Information Processing Letters 30 (1989) 47–49
North-Holland

16 January 1989

THERE ARE NO p-COMPLETE FAMILIES OF SYMMETRIC BOOLEAN FUNCTIONS

Mihály GERÉB-GRAUS *
Department of Mathematics, Statistics and Computer Science, University of Illinois, Chicago, IL 60680, U.S.A.

Ramamohan PATURI **
University of California at San Diego, San Diego, La Jolla, CA 92093, U.S.A.

Endre SZEMERÉDI
Rutgers University, New Brunswick, NJ 08903, U.S.A.

Communicated A.V. Aho
Received 21 March 1988

We present a proof of a negative answer to the question raised by Skyum and Valiant (1981), namely, whether the class of symmetric Boolean functions has a p-complete family.

Keywords: Symmetric function, p-projection, completeness

Valiant [2,3] and Skyum and Valiant [1] developed a complexity theory based on Boolean algebra. In this theory, a problem is represented as a family of Boolean functions and complexity classes are defined as sets of problems, which can be reduced to each other using *projections*. In contrast to the usual Turing machine reducibilities, projection is a very tight notion of reducibility since it does not allow any computation at the reduction except for passing variables. Hence, the reduction can be done by a circuit of depth 1, using only unary gates such as identity, negation, and constants. On the other hand, this reduction is strong enough in the sense that the most well-known NP-complete, and #P-complete problems are reducible to each other through projections as well, and they comprise the most difficult problems in their corresponding complexity classes.

Moreover, the notion of *completeness* with respect to projections identifies those families of functions which are general purpose. Any efficient computational techniques to compute complete families will have wide applicability.

The question raised by Skyum and Valiant concerns the existence or nonexistence of complete families of functions for the class of symmetric Boolean functions. We need some definitions to formulate this question precisely.

A *family* $\boldsymbol{P}$ of Boolean functions is a sequence P_i of Boolean functions indexed by the subscript i such that no two members have the same index, and P_i depends on at most i Boolean arguments.

A function f is said to be a *projection* of function g iff there is a mapping

$$\sigma: \{y_1, \ldots, y_m\} \to \{0, 1, x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n\}$$

* Supported in part by the National Science Foundation under Grant No. DCR81-21431. This work was performed while the author was at Harvard University.
** Supported in part by the National Science Foundation under Grant No. DCR83-02385 while the author was at Harvard university.

such that

$$f(x_1,\ldots,x_n)=g(\sigma(y_1)\ldots,\sigma(y_m)).$$

We say that a family $\boldsymbol{P}$ is a *p-projection* of the family $\boldsymbol{Q}$, if there is a polynomial p such that if P_i is in $\boldsymbol{P}$, then there is a Q_j in $\boldsymbol{Q}$ such that (i) P_i is a projection of Q_j, and (ii) $j<p(i)$. This bound on the size of projection makes the notion of projection more practical.

For a class $\mathscr{C}$ of families, the family $\boldsymbol{U}$ is *p-complete* iff $\boldsymbol{U}$ is in $\mathscr{C}$ and if $\boldsymbol{Q}$ is in $\mathscr{C}$, then $\boldsymbol{Q}$ is a p-projection of $\boldsymbol{U}$.

A function is called *symmetric* if it is invariant under any permutation of its inputs. For Boolean functions, this means that the value of a symmetric function depends only on the number of input variables which are set to 1. This implies that there are 2^{n+1} symmetric functions of n-variables. We use the same symbol to denote a symmetric function and the associated set of numbers.

Skyum and Valiant [1] ask whether the class of symmetric boolean functions has a p-complete family. We prove that it does not.

Theorem. *There is no p-complete family in the class of symmetric Boolean functions.*

Proof. Suppose by way of contradiction that there exists a polynomial $p(n)$ and a family $U_1,\ldots,U_n,\ldots$ of symmetric Boolean functions such that every n-variable symmetric Boolean function is a projection of one of the U_i's with $i<p(n)$.

Now, for all n-variable symmetric functions I, there is some U_m where $m<p(n)$ and a mapping

$$\sigma_I:\{y_1,\ldots,y_m\}\to\{0,1,x_1,\ldots,x_n,\bar{x}_1,\ldots,\bar{x}_n\}$$

such that

$$I(x_1,\ldots,x_n)=U_m(\sigma_I(y_1),\ldots,\sigma_I(y_m)).$$

Let us define $w_{I,i}$, the weight of x_i in the projection σ_I as

$$w_{I,i}=|\{l\leqslant m:\sigma_I(y_l)=x_i\}|-|\{l\leqslant m:\sigma_I(y_l)=\bar{x}_i\}|.$$

Also, define

$$c_I=|\{l\leqslant m:\sigma_I(y_l)=1\}|+\sum_{i=1}^{n}|\{l\leqslant m:\sigma_I(y_l)=\bar{x}_i\}|.$$

Note that c_I is the number of 1's in the input of U_m under the projection σ_I when each of the variables x_i is set to 0 and $w_{I,i}$ is the increase in the number of 1's in the input of U_m under the projection σ_I when the variable x_i is turned on.

With these parameters, it is easy to see that, for any $A\subset\{x_1,\ldots,x_n\}$, $|A|\in I$ iff $\Sigma_{i:x_i\in A}w_{I,i}+c_I\in U_m$. Also note that $0\leqslant c_I<p(n)$ and that

$$-p(n)<\sum_{i:x_i\in A}w_{I,i}<p(n).$$

By the pigeonhole principle, there is an $m\leqslant p(n)$ such that at least $1/p(n)$ of all the symmetric functions are projections of U_m. Let us denote the set of these symmetric functions by E_0. Note that $|E_0|>2^{n+1}/p(n)$.

For a symmetric function I in E_0, define the characteristic sequence $c=\{c_0,\ldots,c_{\lfloor\log n\rfloor}\}$ such that $c_0=c_I$ and, for $1\leqslant j\leqslant\lfloor\log n\rfloor$,

$$c_j=\sum_{i=2^{j-1}}^{2^j-1}w_{I,i}.$$

If n is not of the form 2^i-1 for some i, then

$$c_{\lfloor\log n\rfloor}=\sum_{i=2^{\lfloor\log n\rfloor}}^{n}w_{I,i}.$$

Note that $-p(n)<c_j<p(n)$ for each j.

The characteristic sequence uniquely determines the function I. To see this, for each $0\leqslant k\leqslant n$, let B_k be the unique set of numbers such that $k=\Sigma_{i\in B_k}2^{i-1}$.

$$k\in I \text{ iff } c_I+\sum_{r\in B_k,2^{r-1}\leqslant l\leqslant 2^r-1}w_{I,l}\in U_m.$$

But,

$$c_I+\sum_{r\in B_k,2^{r-1}\leqslant l\leqslant 2^r-1}w_{i,l}=\sum_{i\in\{0\}\cup B_k}c_i.$$

The number of different characteristic sequences is at most $(2p(n))^{\lfloor\log n+1\rfloor}$ and this con-

tradicts the fact that there are at least $2^{n+1}/p(n)$ different functions in E_0. □

From the proof, it easily follows that complete families in the class of symmetric Boolean functions do not exist unless we allow projections of size at least $2^{O(n/\log n)}$. Clearly, $2^{O(n)}$ size projections are enough. The exact bound remains open.

References

[1] S. Skyum and L.G. Valiant, A complexity theory based on Boolean algebra, In: *22nd Ann. IEEE Symp. on Foundations of Computer Science* (IEEE Computer Society, New York, 1981) 244–253.

[2] L.G. Valiant, Completeness classes in algebra, In: *Proc. 11th Ann. ACM Symp. on Theory of Computing*, Atlanta, GA (ACM, New York, 1979) 249–261.

[3] L.G. Valiant, Reducibility by Algebraic Projections, *L'Enseignement Mathématique, Monographie No. 30* (1982) 365–380.