
Proceedings Paper:
Beyersdorff, O (2008) Logical closure properties of propositional proof systems - (Extended abstract). In: Agrawal, M, Du, D, Duan, Z and Li, A, (eds.) Theory and Applications of Models of Computation. 5th International Conference on Theory and Applications of Models of Computation, 25-28 Apr 2009, Xi'an, China. Lecture Notes in Computer Science, 4978 (Lectur). Springer Verlag, Germany, 318 - 329 . ISBN: 978-3-540-79227-7. ISSN: 0302-9743.

https://doi.org/10.1007/978-3-540-79228-4_28

Logical Closure Properties of Propositional Proof Systems

(Extended Abstract)

Olaf Beyersdorff*

Institut für Theoretische Informatik, Leibniz Universität Hannover, Germany
beyersdorff@thi.uni-hannover.de

Abstract. In this paper we define and investigate basic logical closure properties of propositional proof systems such as closure of arbitrary proof systems under modus ponens or substitutions. As our main result we obtain a purely logical characterization of the degrees of schematic extensions of *EF* in terms of a simple combination of these properties. This result underlines the empirical evidence that *EF* and its extensions admit a robust definition which rests on only a few central concepts from propositional logic.

1 Introduction

In their seminal paper [11] Cook and Reckhow gave a very general complexity-theoretic definition of the concept of a propositional proof system, focusing on efficient verification of propositional proofs. Due to the expressivity of Turing machines (or any other model of efficient computation) this definition includes a variety of rather unnatural propositional proof systems. In contrast, proof-theoretic research concentrates on propositional proof systems which, beyond efficient verification, satisfy a number of additional natural properties. Proof systems with nice structural properties are also exclusively used in practice (e.g. for automated theorem proving). Supported by this empirical evidence, we therefore formulate the thesis, that the Cook-Reckhow framework is possibly too broad for the study of natural proof systems of practical relevance. Motivated by these observations, we investigate the interplay of central logical closure properties of propositional proof systems, such as the ability to use modus ponens or substitutions in arbitrary proof systems.

Proof systems are compared with respect to their strength by simulations, and all equivalent systems form one degree of proof systems. Since in proof complexity we are mostly interested in the degree of a propositional proof system and not so much in specific representatives of this degree, we only study properties which are preserved inside a simulation degree. In particular, we think that it would be desirable to characterize the degrees of important proof systems

* Part of this work was done while at Humboldt University Berlin. Supported by DFG grant KO 1053/5-1.

(e.g. resolution, cutting planes, or Frege) by meaningful and natural properties. Such results would provide strong confirmation for the empirical evidence, that these systems have indeed a natural and robust definition. One would expect that according to the general classification of propositional proof systems into logical systems (such as resolution, Frege, QBF), algebraic systems (polynomial calculus, Nullstellensatz) and geometric systems (cutting planes), these underlying principles should also be of logical, algebraic, and geometrical character, respectively.

As a first step of this more general program we exhibit a purely logical characterization of the degrees of schematic extensions of the extended Frege system EF. These schematic extensions enhance the extended Frege system by additional sets of polynomial-time decidable axiom schemes. Such systems are of particular importance: Firstly, because every propositional proof system is simulated by such an extension of EF, and secondly, because these systems admit a fruitful correspondence to theories of bounded arithmetic [8, 14, 16].

For our characterization we formalize closure properties such as modus ponens and substitutions in such a way that they are applicable for arbitrary propositional proof systems. We analyse the mutual dependence of these properties, providing in particular strong evidence for their independence. Our characterization of extensions of EF involves the properties modus ponens, substitutions, and reflection. This result tells us that the essence of extended Frege systems (and its generalizations) lies in the ability to use modus ponens and substitutions, and to prove the consistency of the system with short proofs (this property is known as reflection). Thus schematic extensions of EF are exactly those systems (up to p-equivalence) which can prove their consistency and are closed under modus ponens and substitutions. This result also allows the characterization of the existence of optimal propositional proof systems (which simulate every other system).

The paper is organized as follows. We start in Sect. 2 by recalling some background information on propositional proof systems and particularly Frege systems and their extensions. In Sect. 3 we define and investigate natural properties of proof systems which we use throughout this paper. A particularly important property for strong systems is the reflection property, which gives a propositional description of the correctness of a proof system. Different versions of such consistency statements are discussed in Sect. 4, leading in particular to a robust definition of the reflection property.

Section 5 contains the main result of this paper, consisting of a purely logical characterization of the degrees of schematic extensions of EF. This directly leads to a similar characterization of the existence of p-optimal proof systems. These results can also be explained in the more general context of the correspondence between strong propositional proof systems and arithmetic theories, of which we will sketch an axiomatic approach. Finally, in Sect. 6 we conclude with some open problems.

Most definitions and results of this paper can be given in two versions, one for simulations and the other, using slightly stronger assumptions, for the case

of p-simulations between proof systems (cf. Sect. 2). For brevity we will restrict this exposition to the efficient case of p-simulations.

Due to space limitations we only sketch proofs or omit them in this extended abstract.

2 Propositional Proof Systems

Propositional proof systems were defined in a very general way by Cook and Reckhow [11] as polynomial-time functions P which have as their range the set TAUT of all propositional tautologies. A string π with $P(\pi) = \varphi$ is called a P-proof of the tautology φ. By $P \vdash_{\leq m} \varphi$ we indicate that there is a P-proof of φ of size $\leq m$. If Φ is a set of propositional formulas we write $P \vdash_* \Phi$ if there is a polynomial p such that $P \vdash_{\leq p(|\varphi|)} \varphi$ for all $\varphi \in \Phi$. If $\Phi = \{\varphi_n \mid n \geq 0\}$ is a sequence of formulas we also write $P \vdash_* \varphi_n$ instead of $P \vdash_* \Phi$.

Proof systems are compared according to their strength by simulations, introduced in [11] and [18]. A proof system S *simulates* a system P (denoted by $P \leq S$) if there exists a polynomial p such that for all tautologies φ and P-proofs π of φ there is an S-proof π' of φ with $|\pi'| \leq p(|\pi|)$. If such a proof π' can even be computed from π in polynomial time we say that S *p-simulates* P and denote this by $P \leq_p S$. Systems P and S, that mutually (p-)simulate each other, are called *(p-)equivalent*, denoted by $P \equiv_{(p)} S$. A proof system is *(p-)optimal* if it (p-)simulates all proof systems.

A prominent example of a class of proof systems is provided by *Frege systems* which are usual textbook proof systems based on axioms and rules. In the context of propositional proof complexity these systems were first studied by Cook and Reckhow [11], and it was proven there that all Frege systems, i.e., systems using different axiomatizations and rules, are p-equivalent. A different characterization of Frege systems is provided by *Gentzen's sequent calculus* [12], that is historically one of the first and best analysed proof systems. The sequent calculus is widely used, both for propositional and first-order logic, and it is straightforward to verify that Frege systems and the propositional sequent calculus LK p-simulate each other [11].

Augmenting Frege systems by the possibility to abbreviate complex formulas by propositional variables, we arrive at the *extended Frege proof system* EF. The extension rule might further reduce the proof size, but it is not known whether EF is really stronger than ordinary Frege systems. Both Frege and the extended Frege system are very strong systems for which no non-trivial lower bounds to the proof size are currently known (cf. [6]).

It is often desirable to further strengthen the proof system EF by additional axioms. This can be done by allowing a polynomial-time computable set Φ as new axioms, i.e., formulas from Φ as well as their substitution instances may be freely used in EF-proofs. These schematic extensions of EF are denoted by $EF + \Phi$. In this way, we obtain proof systems of arbitrary strength (cf. Theorem 15). More detailed information on Frege systems and its extensions can be found in [9, 16].

3 Closure Properties of Proof Systems

In this section we define and investigate natural properties of propositional proof systems that are satisfied by many important proof systems. One of the most common rules is modus ponens, which serves as the central rule in Frege systems. Carrying out modus ponens in a general proof system might be formalized as:

Definition 1. *A proof system P is* closed under modus ponens *if there exists a polynomial-time computable algorithm that takes as input P-proofs $\pi_1, \ldots, \pi_k$ of propositional formulas $\varphi_1, \ldots, \varphi_k$ together with a P-proof π_{k+1} of the implication $(\varphi_1 \to (\varphi_2 \to \ldots (\varphi_k \to \varphi_{k+1}) \ldots))$ and outputs a P-proof of φ_{k+1}.*

Defining closure under modus ponens by requiring $k = 1$ in the above definition seems to lead to a too restrictive notion. Namely, in some applications we need to use modus ponens polynomially many times (cf. Theorem 11). In this case, the above definition with $k = 1$ would only guarantee an exponential upper bound on the size of the resulting proof, whereas Definition 1 results only in a polynomial increase.

If π is a Frege proof of a formula φ, then we can prove substitution instances $\sigma(\varphi)$ of φ by applying the substitution σ to every formula in the proof π. This leads us to the general concept of closure of a proof system under substitutions.

Definition 2. *P is* closed under substitutions *if there exists a polynomial-time procedure that takes as input a P-proof of a formula φ as well as a substitution instance $\sigma(\varphi)$ of φ and computes a P-proof of $\sigma(\varphi)$.*

It also makes sense to consider other properties like closure under conjunctions or disjunctions. A particularly simple property is the following: a proof system *evaluates formulas without variables* if formulas using only constants but no propositional variables have polynomial-size proofs. As this is true even for truth-table evaluations, all proof systems simulating the truth-table system evaluate formulas without variables.

We can classify properties of proof systems like those above along the following lines. Some properties are *monotone* in the sense that they are preserved from weaker to stronger systems, i.e., if $P \leq Q$ and P has the property, then also Q satisfies the property. Evaluation of formulas without variables is such a monotone property. Other properties might not be monotone but still *robust* in the sense that the property is preserved when we switch to a p-equivalent system. Since we are interested in the degree of a proof system and not in the particular representative of that degree, it is desirable to investigate only robust or even monotone properties. It is straightforward to verify that closure under modus ponens and closure under substitutions are robust properties.

We remark that Frege systems and their extensions have very good closure properties.

Proposition 3. *The Frege system F, the extended Frege system EF, and all extensions $EF + \Phi$ by polynomial-time computable sets of axioms $\Phi \subseteq$ TAUT are closed under modus ponens and under substitutions.*

It is interesting to ask whether these properties of propositional proof systems are independent from each other. With respect to this question we observe the following.

Proposition 4. *Assume that the extended Frege proof system is not optimal. Then there exist proof systems which are closed under substitutions but not under modus ponens.*

Proof. (Idea) We use the assumption of the non-optimality of EF to obtain polynomial-time constructable sequences φ_n and ψ_n of tautologies, such that $EF \vdash_* \varphi_n$, but $EF \nvdash_* \psi_n$. We then encode the implications $\varphi_n \to \psi_n$ into an extension of EF, thus obtaining a system Q that is closed under substitutions, but not under modus ponens, because $Q \vdash_* \varphi_n$, $Q \vdash_* \varphi_n \to \psi_n$, and $Q \nvdash_* \psi_n$. □

Candidates for proof systems that are closed under modus ponens but not under substitutions come from extensions of Frege systems by polynomial-time computable sets $\Phi \subseteq \mathrm{TAUT}$ as new axioms. Clearly these systems are closed under modus ponens. In [3], however, we exhibit a suitable hypothesis, involving disjoint NP-pairs, which guarantees that these proof systems are not even closed under substitutions by constants for suitable choices of Φ.

4 Consistency Statements

Starting with this section, we will use the correspondence of propositional proof systems to theories of bounded arithmetic. Bounded arithmetic is the general denomination of a whole collection of weak fragments of Peano arithmetic, that are defined by adding a controlled amount of induction to a set of basic axioms (cf. [14]). One of the most prominent examples of these arithmetic theories is Buss' theory S^1_2, defined in [8]. In addition to the usual ingredients, the language L of S^1_2 uses a number of technical symbols to allow a smooth formalization of syntactic concepts.

A central ingredient of the correspondence of arithmetic theories to propositional proof systems is the translation of first-order arithmetic formulas into propositional formulas [10, 19]. An L-formula in prenex normal form with only bounded existential quantifiers is called a Σ^b_1-formula. These formulas describe NP-predicates in the sense that the class of all Σ^b_1-definable subsets of $\mathbb{N}$ coincides with the class of all NP-subsets of $\mathbb{N}$ (cf. [25, 8]). Likewise, Π^b_1-formulas only have bounded universal quantifiers and describe coNP-predicates. A Π^b_1-formula $\varphi(x)$ is translated into a sequence $\|\varphi(x)\|^n$ of propositional formulas containing one formula per input length for the number x, such that $\varphi(x)$ is true, i.e., $\mathbb{N} \models (\forall x)\varphi(x)$, if and only if $\|\varphi(x)\|^n$ is a tautology where $n = |x|$ (cf. [16]). We use $\|\varphi(x)\|$ to denote the set $\{\|\varphi(x)\|^n \mid n \geq 1\}$.

The consistency of a proof system P is described by the *consistency statement* $Con(P) = (\forall \pi)\neg Prf_P(\pi, \bot)$, where $Prf_P(\pi, \varphi)$ is a suitable arithmetic formula describing that π is a P-proof of φ. The formula Prf_P can be chosen such that

Prf_P is provably equivalent in S^1_2 both to a Σ^b_1- and a Π^b_1-formula (such formulas are called Δ^b_1-formulas with respect to S^1_2, cf. [16]).

A somewhat stronger formulation of consistency is given by the *reflection principle* of a propositional proof system P, which is defined by the arithmetic formula

$$RFN(P) = (\forall\pi)(\forall\varphi)Prf_P(\pi,\varphi) \rightarrow Taut(\varphi) \ ,$$

where $Taut$ is a Π^b_1-formula formalizing propositional tautologies. Therefore $Con(P)$ and $RFN(P)$ are $\forall\Pi^b_1$-formulas, i.e., these formulas are in prenex normal form with unbounded $\forall$-quantifiers followed by bounded $\forall$-quantifiers and can therefore be translated via $\|.\|$ into sequences of propositional formulas.

The two consistency notions $Con(P)$ and $RFN(P)$ are compared by the following well-known observation, contained e.g. in [16]:

Proposition 5. *Let P be a proof system that is closed under substitutions and modus ponens and evaluates formulas without variables, and assume that these properties are provable in S^1_2. Then $S^1_2 \vdash RFN(P) \leftrightarrow Con(P)$.*

Very often propositional descriptions of the reflection principle are needed. These can be simply obtained by translating $RFN(P)$ to a sequence of propositional formulas using the translation $\|.\|$.

Definition 6. *A propositional proof system P has the* reflection property *if there exists a polynomial-time algorithm that on input 1^n outputs a P-proof of $\|RFN(P)\|^n$.*

There is a subtle problem with Definition 6 which is somewhat hidden in the definition. Namely, the formula Prf_P describes the computation of some Turing machine computing the function P. However, the provability of the formulas $\|RFN(P)\|^n$ with polynomial-size P-proofs might depend on the actual choice of the Turing machine computing P. Let us illustrate this with the following example.

Proposition 7. *If EF is not p-optimal, then there exists a proof system $Q \equiv_p EF$ such that S^1_2 does not prove the reflection principle of Q, i.e., S^1_2 does not prove the formula $(\forall\pi)(\forall\varphi)Prf_Q(\pi,\varphi) \rightarrow Taut(\varphi)$ for some suitable choice of the Turing machine that computes Q and is used for the formula Prf_Q.*

Proof. (Sketch) If EF is not p-optimal, then there exists a proof system R such that $R \not\leq_p EF$. We define the system P as $EF + \|RFN(R)\|$ and the system Q as

$$Q(\pi) = \begin{cases} \varphi & \text{if } \pi = 0\pi' \text{ and } \pi' \text{ is an } EF\text{-proof of } \varphi \\ P(\pi') & \text{if } \pi = 1\pi' \text{ and } P(\pi') \in \{\top, \bot\} \\ \top & \text{otherwise.} \end{cases}$$

It is easily checked that EF and Q are $\leq_p$-equivalent. We have to show that S^1_2 does not prove the formula $RFN(Q)$ where for the predicate Prf_Q we use the canonical Turing machine M according to the above definition of Q, i.e., on input $0\pi'$ the machine M checks whether π' is a correct EF-proof and on

input $1\pi'$ the machine M evaluates $P(\pi')$. Assume on the contrary that $S_2^1 \vdash RFN(Q)$. Because of line 2 of the definition of Q this means that S_2^1 can prove that there is no P-proof of $\bot$, i.e., S_2^1 proves the consistency statement of P. The system P is closed under substitutions by constants and modus ponens. Therefore $Con(P)$ and $RFN(P)$ are equivalent in S_2^1 by Proposition 5. Hence S_2^1 not only proves $Con(P)$, but also $RFN(P)$, which gives a p-simulation of P by EF (cf. Definition 13 and Theorem 14 below). This, however, contradicts the choice of P, and hence $S_2^1 \nvdash RFN(Q)$. □

Note that $S_2^1 \vdash RFN(EF)$ (cf. [18]), contrasting $S_2^1 \nvdash RFN(Q)$ in the above proposition. This observation tells us that we should understand the meaning of Definition 6 in the following, more precise way:

Definition 8. *A propositional proof system P has the* robust reflection property *if there exists a deterministic polynomial-time Turing machine M computing the function P such that for some Δ_1^b-formalization Prf_P of the computation of M with respect to S_2^1 we have a polynomial-time algorithm that constructs on input 1^n a P-proof of the formula $\|(\forall\pi)(\forall\varphi)Prf_P(\pi,\varphi) \to Taut(\varphi)\|^n$.*

For this definition of reflection we can show the robustness of the reflection principle under p-simulations:

Proposition 9. *Let P and Q be p-equivalent proof systems. Then P has the robust reflection property if and only if Q has the robust reflection property.*

Proof. (Idea) If Q proves its reflection principle with respect to the Turing machine M, then P can prove its reflection for the Turing machine $M \circ N$, where the machine N computes a p-simulation of Q by P. □

It is known that strong propositional proof systems like EF and its extensions have the reflection property [18]. In contrast, weak systems like resolution do not have reflection. Pudlák [21] proved that the cutting planes system CP requires nearly exponential-size refutations of some *canonical* formulation of the formulas $RFN(CP)$. Atserias and Bonet [1] obtained the same result for the resolution system Res. This, however, does not exclude the possibility that we have short proofs for the reflection principle of resolution or CP with respect to some other formalization of Prf_{CP}, Prf_{Res}, or $Taut$. It therefore remains as an open question whether these systems have the robust reflection property.

Alternatively, we can view robust reflection as a condition on the *canonical disjoint* NP*-pair* $(Ref(P), Sat^*)$ of a proof system P, introduced by Razborov [22]. Its first component $Ref(P) = \{(\varphi, 1^m) \mid P \vdash_{\leq m} \varphi\}$ contains information about proof lengths in P, and the second component $Sat^* = \{(\varphi, 1^m) \mid \neg\varphi \in \text{SAT}\}$ is a padded version of SAT. The link of the canonical pair with the reflection property was already noted by Pudlák [21]. We can extend this idea to obtain a characterization of robust reflection for weak proof systems.

Proposition 10. *Let P be the resolution or cutting planes system. Then P has the robust reflection property if and only if the canonical pair of P is p-separable, i.e., there exists a polynomial-time decidable set S such that $Ref(P) \subseteq S$ and $S \cap Sat^* = \emptyset$.*

Proof. (Idea) Robust reflection for P means that we can efficiently generate P-proofs for the disjointness of $(Ref(P), Sat^*)$ with respect to some propositional representations of its components. Using feasible interpolation for P [17, 7, 20], we get a polynomial-time computable separator for $(Ref(P), Sat^*)$.

Conversely, if the canonical P-pair is p-separable, then it can be given a simple propositional description, for which we can devise short P-proofs of the disjointness of the pair. This is possible, as all p-separable disjoint NP-pairs are equivalent (via suitable reductions for pairs [13]). We can then choose a simple p-separable pair, prove its disjointness in P, and translate these proofs into proofs for the disjointness of $(Ref(P), Sat^*)$ (cf. [2] for the details of this approach). □

As it is conjectured that none of the canonical pairs of natural proof systems is p-separable [21], Proposition 10 indicates the absence of robust reflection for weak systems that satisfy the interpolation property.

5 Characterizing the Degree of Extended Frege Systems

Using the results from the previous section, we will now exhibit a characterization of the degrees of schematic extensions of EF.

Theorem 11. *For all proof systems $P \geq_p EF$ the following conditions are equivalent:*

1. *P is p-equivalent to a proof system of the form $EF + \|\varphi\|$ with a true Π_1^b-formula φ.*
2. *P is p-equivalent to a proof system of the form $EF + \|\Phi\|$ with a polynomial-time decidable set of true Π_1^b-formulas Φ.*
3. *P has the robust reflection property and is closed under modus ponens and substitutions.*

Proof. Item 1 trivially implies item 2. For the implication $2 \Rightarrow 3$ let $P \equiv_p EF + \|\Phi\|$. Then the closure properties of $EF + \|\Phi\|$ are transferred to P. Systems of the form $EF + \|\Phi\|$ are known to have the reflection property (cf. [19] and Theorem 14 below). By Proposition 9 robust reflection for $EF + \|\Phi\|$ is transferred to P.

The main part of the proof is the implication $3 \Rightarrow 1$. Its proof involves a series of results that are also of independent interest. The first step is an efficient version of the deduction theorem for EF:

1. Efficient Deduction theorem for EF. *There exists a polynomial-time procedure that takes as input an EF-proof of a formula ψ from a finite set of tautologies Φ as extra assumptions, and produces an EF-proof of the implication $(\bigwedge_{\varphi \in \Phi} \varphi) \to \psi$.*

A similar deduction theorem was shown for Frege systems by Bonet and Buss [4, 5]. For stronger systems like EF we just remark that there are different ways to formalize deduction. These deduction properties seem to be quite powerful, as

they allow the characterization of the existence of optimal and even polynomially bounded proof systems [3].

In the second step we compare schematic extensions of EF and strong proof systems with sufficient closure properties.

2. Simulation of extensions of EF by sufficiently closed systems. *Let P be a proof system such that $EF \leq_p P$ and P is closed under substitutions and modus ponens. Let Φ be some polynomial-time decidable set of tautologies such that P-proofs of all formulas from Φ can be constructed in polynomial time. Then $EF + \Phi \leq_p P$.*

The idea of the proof of this simulation is the following: if $EF + \Phi \vdash_{\leq m} \varphi$, then there are substitution instances $\psi_1, \ldots, \psi_k$ of formulas from Φ such that we have an EF-proof of φ from $\psi_1, \ldots, \psi_k$. Using the deduction theorem for EF, we get a polynomial-size EF-proof of $(\bigwedge_{i=1}^{k} \psi_i) \to \varphi$. By the hypotheses $P \geq_p EF$ and $P \vdash_* \Phi$, together with the closure properties of P, we can transform this proof into a polynomial-size P-proof of φ.

Item 2 is most useful in the following form:

3. *If the proof system $P \geq_p EF$ has the robust reflection property and P is closed under substitutions and modus ponens, then we get the p-simulation $EF + \|RFN(P)\| \leq_p P$.*

The converse simulation extends a result of Krajíček and Pudlák [18], namely that every proof system P is p-simulated by the system $EF + \|RFN(P)\|$.

4. Simulation of arbitrary systems by extensions of EF. *Let P be an arbitrary proof system, and let Φ be some polynomial-time decidable set of tautologies. If $EF + \Phi$-proofs of $\|RFN(P)\|^n$ can be generated in polynomial time, then $P \leq_p EF + \Phi$.*

After these preparations we can now prove the implication $3 \Rightarrow 1$. Let P be a proof system which has the robust reflection property and is closed under modus ponens and substitutions. We choose the formula φ as $RFN(P)$. Then $EF + \|\varphi\| \leq_p P$ by the above item 3. The converse simulation $P \leq_p EF + \|\varphi\|$ follows from item 4. □

The equivalence of items 1 and 2 in the above corollary expresses some kind of compactness for extensions of EF: systems of the form $EF + \|\Phi\|$ are always equivalent to a system $EF + \|\varphi\|$ with a single arithmetic formula φ. The equivalence to item 3 shows that these systems have a robust logical definition, independent of the particular axiomatization chosen for EF.

We will now apply Theorem 11 to characterize the existence of optimal and p-optimal proof systems. These problems were posed by Krajíček and Pudlák [18] and have been intensively studied during the last years [15, 23, 24]. We call a set A *printable* if there exists a polynomial-time algorithm which on input 1^n outputs all words from A of length n.

Corollary 12. *The following conditions are equivalent:*

1. *P is a p-optimal propositional proof system.*
2. *$P \geq_p EF$ and P is closed under modus ponens and substitutions. Further, for every printable set of tautologies, P-proofs can be constructed in polynomial time.*

Using non-constructive versions of the conditions in item 2 we get a similar characterization of the existence of optimal proof systems.

Probably the strongest available information on *EF* and its extensions stems from the connection of these systems to theories of bounded arithmetic. Actually, also Theorem 11 can be derived as a consequence from this more general context. In the remaining space we will sketch an axiomatic approach to this correspondence, as suggested by Krajíček and Pudlák [19]. The correspondence works for pairs (T, P) of arithmetic theories T and propositional proof systems P. It can be formalized as follows:

Definition 13. *A propositional proof system P is called* regular *if there exists an L-theory T such that the following two properties are fulfilled for (T, P).*

1. *Let $\varphi(x)$ be a Π_1^b-formula such that $T \vdash (\forall x)\varphi(x)$. Then there exists a polynomial-time computable function which on input 1^n outputs a P-proof of $\|\varphi(x)\|^n$.*
2. *T proves the correctness of P, i.e., $T \vdash RFN(P)$. Furthermore, P is the strongest proof system for which T proves the correctness, i.e., $T \vdash RFN(Q)$ for a proof system Q implies $Q \leq_p P$.*

Probably the most important instance of the general correspondence is the relation between S_2^1 and *EF*. Property 1 of the correspondence, stating the simulation of S_2^1 by *EF*, is essentially contained in [10], but for the theory *PV* instead of S_2^1. Examining the proof of this result, it turns out that the theorem is still valid if both the theory S_2^1 and the proof system *EF* are enhanced by further axioms. Property 2 of the correspondence between S_2^1 and *EF* was established by Krajíček and Pudlák [19]. Again, this result can be generalized to extensions of S_2^1 and *EF* by additional axioms. Combining these results, we can state:

Theorem 14 (Cook [10], Buss [8], Krajíček, Pudlák [19]). *Let Φ be a polynomial-time decidable set of true Π_1^b-formulas. Then the proof system $EF + \|\Phi\|$ is regular and corresponds to the theory $S_2^1 + \Phi$.*

Using these results, we can exhibit sufficient conditions for the regularity of a propositional proof system. From the definition of a regular system it is clear that regular proof systems have the reflection property. Furthermore, a combination of the properties of proof systems introduced in Sects. 3 and 4 guarantees the regularity of the system, namely:

Theorem 15. *If P is a proof system such that $EF \leq_p P$ and P has the robust reflection property and is closed under substitutions and modus ponens, then P is regular and corresponds to the theory $S_2^1 + RFN(P)$.*

Proof. The hypotheses on P imply $EF + \|RFN(P)\| \equiv_p P$ by Theorem 11. We will now check the axioms of the correspondence for $S^1_2 + RFN(P)$ and P. Suppose φ is a $\forall\Pi^b_1$-formula such that $S^1_2 + RFN(P) \vdash \varphi$. By Theorem 14 we can construct $EF + \|RFN(P)\|$-proofs of $\|\varphi\|^n$ in polynomial time. As we already know that $EF + \|RFN(P)\|$ is p-simulated by P, we obtain polynomial-size P-proofs of $\|\varphi\|^n$. This proves part 1 of the correspondence.

It remains to verify the second part. Clearly $S^1_2 + RFN(P) \vdash RFN(P)$. Finally, assume $S^1_2 + RFN(P) \vdash RFN(Q)$ for some proof system Q. By Theorem 14 this implies that we can efficiently construct proofs of $\|RFN(Q)\|$ in the system $EF + \|RFN(P)\|$. Applying items 3 and 4 from the proof of Theorem 11 we infer $Q \leq_p EF + \|RFN(P)\| \leq_p P$. □

6 Conclusion

The results of this paper suggest that logical closure properties can be used to give robust definitions of strong proof systems such as EF and its extensions. Continuing this line of research, it is interesting to ask, whether we can also characterize the degrees of weak systems like resolution or cutting planes in terms of similar closure properties. In particular, these weak systems are known to satisfy the feasible interpolation property [17]. Can interpolation in combination with other properties be used to characterize the degrees of weak systems? Pudlák [21] provides strong evidence that interpolation and reflection are mutually exclusive properties. Which other combinations of such properties are possible? Further investigation of these questions will hopefully contribute to a better understanding of propositional proof systems.

Acknowledgements. I am indebted to Jan Krajíček for many helpful and stimulating discussions on the topic of this paper. I also thank Sebastian Müller for detailed suggestions on how to improve the presentation of the paper.

References

1. A. Atserias and M. L. Bonet. On the automatizability of resolution and related propositional proof systems. *Information and Computation*, 189(2):182–201, 2004.
2. O. Beyersdorff. Classes of representable disjoint NP-pairs. *Theoretical Computer Science*, 377:93–109, 2007.
3. O. Beyersdorff. The deduction theorem for strong propositional proof systems. In *Proc. 27th Conference on Foundations of Software Technology and Theoretical Computer Science*, volume 4855 of *Lecture Notes in Computer Science*, pages 241–252. Springer-Verlag, Berlin Heidelberg, 2007.
4. M. L. Bonet. Number of symbols in Frege proofs with and without the deduction rule. In P. Clote and J. Krajíček, editors, *Arithmetic, Proof Theory and Computational Complexity*, pages 61–95. Oxford University Press, Oxford, 1993.
5. M. L. Bonet and S. R. Buss. The deduction rule and linear and near-linear proof simulations. *The Journal of Symbolic Logic*, 58(2):688–709, 1993.

6. M. L. Bonet, S. R. Buss, and T. Pitassi. Are there hard examples for Frege systems? In P. Clote and J. Remmel, editors, *Feasible Mathematics II*, pages 30–56. Birkhäuser, 1995.
7. M. L. Bonet, T. Pitassi, and R. Raz. Lower bounds for cutting planes proofs with small coefficients. *The Journal of Symbolic Logic*, 62(3):708–728, 1997.
8. S. R. Buss. *Bounded Arithmetic*. Bibliopolis, Napoli, 1986.
9. S. R. Buss. An introduction to proof theory. In S. R. Buss, editor, *Handbook of Proof Theory*, pages 1–78. Elsevier, Amsterdam, 1998.
10. S. A. Cook. Feasibly constructive proofs and the propositional calculus. In *Proc. 7th Annual ACM Symposium on Theory of Computing*, pages 83–97, 1975.
11. S. A. Cook and R. A. Reckhow. The relative efficiency of propositional proof systems. *The Journal of Symbolic Logic*, 44:36–50, 1979.
12. G. Gentzen. Untersuchungen über das logische Schließen. *Mathematische Zeitschrift*, 39:68–131, 1935.
13. J. Grollmann and A. L. Selman. Complexity measures for public-key cryptosystems. *SIAM Journal on Computing*, 17(2):309–335, 1988.
14. P. Hájek and P. Pudlák. *Metamathematics of First-Order Arithmetic*. Perspectives in Mathematical Logic. Springer-Verlag, Berlin Heidelberg, 1993.
15. J. Köbler, J. Messner, and J. Torán. Optimal proof systems imply complete sets for promise classes. *Information and Computation*, 184:71–92, 2003.
16. J. Krajíček. *Bounded Arithmetic, Propositional Logic, and Complexity Theory*, volume 60 of *Encyclopedia of Mathematics and Its Applications*. Cambridge University Press, Cambridge, 1995.
17. J. Krajíček. Interpolation theorems, lower bounds for proof systems and independence results for bounded arithmetic. *The Journal of Symbolic Logic*, 62(2):457–486, 1997.
18. J. Krajíček and P. Pudlák. Propositional proof systems, the consistency of first order theories and the complexity of computations. *The Journal of Symbolic Logic*, 54:1963–1079, 1989.
19. J. Krajíček and P. Pudlák. Quantified propositional calculi and fragments of bounded arithmetic. *Zeitschrift für mathematische Logik und Grundlagen der Mathematik*, 36:29–46, 1990.
20. P. Pudlák. Lower bounds for resolution and cutting planes proofs and monotone computations. *The Journal of Symbolic Logic*, 62:981–998, 1997.
21. P. Pudlák. On reducibility and symmetry of disjoint NP-pairs. *Theoretical Computer Science*, 295:323–339, 2003.
22. A. A. Razborov. On provably disjoint NP-pairs. Technical Report TR94-006, Electronic Colloquium on Computational Complexity, 1994.
23. Z. Sadowski. On an optimal propositional proof system and the structure of easy subsets of TAUT. *Theoretical Computer Science*, 288(1):181–193, 2002.
24. Z. Sadowski. Optimal proof systems, optimal acceptors and recursive presentability. *Fundamenta Informaticae*, 79(1–2):169–185, 2007.
25. C. Wrathall. Rudimentary predicates and relative computation. *SIAM Journal on Computing*, 7(2):149–209, 1978.