Simple Characterization of Functionally Complete One-Element Sets of Propositional Connectives

Petar Maksimović
Faculty of Mathematics, University of Belgrade
Studentski trg 16, 11000 Belgrade
Serbia
petarmax@sezampro.yu

Predrag Janičić
Faculty of Mathematics, University of Belgrade
Studentski trg 16, 11000 Belgrade
Serbia
janicic@matf.bg.ac.yu

Abstract

A set of propositional connectives is said to be *functionally complete* if all propositional formulae can be expressed using only connectives from that set. In this paper we give sufficient and necessary conditions for a one-element set of propositional connectives to be functionally complete. These conditions provide a simple and elegant characterization of functionally complete one-element sets of propositional connectives (of arbitrary arity).

1 Introduction

Transforming a propositional formula (in this paper, we consider only classical propositional logic) into a logically equivalent one is used in many different contexts. In many situations, it is plausible to have a formula represented via only a limited set of propositional connectives. A set of propositional connectives is said to be *functionally complete* if all propositional formulae can be expressed using only connectives from that set.

Digital systems that require use of certain logic circuits may use complete sets of connectives, as all logical gates can be constructed in terms of connectives from that set. For instance, many circuits are constructed using only the connective $\uparrow$, which constitutes a functionally complete set of connectives on its own. It is known that there is exactly one more connective of arity 2 which constitutes a functionally complete set on its own: $\downarrow$.

Functionally complete sets of connectives can also be used in developing deductive systems, with axioms and production rules that use only the connectives from that set. This leads to elegant deductive systems, appropriate for different kinds of formal analysis.

In 1941., Post gave the necessary and sufficient conditions for an arbitrary set of connectives to be functionally complete [6]. The main purpose of this work done by Post was the complete description of the lattice of functionally closed sets of Boolean functions. As a byproduct, he obtained the five precomplete sets (today also called *Post's classes*), and developed the following criterion for the completeness of an arbitrary set of Boolean functions: a set of Boolean functions is complete if and only if for each of the five conditions for precompleteness there is a function in that set which lacks that property. An overview of Post's results can be found in [2]. In [5], the authors concentrate on Post's criterion for the completeness of an arbitrary set of Boolean functions and rewrite his proof. This result is also reported in various works in computer switching theory. In a more general context, complete sets of connectives (not necessarily Boolean), have been studied — under the name *primal algebras* — in the field of universal algebra and different properties of primal algebras, related to Post's theorem, have been proved [1, 7]. There are also results regarding complete sets of connectives (i.e., universal p-valued logic gates) for multiple-valued logic [3] and characterization conditions for some special cases.

In this paper, we give a simple characterization of functionally complete one-element sets of connectives of arbitrary arity with a new, short proof, independent of Post's theorem. From that characterization, it simply follows that there are $2^{2^n-2} - 2^{2^{n-1}-1}$ functionally complete one-element sets of connectives of arity n.

2 Preliminaries

Let $\mathcal{F}$ be any set of Boolean functions of arbitrary arity. Each $\varphi \in \mathcal{F}$ is designated by a unique connective c_φ, and often we will identify a Boolean function with its corresponding connective. By $\mathrm{F}m(\mathcal{F})$ we denote the set of all logical formulae built with the connectives c_φ ($\varphi \in \mathcal{F}$) and a given countable set $S = \{p_1, p_2, \ldots\}$ of propositional variables, written in any canonical form. From an algebraic viewpoint, we can see $\mathrm{F}m(\mathcal{F})$ as the free algebra of type $(c_\varphi : \varphi \in \mathcal{F})$ generated by the set S. If $A = A(p_{i_1}, \ldots, p_{i_k})$ is a formula containing k variables $p_{i_1}, \ldots, p_{i_k}$, then A induces a k-ary Boolean function $\overline{A} : \{0,1\}^k \longrightarrow \{0,1\}$ as follows: the value $\overline{A}(x_1, \ldots, x_k)$ is obtained by interpreting the variables by a valuation $v : S \longrightarrow \{0,1\}$ with $v(p_{i_\kappa}) = x_\kappa$ ($\kappa = 1, \ldots, k$) and the connectives c_φ in A by φ as

$$\overline{A}(x_1, \ldots, x_k) = v(A(p_{i_1}, \ldots, p_{i_k})) ,$$

where $v : \mathrm{F}m(\mathcal{F}) \longrightarrow \{0,1\}$ denotes the canonical homomorphism of type $(c_\varphi : \varphi \in \mathcal{F})$ given by the valuation v of the variables and the interpretation $c_\varphi \longrightarrow \varphi$ of the connectives. The set of all valuations of the variables in S is denoted by

Ω, and $v(A)$, for $A \in \mathrm{F}m(\mathcal{F})$ and $v \in \Omega$, is called the *value* of the formula A by the valuation v. Formulae $A, B \in \mathcal{F}$ are called logically equivalent (denoted by $A \equiv B$), if $v(A) = v(B)$ for all $v \in \Omega$. It is clear that $v(A(p_{i_1}, \dots, p_{i_k})) = \overline{A}(v(p_{i_1}), \dots, v(p_{i_k}))$.

A Boolean function φ (its corresponding connective c_φ) is called *definable by a set* $\mathcal{F}$ of Boolean functions (by the corresponding set of connectives), if $\varphi = \overline{A}$ for some formula $A \in \mathrm{F}m(\mathcal{F})$. The set of all Boolean functions definable by $\mathcal{F}$ is called the *functional closure* of $\mathcal{F}$, and is denoted by $[\mathcal{F}]$. A set $\mathcal{F}$ is called *functionally closed*, if $\mathcal{F} = [\mathcal{F}]$. If $\mathcal{F}$ is functionally closed and $\mathcal{E} \subseteq \mathcal{F}$ such that $[\mathcal{E}] = \mathcal{F}$, we say that $\mathcal{F}$ is generated by $\mathcal{E}$, and if $\mathcal{E}$ is functionally independent as well (i.e. a minimal generator), then $\mathcal{E}$ is called a *basis* for $\mathcal{F}$. A set $\mathcal{F}$ of Boolean functions is called *functionally complete* if $[\mathcal{F}]$ is equal to the set of all Boolean functions.

An n-ary Boolean function φ (and its corresponding connective c_φ) can be defined via a truth-table

p_1	p_2	$\dots$	p_{n-1}	p_n	$\varphi(p_1, \dots, p_n)$
0	0	$\dots$	0	0	t_0
$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$
α_1	α_2	$\dots$	α_{n-1}	α_n	t_α
$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$
1	1	$\dots$	1	1	t_{2^n-1}

where t_α is the value of the formula $c_\varphi(p_1, \dots, p_n)$ for a given valuation $v \in \Omega$ and α is a number with a binary representation made of the digits $v(p_1) = \alpha_1, \dots, v(p_n) = \alpha_n$. For instance:

p_1	p_2	p_3	if-then-else(p_1, p_2, p_3)
0	0	0	$t_0 = 0$
0	0	1	$t_1 = 1$
0	1	0	$t_2 = 0$
0	1	1	$t_3 = 1$
1	0	0	$t_4 = 0$
1	0	1	$t_5 = 0$
1	1	0	$t_6 = 1$
1	1	1	$t_7 = 1$

Another possibility is the description of an n-ary function $\varphi \in [\mathcal{F}]$ or its corresponding connective c_φ via a defining formula $A \in \mathrm{F}m(\mathcal{F})$ as $\varphi = \overline{A}$. For instance, a defining formula for if-then-else(p_1, p_2, p_3) is $A(p_1, p_2, p_3) = (p_1 \wedge p_2) \vee (\neg p_1 \wedge p_3)$.

Examples of logical connectives are $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\uparrow$, $\downarrow$, defined by the following truth-tables:

p_1	$\neg(p_1)$
0	$t_0 = 1$
1	$t_1 = 0$

p_1	p_2	$\wedge(p_1, p_2)$
0	0	$t_0 = 0$
0	1	$t_1 = 0$
1	0	$t_2 = 0$
1	1	$t_3 = 1$

p_1	p_2	$\vee(p_1, p_2)$
0	0	$t_0 = 0$
0	1	$t_1 = 0$
1	0	$t_2 = 0$
1	1	$t_3 = 1$

p_1	p_2	$\Rightarrow (p_1, p_2)$
0	0	$t_0 = 1$
0	1	$t_1 = 1$
1	0	$t_2 = 0$
1	1	$t_3 = 1$

p_1	p_2	$\uparrow (p_1, p_2)$
0	0	$t_0 = 1$
0	1	$t_1 = 1$
1	0	$t_2 = 1$
1	1	$t_3 = 0$

p_1	p_2	$\downarrow (p_1, p_2)$
0	0	$t_0 = 1$
0	1	$t_1 = 0$
1	0	$t_2 = 0$
1	1	$t_3 = 0$

The sets $\{\neg, \wedge\}$, $\{\neg, \vee\}$ and $\{\neg, \Rightarrow\}$ are complete and independent. The connectives $\vee$, $\Rightarrow$, $\uparrow$, $\downarrow$, if-then-else are definable in $\{\neg, \wedge\}$, as follows:

$$
\begin{array}{rcl}
A \vee B & = & \neg(\neg A \wedge \neg B) \\
A \Rightarrow B & = & \neg(A \wedge \neg B) \\
A \uparrow B & = & \neg(A \wedge B) \\
A \downarrow B & = & \neg A \wedge \neg B.
\end{array}
$$

The sets $\{\uparrow\}$ and $\{\downarrow\}$ (with connectives known as the *Sheffer stroke* (or *nand*) and *Lukasiewicz's function* (or *nor*)) are examples of functionally complete one-element sets of binary connectives (it was first proved in [8] that $\{\uparrow\}$ is a functionally complete set of connectives), and it is well-known that these are the only such sets with a binary connective.

3 Characterization Theorem

The connectives $\uparrow$ and $\downarrow$ are the only two (out of $2^{2^2} = 16$) binary connectives which constitute functionally complete sets on their own. This gives a characterization of functionally complete one-element sets of connectives of arity 2. In the following text, we give sufficient and necessary conditions for a one-element set of connectives of arbitrary arity to be complete. Since it can be trivially shown that there are no unary connectives which constitute functionally complete sets on their own, in the further discussion we consider only connectives of arity bigger than 1.

In the following text we use the values denoted t_α, defined as in the previous section.

Lemma 3.1 *If an n-ary connective ρ fulfills the conditions*

- $t_0 = 1$*;*
- $t_{2^n-1} = 0$*;*

- *there is an x, $0 < x < 2^{n-1}$, such that t_x and t_{2^n-1-x} are equal;*

then the set $\{\rho\}$ is a functionally complete one-element set.

Proof: Let there be an x, $0 < x < 2^{n-1}$, such that $t_x = t_{2^n-1-x}$. Binary representations for x and for $2^n - 1 - x$ have all digits distinct (i.e., complementary), so the truth table for $\rho(p_1, \ldots, p_n)$ has the following form:

p_1	p_2	$\ldots$	p_{n-1}	p_n	$\rho(p_1, \ldots, p_n)$
0	0	$\ldots$	0	0	t_0
$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$
x_1	x_2	$\ldots$	x_{n-1}	x_n	t_x
$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$
$1 - x_1$	$1 - x_2$	$\ldots$	$1 - x_{n-1}$	$1 - x_n$	t_{2^n-1-x}
$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$
1	1	$\ldots$	1	1	t_{2^n-1}

Let us define a binary connective τ in the following way: $\tau(p_1, p_2) \equiv \rho(A_1, \ldots, A_n)$, where

$$A_i = \begin{cases} p_1, & \text{if } x_i = 0, \\ p_2, & \text{if } x_i = 1. \end{cases}$$

For $v(p_1) = 0, v(p_2) = 0$, it holds that $v(A_i) = 0$, and for $v(p_1) = 1, v(p_2) = 1$, it holds that $v(A_i) = 1$.

For $v(p_1) = 0, v(p_2) = 1$, it holds:

$$v(A_i) = \begin{cases} 0, & \text{if } x_i = 0, \\ 1, & \text{if } x_i = 1. \end{cases}$$

i.e., $v(A_i) = x_i$.

For $v(p_1) = 1, v(p_2) = 0$, it holds:

$$v(A_i) = \begin{cases} 1, & \text{if } x_i = 0, \\ 0, & \text{if } x_i = 1. \end{cases}$$

i.e., $v(A_i) = 1 - x_i$.

Therefore, the truth table for τ is as follows:

p_1	p_2	A_1	A_2	$\ldots$	A_n	$\tau(p_1, p_2)\,(\equiv \rho(A_1, \ldots, A_n))$
0	0	0	0	$\ldots$	0	t_0
0	1	x_1	x_2	$\ldots$	x_n	t_x
1	0	$1 - x_1$	$1 - x_2$	$\ldots$	$1 - x_n$	t_{2^n-1-x}
1	1	1	1	$\ldots$	1	t_{2^n-1}

According to the assumptions, it holds that $t_0 = 1$ and $t_{2^n-1} = 0$, and also $t_x = t_{2^n-1-x} = 1$ or $t_x = t_{2^n-1-x} = 0$.

If $t_x = t_{2^n-1-x} = 1$, then the truth table for τ is:

p_1	p_2	$\tau(p_1, p_2)$
0	0	1
0	1	1
1	0	1
1	1	0

which is the truth table for the connective $\uparrow$. Since $\{\uparrow\}$ is a functionally complete set of connectives and since $\uparrow$ is definable by $\{\rho\}$, it follows that $\{\rho\}$ is also a complete set of connectives.

If $t_x = t_{2^n-1-x} = 0$, then the truth table for τ is:

p_1	p_2	$\tau(p_1, p_2)$
0	0	1
0	1	0
1	0	0
1	1	0

which is the truth table for the connective $\downarrow$. Since $\{\downarrow\}$ is a functionally complete set of connectives and since $\downarrow$ is definable by $\{\rho\}$, it follows that $\{\rho\}$ is also a complete set of connectives. $\Box$

Before we proceed with proving that the above conditions are necessary, we have to prove one more lemma.

Lemma 3.2 *Let us suppose that $\{\rho\}$ is a functionally complete one-element set with an n-ary connective ρ, and that there is no x, $0 \leq x < 2^{n-1}$, such that t_x and t_{2^n-1-x} are equal. Then $\rho(A_1, \ldots, A_n)$, where $A_i \in \{p_1, p_2, \neg p_1, \neg p_2\}$, is logically equivalent to one of the following formulae: p_1, $\neg p_1$, p_2, $\neg p_2$.* [1]

Proof: The truth table for $\rho(A_1, \ldots, A_n)$, where $A_i \in \{p_1, p_2, \neg p_1, \neg p_2\}$ has the following form:

p_1	p_2	$\neg p_1$	$\neg p_2$	A_1	A_2	$\ldots$	A_n	$\rho(A_1, \ldots, A_n)$
0	0	1	1	α_1	α_2	$\ldots$	α_n	t_α
0	1	1	0	β_1	β_2	$\ldots$	β_n	t_β
1	0	0	1	γ_1	γ_2	$\ldots$	γ_n	t_γ
1	1	0	0	δ_1	δ_2	$\ldots$	δ_n	t_δ

Notice that for each A_i, it holds that $\delta_i = 1 - \alpha_i$ and $\gamma_i = 1 - \beta_i$, which means that $\delta = 2^n - 1 - \alpha$ and $\gamma = 2^n - 1 - \beta$. Following the assumption

[1] Note that here $\neg$ stands for a definition of this connective in the complete set $\{\rho\}$, for instance, $\neg p = \rho(p, p, \ldots, p)$.

of the lemma, it holds that $t_\delta \neq t_\beta$ and $t_\gamma \neq t_\beta$, and so (since these values can only be 0 or 1) $t_\delta = 1 - t_\beta$ and $t_\gamma = 1 - t_\beta$. We prove the lemma by considering the following four cases:

1. If $t_\alpha = 0$ and $t_\beta = 0$, then $t_\gamma = 1$ and $t_\delta = 1$, which means that $\rho(A_1, \ldots, A_n) \equiv p_1$.
2. If $t_\alpha = 0$ and $t_\beta = 1$, then $t_\gamma = 0$ and $t_\delta = 1$, which means that $\rho(A_1, \ldots, A_n) \equiv p_2$.
3. If $t_\alpha = 1$ and $t_\beta = 0$, then $t_\gamma = 1$ and $t_\delta = 0$, which means that $\rho(A_1, \ldots, A_n) \equiv \neg p_2$.
4. If $t_\alpha = 1$ and $t_\beta = 1$, then $t_\gamma = 0$ and $t_\delta = 0$, which means that $\rho(A_1, \ldots, A_n) \equiv \neg p_1$.

$\square$

Now, we are ready to prove that the above conditions are necessary.

Lemma 3.3 *If $\{\rho\}$ is a functionally complete one-element set with an n-ary connective ρ, then the following conditions are fulfilled:*

- $t_0 = 1$;
- $t_{2^n-1} = 0$;
- *there is an x, $0 < x < 2^{n-1}$, such that t_x and t_{2^n-1-x} are equal.*

Proof: If $t_0 = 0$ or if $t_{2^n-1} = 1$, then $\neg$ would not be definable by $\{\rho\}$ and, hence, $\{\rho\}$ would not be a complete set of connectives. Hence, it holds that $t_0 = 1$ and $t_{2^n-1} = 0$.

Let us suppose that there is no x, $0 < x < 2^{n-1}$, such that t_x and t_{2^n-1-x} are equal. Then, by Lemma 3.2 (as t_0 and t_{2^n-1} are not equal and also there is no x, $0 < x < 2^{n-1}$, such that t_x and t_{2^n-1-x} are equal), $\rho(A_1, \ldots, A_n)$, where $A_i \in \{p_1, p_2, \neg p_1, \neg p_2\}$, is logically equivalent to p_1, $\neg p_1$, p_2, or $\neg p_2$. If $\{\rho\}$ is a functionally complete set of connectives, then $p_1 \uparrow p_2$ can be represented in terms of ρ. In that representation, each subexpression $\rho(A_1, \ldots, A_n)$, where $A_i \in \{p_1, p_2, \neg p_1, \neg p_2\}$ (and of course, each subexpression $\rho(A_1, \ldots, A_n)$, where $A_i \in \{p_1, p_2\}$) can be rewritten to p_1, $\neg p_1$, p_2, or $\neg p_2$, keeping the current formula logically equivalent to the original one. Trivially, this iterative rewriting process terminates and the representation for $p_1 \uparrow p_2$ is rewritten to p_1, $\neg p_1$, p_2, or $\neg p_2$. However, this is a contradiction as $p_1 \uparrow p_2$ is not logically equivalent to either of these formulae. Therefore, we conclude that our assumption was wrong and hence, there must be an x, $0 < x < 2^{n-1}$, such that t_x and t_{2^n-1-x} are equal, which we wanted to prove. $\square$

The lemmas 3.1 and 3.3 give the characterization theorem:

Theorem 3.4 *For a connective ρ, the set $\{\rho\}$ is complete if and only if the following conditions are fulfilled:*

- $t_0 = 1$;
- $t_{2^n-1} = 0$;
- *there is an x, $0 < x < 2^{n-1}$, such that t_x and t_{2^n-1-x} are equal.*

¿From the above characterization, it simply follows that there are $2^{2^n-2} - 2^{2^{n-1}-1}$ (out of 2^{2^n}) complete one-element sets of connectives of arity n. Indeed, from the set of all one-element sets of connectives we have to discard all having $t_0 = 0$ (thus halving the starting current number 2^{2^n}); next we have to discard all having $t_{2^n-1} = 0$ (again, halving the current number and getting 2^{2^n-2}); finally, in the remaining set, we have to discard all the connectives such that pairs t_x and t_{2^n-x-1} are distinct for each x $(0 < x < 2^n - 1)$ — there is one such connective for each combination of the values t_1, t_2, ...,$t_{2^{n-1}-1}$ (there are $2^{n-1} - 1$ of these values t_i), hence, there are $2^{2^{n-1}-1}$ of them.

Theorem 3.5 *There are $2^{2^n-2} - 2^{2^{n-1}-1}$ functionally complete one-element sets of connectives of arity n $(n \geq 1)$.*

Example 3.6 *The connectives* if-then-else (left) and (*ad-hoc* defined) ρ (right) of arity 3 are given by the following tables.

p_1	p_2	p_3	if-then-else(p_1, p_2, p_3)	
0	0	0	$t_0 = 0$	
0	0	1	$t_1 = 1$	$\leftarrow$
0	1	0	$t_2 = 0$	
0	1	1	$t_3 = 1$	
1	0	0	$t_4 = 0$	
1	0	1	$t_5 = 0$	
1	1	0	$t_6 = 1$	$\leftarrow$
1	1	1	$t_7 = 1$	

p_1	p_2	p_3	$\rho(p_1, p_2, p_3)$	
0	0	0	$t_0 = 1$	$\leftarrow$
0	0	1	$t_1 = 0$	
0	1	0	$t_2 = 0$	
0	1	1	$t_3 = 1$	$\leftarrow$
1	0	0	$t_4 = 1$	$\leftarrow$
1	0	1	$t_5 = 1$	
1	1	0	$t_6 = 1$	
1	1	1	$t_7 = 0$	$\leftarrow$

For if-then-else, the values t_1 and t_{2^3-1-1} are equal, however, $t_0 \neq 1$, so {if-then-else} is not a complete set. For ρ, the values t_3 and t_{2^3-1-3} are equal. Since $t_0 = 1$ and $t_{2^3-1} = 0$, $\{\rho\}$ is a complete set. We can represent $a \uparrow b$ in terms of ρ in the following way: $a \uparrow b \equiv \rho(a, b, b)$.

4 Conclusions and Future Work

In this paper, we have given a complete characterization of functionally complete one-element sets of connectives. This characterization can be seen as a consequence of Post's theorem [6], while our simple proof is new and independent of previous results. We have also shown that there are $2^{2^n-2} - 2^{2^{n-1}-1}$ functionally complete one-element sets of connectives of arity n.

In our further work, we will look for applications of this result in expressing logical circuits in terms of only one available gate, but also in building deductive systems using only one connective. For instance, in [4], short single axiom systems are discussed and explored; the shortest presented axiom is of length 15 and has 3 variables. By analogy, axiom systems for propositional calculus can be built using propositional connectives which constitute complete sets on their own. We will investigate if the given characterization conditions for complete sets of connectives can have an impact on the corresponding deductive systems.

Acknowledgment. We are grateful to an anonymous reviewer for a number of detailed and useful comments and suggestions on the previous version of this paper.

References

[1] Alfred L. Foster and Alden F. Pixley. Semi-categorical algebras. *Mathematische Zeitschrift*, 85(2), 1964.

[2] S. W. Jablonski, G. P. Gawrilow, and W. P. Kudrjawzew. *Boolean functions and Posts classes (in Russian)*. Nauka, Moskow, 1968. (German translation: Boolesche Funktionen und Postsche Klassen, Akademie-Verlag, Berlin 1970).

[3] Pawel Kerntopf, Marek A. Perkowski, and Mozammel H. A. Khan. On universality of general reversible multiple-valued logic gates. In *34th International Symposium on Multiple-Valued Logic (ISMVL'04)*, 2004.

[4] W. McCune, R. Veroff, B. Fitelson, K. Harris, A. Feist, and L. Wos. Short single axioms for boolean algebra. *Journal of Automated Reasoning*, 29(1):1–16, 2002.

[5] Francis Jeffry Pelletier and Norman M. Martin. Post's Functional Completeness Theorem. *Notre Dame Journal of Formal Logic*, 31(2), 1990.

[6] E. Post. The Two-Valued Iterative Systems of Mathematical Logic. *Annals of Mathematics Series #5*, 1941.

[7] I. G. Rosenberg. Über die funktionale Vollständigkeit in den mehrwertigen Logiken (Struktur der Funktionen von mehreren Veränderlichen auf endlichen Mengen). *Rozpravy Ceskoslovenske Akad.*, 80, 1970.

[8] Henry Sheffer. A set of five independent postulates for boolean algebras, with application to logical constants. *Trans. AMS*, 14(4):481–488, 1913.