# On Ultrafilters and NP

S. Ben-David
Dept. of Computer Science
The Technion
Haifa, Israel

M. Karchmer*
Mathematics Dept.
MIT
Cambridge, MA 02139

E. Kushilevitz
Dept. of Computer Science
The Technion
Haifa, Israel

## Abstract

We further develop the *Fusion Method* by exploring its similarities with the Ultraproduct Construction in Model Theory. We use this analogy to re-prove a result of Sipser regarding countable circuits, in a simpler way. In the finite case this analogy allows us to give a new characterization of co-NP in terms of the CLIQUE function. This gives a natural interpretation to the NP-completeness of the CLIQUE function.

## Introduction

In this paper we further develop the analogy between Razborov's Generalized Approximation Method and the Ultraproduct Construction in Model Theory [3]. This analogy, in all its variations, has been named the *Fusion Method* [10].

The *Fusion Method* has many different incarnations (see [10] for a survey). Razborov originally used it to characterize the classes $P$ and $NL$ [6, 7]. He also used it to give a super-linear lower bound for the complexity of the Majority function on Switching-and-Rectifying Networks [7]. Karchmer [3] shows that the monotone size lower bounds for clique can be cleanly stated using this method. Also, he shows that the method can be used to characterize $NP$. Karchmer & Wigderson [4] use the method to give a different characterization of $NP$, more algebraic in its nature. Finally, Karchmer & Wigderson [5] give a characterization of $\oplus \cdot L$ and a non-linear lower bound for the majority function on this model.

Here we show that the method can be used to generalize Sipser's theorem that Analytic Sets are not closed under complementation and to simplify his proof [8]. Stated in the words of Boolean Circuits, this result says that there is a function $f : \{0,1\}^\omega \mapsto \{0,1\}$ which can be computed by non-deterministic countable circuits but whose negation $\bar{f}$ cannot be so computed. That is, in the infinite case, $NP \neq co-NP$.

Our proof is simpler in two ways. First, we do not have to convert the circuit into a CNF formula as Sipser does. Last, and most importantly, we do not have to instantiate every input and non-deterministic variable as in the original proof. Rather, we use the Theory of Ultrafilters to instantiate only the necessary variables to get a contradiction. Other than these two differences, the two proofs are essentially identical. One of the aims of this paper is to show that the Fusion Method is the right framework to carry out the idea of *Limit Points* as outlined by Sipser [9].

In the second part of this paper we propose a finite analogue to the proof of the infinite case. We do this by extracting some of the combinatorial arguments in the proof. At the end, we get a characterization of $co-NP$ based on the CLIQUE function. This characterization is particularly appealing in the case that the function $f$ is monotone or anti-monotone. In this case, it is enough to concentrate on the minterms and maxterms of $f$ and the characterization captures the monotonicity in a very natural way.

*Partially supported by NSF grant CCR-9212184 and DARPA contract N00014-92-J-1799.

This characterization is not much different than the statement that CLIQUE is $NP$-complete. In fact, in retrospect, it is not difficult to come up with this characterization from first principles rather than going through the analogy with Ultraproducts. We feel however that the present proof endows the $NP$-completeness proof of CLIQUE with a very natural interpretation.

# 1 Background

## 1.1 Boolean Circuits

Let $B_\alpha$, for $\alpha \leq \omega$, denote the set of all Boolean functions $f : \{0,1\}^\alpha \mapsto \{0,1\}$. A *Boolean Circuit* is a directed acyclic graph with $2\alpha$ sources and one sink. Sources are labeled by literals from $\{x_1, \cdots, x_\alpha\} \cup \{\neg x_1, \cdots, \neg x_\alpha\}$ and nodes are labeled by one of the two Boolean operations (gates) $\{\vee, \wedge\}$. In the finite case, i.e. when $\alpha < \omega$, we assume that the fan-in of all inner nodes is 2; In the infinite case, where $\alpha = \omega$, we allow arbitrary (possibly infinite) fan-in. A Boolean circuit $C$ computes a function in $B_\alpha$ in a natural way. In the same way, any inner node of $C$ computes a function in $B_\alpha$. For a function $f \in B_\alpha$ let $s(f)$ and $s_\wedge(f)$ denote the size and number of $\wedge$-gates of an optimal circuit that computes $f$.

A *non-deterministic* circuit is a circuit whose sources are labeled by $\{x_1, \cdots, x_\alpha\} \cup \{\neg x_1, \cdots, \neg x_\alpha\} \cup \{y_1, \cdots, y_\beta\} \cup \{\neg y_1, \cdots, \neg y_\beta\}$. A non-deterministic circuit computes a function $f \in B_\alpha$ as follows: For $x \in \{0,1\}^\alpha$, $f(x) = 1$ iff there exists a setting of the non-deterministic variables, $\{y_1, \cdots, y_\beta\}$, which makes the circuit output 1. For a function $f$, denote by $ns(f)$ and $ns_\wedge(f)$ the size and number of $\wedge$-gates of an optimal non-deterministic circuit for $f$.

A *co-non-deterministic* circuit is a non-deterministic circuit with the following acceptance criteria: For $x \in \{0,1\}^\alpha$, $f(x) = 0$ iff there exist a setting of the non-deterministic variables which makes the circuit output 0. For a function $f$, denote by $\bar{n}s(f)$ and $\bar{n}s_\wedge(f)$ the size and number of $\wedge$-gates of an optimal co-non-deterministic circuit for $f$.

Even though it is known that most functions in $B_n$ require exponential size, to this date, the best lower bound on circuit size for an explicit function is $4n$ [11]. In particular, the following problem is beyond our present capabilities: Show that, for some $L \in \cup_{c>0} DTIME(2^{cn})$ the family of functions $f = \{f_n\}$, $n < \omega$ with $f_n \in B_n$ defined by $f_n^{-1}(1) = L \cap \{0,1\}^n$ requires super-linear circuit size (i.e. $s(f_n) = \omega(n)$). This problem precludes the obvious diagonalization argument and seems to require a *combinatorial* proof. For more background on Circuit Complexity the reader is referred to [1].

## 1.2 Ultrafilters

We now give the basic definitions concerning Ultrafilters. We refer the interested reader to [2] for a good introduction to Ultrafilters and Ultraproducts. Let $U$ be any set. For a set $A \subseteq U$, we denote its complement by $A^c$. A collection $\mathcal{C}$ of subsets of $U$ is *upward-closed* iff $A \in \mathcal{C}$ and $A \subseteq B$ implies $B \in \mathcal{C}$.

**Definition 1** *An* Ultrafilter $\mathcal{U}$ *over* $\mathcal{P}(U)$ *is an upward-closed collection of subsets of* $U$ *which is closed under finite intersections and such that for every* $A \subseteq U$*, exactly one of* $A$ *and* $A^c$ *is in* $\mathcal{U}$*.*

For example, the collection of all subsets that contain a given element $u_0 \in U$ is an Ultrafilter. Such Ultrafilters are called *principal* and are said to be *generated* by $u_0$. A *non-principal* Ultrafilter is one which is not principal. It is well known that if $U$ is infinite then there are non-principal Ultrafilters over $\mathcal{P}(U)$. Also, an Ultrafilter is non-principal iff it does not contain a finite set. Finally, note that for every Ultrafilter $\mathcal{U}$ over $\mathcal{P}(U)$, $\emptyset \notin \mathcal{U}$ and $U \in \mathcal{U}$.

Intuitively, we use a non-principal Ultrafilter over $\mathcal{P}(U)$ to define a notion of "large subsets". Clearly, co-finite subsets should be considered large. Similarly, the intersection of a finite number of large subsets should also be considered large. Therefore, if we have a non-principal Ultrafilter $\mathcal{U}$ we can say that a set $A$ is large iff $A \in \mathcal{U}$.

The Ultraproduct construction in Model Theory uses Ultrafilters to *combine* different models over the same language to obtain a new model. The new model is essentially different from any of the original models. However, the new model behaves like an average model in the original collection in that it satisfies a sentence $\phi$ iff *most* of the original models satisfy $\phi$. The analogy with the *Fusion Method* will become clear in the next section. The following definition and lemma are fundamental:

**Definition 2** *A collection $\mathcal{C}$ of subsets of $U$ has the* finite intersection property *(f.i.p.) iff any finite number of subsets from $\mathcal{C}$ has a non-empty intersection.*

**Lemma 1** *A collection $\mathcal{C}$ of subsets of $U$ can be extended to an Ultrafilter over $\mathcal{P}(U)$ iff $\mathcal{C}$ has the finite intersection property.*

For example, if $U$ is infinite then the collection of all co-finite subsets has the f.i.p. and by the lemma, it can be extended to a (non-principal) Ultrafilter.

## 2 The method & Countable Circuits

In this section we describe the method in a loose manner. For a more formal description we refer the reader to [3]. Lets say that we want to show that a given function $f \in B_\omega$ cannot be computed by countable co-non-deterministic circuits. The idea is to prove that if the circuit rejects all the inputs that should be rejected, then it also rejects an input that should be accepted. More formally, let $U = f^{-1}(0)$ and let $C$ be a countable co-non-deterministic circuit which allegedly computes $f$. We will assume that $C$ rejects all vectors in $U$. We are going to *combine* rejecting computations of vectors in $U$ to form a rejecting computation for a vector in $f^{-1}(1)$, together with its witness for rejection, thereby providing a proof that $C$ does not compute $f$ correctly.

We will proceed in two stages. In the first stage we will assign to each wire of $C$ a value from the Boolean Algebra $\mathcal{P}(U)$. This will be done as follows: Fix a rejecting witness $w_u$ for each $u \in U$. For a sub-function (wire) $g$ of $C$ let $[|g|] = \{u \in U : g(u, w_u) = 1\}$. It is easy to see that $[|\cdot|]$ can be extended to a homomorphism from $B_\omega$ to $\mathcal{P}(U)$. Furthermore, it is clear that $[|\bar{C}|] = \emptyset$ where $\bar{C}$ is the output wire of $C$ (this is because for each $u \in U$, $w_u$ is a rejecting witness).

In the second stage we will choose an Ultrafilter $\mathcal{U}$ over $\mathcal{P}(U)$. We will use $\mathcal{U}$ to give Boolean values to the functions in $B_\omega$. We will give a function $g$ the value 1 iff $[|g|] \in \mathcal{U}$. In this way, any Ultrafilter $\mathcal{U}$ *defines* a Boolean vector $z \in \{0,1\}^\omega$ by letting $z_i = 1$ iff $[|x_i|] \in \mathcal{U}$.

Recall that $[|\bar{C}|] = \emptyset$ where $\bar{C}$ is the output wire of $C$. As $\emptyset \notin \mathcal{U}$, any Ultrafilter will assign the value 0 to the output of $C$. Also, note that $\mathcal{U}$ gives values to the non-deterministic inputs of $C$ ($\mathcal{U}$ gives a non-deterministic input $y_i$ a value according to whether $[|y_i|] \in \mathcal{U}$. Note that $[|y_i|] = \{u \in U :$ the $i$th bit of $w_u$ is $1\}$). Therefore, any Ultrafilter $\mathcal{U}$ which gives consistent values to the wires of the circuit and which defines a vector in $f^{-1}(1)$, constitutes a proof that $C$ does not compute $f$ correctly.

Clearly, if for some $u_0 \in U$ we use the principal Ultrafilter generated by $u_0$, then any function $g \in B_\omega$ gets the value $g(u_0)$. This Ultrafilter will give consistent values to the wires of $C$ giving a proof that $C$ rejects $u_0$. This is no surprise as we assumed that $C$ rejects all members of $U$. Clearly, if we wish to get a vector in $f^{-1}(1)$ we have to use non-principal Ultrafilters.

Actually, as discussed in [3], it is enough to make sure that the values given by $\mathcal{U}$ to the wires of $C$ are *greater* than the actual values. This is because $\mathcal{U}$ will give $\bar{C}$ the value 0 and therefore $\mathcal{U}$ constitutes a proof that $C$ rejects the vector defined by $\mathcal{U}$. Notice that, because any Ultrafilter is upward-closed, the value given to the output wire of an $\vee$-gate is always greater than the $\vee$ of the values given to the input gates. Therefore, we do not have to worry about the consistency of the $\vee$-gates.

From now on, we shall view any Boolean functions $g$ as the subset $[|g|] \subseteq U$. Similarly, we shall view any $\wedge$-gate, with countable fan-in $\wedge_{j<\omega} g_j$, as the countable collection of subsets $\{[|g_j|]\}_{j<\omega}$.

We say that an Ultrafilter *preserves* the $\wedge$-gate if it gives consistent values to the wires of the gate. Consider an $\wedge$-gate $\{A_j\}_{j<\omega}$. To make sure that an Ultrafilter $\mathcal{U}$ preserves this gate, we have to make sure that it contains either $\cap_{j<\omega} A_j$ or one of the sets $A_j^c$, for some $j < \omega$. Note that these sets constitute a *countable cover* of $U$. Therefore, every $\wedge$-gate defines a countable cover of $U$ and an Ultrafilter $\mathcal{U}$ preserves the $\wedge$-gate iff it contains at least one of the subsets of the cover. We encapsulate this in the following proposition:

**Proposition 1** *A countable co-non-deterministic circuit for $f$ induces a countable collection of countable covers of $U = f^{-1}(0)$, one for each $\wedge$-gate. Any Ultrafilter $\mathcal{U}$ preserves the $\wedge$-gates of $C$ iff it contains at least one set from each cover.*

We conclude this subsection with a countable analogue of the characterization, due to Karchmer [3], of co-non-deterministic circuit size in terms of sets of covers of the zeros of a function.

**Theorem 1** *For every function, $f \in B_\omega$, the following conditions are equivalent:*

1. *For any countable collection of countable covers of $U = f^{-1}(0)$ there exists some $x \in f^{-1}(1)$ and a collection of subsets, one from each cover, which, together with the sets $\{\{u \in U : u_i = x_i\} : i \in \omega\}$, have the finite intersection property.*
2. *There is no countable co-non-deterministic circuit for $f$.*

**Proof:**

$(1 \Rightarrow 2)$ The general idea of the proof is as follows: Assume that $C$ is a countable co-non-deterministic circuit for $f$. Apply the assumption of the theorem to the collection of covers induces, as in Proposition 1, by this circuit. Now apply Lemma 1 to extend this collection of subsets to an ultrafilter (over $U$). The vector defined by such an ultrafilter is the vector $x$, which is a member of $f^{-1}(1)$, and, by Proposition 1, the ultrafilter preserves the gates of $C$. The above discussion have shown that such an ultrafilter constitutes a counter-example to the assumption that $C$ computes the function $f$.

$(2 \Rightarrow 1)$ Assume, by way of contradiction, that $\{K_i : i \in \mathcal{N}\}$ is a sequence of countable covers of $U$ such that, $x \in f^{-1}(1)$ implies that no collection of subsets, one from each cover, together with the sets $\{\{u \in U : u_i = x_i\} : i \in \omega\}$, has the finite intersection property. Note that, for every $x \in f^{-1}(0)$, choosing from each $K_i$ a set to which $x$ belongs, does amount to a collection that, with $\{\{u \in U : u_i = x_i\} : i \in \omega\}$, has the finite intersection property. We conclude that the problem of computing $f(x)$ reduces to determining whether there exists a collection of members of the $K_i$'s that, together with $\{\{u \in U : u_i = x_i\} : i \in \omega\}$, has the finite intersection property. As the collection of relevant sets, as well as the collection of all finite intersections of these sets, is countable, the answer to this question can be computed by a countable non-deterministic circuit. (For further details, see [3] where the finite analogue of this theorem is proved).

■

### 2.1 The lower bound for clique

Let $\mathcal{G}$ denote the class of all countable undirected graphs. We think of such graphs as encoded by the set of variables $\{x_{i,j} : i, j \in \mathcal{N}\}$ where $x_{i,j} = 1$ iff the graph has the edge $\{i, j\}$. Let $CLIQUE_\omega \in B_\omega$ be the function defined by: '$CLIQUE_\omega(x) = 1$ *iff $x$ has an infinite clique*'.

**Theorem 2** *There is no countable co-non-deterministic circuit for $CLIQUE_\omega$.*

**Proof:** We wish to apply Theorem 1. Given any countable collection of countable covers of ${CLIQUE_\omega}^{-1}(1)$, let us enumerate its members by $\{K_i : i \in \mathcal{N}\}$. We will show that, for some infinite $S \subseteq \mathcal{N}$, there is a collection of subsets, one from each cover, which, together with the sets of the form $[|x_{i,j}|]$ where $i, j \in S$, has the finite intersection property (note that any vector, $x$, such that for all $i, j \in S$, $x_{i,j} = 1$, is a member of ${CLIQUE_\omega}^{-1}(1)$).

For technical convenience, let us concentrate on the set of subgraphs of $< \mathcal{N}^*, E^* >$, where $\mathcal{N}^*$ denotes the set of all finite sequences of natural numbers and $E^* \rightleftharpoons \{(\sigma, \tau) : \sigma$ *is an initial segment of* $\tau$*, or* $\tau$ *is an initial segment of* $\sigma\}$. Let $U$ be the set of all such subgraphs that have no infinite clique. We shall define inductively a sequence $U = U_0 \supseteq U_1 \supseteq U_2 \supseteq \ldots$ and a sequence $\sigma_1, \sigma_2, \ldots$ of finite sequences of natural numbers such that (1) for all $i < j$, $\sigma_i$ is a proper initial segment of $\sigma_j$, and (2) $U_i$ is a subset of one of the members in the $i$th cover, $K_i$, and of $\cap_{i<j}[|x_{\sigma_i,\sigma_j}|]$. Clearly, the collection $\{U_i\}_{i<\omega}$ together with the collection $\{[|x_{\sigma_i,\sigma_j}|]\}_{i<j}$ has the f.i.p..

The following definition and lemma, which are modeled after an idea of Sipser [8], play a central role in the proof of the theorem:

**Definition 3** *Let $H$ be a graph and $Q \subseteq H$ a clique in $H$. Let $\sigma^Q$ denote the maximal sequence in $Q$ (i.e, every $\tau$ in $Q$ is an initial segment of $\sigma^Q$).*

- *$H/Q$ denotes the operation of "shrinking" $Q$ in $H$ into a single vertex $(0)$ (i.e., $H/Q$ has an edge between $\tau$ and $(0)$ iff $\tau$ is connected in $H$ to all members of $Q$), and "re-naming" the vertices accordingly (each sequence of the form $\sigma^Q\tau$ is replaced by the sequence $0\tau$).*

*Let $U' \subseteq U$ be the set of all connected graphs in $U$.*

- *We say that $\mathcal{A} \subseteq U$ is $Q$-*big *iff $\{H/Q : H \in \mathcal{A}$, and $Q$ is a clique in $H\} \supseteq U'$. Note that $\mathcal{A}$ is $Q$-big iff so is the set $\mathcal{A} \cap \{H : Q$ is a clique in $H\}$.*

**Lemma 2** *Let $Q$ be a finite set (of natural numbers) and $\mathcal{A}$ be $Q$-big. Then, for every $\{\mathcal{A}_i\}_{i<\omega}$, a cover of $\mathcal{A}$, and every sequence $j_1 < j_2 < \ldots$ of natural numbers, there exists $i \in \mathcal{N}$ such that $\mathcal{A}_i$ is $Q \cup \{\sigma^Q j_i\}$-big.*

**Proof:** Assume, by way of contradiction, that for all $i$, there exists some $G_i \in U'$ such that there is no $G \in \mathcal{A}_i$ for which $Q_i = Q \cup \{\sigma^Q j_i\}$ is a clique in $G$ and $G/Q_i = G_i$. Let $\otimes G_i$ be a graph in $U'$ such that $(\otimes G_i)/\{(0j_i)\} = G_i$, for every $i$ (to construct such a graph, replace the minimal vertex of $G_i$ by the singleton sequence $(j_i)$, then connect the root $(0)$ to this smallest vertex in each $G_i$, and finally, rename the vertices as needed). As $\mathcal{A}$ is $Q$-big, there exists $H \in \mathcal{A}$ such that $Q$ is a clique in $H$ and $H/Q = \otimes G_i$. The definition of $H/Q$ implies that for all $i$, $Q_i$ is a clique in $H$ and $H/Q_i = G_i$. As $\{\mathcal{A}_i\}_{i<\omega}$ covers $\mathcal{A}$, there exists some $i$ such that $H \in \mathcal{A}_i$ contradicting the choice of $G_i$. ■

We now inductively define the sets $U_i$ and the sequence $\{\sigma_i\}_{i<\omega}$. Assume $U = U_0 \supseteq U_1 \supseteq \ldots \supseteq U_k$ are already defined, in a way that $U_k$ is $\{\sigma_1, \ldots, \sigma_k\}$-big. Let $\{B_i\}_{i<\omega}$ be the cover of $U$ corresponding to the $(k+1)$th $\wedge$-gate. Let $U'_k = U_k \cap \{H : Q$ is a clique in $H\}$ and $\mathcal{A}_i = B_i \cap U'_k$. Note that $\{H : Q$ is a clique in $H\}$ is exactly $\cap_{i<j\leq k}[|x_{\sigma_i,\sigma_j}|]$. We get that the set $U'_k$ is $Q$-big and is covered by $\{\mathcal{A}_i\}_{i<\omega}$. Apply the lemma to get a subset $\mathcal{A}_i$ which is $Q \cup \{\sigma^Q i\}$-big. We can now take this $\mathcal{A}_i$ to be $U_{k+1}$ and $\sigma^Q i$ to be $\sigma_{k+1}$. ■

The reader is encouraged to compare this proof with the original one due to Sipser. The main difference is that, in the present proof, we do not have to instantiate every single input and non-deterministic variable. It is enough to make sure that the Ultrafilter contains enough sets to ensure that it preserves all of the $\wedge$-gates of the circuit and that it defines a graph with an infinite clique.

## 3 Finite Ultrafilters and $NP$

In this section we propose a *finite analogue* to the previous argument. Fix a function $f \in B_n$ which we believe is not in $co - NP$ and let $U = f^{-1}(0)$. We start by giving a finite analogue to the concept of Ultrafilters.

**Definition 4** *Let $U$ be a finite set. A* Finite Ultrafilter *$\mathcal{U}$ over $U$ is an upward-closed collection of subsets of $U$ such that for every $A \subseteq U$, exactly one of $A$ or $A^c$ is in $\mathcal{U}$.*

This definition is a slight variation of a definition in [3] in which it was only required that for every $A$, *at least one* of $A$ or $A^c$ be in $\mathcal{U}$. Note that we do not require that $\mathcal{U}$ be closed under intersections. As in the previous section, we say that $\mathcal{U}$ *defines* a vector $z \in \{0,1\}^n$ by letting $z_i = 1$ iff $[|x_i|] \in \mathcal{U}$. Similarly, $\mathcal{U}$ preserves (a fan-in 2) $\wedge$-gate, $g \wedge h$, iff $[|g|] \in \mathcal{U}$ and $[|h|] \in \mathcal{U}$ implies that $[|g|] \cap [|h|] \in \mathcal{U}$. We will view the $\wedge$-gate, $g \wedge h$, as the pair of subsets $([|g|], [|h|])$.

In [3], it was shown that one could use Finite Ultrafilters to 'fuse' rejecting computations of 0's of a hard function (not in $co-NP$) to get a rejecting computation of a 1 of the function (just as we did in the previous section). As stated in the introduction, this is merely a reformulation of Razborov's Generalized Method of Approximations [6] coupled with the observation due to Karchmer & Wigderson [4] that using Finite Ultrafilters (instead of the Finite Filters proposed by Razborov) one could characterize $co - NP$. The following definition and theorem makes this precise.

**Definition 5 ([3])** *For a function $f \in B_n$ let $\varrho(f)$ be the minimum size of a collection $\Lambda$ of pairs of subsets of $f^{-1}(0)$ such that there is no Finite Ultrafilter which defines a vector in $f^{-1}(1)$ and which preserves $\Lambda$.*

**Theorem 3** *[[3]] For any $f \in B_n$, $\bar{n}s_\wedge(f) \geq \varrho(f)$. Conversely, $\bar{n}s_\wedge(f) = O(\varrho(f))$.*

Our aim is to further develop this idea by following along the steps taken in the proof of the infinite case. We start by giving a finite analogue to the *finite intersection property*. For the rest of this section, we will only consider *Finite* Ultrafilters and we will refer to them only as Ultrafilters.

**Definition 6** *A collection $\mathcal{C}$ of subsets has the* pair-wise intersection property (p.i.p) *if for any two subsets $A, B \in \mathcal{C}$, $A \cap B \neq \emptyset$.*

**Proposition 2** *A collection of subsets $\mathcal{C}$ can be extended to a finite Ultrafilter $\mathcal{U}$ iff $\mathcal{C}$ has the p.i.p.*

**Proof:** Note that any Ultrafilter has the p.i.p. and therefore, if $\mathcal{C} \subseteq \mathcal{U}$ then $\mathcal{C}$ has the p.i.p. as well.

Conversely, Suppose that $\mathcal{C}$ has the p.i.p.. Let $\mathcal{C}'$ be a maximal upward-closed collection which includes $\mathcal{C}$ and which has the p.i.p.. We claim that $\mathcal{C}'$ is an Ultrafilter. Otherwise, there exist a set $A$ such that neither it nor its complement is in $\mathcal{C}'$. As $A \notin \mathcal{C}$, there is a set $B \in \mathcal{C}$ such that $A \cap B = \emptyset$. But $B \subseteq A^c$ and $C'$ is upward-closed, a contradiction. ∎

Now, suppose that we want to show the existence of an Ultrafilter that preserves a collection of $\wedge$-gates. The idea is to use a collection $\mathcal{C}$ that guarantees that the $\wedge$-gates of the circuit are preserved. Then if $\mathcal{C}$ has the p.i.p. we can extend $\mathcal{C}$ to an Ultrafilter $\mathcal{U}$ and finish the proof.

For an Ultrafilter $\mathcal{U}$ to preserve an $\wedge$-gate $(A, B)$, it has to contain at least one of the sets $A^c$, $B^c$ or $A \cap B$. Clearly, these sets form a cover of $U$. We now claim that, without loss of generality, these sets form a *partition* of $U$. This is because, intuitively, it is more restrictive to put a smaller set in $\mathcal{U}$ than it is to put a bigger set. If $A^c \cap B^c \neq \emptyset$ then pick subsets $\bar{A} \subseteq A^c$ and $\bar{B} \subseteq B^c$ such that $\bar{A} \cap \bar{B} = \emptyset$ and $\bar{A} \cup \bar{B} = A^c \cup B^c$. Any $\mathcal{U}$ that contains one of the sets of the partition, contains also one of the sets of the cover. To conclude, any $\wedge$-gate induces a partition of $U$ into 3 classes (a *3-partition*) such that an Ultrafilter preserves the $\wedge$-gate iff it contains exactly one class of the partition. We encapsulate this in the following proposition.

**Proposition 3** *A co-non-deterministic circuit with $t$ $\wedge$-gates induces a collection of $t$ 3-partitions of $U$. An Ultrafilter preserves all $\wedge$-gates iff it contains exactly one set in each of the 3-partitions.*

If we want to define an Ultrafilter that preserves a collection of partitions, it is enough to pick one class from each partition in such a way that the chosen classes have the p.i.p.. We can then use proposition 2 to extend this collection to an Ultrafilter that will necessarily preserve all the partitions.

Similarly, if we want to define an Ultrafilter $\mathcal{U}$ that defines a given vector $z \in \{0,1\}^n$, we have to include in $\mathcal{U}$ the sets $[|x_i|]$ if $z_i = 1$ and $[|\neg x_i|]$ if $z_i = 0$. Note that if the function $f$ is such that for every $i \neq j$ and $a, b \in \{0,1\}$ there exists a vector $u \in U$ such that $u_i = a$ and $u_j = b$, then for any vector $z \in \{0,1\}^n$ there is always an Ultrafilter that defines $z$. This is because the collection of sets of the form $[|x_i|]$ or $[|\neg x_i|]$ that we need to include to define $z$ has the p.i.p.. Of course, the challenge is to show the existence of an Ultrafilter that both preserves the $\wedge$-gates of the circuit *and* defines a vector in $f^{-1}(1)$.

For a subset $A \subseteq U$, define a vector $\rho^A \in \{0,1,*\}^n$ by

$$\rho_i^A = \begin{cases} 0 & \text{if } A \cap [|x_i|] = \emptyset \\ 1 & \text{if } A \cap [|\neg x_i|] = \emptyset \\ * & \text{otherwise} \end{cases}$$

For a vector $\rho \in \{0,1,*\}^n$ and a vector $x \in \{0,1\}^n$ we write $\rho \sqsubseteq x$ iff for every $i \in \{1,...,n\}$, $\rho_i \in \{0,1\}$ implies that $\rho_i = x_i$. In this case we say that $x$ is an *extension* of $\rho$. Two vectors $\rho, \rho' \in \{0,1,*\}^n$ are *compatible* if they have a common extension. The following proposition is immediate:

**Proposition 4** *If $\rho^A$ and $\rho^B$ are incompatible then $A \cap B = \emptyset$.*

Note that any Ultrafilter $\mathcal{U}$ which contains $A$ can only define extensions of $\rho^A$. The following Proposition generalizes this fact:

**Proposition 5** *Let $\mathcal{C}$ be a collection of subsets with the p.i.p. and such that there exists a common extension $z$ of the vectors $\rho^C$ for $C \in \mathcal{C}$. Then $\mathcal{C}$ can be extended to an Ultrafilter $\mathcal{U}$ that defines $z$.*

This motivates the following definition:

**Definition 7** *A* Graph System *of dimension $n$ consistes of a graph $G = (V, E)$, an integer $t \geq 0$ and for each $v \in V$, a vector $\rho(v) \in \{0,1,*\}^n$. For $x \in \{0,1\}^n$, let $V_x \rightleftharpoons \{v \mid \rho(v) \sqsubseteq x\}$. The* size *of the system is the cardinality of $V$.*

**Definition 8** *We say that a Graph System of dimension $n$* computes *a function $f \in B_n$ if for every $x \in \{0,1\}^n$, $f(x) = 0$ iff the induced graph on $V_x$ has a clique of size $t$.*

It is easy to see that any function can be computed by a Graph System of exponential size. The following is the main theorem of this section:

**Theorem 4** *A language $L$ defined by $\{f_n\}_{n<\omega}$ is in $co-NP$ iff there exists a polynomial $p(n)$ such that for every $n$, the function $f_n$ is computed by a Graph System of dimension $n$ and size $p(n)$.*

**Proof:** Suppose that for every $n$, the function $f_n$ is computed by a Graph System of size $p(n)$. Then, for every $n$ there is a co-non-deterministic circuit of polynomial size which, on input $z$, checks whether the induced graph on $V_z$ has a clique of size $t$.

Conversely, suppose that for every $n$, $C_n$ is a co-non-deterministic circuit for $f_n$ with $t$ $\wedge$-gates. Consider the collection of $t$ 3-partitions of Proposition 3. Let $G$ be the intersection graph of the $3t$ subsets of the partitions. Furthermore, for a node $v$ associated with the set $A$, let $\rho(v) = \rho^A$. We claim that this Graph System computes $f_n$.

Let $z \in \{0,1\}^n$ be such that the induced subgraph on $V_z$ has a clique of size $t$. Note that this clique contains one node associated with one set from each of the $t$ 3-partitions (this is because 2 sets from the same 3-partition are disjoint). Also, the associated sets have the p.i.p.. Furthermore, $z$ is a common extension of the corresponding vectors. By Proposition 5, we can define an Ultrafilter $\mathcal{U}$ that contains each of the sets from the clique and which defines $z$. This Ultrafilter defines a rejecting computation for $z$.

Now let $z \in \{0,1\}^n$ be such that $f(z) = 0$. Then $z \in U$ so that each of the 3-partitions has a set which contains $z$. Therefore, all of these sets intersect and the corresponding nodes in $G$ form a clique of size $t$. From the definition of $\rho(v)$, it is clear that $z$ is a common extension of the corresponding vectors. This is because if $z \in A$ and $z_i = 1$ then $A \cap [|x_i|] \neq \emptyset$ and hence, $\rho_i^A \in \{1,*\}$ (similarly if $z_i = 0$). ■

Note that the proof says a bit more. It says that any function which has co-non-deterministic circuits with $t$ $\wedge$-gates can be computed by a Graph System of size $3t$. The graph $G$ is $t$-partite with 3 nodes in each class, is $t$-colorable and its clique number is $t$.

Also, note that if a Graph System with graph $G$ computes $f$ then we can define the corresponding vectors $\rho(v)$. This is done as follows. For each $z$ such that $f(z) = 0$ there is a clique, $q_z$, in $G$ of size $t$ such that all the nodes in $q_z$ have vectors below $z$. For a node $v$ in $G$ define $\rho(v)$ as the largest vector below all $z$'s such that $v \in q_z$. It is easy to see that these vectors together with $G$ constitute a Graph System for $f$.

**Corollary 1** *CLIQUE is $NP$-complete.*

We say that a function $f \in B_n$ is a *read-once clique* function if it can be computed by a Graph System of size $n$ such that for every $v_i \in V$, $\rho(v_i)$ is the vector with a 1 in coordinate $i$ and *'s elsewhere. Clearly, $\rho(v_i) \sqsubseteq x$ iff $x_i = 1$. These functions are clearly anti-monotone. Their minimal 0's are precisely the cliques of $G$ of size $t$.

**Corollary 2** *There are read-once clique functions which are $co-NP$ complete.*

We can modify the definition of a Graph System to get a cleaner characterization for the class of monotone, or anti-monotone, functions in $co-NP$. A function is *anti-monotone* if its negation is monotone. We want to stress that the following characterization does not weaken the system in any way. It just uses the monotonicity of the function in a natural way without restricting the computational power of the Graph Systems.

**Definition 9** *An* (anti)-monotone *Graph System is a Graph System where, for every $v \in V$, $\rho(v) \in \{0,*\}^n$ ($\rho(v) \in \{1,*\}^n$).*

It is easy to see that an (anti)-monotone Graph System computes only (anti)-monotone functions. The following companion to Theorem 4 relates (anti)-monotone Graph System's to the class of (anti)-monotone languages in $co-NP$.

**Theorem 5** *An (anti)-monotone language $L$ defined by a familiy of (anti)-monotone functions $\{f_n\}_{n<\omega}$ is in $co-NP$ iff there exists a polynomial $p(n)$ such that for every $n$, the function $f_n$ is computed by an (anti)-monotone Graph System of dimension $n$ and size $p(n)$.*

**Proof:** The "if" part is obvious. The converse follows from the following claim: If $G$ is a Graph System that computes a monotone function $f$, then $G'$ is a monotone Graph System that also computes $f$, where $G'$ is based on the same graph as $G$ is but with the following $\rho$-vectors: For $v \in V$, $\rho'(v)$ is the same as $\rho(v)$ except that if $\rho(v)_i = 1$ then $\rho'(v)_i = *$. We omit the easy proof of this claim in this extended abstract. The anti-monotone case is identical. ■

Note that in the case that $f$ is monotone, or anti-monotone, it is enough to test the Graph System on the minterms and maxterms of $f$. In this case, every maxterm of $f$ corresponds to a clique of its Graph System.

## References

[1] R. Boppana, M. Sipser, "The Complexity of finite functions", In: *The Handbook of Theoretical Computer Science*, (J. van Leeuwen, ed.), Elsevier Science Publishers B.V., 1990 pp. 759-804.

[2] C.C. Chang, and H.J. Keisler, "Model Theory", Studies in Logic, Vol. 73, North Holland, 1990.

[3] M. Karchmer, "On proving lower bounds for circuit size", *Proceedings of the 8th Annual Symposium on Structure in Complexity Theory*, (1993).

[4] M. Karchmer, A. Wigderson, "Characterizing non-deterministic circuit size", *Proceedings of the 25th STOC*, (1993).

[5] M. Karchmer, A. Wigderson, "On Span Programs", *Proceedings of the 8th Annual Symposium on Structure in Complexity Theory*, (1993).

[6] A.A. Razborov, "On the method of approximations", *Proceedings of* $21^{st}$ *STOC*, (1989) pp. 167-176.

[7] A.A. Razborov, "Lower bounds on the size of switching-and-rectifier networks for symmetric Boolean functions", *Math. Notes of the Academy of Sciences of the USSR*, 48(6), pp. 79-91, (1990).

[8] M. Sipser, "A topological view of some problems in complexity theory", *Colloquia Mathematica Societatis János Bolyai* **44**, pp. 387-391, (1984).

[9] M. Sipser, "The history and status of the $P$ versus $NP$ question", *Proceedings of* $24^{th}$ *STOC*, pp. 603-618, (1992).

[10] A. Wigderson, "The fusion method for lower bounds in circuit complexity", *Combinatorics, Paul Erdös is Eighty (Vol 1)*, Miklós, Sós and Szönyi (Eds.), Bolyai Math. Society, pp. 453–468, (1993).

[11] U. Zwick, "A $4n$ lower bound on the combinatorial complexity of certain symmetric Boolean functions over the basis of unary dyadic Boolean functions", *SIAM J. on Computing*, 20(3), pp. 499-505 (1991).