1 Abstract

Given two sets of variable assignments, E^+ and E^- say, over a finite set of propositional variables, along with a propositional formula φ, we assert that φ *fits* E^+, E^- if,

- for every $t \in E^+$, $t \models \varphi$, and
- for every $t \in E^-$, $t \not\models \varphi$.

Moreover, E^+, E^- *uniquely characterizes* φ if, φ fits E^+, E^-, and for every ψ fitting E^+, E^-, ψ is equivalent to φ. It can established, somewhat easily, that for every propositional formula φ, there is a pair E^+_φ, E^-_φ that uniquely characterizes it.

Every truth table over a finite number of propositional variables can be divided into two sets of variable assignments, E^+ and E^- say, representing the *true* and *false* truth assignments of the table, respectively. It follows from a well-known result [3] that there is exactly one formula fitting E^+, E^-, modulo equivalence.

Building upon this result, by fixing a set of propositional variables, PROP say, one can derive an unique characterization of every φ from its truth table (provided that the variables occurring in φ are in PROP). The unique characterization thus obtained should have *all* the variable assignments over the previously fixed set of propositional variables, i.e. PROP[1]. The purpose of this paper, in an informal manner, is to address the question: *What happens to the size of the unique characterization if we consider formulas, not from the full propositional fragment, but within some reduced fragment of propositional logic?*

A *Boolean connective* is function $f : \{0,1\}^n \to \{0,1\}$, where $n \geq 0$. Upon fixing a set O of connectives and a finite set of variables PROP, $\mathrm{PL}_O[\mathrm{PROP}]$ is defined as the smallest class that

- contains all the projections, $\pi^n_k(x_1, \ldots, x_n) = x_k$ for $n \geq k > 0$ and $x_1 \ldots x_n \in$ PROP.
- is closed under composition, $f(x_1, \ldots, x_n), g_1, \ldots, g_n \in \mathrm{PL}_O[\mathrm{PROP}]$ then $f(g_1, \ldots g_n) \in \mathrm{PL}_O[\mathrm{PROP}]$, where $x_1 \ldots x_n \in$ PROP.

The study of fragments then corresponds to study of such aforementioned sets. One good example is that of $\mathrm{PL}_\wedge[\mathrm{PROP}]$[1].

$\mathrm{PL}_\wedge[\mathrm{PROP}]$ doesn't have the property that corresponding to *every* truth table has a fitting formula. But every formula ψ in $\mathrm{PL}_\wedge[\mathrm{PROP}]$ can be uniquely characterized by pair E^+, E^- s.t. $|E^+| + |E^-| \leq |\mathrm{PROP}|$. So indeed there are fragments with better bounds for size of unique characterization.

The preceding example motivates us to play with the bounds for unique characterizations with respect to different fragments. We consider and classify three cases in this paper:

1. The bound on the unique characterization is a bi-variate polynomial in |PROP| and the size of the formula.
2. The bound on the unique characterization is exponential, but only in the size of the formula.
3. The bound on the unique characterization is a polynomial only in the size of the formula.

The statement of our results requires a little bit of familiarity with Post's Lattice and definition of *clones generated by a set of Boolean connectives*, denoted by $CL(O)$. The statement of our classifications are as follows:

Theorem 1.1. *For any set of Boolean connectives O, the following the equivalent:*

- *There exists a polynomial $p(x, y)$ s.t. for every PROP, and every $\varphi \in PL_O$[PROP], there is a pair E^+, E^- that uniquely characterizes φ with $|E^+| + |E^-| < p(|\varphi|, |PROP|)$*
- *$CL(O)$ is a subset of either of the three (i) $CL(\wedge, \bot, \top)$, (ii) $CL(\vee, \bot, \top)$ or (iii) $CL(\oplus, \top)$.*

Theorem 1.2. *For any set of Boolean connectives O, the following the equivalent:*

- *For every PROP, and every $\varphi \in PL_O$[PROP], there is a pair E^+, E^- that uniquely characterizes φ with $|E^+| + |E^-| < 2^{(|\varphi|)}$*
- *$CL(O)$ is a subset of either of the three (i) $CL(\wedge, \bot, \top)$, (ii) $CL(\vee, \bot, \top)$ or (iii) $CL(\oplus, \top)$.*

Theorem 1.3. *For any set of Boolean connectives O, the following the equivalent:*

- *There exists a polynomial $p(x, y)$ s.t. for every PROP, and every $\varphi \in PL_O$[PROP], there is a pair E^+, E^- that uniquely characterizes φ with $|E^+| + |E^-| < p(|\varphi|)$*
- *$CL(O)$ is a subset of either of the three (i) $CL(\wedge, \bot, \top)$, (ii) $CL(\vee, \bot, \top)$ or (iii) $CL(\oplus, \top)$.*

Although ($\Leftarrow$) direction of the above mentioned results can be established through combinatorial methods, the ($\Rightarrow$) direction requires some sophisticated machinery. We use a special kind of reduction, inspired from [2]. In fact theorem 1.1 has strong correspondence to the main result in [2]. We can refine theorem 1.1 even further based on the techniques used.

Corollary 1.3.1. *For any set of Boolean connectives O, the following the equivalent:*

- *For every PROP, and every $\varphi \in PL_O$[PROP], there is a pair E^+, E^- that uniquely characterizes φ with $|E^+| + |E^-| < |PROP| + 1$*
- *$CL(O)$ is a subset of either of the three (i) $CL(\wedge, \bot, \top)$, (ii) $CL(\vee, \bot, \top)$ or (iii) $CL(\oplus, \top)$.*

The results we have provided so far are concerned with upper bounds, to finish off we would establish a result on the lower bounds as well. As it turns out, the problem with coming up *reasonable* lower bounds is harder, but we have the following result:

Theorem 1.4. *Any unique characterization E^+, E^- of φ, where $\varphi \in PL_\oplus$[PROP], we get that $|E^+| + |E^-| = |PROP|$.*

Currently we are aiming to extend the results to modal fragments as well, but instead, we are looking at finite characterizations.

References

[1] Martin Anthony, Graham Brightwell, Dave Cohen, and John Shawe-Taylor. On exact specification by examples. In *Proceedings of COLT'92*, page 311–318. ACM, 1992.

[2] Victor Dalmau. Boolean formulas are hard to learn for most gate bases. In *Algorithmic Learning Theory*, page 301, 1999.

[3] Elliott Mendelson. *Introduction to mathematical logic, proposition 1.5.* CRC press, 2009.