Annals of Pure and Applied Logic 164 (2013) 702–732

Contents lists available at SciVerse ScienceDirect

Annals of Pure and Applied Logic

www.elsevier.com/locate/apal

Canonical proof nets for classical logic

Richard McKinley [1]

Logic and Theory Group, Institut für Informatik und Angewandte Mathematik, Üniversität Bern, Switzerland

ARTICLE INFO

Article history:
Available online 21 May 2012

MSC:
03B05
03F05
03F07

Keywords:
Proof nets
Identity of proofs
Classical logic
Cut elimination

ABSTRACT

Proof nets provide abstract counterparts to sequent proofs modulo rule permutations; the idea being that if two proofs have the same underlying proof-net, they are in essence the same proof. Providing a convincing proof-net counterpart to proofs in the classical sequent calculus is thus an important step in understanding classical sequent calculus proofs. By convincing, we mean that (a) there should be a canonical function from sequent proofs to proof nets, (b) it should be possible to check the correctness of a net in polynomial time, (c) every correct net should be obtainable from a sequent calculus proof, and (d) there should be a cut-elimination procedure which preserves correctness.

Previous attempts to give proof-net-like objects for propositional classical logic have failed at least one of the above conditions. In Richard McKinley (2010) [22], the author presented a calculus of proof nets (expansion nets) satisfying (a) and (b); the paper defined a sequent calculus corresponding to expansion nets but gave no explicit demonstration of (c). That sequent calculus, called $\mathbf{LK}^*$ in this paper, is a novel one-sided sequent calculus with both additively and multiplicatively formulated disjunction rules. In this paper (a self-contained extended version of Richard McKinley (2010) [22]), we give a full proof of (c) for expansion nets with respect to $\mathbf{LK}^*$, and in addition give a cut-elimination procedure internal to expansion nets – this makes expansion nets the first notion of proof-net for classical logic satisfying all four criteria.

1. Introduction

Proof theory, the study of formal proofs, was invented as a tool to study the consistency of mathematical theories, one of Hilbert's famous 23 problems. However, Hilbert had originally considered presenting at his Paris lecture a 24th problem [26] which concerned proofs directly: he proposed "develop(ing) a theory of mathematical proof in general". Central to this question is the idea that usual proofs, as written down by mathematicians, or formalized in, for example, Gentzen's sequent calculus [11], are syntactic representations of much more abstract proof objects. Given that, we should be able to tell when two syntactic proofs represent the same abstract proof.

It is striking how difficult this question seems to be, even for propositional classical logic. In contrast to the well-developed theory of proof-identity for intuitionistic natural deduction (given by interpretation of proofs in a Cartesian-closed category), the theory of identity for proofs in classical logic is very poorly understood. Investigations by several researchers over the last ten years [25,10,19,20,3,17] have only served to underline the difficulty of the problem. Many of these difficulties concern proofs with cuts. The identity of non-analytic proofs is not problematic for intuitionistic logic; since each proof has a unique normal form, he problem reduces to that of the identity of normal proofs. Reduction to

E-mail address: mckinley@iam.unibe.ch.

[1] Supported by a Swiss National Science Foundation *Ambizione* Fellowship.

0168-0072/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.apal.2012.05.007

$$\frac{}{a,\ \bar{a}}\,\mathrm{Ax} \qquad \frac{}{\top}\,\mathrm{Ax}_{\top}$$

$$\frac{\Gamma,\ A}{\Gamma, A \vee B}\,\vee_0 \qquad \frac{\Gamma,\ A, B}{\Gamma, A \vee B}\,\vee \qquad \frac{\Gamma,\ B}{\Gamma, A \vee B}\,\vee_1 \qquad \frac{\Gamma, A \qquad \Delta, B}{\Gamma, \Delta,\ A \wedge B}\,\wedge$$

$$\frac{\Gamma \qquad \Delta}{\Gamma, \Delta}\,\textsc{Mix} \qquad \frac{\Gamma,\ a, a}{\Gamma, a}\,\mathrm{C} \qquad \frac{\Gamma,\ \bar{a}, \bar{a}}{\Gamma, \bar{a}}\,\mathrm{C} \qquad \frac{\Gamma,\ A \wedge B, A \wedge B}{\Gamma, A \wedge B}\,\mathrm{C}$$

Fig. 1. $\mathbf{LK}^*$: A variant sequent calculus without weakening.

normal form in the classical sequent calculus is in general neither confluent nor strongly normalizing, and so the identity of proofs containing cuts must also be considered.

Yet even for cut-free proofs, opinions on the "right notion" of proof-identity differ. It is not reasonable, as it is for natural deduction proofs, to declare two cut-free sequent proofs equal only if they are syntactically identical; a good minimum notion of equality is that proofs differing by *commuting conversions* of non-interfering sequent rules should be equal. Proof-nets [14] are a tool for providing canonical representants of such equivalence classes of proofs in linear logic [12]. A proposal by Robinson [25], following ideas from Girard [13], gives proof-nets for propositional classical logic, and these nets do indeed identify proofs differing by commutative conversions. However, they fail to provide canonical representants for sequent proofs owing to the presence of *weakening attachments*; explicit information about the context of a weakening not present in sequent proofs. As a result one sequent proof corresponds to many different nets, the exact opposite of the situation one expects. In addition, the proof-identities induced by Robinson's nets do not include, among other desirable equations, commutativity/associativity of contraction, a key assumption in the development of abstract models of proofs (such identities are assumed in [10], in [3] and also in [20]). Other notions of abstract proof for classical logic (Combinatorial proofs [16] and $\mathbb{B}/\mathbb{N}$-nets [19]) make such identifications, but at the cost of losing sequentialization into a sequent calculus.

The current paper concerns *expansion-nets*: a calculus of proof-nets for classical logic first presented in [22] which, unlike Robinson's nets, provide canonical representants of equivalence classes of classical sequent proofs. To avoid the problems inherent in weakening, we restrict attention to proofs in a new sequent calculus, $\mathbf{LK}^*$ (see Fig. 1). This calculus has no weakening rule, nor does it have implicit weakening at the axioms: instead, it has both the multiplicative and additive forms of disjunction rule. This new calculus has all the properties one might hope of a sequent calculus for classical logic (except, perhaps, terminating proof search): it has the subformula property, is cut-free complete, and even has syntactic cut-elimination (although this is perhaps easier to see via the proof nets than directly in the sequent calculus, owing to the curious nature of the cut-elimination theorem: if Γ is provable in $\mathbf{LK}^*$ with cut, then some subsequent $\Delta \subseteq \Gamma$ is provable without cut). Treating the introduction of weak formulae in this way allows us to define a canonical function mapping sequent proofs in $\mathbf{LK}^*$ to expansion nets. Correctness for expansion nets (whether a net really corresponds to a sequent proof) can be checked in polynomial time, using small adaptations of standard methods from the theory of proof nets for $\mathbf{MLL}^- + \textsc{Mix}$ (multiplicative linear logic, plus the mix rule, without units, as studied in [1,7,8]) – meaning that expansion-nets form a *propositional proof system* [6]. Translating from sequent proofs to expansion nets identifies, in addition to nets differing by commuting conversions, nets differing by the order in which contractions are performed. The current paper (a self-contained extension of [22]) gives a detailed account of the connection between expansion-nets and their associated sequent calculus: in particular, an explicit proof of sequentialization for expansion nets as (Theorem 49), which was missing in [22]. In addition, we present a cut-elimination procedure for expansion nets (proof transformations which we prove, in Propositions 56–59 to preserve correctness) which are weakly normalizing (Lemma 60 and Theorem 61 detail a strategy for reducing any net with cuts to a cut-free net). This result was absent from [22]: with it, we can see that expansion nets have polynomial-time proof checking, sequentialization into a sequent calculus and cut-elimination preserving sequent-calculus correctness – the first notion of abstract proof for propositional classical logic to satisfy all of these properties.

1.1. Structure of the paper

Section 2 gives some preliminaries, and then Section 3 introduces the variant sequent calculus $\mathbf{LK}^*$, showing completeness and some other key properties. Section 4 surveys the existing notions of abstract proof in propositional classical logic. Section 5 defines expansion nets, and compares them with the existing notions of abstract proof in the literature.

The next two chapters contain most of the novel technical material in the paper. Section 6 deals with the notion of *subnet*, a key analogue of the notion of subproof in sequent calculus which we will need to define cut-reduction. This technology (including the new notion of *contiguous empire*) also affords a proof of sequentialization of expansion-nets into $\mathbf{LK}^*$. Section 7 then provides the cut-reduction steps themselves, and a proof of cut-elimination for expansion nets.