

Investigation of the Proof Complexity Measures of Strongly Equal K-Tautologies in Some Proof Systems

Anahit Chubaryan, Artur Khamisyan, Garik Petrosyan
Department of Informatics and Applied Mathematics
Yerevan State University

achubaryan@ysu.am, Artur.Khamisyan@gmail.com, garik.petrosyan.1@gmail.com

ABSTRACT

Here we generalize the notions of determinative conjunct and strongly equal tautologies for many-valued logic (MVL) and compare the proof complexity measures of strongly equal many-valued tautologies in some proof systems of MVL. It is proved that in some “weak” proof system the strongly equal many-valued tautologies have the same proof complexities, while in the “strong” proof systems the measures of proof complexities for strongly equal tautologies can essentially differ from each other.

Keywords: many-valued logic, determinative conjunct, strongly equal tautologies, proof complexity characteristics.

1 Introduction

In the mean time many interesting applications of many-valued logic (MVL) were found in such fields as Logic, Mathematics, Formal Verification, Artificial Intelligence, Operations Research, Computational Biology, Cryptography, Data Mining, Machine Learning, Hardware Design etc., therefore the investigations of proof complexity for different systems of MVL are very important.

The traditional assumption that all tautologies as Boolean functions are equal to each other is not fine-grained enough to support a sharp distinction among tautologies. The authors of [1] have provided a different picture of equality for classical tautologies. They have introduced the notion of strong equality of 2-valued tautologies on the basis of determinative conjunct notion. The idea to revise the notion of equivalence between tautologies in such way that it takes into account an appropriate measure of their “complexity”.

It was proved in [2,3] that in “weak” proof systems the strongly equal 2-valued tautologies have the same proof complexities, while in the “strong” proof systems the measures of proof complexities for strongly equal tautologies can essentially differ from each other.

Here we generalize the notions of determinative conjunct and strongly equal tautologies for MVL and compare the proof complexity measures of **strongly equal many-valued tautologies** in some proof systems of MVL.

2 Preliminaries.

2.1 Main notions and notations of k-valued logic.

Let E_k be the set $\left\{0, \frac{1}{k-1}, \dots, \frac{k-2}{k-1}, 1\right\}$. We use the well-known notions of propositional formula, which defined as usual from propositional variables with values from E_k (may be also propositional constants), parentheses (,), and logical connectives $\&, \vee, \supset, \neg$, every of which can be defined by different mode. Additionally we use two modes of exponential function p^σ and introduce the additional notion of formula: for every formulas A and B the expression A^B (for both modes) is formula also.

In the considered logics either only **1** or every of values $\frac{1}{2} \leq \frac{i}{k-1} \leq 1$ can be fixed as **designated values**.

Definitions of main logical functions are:

$$p \vee q = \max(p, q) \quad (1) \text{ disjunction or}$$

$$p \vee q = ((k-1)(p+q)) \pmod{k} / (k-1) \quad (2) \text{ disjunction,}$$

$$p \& q = \min(p, q) \quad (1) \text{ conjunction or}$$

$$p \& q = \max(p+q-1, 0) \quad (2) \text{ conjunction}$$

Sometimes (1) conjunction is denoted by \wedge .

For implication we have two following versions:

$$p \supset q = \begin{cases} 1, & \text{for } p \leq q \\ 1-p+q, & \text{for } p > q \end{cases} \quad (1) \text{ Łukasiewicz's implication or}$$

$$p \supset q = \begin{cases} 1, & \text{for } p \leq q \\ q, & \text{for } p > q \end{cases} \quad (2) \text{ Gödel's implication}$$

And for negation two versions also:

$$\neg p = 1-p \quad (1) \text{ Łukasiewicz's negation or}$$

$$\neg p = ((k-1)p+1) \pmod{k} / (k-1) \quad (2) \text{ cyclically permuting negation.}$$

Sometimes we can use the notation \bar{p} instead of $\neg p$.

For propositional variable p and $\delta = \frac{i}{k-1}$ ($0 \leq i \leq k-1$) additionally "exponent" functions are defined in (4):

$$p^\delta \quad \text{as } (p \supset \delta) \& (\delta \supset p) \text{ with (1) implication} \quad (1) \text{ exponent,}$$

$$p^\delta \quad \text{as } p \text{ with } (k-1)(1-\delta) \text{ (2) negations.} \quad (2) \text{ exponent.}$$

Note, that both (1) exponent and (2) exponent are no new logical functions.

If we fix "1" (every of values $\frac{1}{2} \leq \frac{i}{k-1} \leq 1$) as designated value, so a formula ϕ with variables p_1, p_2, \dots, p_n is called **1-k-tautology** ($\geq 1/2$ -k-tautology) if for every $\delta = (\delta_1, \delta_2, \dots, \delta_n) \in E_k^n$ assigning δ_j ($1 \leq j \leq n$) to each p_j gives the value 1 (or some value $\frac{1}{2} \leq \frac{i}{k-1} \leq 1$) of ϕ .

Sometimes we call 1-k-tautology or $\geq 1/2$ -k-tautology simply k-tautology.

2.2 Determinative Disjunctive Normal Form for MVL

The notions of determinative conjunct and determinative disjunctive normal forms are introduced at first in [1]. Based on these notions some new proof system for classical propositional logic, dual to resolution system, was defined. Then the analogous systems were given for intuitionistic, minimal, monotone, positive and some others two-valued propositional logics.

The notions of determinative conjunct and determinative disjunctive normal form are generalized for all variants of MVL in [4]. For every propositional variable p in k -valued logic $p^0, p^{1/k-1}, \dots, p^{k-2/k-1}$ and p^1 in sense of both exponent modes are the literals. The conjunct K (term) can be represented simply as a set of literals (no conjunct contains a variable with different measures of exponents simultaneously), and DNF can be represented as a set of conjuncts.

Each of the following trivial identities for a propositional formula ψ are called *replacement-rule*:

for both conjunction and (1) disjunction

$$\varphi \& 0 = 0 \& \varphi = 0, \quad \varphi \vee 0 = 0 \vee \varphi = \varphi, \quad \varphi \& 1 = 1 \& \varphi = \varphi, \quad \varphi \vee 1 = 1 \vee \varphi = 1,$$

for (2) disjunction

$$\left(\varphi \vee \frac{i}{k-1} \right) = \left(\frac{i}{k-1} \vee \varphi \right) = \overbrace{\neg \neg \dots \neg}^i \varphi \quad (0 \leq i \leq k-1),$$

for (1) implication

$$\varphi \supset 0 = \bar{\varphi} \text{ with (1) negation, } 0 \supset \varphi = 1, \quad \varphi \supset 1 = 1, \quad 1 \supset \varphi = \varphi,$$

for (2) implication

$$\varphi \supset 1 = 1, \quad 0 \supset \varphi = 1, \quad \varphi \supset 0 = \overline{s\bar{g}}\varphi, \text{ where } \overline{s\bar{g}}\varphi \text{ is } 0 \text{ for } \varphi > 0 \text{ and } 1 \text{ for } \varphi = 0,$$

for (1) negation

$$\neg(i/k-1) = 1-i/k-1 \quad (0 \leq i \leq k-1), \quad \neg\psi = \psi,$$

for (2) negation

$$\neg(i/k-1) = i+1/k-1 \quad (0 \leq i \leq k-2), \quad \neg 1 = 0, \quad \overbrace{\neg \neg \dots \neg}^k \psi = \psi.$$

Application of a replacement-rule to some word consists in replacing of its subwords, having the form of the left-hand side of one of the above identities, by the corresponding right-hand side.

The following *auxiliary relations for replacement* are introduced in [5] as well:

for both variants of conjunction

$$\left(\varphi \&_{k-1} \frac{i}{k-1}\right) = \left(\frac{i}{k-1} \& \varphi\right) \leq \frac{i}{k-1} \quad (1 \leq i \leq k-2),$$

for (1) implication

$$\left(\varphi \supset \frac{i}{k-1}\right) \geq \frac{i}{k-1} \quad \text{and} \quad \left(\frac{i}{k-1} \supset \varphi\right) \geq \frac{k-(i+1)}{k-1} \quad (1 \leq i \leq k-2),$$

for (2) implication

$$\left(\varphi \supset \frac{i}{k-1}\right) \geq \frac{i}{k-1} \quad (1 \leq i \leq k-2), \quad \left(\frac{i}{k-1} \supset \varphi\right) \geq \varphi \quad (1 \leq i \leq k-1).$$

Let φ be a propositional formula of k -valued logic, $\mathbf{P} = \{p_1, p_2, \dots, p_n\}$ be the set of all variables of φ and $\mathbf{P}' = \{p_{i_1}, p_{i_2}, \dots, p_{i_m}\}$ ($1 \leq m \leq n$) be some subset of \mathbf{P} .

Definition 1: Given $\tilde{\sigma} = (\sigma_1, \sigma_2, \dots, \sigma_m) \in \mathbf{E}_k^m$, the conjunct $\mathbf{K}^\sigma = \{p_{i_1}^{\sigma_1}, p_{i_2}^{\sigma_2}, \dots, p_{i_m}^{\sigma_m}\}$ is called $\varphi - \frac{i}{k-1}$ -determinative ($0 \leq i \leq k-1$), if assigning σ_j ($1 \leq j \leq m$) to each p_{i_j} and successively using replacement-rules and, if it is necessary, the auxiliary relations for replacement also, we obtain the value $\frac{i}{k-1}$ of φ independently of the values of the remaining variables.

Every $\varphi - \frac{i}{k-1}$ -determinative conjunct is called also φ -determinative or determinative for φ .

Example. It is not difficult to see that the conjuncts $\{p_1\}$, $\{\neg p_3\}$, $\{p_2\}$, $\{\neg p_1, \neg p_2\}$ are determinative for formula $(p_1 \supset p_2) \supset (p_3 \supset (\neg p_2 \supset p_1))$ in 3-valued Łukasiewicz's system based on (1) conjunction, (1) disjunction, (1) implication, (1) negation and (1) exponent. Note that correctness of this statement for conjunct $\{\neg p_1, \neg p_2\}$ must be proved by using the auxiliary relations for replacement as well.

Definition 2. A DNF $\mathbf{D} = \{K_1, K_2, \dots, K_j\}$ is called determinative DNF (dDNF) for φ if $\varphi = \mathbf{D}$ and if "1" (every of values $\frac{1}{2} \leq \frac{i}{k-1} \leq 1$) is (are) fixed as designated value, then every conjunct K_i ($1 \leq i \leq j$) is 1-determinative ($\frac{i}{k-1}$ - **determinative from indicated intervals**) for φ .

Remark As in [3] it is also easily proved, that

- 1) if for some k -tautology φ , the minimal number of literals, containing in φ -determinative conjunct, is m , then φ -determinative DNF has at least k^m conjuncts;
- 2) if for some k -tautology φ there is such m that every conjunct with m literals is φ -determinative, then there is φ -determinative DNF with no more than k^m conjuncts.

Main Definition. The k -tautologies φ and ψ are strongly equal in given version of many-valued logic if every φ -determinative conjunct is also ψ -determinative and vice versa.

2.3 Definition of considered systems.

First of considered system is the following universal elimination system **UE** for all versions of MVL, which is defined in mentioned paper [5].

The axioms of Elimination systems **UE** aren't fixed, but for every formula k -valued φ each conjunct from some DDNF of φ can be considered as an axiom.

For k -valued logic the inference rule is **elimination rule** (ε -rule)

$$\frac{K_0 \cup \{p^0\}, K_1 \cup \{p^{\frac{1}{k-1}}\}, \dots, K_{k-2} \cup \{p^{\frac{k-2}{k-1}}\}, K_{k-1} \cup \{p^1\}}{K_0 \cup K_1 \cup \dots \cup K_{k-2} \cup K_{k-1}}$$

where mutual supplementary literals (variables with corresponding (1) or (2) exponents) are eliminated.

A finite sequence of conjuncts such that every conjunct in the sequence is one of the axioms of **UE** or is inferred from earlier conjuncts in the sequence by ε -rule is called a proof in **UE**.

A DNF $D = \{K_1, K_2, \dots, K_l\}$ is k -tautological if by using ε -rule can be proved the empty conjunct (\emptyset) from the axioms $\{K_1, K_2, \dots, K_l\}$.

We consider also the well-known Frege style systems of MVL. We define Gödel's (**G**) and Łukasiewicz's (**L**) systems following [6,7].

Łukasiewicz's proof system (**L**) uses (1) definitions for all logical functions.

For every formula A, B, C of k -valued logic the following formulas are axioms schemes of **L** [6]:

1. $A \supset (B \supset A)$ 2. $(A \supset (B \supset C)) \supset (B \supset (A \supset C))$
3. $(A \supset B) \supset ((B \supset C) \supset (A \supset C))$
4. $(A \supset (A \supset B)) \supset ((\neg B \supset (\neg B \supset \neg A)) \supset (A \supset B))$
5. $(A \supset B) \supset (\neg B \supset \neg A)$ 6. $A \supset \neg \neg A$ 7. $\neg \neg A \supset A$
8. $A \& B \supset B$ 9. $A \& B \supset A$ 10. $(C \supset A) \supset ((C \supset B) \supset (C \supset A \& B))$
11. $A \supset A \vee B$ 12. $B \supset A \vee B$ 13. $(A \supset C) \supset ((B \supset C) \supset (A \vee B \supset C))$

Inference rule is modus ponens /m.p./ $A, A \supset B \vdash B$.

Gödel's proof system (**G**) uses (1) definitions for conjunction and disjunction, (2) for implication and negation.

For every formula A, B, C of k -valued logic the following formulas are axioms schemes of **G** [7]:

1. $(A \supset B) \supset ((B \supset C) \supset (A \supset C))$
2. $A \supset A \vee B$ 3. $B \supset A \vee B$ 4. $(A \supset C) \supset ((B \supset C) \supset (A \vee B \supset C))$
5. $A \& B \supset B$ 6. $A \& B \supset A$ 7. $(C \supset A) \supset ((C \supset B) \supset (C \supset A \& B))$
8. $(A \supset (B \supset C)) \supset (A \& B \supset C)$ 9. $(A \& B \supset C) \supset (A \supset (B \supset C))$
10. $A \& \neg A \supset B$ 11. $(A \supset \& \neg A) \supset \neg A$ 12. $(A \supset B) \vee (B \supset A)$.

Inference rule is modus ponens /m.p./ $A, A \supset B \vdash B$.

In both systems "1" is fixed as designated value.

2.4 Proof complexity measures

In the theory of proof complexity two main characteristics of the proof are: t – **complexity**, defined as the number of proof steps (length) and l – **complexity**, defined as total number of proof symbols (size). We consider two measures (space and width) as well : s – **complexity** (space), informal defined as maximum of minimal number of symbols on blackboard, needed to verify all steps in the proof and w – **complexity** (width), defined as the maximum of widths of proof formulas (the strong definitions of all proof complexity characteristics see in [9]).

Let Φ be a proof system and φ be a k -tautology. We denote by $t_\varphi^\Phi(l_\varphi^\Phi, s_\varphi^\Phi, w_\varphi^\Phi)$ the minimal possible value of t – **complexity** (l – **complexity**, s – **complexity**, w – **complexity**) for all proofs of tautology φ in Φ .

By $|\varphi|$ we denote the size of a formula φ , defined as the number of all logical signs entries. It is obvious that the full size of a formula, which is understood to be the number of all symbols is bounded by some linear function in $|\varphi|$.

2.5 Essential subformulas of tautologies

For proving the main results we use also the notion of *essential subformulas*, introduced in [8].

Let F be some formula and $Sf(F)$ be the set of all non-elementary subformulas of formula F .

For every formula F , for every $\varphi \in Sf(F)$ and for every variable p by F_φ^p is denoted the result of the replacement of the subformulas φ everywhere in F by the variable p . If $\varphi \notin Sf(F)$, then F_φ^p is F .

We denote by $Var(F)$ the set of variables in F .

Definition 3. Let p be some variable that $p \notin Var(F)$ and $\varphi \in Sf(F)$ for some tautology F . We say that φ is an **essential subformula** in F iff F_φ^p is non-tautology.

We denote by $Essf(F)$ the set of essential subformulas in tautology F .

If F is minimal tautology, i.e. F is not a substitution of a shorter tautology, then $Essf(F) = Sf(F)$.

It is not difficult to prove the following statement.

Proposition. Let F be a minimal tautology and $\varphi \in Essf(F)$, then in every L -proof (G -proof) of F subformula φ must be essential either at least in some axiom of this system.

Really, if some subformula is essential in formula B , which is derived from formulas A and $A \supset B$, then this subformula must be essential in A or in $A \supset B$.

Note that for both systems L and G the number of essential subformulas in every axioms is bounded with some constant.

3 Main results.

Here we compare the proof complexities measures of strongly equal k -tautologies in above defined systems of some versions of MVL.

Theorem 1. The strongly equal k -tautologies have the same t, l, s, w complexities in the systems **UE** for all versions of MVL.

The proof is based on the fact that refutations in the systems UE deal exclusively with the conjuncts of dDNF, which are the same for strongly equal tautologies.

The situation for the systems **L** and **G** is the essentially other.

For simplification of our result presentation, we demonstrate them only for 3-tautoogies.

Let us consider

a) for Łukasiewicz's 3-valued logic the following two 3-tautologies:

$$A_n = (p^1 \& p^{1/2} \& p^0)^{1/2} \supset ((p^1 \& p^{1/2} \& p^0)^1 \supset (\overbrace{\neg \neg \dots \neg}^{2n} (p^1 \vee p^{1/2} \vee p^0))) \text{ with (1) exponent, } (n \geq 0),$$

$$B_n = (p^1 \vee p^{1/2} \vee p^0) \& (\overbrace{\neg \neg \dots \neg}^{2n} (p^1 \vee p^{1/2} \vee p^0)) \text{ with (1) exponent, } (n \geq 0),$$

b) for Gödel's 3-valued logic the following two 3-tautologies:

$$C_n = \neg(\neg \neg p \& \neg p \& p) \supset ((\neg \neg p \& \neg p \& p) \supset (\overbrace{\neg \neg \dots \neg}^{3n} (\neg \neg p \vee \neg p \vee p))) \text{ } (n \geq 0),$$

$$D_n = (\neg \neg p \vee \neg p \vee p) \& (\overbrace{\neg \neg \dots \neg}^{3n} (\neg \neg p \vee \neg p \vee p)) \text{ } (n \geq 0).$$

It isn't difficult to see that dDNF for both A_n and B_n is $\{p^1, p^{1/2}, p^0\}$ and for both C_n and D_n is $\{\neg \neg p, \neg p, p\}$, therefore A_n and B_n are strongly equal and C_n and D_n are strongly equal as well.

Note also that the sizes of all above formulas are $\Theta(n)$.

Theorem 2. a) $t_{A_n}^L = O(1), l_{A_n}^L = O(n)$
 $t_{B_n}^L = \Omega(n), l_{B_n}^L = \Omega(n^2).$
 b) $t_{C_n}^G = O(1), l_{C_n}^G = O(n),$
 $t_{D_n}^G = \Omega(n), l_{D_n}^G = \Omega(n^2).$

Proof. a) We can derive A_n as follow.

At first we derive the 3-tautology $(p^1 \& p^{1/2} \& p^0)^0$, then the 3-tautology

$(p^1 \& p^{1/2} \& p^0)^0 \supset ((p^1 \& p^{1/2} \& p^0)^{1/2} \supset ((p^1 \& p^{1/2} \& p^0)^1 \supset (\overbrace{\neg \neg \dots \neg}^{2n} (p^1 \vee p^{1/2} \vee p^0))))$, after them we derive by *modus ponens* the formula A_n . The lower bounds can be received by the same techniques as for 2-valued logic.

b) We can derive C_n as follow.

At first we derive the 3-tautology $\neg \neg(\neg \neg p \& \neg p \& p)$, then the 3-tautology

$$\neg \neg(\neg \neg p \& \neg p \& p) \supset (\neg(\neg \neg p \& \neg p \& p) \supset ((\neg \neg p \& \neg p \& p) \supset (\overbrace{\neg \neg \dots \neg}^{3n} (\neg \neg p \vee \neg p \vee p))))$$

after them we derive by *modus ponens* the formula C_n . The lower bounds can be received by the same techniques as for 2-valued logic.

Remark. If as formula $A_n(C_n)$ we take the new one, in which the number of repeated “negations” before the last subformula is 2^n , and in $B_n(D_n)$ is 3^m for $m=\lceil n \log_3 2 \rceil$, then the sizes for such formulas will be the same by order as well, but the bounds for steps will be more contrast: $O(1)$ and $\Omega(2^n)$ for strongly equal new 3-tautologies $A_n(C_n)$ and $B_n(D_n)$ accordingly.

4 Conclusion

We introduce the notion of strong equality of many-valued tautologies on the basis of determinative conjunct notion. The idea to revise the notion of equivalence between tautologies in such way that it takes into account an appropriate measure of their “complexity”.

It is proved that in “weak” proof systems the strongly equal many-valued tautologies have the same proof complexities, while in the “strong” proof systems the measures of proof complexities for strongly equal tautologies can essentially differ from each other.

ACKNOWLEDGMENTS

This work was supported by the RA MES State Committee of Science, in the frames of the research project № 18T-1B034.

REFERENCES

- (1) An. Chubaryan, Arm. Chubaryan, "A new conception of Equality of Tautologies", L&PS, Vol.V, No,1, 3-8, Triest, Italy, 2007.
- (2) A.Chubaryan, G.Petrosyan, The relations between the proof complexities of strongly equal classical tautologies in Frege systems, *Российско-китайский научный журнал «Содружество» № 1 (1), 2016 / ФИЗ-МАТ НАУКИ, 78-80.*
- (3) An. Chubaryan, A.Mnatsakanyan, On the bounds of the main proof measures in some propositional proof systems, *Scholar Journal of Phis. Math. And Stat., 2014, Vol.1, Issue-2, pp.111-117.*
- (4) Chubaryan Anahit, Khamisyan Artur, Arman Tshitoyan, On some systems for Łukasiewicz’s many-valued logic and its properties, *Fundamentalis Scientiam, Vol.8(8), Spain, 2017, 74-79.*
- (5) Anahit Chubaryan, Artur Khamisyan, Two types of universal proof systems for all variants of many-valued logics and some properties of them, *Iran Journal of Computer Science*, <https://doi.org/10.1007/s42044-018-0015-4>.
- (6) J. Lukasiewicz, *O Logice Trojwartosciowej, Ruch filoseficzny (Lwow)*, Vol. 5, 1920, 169-171.
- (7) K.Godel, *Zum intuitionistischen Aussagenkalkul*, Akademie der Wissenschaften in Wien, Mathematische-naturwissenschaftliche Klasse, *Auzeiger*, Vol. 69, 1932, 65-66.
- (8) A.A.Chubaryan: Comparison of proof sizes in systems and substitution systems of Frege, *Izvestiya NAN Armenii, Matematika, vol. 35, No. 5, 2002, 71-84.*
- (9) Y. Filmus, M. Lauria, J. Nordstrom, N. Thapen, N. Ron-Zewi: Space Complexity in Polynomial Calculus, 2012 IEEE Conference on Computational Complexity (CCC), 2012, 334-344.