COMPOSITIONAL COMPLEXITY OF BOOLEAN FUNCTIONS

Harold ABELSON
Laboratory for Computer Science, Massachusetts Institute of Technology, Cambridge, MA 02165, USA

Andrzej EHRENFEUCHT
Department of Computer Science, University of Colorado, Boulder, CO 80309, USA

James FICKETT and Jan MYCIELSKI
Department of Mathematics, University of Colorado, Boulder, CO 80309, USA

Received 9 November 1979
Revised 4 March 1981

We define two measures, $\gamma$ and $c$, of complexity for Boolean functions. These measures are related to issues of functional decomposition which (for continuous functions) were studied by Arnol’d, Kolmogorov, Vituškin and others in connection with Hilbert’s 13th Problem. This perspective was first applied to Boolean functions in [1]. Our complexity measures differ from those which were considered earlier [3, 5, 6, 9, 10] and which were used by Ehrenfeucht and others to demonstrate the great complexity of most decision procedures. In contrast to other measures, both $\gamma$ and $c$ (which range between 0 and 1) have a more combinatorial flavor and it is easy to show that both of them are close to 0 for literally all “meaningful” Boolean functions of many variables. It is not trivial to prove that there exist functions for which $c$ is close to 1, and for $\gamma$ the same question is still open. The same problem for all traditional measures of complexity is easily resolved by statistical considerations.

1. Basic definitions and results

For any set $A$ let $B(A)$ be the set of all functions $\{0, 1\}^A \rightarrow \{0, 1\}$, i.e., $B(A)$ is the set of all Boolean functions of Boolean variables indexed by elements of $A$. If $n$ is a positive integer, then for notational convenience, we let $n$ denote a standard set containing $n$ elements, $n = \{1, \ldots, n\}$.

Our definition of complexity relies on the concept of a support system which was first introduced in [1]:

Definition. A finite sequence $H = (S_1, \ldots, S_r)$ of (not necessarily distinct) subsets of $A$ is called a support system on $A$, in symbols $H \in S(A)$. A support system $H$ is said to admit a function $f \in B(A)$ if there exist $g \in B(r)$ and $h_i \in B(S_i)$, $i \in r$, such that $f = g(h_1, \ldots, h_r)$. 

0166-218X/82/0000-0000/$02.75 © 1982 North-Holland
Intuitively, we can regard a support system as an abstract "circuit diagram" for a one-stage decomposition of a function. Each $h_i$ is a "partial function" whose value depends only on the variables specified by $S_i$. The values of all the $h_i$ are then combined by $g$. Saying that the support system admits a function $f$ is saying that $f$ can be computed according to such a decomposition scheme.

Given a support system $H \in S(n)$, we define $N(H, n)$ to be the number of functions which $H$ admits:

$$N(H, n) = | \{ f \in B(n) \mid H \text{ admits } f \} |$$

We can now define two measures of compositional complexity for functions $f \in B(n)$:

$$\gamma(f) = \min \{ 2^{-2^n} N(H, n) \mid H \in S(n) \text{ admits } f \},$$

$$c(f) = \min \{ 2^{-n \log_2 N(H, n)} \mid H \in S(n) \text{ admits } f \}.$$

Note that $\gamma(f) \leq c(f)$. In the following sections we shall write $N(H)$ rather than $N(H, n)$ since $n$ will always be clear from the context.

For any $H \in S(n)$, $2^{-2^n} N(H)$ is the probability that an arbitrary $f \in B(n)$ is admitted by $H$. Thus $\gamma(f)$ and $c(f)$ are natural measures of the complexity of $f$ relative to one-level decompositions. For $f$ to have complexity near 1 means that any decomposition (support structure) which is "powerful enough" to admit $f$ must perforce admit most other functions in $B(n)$.

The first natural questions to ask concern the existence and size of the set of compositionally complex functions:

(A) Does there exist a sequence $f_n \in B(n)$ such that the compositional complexity of $f_n$ approaches 1 as $n \to \infty$?

(B) Do most functions have high compositional complexity?

Although we conjecture that the answer to these questions is yes for both measures $\gamma(f)$ and $c(f)$, we are able to prove this only for $c(f)$. Indeed, we conjecture that, for most functions, $\gamma(f) = 1$.

**Theorem 1.** (i) For every positive integer $n$ there exists $f_n \in B(n)$ with

$$c(f_n) > 1 - n^2/2^n$$

(ii) For every $\epsilon > 0$,

$$\frac{1}{|B(n)|} | \{ f \in B(n) \mid c(f) < 1 - \epsilon \} | < 2^{n^2 - \epsilon 2^n}$$

The proof of Theorem 1 is given below in Section 4. We are grateful to James Lynch for suggesting the formulation given in (ii).

2. Functions with low compositional complexity

Despite the fact that "most" functions have large values $c(f)$, we find, for many
interesting classes of functions, that \( c(f) \) approaches 0 (and hence \( \gamma(f) \) approaches 0) as \( n \) becomes large. Consider, for example, functions of \( n \) variables which can be computed in terms of weighted sums of functions of smaller numbers of variables. Say that \( h \in B(n) \) is a \( k \)-variable function if \( h \) depends on at most \( k \) variables. Then \( f \in B(n) \) is a function of an integral weighted sum of \( k \) variable functions if there exists \( g: \{1, 2, \ldots \} \to \{0, 1\} \) with

\[
f = g \left( \sum_{\alpha} w_{\alpha} h_{\alpha} \right)
\]

where \( \alpha \) ranges over all \( k \)-element subsets of \( n \), \( h_{\alpha} \) depends at most on the variables with indices in \( \alpha \) and the \( w_{\alpha} \) are integers. Notice that if the \( w_{\alpha} \) are allowed to be as large as \( 2^n \), then any function in \( B(n) \) can be represented in this form (in fact, with \( k = 1 \)). On the other hand, if the \( w_{\alpha} \) are restricted to smaller values, then the resulting functions have small complexity.

**Theorem 2.** Let \( k \) be a positive integer and \( f_n \in B(n) \) a sequence of functions, each of which can be represented as function of an integral weighted sum of \( k \)-variable functions. Suppose that the weights \( w_{\alpha,n} \) are bounded in absolute value by \( W_n \), with

\[
\log W_n = \frac{n}{k+1} - k \log_2 n - \psi(n)
\]

where \( \lim_{n \to \infty} \psi(n) = \infty \). Then \( \lim_{n \to \infty} c(f_n) = 0 \).

One class of functions subsumed by this result is the class of symmetric functions, which can be computed with \( w = 1 \), since the value of a symmetric function depends only on the number of 1's in the argument. Another nontrivial class contains most of the "fixed order perceptrons" studied by Minsky and Papert [7] in their investigation of computational geometry. (Although these need not satisfy the coefficient bound in general, most of the examples given in [7] have small values of \( w \).)

A second result on compositional complexity shows that a Boolean function cannot have large complexity if the number of elements it maps to zero is too small a fraction of the total number of elements. More precisely, for \( f \in B(A) \), let

\[
f^{-1}(0) = \{x \in \{0, 1\}^A \mid f(x) = 0\}
\]

Then we have:

**Theorem 3.** (i) Let \( f_n \in B(n) \) be a sequence of functions such that

\[
|f_n^{-1}(0)| \leq 2^n - \log_2 n - \psi(n)
\]

where \( \lim_{n \to \infty} \psi(n) = \infty \). Then \( \lim_{n \to \infty} c(f_n) = 0 \).

(ii) If \( f \in B(n) \) and \( |f^{-1}(0)| < 2^{n-2} \), then

\[
c(f) < 5 \sqrt{n} 2^{-n/2} |f^{-1}(0)|^{1/2} + n 2^{-n}.
\]
As a consequence, all Boolean functions which are significant in pattern recognition have small compositional complexity, since the significant patterns typically constitute a tiny fraction of the space of all possible (random) patterns. For example, let \( \text{CON}_k \) be the Boolean function defined over the set of all \( k \times k \) matrices of 0's and 1's with \( \text{CON}_k(M) = 1 \) if and only if the pattern of 1's in \( M \) is "kingwise connected," i.e., a chess king can visit all the 1's without stepping over a 0. Alternatively, we can consider patterns which are rookwise connected. The following result holds in either case:

**Corollary 4.** \( c(\text{CON}_k) \to 0 \) as \( k \to \infty \).

**Proof.** Partition the matrix into \( \left\lfloor k/3 \right\rfloor ^2 \) disjoint \( 3 \times 3 \) blocks, plus the remaining at most \( 4k \) elements. Now, unless there is just one 1 in the matrix, the existence of the subpattern

\[
\begin{array}{ccc}
0 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 0 \\
\end{array}
\]

in any block will make the whole pattern disconnected. So if we enumerate patterns by specifying, for each block, which of the \( 2^9 \) possible subpatterns it induces, together with the pattern induced in the remaining squares, we see that the number of connected patterns is bounded by

\[
k^2 + 2^{4k}(2^9 - 1)^{\lfloor k/3 \rfloor ^2} \leq k^2 + 2^{a k^2}
\]

where

\[
a = \frac{\log_2 511}{9} + \frac{4}{k}
\]

So for any sufficiently small fixed \( \varepsilon > 0 \) we have \( a < 1 - \varepsilon \) for \( k \) sufficiently large. Then applying Theorem 3(i) with \( n = k^2 \) yields the result. \( \square \)

(Other estimates of the number of connected patterns on a \( k \times k \) grid are given in [8].)

A final result relates compositional complexity to the decomposition techniques of traditional switching theory [2]. A function will turn out to have small complexity if it can be expressed as the superposition of two functions, each of a significantly smaller number of variables than the original, even when the decomposition is not disjoint:

**Proposition 5.** If \( f_n \in B(n) \) is a sequence of functions admitted by a sequence of support systems of the form \( (A_n, B_n) \), where \( n = |A_n| \) and \( n = |B_n| \) both approach infinity as \( n \to \infty \), then \( \lim_{n \to \infty} c(f_n) = 0 \).
3. Universal support systems

This section includes some remarks on support systems which admit all functions of \( n \) variables. A support system \( H \in S(n) \) is called universal if \( N(H) = 2^{2^n} \). Two obviously universal systems are \( H = \{1, 2, \ldots, n\} \) and \( H = (\{1\}, \{2\}, \ldots, \{n\}) \).

Another example of a universal system is \( H = (S_1, S_2, S_3, S_4) \) where \( S_1 = \{1\}, S_2 = \{n\}, S_3 = \{2, \ldots, n\} \), and \( S_4 = \{1 \ldots n - 1\} \). To show that this is universal, given any \( f \in B(n) \), let \( h_1(x_1) = x_1, h_2(x_n) = x_n \) and define \( h_3 \) and \( h_4 \) by

\[
\begin{align*}
  h_3(0, x_2, \ldots, x_{n-1}) &= f(0, x_2, \ldots, x_{n-1}, 0), \\
  h_3(1, x_2, \ldots, x_{n-1}) &= f(1, x_2, \ldots, x_{n-1}, 1), \\
  h_4(x_2, \ldots, x_{n-1}, 0) &= f(1, x_2, \ldots, x_{n-1}, 0), \\
  h_4(x_2, \ldots, x_{n-1}, 1) &= f(0, x_2, \ldots, x_{n-1}, 1).
\end{align*}
\]

Then \( g(x_1, x_n, h_3, h_4) \) examines the values of \( x_1 \) and \( x_n \) and returns the value of the appropriate \( h \).

In general, the number of sets \( r \) in a support system \( H = (S_1, \ldots, S_r) \) is called the length of the system, and \( p = \max_i |S_i| \) is called the order. Thus, for the three universal systems given above, the first has length 1 and order \( n \) the second has length \( n \) and order 1, the third has length 4 and order \( n - 1 \). We will show that, in any universal system, either the length or the order must be close to \( n \).

First of all, note that in the functional decomposition \( f = g(h_1, \ldots, h_r) \) given by \( H \) there are \( 2^{2^r} \) possible choices for the function \( g \). In addition, there are \( 2^{2^{|S_i|}} \) possible choices for each \( h_i \in B(S_i) \). However, if \( \overline{h} \) denotes the function whose value is the Boolean complement of the value of \( h \), then any composition \( f = g(h_1, \ldots, h_r) \) which can be constructed using \( \overline{h} \) can also be constructed by using \( h \) and suitably modifying the function \( g \). Therefore, in counting the number of distinct compositions, we need consider only half of the possible \( h_i \). The number of functions admitted by a support system \( H \) of length \( r \) and order \( p \) is therefore bounded by

\[
\log_2 N(H) \leq 2^r + \sum_{i=1}^r 2^{|S_i|} - r \leq 2^r + r(2^p - 1)
\]

(1)

This yields the following facts:

**Proposition 6.** If \( r \) and \( p \) are, respectively, the length and order of a universal support system \( H \in S(n) \), then

(i) \( 2^r + r(2^p - 1) \geq 2^n \).

(ii) If \( r < n \), then \( p > (n - 1) - \log_2(n - 1) \).

(iii) If \( p < n - \log_2 n \), then \( r > n - \log_2 n \).

The following example provides a family of universal support systems with length and order close to the limits given by Proposition 6. For any positive integer \( b < n \), set \( p = n - b \), \( S_i = \{1, \ldots, p\} \) for \( i = 1, \ldots, 2^b \), and \( S_{2^b+i} = \{p+i\} \) for \( i = 1, \ldots, b \). This system has order \( p = n - b \) and length \( r = b + 2^b \), and we claim that it is universal.
Note that, for any positive integer $k$, choosing $b = \log_2(n/k)$ yields a system with $p = n - \log_2(n/k)$ and $r = (n/k) + \log_2(n/k)$.

To demonstrate the claim of universality, set, for clarity, $y_i = x_{p+i}, i = 1, \ldots, b$. Now let $h_i, i = 1, \ldots, 2^b$ be defined by

$$h_i(x_1, x_2, \ldots, x_p) = h_{y_1 y_2 \cdots y_b}(x_1, x_2, \ldots, x_p) = f(x_1, x_2, \ldots, x_p, y_1, \ldots, y_b)$$

where the $y_1 y_2 \cdots y_b$ is the $b$-bit binary representation of $i$. Then

$$f(x_1, \ldots, x_p, y_1, \ldots, y_b) = \text{select}(y_1, \ldots, y_b; h_1(x_1, x_2, \ldots, x_p), \ldots, h_{2^b}(x_1, x_2, \ldots, x_p))$$

where select uses the values of the $y_i$ to select the appropriate $h_i$.

This example is "minimal" in another sense. If we set $A = \bigcup_k x_k$ and $B = \bigcup_k y_k$, then no partial function in the support system depends both on elements of $A$ and elements of $B$. (That is, the support system is disconnected when viewed as a bipartite graph in the obvious way). Moreover, if we choose $b$ such that $2^b < p$, then there will be fewer than $|A|$ functions $h_i$ with supports in $A$. We show that, for a universal support system which is "disconnected", at most one of the "components" can have this property.

**Proposition 7.** Let $A$ and $B$ be disjoint finite sets, with $|A| \leq |B|$. Let $H_1 \in S(A), H_2 \in S(B)$, and suppose that $H_1 \cup H_2 \in S(A \cup B)$ is universal. Then length $(H_1) \geq |A|$.

**Proof.** We may assume, without loss of generality, that $A = \{1, \ldots, m\}$ and $B = \{m+1, \ldots, n\}$ where $m \leq \frac{1}{2} n$. Consider the function $f \in B(n)$ such that

$$f^{-1}(1) = \{x \in \{0, 1\}^n \mid (x_1, \ldots, x_m) = (x_{m+1}, \ldots, x_{2m})\}$$

If length $(H_1) < m$, then there must be distinct sequences $(x_1, \ldots, x_m), (x'_1, \ldots, x'_m)$, for which the partial functions on $H_1$ all give the same value, and therefore $f$ cannot be represented using $H_1 \cup H_2$. \[\square\]

In fact, this result can be extended to show that, if length $(H_2) < |B|$, then $\log_2$ length $(H_2)$ $\geq$ length $(H_1)$. See [1], Lemma 2.3.4.

Here is one further observation concerning universal support systems. Notice that if $H = (S_1, \ldots, S_n)$ is a universal support system on a set $A$, then, for any $a \in A$, the system $H_a = (S_1 \setminus \{a\}, \ldots, S_n \setminus \{a\})$ is universal on $A \setminus \{a\}$. But the converse is false. Consider, for example, the support system $H \in B(n)$ defined by

$$H = (\{1, 2\}, \{2, 3\}, \ldots, \{n-1, n\})$$

For any $i \in n$, the system

$$H_i = (\{1, 2\} \setminus \{i\}, \{2, 3\} \setminus \{i\}, \ldots, \{n-1, n\} \setminus \{i\})$$

is easily seen to be universal. But $H$ itself is not universal. This follows from
Proposition 6 for \( n \geq 5 \), and the cases \( n = 2, 3, 4 \) can be verified directly. In fact, the non-universality of \( H \) for \( n = 3 \) shows that the necessary condition (i) of Proposition 6 is not also sufficient: For \( n = 3, p = 2, r = 2 \) we have
\[
2^r + r(2^p - 1) = 10 > 2^n = 8
\]
and yet there is no universal support system on \( \{1, 2, 3\} \) with rank 2 and order 2. (We are grateful to the referee for pointing this out).

4. Proof of Theorem 1

The proof of Theorem 1 is based on the following lemma.

**Lemma 8.** If \( H \in S(n) \), then there exists \( H_0 \in S(n) \) such that:
(i) \( \text{length} (H_0) \leq n \), and if \( H \) is not universal then \( \text{length} (H_0) < n \).
(ii) For any \( f \in B(n) \), \( H \) admits \( f \) if and only if \( H_0 \) admits \( f \).

**Proof.** Let \( H = (S_1, \ldots, S_r) \) and let \( I \subseteq \mathcal{R} \) be a minimal set such that
\[
| \bigcup_{i \in I} S_i | < | I |.
\]
(If no such \( I \) exists then we are done, since then \( r \leq n \)). We may assume that all \( S_i \) are non-empty. For any \( j \in I \) we have
\[
| I | - | \bigcup_{i \in I \setminus \{j\}} S_i | \geq \bigcup_{i \in I \setminus \{j\}} S_i | \geq | I | - 1
\]
where the rightmost inequality arises from the minimality of \( I \). This implies
\[
| \bigcup_{i \in I \setminus \{j\}} S_i | = | I | - 1 \tag{2}
\]
and
\[
S_j \subseteq \bigcup_{i \in I \setminus \{j\}} S_i \tag{3}
\]

Now fix \( j_0 \in I \). By the definition of \( I \), we have
\[
| \bigcup_{i \in J} S_i | \geq | J |
\]
for every \( J \subseteq I \setminus \{j_0\} \). This fact, together with (2) and (3), allows us to apply the matching theorem of Hall [4] to deduce that there exists for every \( i \in I \setminus \{j_0\} \) an \( s_i \in S_i \) such that \( s_i \leftrightarrow S_i \) is a bijection between \( I \setminus \{j_0\} \) and \( \bigcup_{i \in I \setminus \{j_0\}} S_i \). So if we choose \( h_i \) to be \( x_{s_i} \) we have that the sequence \( h_i, i \in I \setminus \{j_0\} \) yields \( x_s \) for all \( s \in \bigcup_{i \in I \setminus \{j_0\}} S_i \). Therefore the set \( S_{j_0} \) can be omitted from the sequence \( H \) without diminishing the set of functions admitted by \( H \). Repeating this procedure wherever applicable, we finally get a subsequence \( H_0 \) of \( H \) satisfying (ii) and the first part of (i).

To get the second part of (i) notice that the above argument yields \( H_0 \) such that
for every subsequence \( S_{i_1}, \ldots, S_{i_t} \) of \( H_0 \) we have

\[
\left| \bigcup_{k=1}^t S_{i_k} \right| > t
\]

Hence using Hall's theorem again we see that \( H_0 \) is universal unless length \((H_0) < n\). \( \square \)

**Completion of Proof of Theorem 1.** To prove part (i) suppose to the contrary that for every \( f \in B(n) \), there exists a support system \( H \) which admits \( f \) and admits at most \( 2^{2n-n^2} \) functions. By Lemma 8 we may assume that the length of \( H \) is at most \( n \). There are \( 2^{n^2} \) support systems of length \( n \), and fewer than \( 2^{n^2} \) non-universal support systems of length \( n \). So our assumption leads to the conclusion that there would be a collection of fewer than \( 2^{n^2} \) sets, each of cardinality at most \( 2^{2n-n^2} \) which cover the set of all functions \( B(n) \). But this is impossible since \( B(n) \) has cardinality \( 2^{2n} \).

To prove (ii), let \( B_c(n) \) be the set \( \{ f \in B(n) \mid c(f) < 1 - \varepsilon \} \). Thus every \( f \in B_c(n) \) is admitted by a support system \( H \) with \( N(H) < 2^{2n(1-\varepsilon)} \). Since \( H \) may be assumed to have length at most \( n \) by Lemma 8, we see that \( B_c(n) \) is covered by \( 2^{n^2} \) sets, each of cardinality less than \( 2^{2n(1-\varepsilon)} \). Thus \( |B_c(n)| < 2^{n^2 + 2^{n(1-\varepsilon)}} \), and (ii) follows. \( \square \)

### 5. Proofs of Theorems 2, 3 and Proposition 5

**Proof of Theorem 2.** We construct a support system which admits \( f_n \). Begin by partitioning the set \( n \) into \( k+1 \) disjoint subsets \( T_1, \ldots, T_{k+1} \) of cardinality \( \lfloor n/(k+1) \rfloor \) or \( \lceil n/(k+1) \rceil + 1 \). Then set \( U_i = n \setminus T_i \), \( i = 1, \ldots, k+1 \). Now any \( \alpha \subseteq n \) of cardinality \( k \) can intersect at most \( k \) of the \( T_i \) and hence must be contained in at least one \( U_i \). So if we define

\[
A_i = \{ \alpha \subseteq n \mid \alpha \subseteq U_i \text{ with } i \text{ minimal} \},
\]

then each \( \alpha \) will be contained in precisely one \( A_i \). If \( f \) is given by

\[
f = g \left( \sum_a w_a h_a \right),
\]

let

\[
p_i = \sum_{a \in A_i} w_a h_a
\]

Then \( p_i \) can be computed by examining only those elements in \( U_i \). Moreover, since the cardinality of \( U_i \) is bounded by \( C_i = nk/(k+1) + 1 \), we have \( |A_i| \) is no greater than the number of \( k \)-element subsets of \( U_i \) which is less than \( \frac{1}{2} C_i^k \). Each \( p_i \) is thus an integer of absolute value less than \( \frac{1}{2} WC_i^k \) and so can be encoded using \( C_2 = \log_2 WC_i^k \) bits. This means that we can construct a support system \( H \) which admits \( f \) by assigning \( C_2 \) sets \( S \) to each of the \( U_i \). Let the \( C_2 \) partial functions assigned to \( U_i \) compute a binary representation of \( p_i \). Then \( f \) can be computed by summing all the \( p_i \) and applying \( g \).
The order of $H$ is at most $C_1$ and the length is $(k+1)C_2$. Therefore by the inequality (1) we have
\[
\sigma(f) \leq 2^{-n} \log_2 N(H) \leq 2^{(k+1)C_2-n} + (k+1)C_2(2^{C_2-n} - 2^{-n})
\]

Since $C_1 = n - \log_2 n - \psi(n)$ and $C_2$ is approximately linear in $n$ for large $n$, we see that the second term in the above equation goes to zero as $n$ approaches infinity. For the first term, the exponent of 2 is
\[
(k+1)\log_2 W + k(k+1)\log_2 C_1 - n = k(k+1)\log_2 \frac{C_1}{n} - (k+1)\psi(n)
\]
which approaches negative infinity as $n$ increases. Hence the first term approaches 0 as well. \(\square\)

**Proof of Theorem 3(i).** Set $k = \left\lfloor n - \log_2 n - \frac{1}{2} \psi(n) \right\rfloor$ and let $J$ be the set of all sequences $(x_1, \ldots, x_k) \in \{0, 1\}^k$ such that there exist $x_{k+1}, \ldots, x_n$ with $f(x_1, \ldots, x_n) = 0$. By hypothesis
\[
\log_2 |J| \leq n - \log_2 n - \psi(n)
\]

Let $H$ be the support system in which the set $\{1, \ldots, k\}$ occurs $\left\lfloor n - \log_2 n - \frac{1}{2} \psi(n) \right\rfloor + 2$ times and each singleton $\{k+1\}, \ldots, \{n\}$ occurs once. We claim that $H$ admits $f_n$. In fact, let $h_1, \ldots, h_{\left\lfloor n - \log_2 n - \frac{1}{2} \psi(n) \right\rfloor + 2}$ be the partial functions with support $\{1, \ldots, k\}$. Then $h_1$ can transmit whether or not $(x_1, \ldots, x_k)$ belongs to $J$. If the answer is yes, then, by (4), the remaining $h$'s can encode which element of $J$ this is. With that information and the values of $x_{k+1}, \ldots, x_n$, we can compute $f(x_1, \ldots, x_n)$.

The support system $H$ contains $\left\lfloor n - \log_2 n - \frac{1}{2} \psi(n) \right\rfloor + 2$ sets of size $k$ and $n-k$ sets of size 1. So, by the inequality (1) we have
\[
\log_2 N(H) \leq 2^n - k + \left\lfloor n - \log_2 n - \frac{1}{2} \psi(n) \right\rfloor + 2
\]
\[
+ (2^k - 1) \left\lfloor n - \log_2 n - \frac{1}{2} \psi(n) \right\rfloor + 2 \right) \div (n-k)
\]
\[
\leq 2^n - \frac{\left\lfloor n - \log_2 n - \frac{1}{2} \psi(n) \right\rfloor + 2}{n} + (n-k)
\]
\[
\leq 5 \cdot 2^n - \frac{\psi(n)/2 + n - \psi(n)/2}{n} + (n-k)
\]
and so $c(f_n) \leq 2^{-n} \log_2 N$ approaches 0 as $n$ becomes large.

The proof of (ii) is similar. \(\square\)

**Proof of Proposition 5.** This is immediate from the inequality (1):
\[
c(f_n) \leq 2^{|A_n|} - n - 1 \div 2^{|B_n|} - n - 1 + 2^{2-n}
\]
approaches 0 as $n \to \infty$. \(\square\)
References