0$ and applying Lemma 2.5 (i) shows that $\alpha_i=\tilde{c}$, which we have already shown to be impossible (in steps (2) and (3) above). This completes the proof that $A'_0=\tilde{C}\cup(A_2-C)$.

Now compare the rows $A'_2$ and $A'_0$. We have shown that they agree in columns $1, 2, \cdots, m$ and also $m+2$. Furthermore $A'_2\neq A'_0$, since $A'_2$ contains $p$ in column $m+1$, while $A'_0$ contains $\alpha'_{m+1}\in A_2-C\subseteqq U$. But this contradicts the maximality of $m$, which shows that in fact $U$ must be a subrectangle of $M$. The elements of $U$ can thus be identified to yield a proper homomorphic image of $\langle\mathcal{A}, \mathcal{B}, X\rangle$. This completes the proof of Lemma 3.3.

The proof of Theorem 3 can now be completed easily by induction on the number of elements in $X$. By Lemma 3.3, $\langle\mathcal{A}, \mathcal{B}, X\rangle$ has a nontrivial homomorphic image $\langle\mathcal{A}', \mathcal{B}', X'\rangle$ which we may assume to be separable. If we denote the incidence matrix of the former by $M$ and that of the latter by $M'$, then $M'$ is obtained from $M$ by identifying certain subrectangles (and removing duplicate rows and columns if necessary). Hence it is clear that any partition of $M'$ into two subrectangles leads immediately to a similar partition of $M$. Hence $\langle\mathcal{A}, \mathcal{B}, X\rangle$ is separable.

(Received April 6, 1976)

Curtis Greene
Massachusetts Institute of Technology
Cambridge, Massachusetts 02139
U. S. A.

Gaisi Takeuti
University of Illinois at Urbana-Champaign
Urbana, Illinois 61801
U. S. A.