The Complexity of Resolution with Generalized Symmetry Rules*

Stefan Szeider†
Department of Computer Science, University of Toronto,
M5S 3G4 Toronto, Ontario, Canada
szeider@cs.toronto.edu

Abstract

We generalize Krishnamurthy's well-studied symmetry rule for resolution systems by considering homomorphisms instead of symmetries; symmetries are injective maps of literals which preserve complements and clauses; homomorphisms arise from symmetries by releasing the constraint of being injective.

We prove that the use of homomorphisms yields a strictly more powerful system than the use of symmetries by exhibiting an infinite sequence of sets of clauses for which the consideration of global homomorphisms allows exponentially shorter proofs than the consideration of local symmetries. It is known that local symmetries give rise to a strictly more powerful system than global symmetries; we prove a similar result for local and global homomorphisms. Finally, we obtain an exponential lower bound for the resolution system enhanced by the local homomorphism rule.

1 Introduction

Informal proofs often contain the phrase "...without loss of generality, we assume that..." indicating that it suffices to consider one of several symmetric cases. Krishnamurthy [8] made this informal feature available for the resolution system; he introduced a global symmetry rule (exploiting symmetries of the refuted CNF formula) and a local symmetry rule (exploiting symmetries of those clauses of the refuted CNF formula which are actually used at a certain stage of the derivation). Similar rules have been formulated for cut-free Gentzen systems by Arai [1, 3].

*Part of this work has been published in preliminary form in the proceedings of the 20th International Symposium on Theoretical Aspects of Computer Science (STACS'03), Berlin, February 27 – March 1, 2003.

†The author gratefully acknowledges the support of the Austrian Science Funds (FWF) Projects J2111 and J2295.

In the quoted paper, Krishnamurthy observes that the resolution system, equipped with the global symmetry rule, permits short proofs (i.e., proofs of polynomial length) of several combinatorial principles, including the pigeon hole formulas; however, it is well known that the pigeon hole formulas require resolution proofs of exponential length ([7]; see also [5]). A formal proof of this separation (resolution from resolution + global symmetry) can be found in [12]. Moreover, Arai and Urquhart [4] showed that for resolution systems the local symmetry rule attains an exponential speedup over the global symmetry rule. Random formulas contain almost no nontrivial global symmetries, but it is expected that random formulas contain a lot of local symmetries [12].

The symmetries of CNF formulas considered by Krishnamurthy are special cases of *CNF homomorphisms*, introduced in [10]. A homomorphism from a CNF formula F to a CNF formula G is a map φ from the literals of F to the literals of G which preserves complements and clauses; i.e., $\varphi(\overline{x}) = \overline{\varphi(x)}$ for all literals x of F, and $\{\, \varphi(x) : x \in C \,\} \in G$ for all clauses $C \in F$ — symmetries are nothing but injective homomorphisms (see Section 3 for a more detailed definition). Allowing homomorphisms instead of symmetries in the formulation of the global and local symmetry rule gives raise to more general rules which we term *global* and *local homomorphism rule*, respectively.

In view of the soundness proof for the local homomorphism rule (Lemma 8), this rule can be considered as a means for omitting a subderivation if the subderivation is the homomorphic image (say, under a homomorphism φ) of another already established subderivation. For the global homomorphism rule, φ must be additionally an endomorphism of the input formula. See Section 4 for a small example which illustrates both variants of the homomorphism rule.

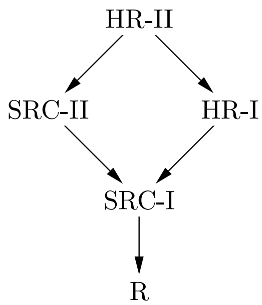
Separation results

We show that the consideration of homomorphisms gives an exponential speedup over symmetries. We provide a sequence of formulas for which even *global* homomorphisms outperform *local* symmetries (Section 5).

Furthermore, in Section 6 we exhibit a sequence of formulas for which proofs using local homomorphisms are exponentially shorter than shortest proofs using global homomorphisms (a similar result is shown in [4] for symmetries). Fig. 1 gives an overview of our results on the relative efficiency of the considered systems in terms of *p-simulation* (system A p-simulates system B if refutations of system B can be transformed in polynomial time into refutations of system A, cf. [11]).

Lower bounds

The exponential lower bound for resolution + local symmetry rule established in [4] does not extend to the more general homomorphism system: to prevent any symmetries, it suffices to modify formulas which are hard for resolution (e.g., pigeon hole formulas) so that all clauses have different width (besides some unit clauses). This can be achieved by adding "dummy variables" to clauses and



R = resolution
SRC-I = resolution + global symmetry rule
SRC-II = resolution + local symmetry rule
HR-I = resolution + global homomorphism rule
HR-II = resolution + local homomorphism rule

Figure 1: Proof system map. $A \to B$ indicates that system A p-simulates system B, but B cannot p-simulate A.

by providing unit clauses which contain the negations of the dummy variables. However, since widths of clauses may decrease under homomorphisms, such approach is not applicable for homomorphisms.

We achieve an exponential lower bound for the local homomorphism rule by a "link construction," which transforms any formula F which is hard for resolution into a formula F° which is hard for resolution + local homomorphism rule. The trick is to take a new variable for every literal occurrence of F, and to interconnect the obtained clauses by certain sets of clauses ("links") which cannot be mapped to F° by a non-trivial homomorphism. This construction is presented in Section 7.

Further Generalizations

The exponential lower bounds for the above systems depend crucially on the fact that the considered homomorphisms/symmetries involve only clauses of the input formula, not derived clauses. In Section 8 we discuss this observation and formulate a generalization of the homomorphism rule, a "dynamic homomorphism rule," where also homomorphisms of derived clauses can be used (a dynamic symmetry rule can be formulated analogously). All formulas considered in the sequel (in particular the formulas of Section 7 that are hard for resolution + local homomorphism rule) have short proofs in presence of the dynamic rules. This yields immediately an exponential separation of dynamic rules from their "static" variants. The complexities of resolution systems with dynamic rules remain open.

2 Definitions and preliminaries

We consider propositional formulas in conjunctive norm form (CNF) represented as sets of clauses: We assume an infinite set var of (propositional) *variables.* A *literal* ℓ is a variable x or a negated variable $\neg x$; we write $\mathsf{lit} := \{ x, \neg x : x \in \mathsf{var} \}$. For a literal ℓ we put $\overline{\ell} := \neg x$ if $\ell = x$, and $\overline{\ell} := x$ if $\ell = \neg x$. For a set of literals C we put $\overline{C} := \{ \overline{\ell} : \ell \in C \}$. We say that sets C, D of literals *clash* if $C \cap \overline{D} \neq \emptyset$, and that C, D *overlap* if $C \cap D \neq \emptyset$. A set of literals is *tautological* if $C \cap \overline{C} \neq \emptyset$. A finite non-tautological set of literals is a *clause*; a finite set of clauses is a *formula*. The *length* of a formula F is given by its cardinality $|F|$, and its *size* by $\|F\| := \sum_{C \in F} |C|$. Note that always $|F| \leq \|F\| + 1$. A formula F *mentions* a variable x if F contains a clause C such that $x \in C \cup \overline{C}$; $\mathsf{var}(F)$ denotes the set of variables mentioned by F. Similarly we put $\mathsf{lit}(F) := \mathsf{var}(F) \cup \overline{\mathsf{var}(F)}$. A literal ℓ is a *pure literal* of a formula F if some clauses of F contain ℓ but no clause contains $\overline{\ell}$.

A formula F is *satisfiable* if there is a map $t : \mathsf{var}(F) \to \{0, 1\}$ such that every clause of F contains either a variable x with $t(x) = 1$ or a literal $\neg x$ with $t(x) = 0$. A formula is *minimally unsatisfiable* if it is unsatisfiable but every proper subset is satisfiable.

If $C_1 \cap \overline{C_2} = \{\ell\}$ for clauses C_1, C_2 and a literal ℓ, then the *resolution rule* allows the derivation of the clause $D = (C_1 \cup C_2) \setminus \{\ell, \overline{\ell}\}$; D is the *resolvent* of C_1 and C_2, and we say that D is obtained by *resolving on* ℓ. Let F be a formula and C a clause. A sequence $S = C_1, \ldots, C_k$ of clauses is a *resolution derivation of* C_k *from* F if for each $i \in \{1, \ldots, k\}$ at least one of the following holds.

1. $C_i \in F$ ("C_i is an axiom");
2. C_i is a resolvent of C_j and $C_{j'}$ for some $1 \leq j < j' < i$ ("C_i is obtained by resolution");
3. $C_i \supseteq C_j$ for some $1 \leq j < i$ ("C_i is obtained by weakening").

We write $|S| := k$ and call k the *length* of S. If C_k is the empty clause, then S is a *resolution refutation* of F. A clause C_i in a resolution derivation may have different possible "histories;" i.e., C_i may be the resolvent of more than one pair of clauses preceding C_i, or C_i may be both an axiom and obtained from preceding clauses by resolution, etc. In the sequel, however, we assume that an arbitrary but fixed history is associated with each considered resolution derivation; a similar convention applies to other types of derivations considered.

It is well known that resolution is a complete proof system for unsatisfiable formulas; i.e., a formula F is unsatisfiable if and only if there exists a resolution refutation of it.

The *resolution complexity* $\mathsf{Comp}_{\mathrm{R}}(F)$ of an unsatisfiable formula F is the length of a shortest resolution refutation of F (for satisfiable formulas we put $\mathsf{Comp}_{\mathrm{R}}(F) := \infty$). Here, R stands for the resolution system, and we will use similar notations for other proof systems considered in the sequel.

We call a resolution derivation *weakening-free* if no clause is obtained by weakening. It is well known that weakening is inessential for the length of resolution refutations:

Lemma 1. *The length of a shortest weakening-free resolution refutation of a formula F is not greater than the length of a shortest resolution refutation of F.*

Proof. See the proof of the more general Lemma 9 below. □

If a formula F contains a unit clause $\{\ell\}$, then we can reduce F to a formula F' by removing $\{\ell\}$ from F and $\overline{\ell}$ from all other clauses. We say that F *can be reduced to* F^* *by unit resolution* if F^* can be obtained from F by multiple applications of this reduction. Evidently, F is satisfiable if and only if F^* is satisfiable. The following can be shown easily.

Lemma 2. *Let F and F^* be formulas such that F can be reduced to F^* by unit resolution. Then* $\mathsf{Comp}_{\mathrm{R}}(F^*) \leq \mathsf{Comp}_{\mathrm{R}}(F)$.

Proof. It suffices to show the lemma for one reduction step. Let $S = C_1, \ldots, C_k$ be a resolution derivation from a formula F with $\{\ell\} \in F$, and let $F^* = \{\, C^\ell : C \in F \,\} \setminus \{\{\ell\}\}$ where C^ℓ is a shorthand for $C \setminus \{\overline{\ell}\}$. It follows by a standard induction on k, that if $\ell \notin C_k$, then $C_1^\ell, \ldots, C_k^\ell$ contains a subsequence S^* which is a resolution derivation of some subset of C_k^ℓ from F^*. ☐

The *pigeon hole formulas* PH_n, $n = 1, 2, \ldots$ encode the fact that $n + 1$ pigeons do not fit into n holes if each hole can hold at most one pigeon (i.e., Dirichlet's Box Principle); formally, we take variables $x_{i,j}$, $1 \leq i \leq n + 1$ and $1 \leq j \leq n$ (with the intended meaning 'pigeon i sits in hole j') and put

$$\begin{aligned}\mathrm{PH}_n \quad := \quad & \{\, \{x_{i,1}, \ldots, x_{i,n}\} : 1 \leq i \leq n+1 \,\} \cup \\ & \{\, \{\neg x_{i,j}, \neg x_{i',j}\} : 1 \leq j \leq n,\ 1 \leq i < i' \leq n+1 \,\}.\end{aligned}$$

Since PH_n contains $n+1$ clauses of width n and $n\binom{n+1}{2}$ clauses of width 2, we have $|\mathrm{PH}_n| = (n^3 + n^2)/2 + n + 1 = \mathcal{O}(n^3)$, and $\|\mathrm{PH}_n\| = n^3 + 2n^2 + n = \mathcal{O}(n^3)$. Furthermore, the following can be verified easily.

Lemma 3. PH_n *is minimally unsatisfiable for every $n \geq 1$.*

Note that the weaker "onto" variant of the pigeon hole formula is not minimally unsatisfiable.

The following seminal result on the length of resolution refutations is due to Haken [7]; see also [5] for a simpler proof. This result is the basis for our separation and lower bound results.

Theorem 1. *Shortest resolution refutations of* PH_n *have length* $2^{\Omega(n)}$.

3 Homomorphisms

Consider a finite set $L \subseteq \mathsf{lit}$ of literals. A map $\rho : L \to \mathsf{lit}$ is a *renaming* if for every pair $\ell, \overline{\ell} \in L$ we have $\overline{\rho(\ell)} = \rho(\overline{\ell})$ (note that in our setting, renamings are not necessarily injective). For a subset $C \subseteq L$ we put $\rho(C) := \{\, \rho(\ell) : \ell \in C \,\}$, and for a formula F with $\mathsf{lit}(F) \subseteq L$ we put $\rho(F) := \{\, \rho(C) : C \in F \,\}$. Since for a clause C, $\rho(C)$ may be tautological, we define $\rho_{\mathsf{cls}}(F)$ as the set of all non-tautological $\rho(C)$ with $C \in F$.

Lemma 4. *Let F be a formula, $\rho : \mathsf{lit}(F) \to \mathsf{lit}$ a renaming, and C, D clauses of F. If C and D overlap, then $\rho(C)$ and $\rho(D)$ overlap. If C and D clash, then $\rho(C)$ and $\rho(D)$ clash.*

Lemma 5. *Let F be a formula, $S = C_1, \ldots, C_k$ a resolution derivation from F, and $\rho : \mathsf{lit}(F) \to \mathsf{lit}$ a renaming. If $\rho(C_k)$ is a clause, then $\rho(C_1), \ldots, \rho(C_k)$ contains a subsequence which is a resolution derivation of $\rho(C_k)$ from $\rho_{\mathsf{cls}}(F)$.*

Proof. If C_k is an axiom or is obtained by the weakening rule, the same holds trivially for $\rho(C_k)$; i.e., if $C_k \in F$, then $\rho(C_k)$ is a clause and belongs to $\rho(F)$, and if $C_k \supseteq C_j$ for some C_j, $1 \le j < k$, then $\rho(C_k) \supseteq \rho(C_j)$. Hence assume that C_k is obtained by the resolution rule from clauses $C_j, C_{j'}$, $1 \le j < j' < k$. Thus, there is a literal ℓ with $C_j \cap \overline{C_{j'}} = \{\ell\}$, and we have

$$\rho(C_j) \subseteq \rho(C_k) \cup \{\rho(\ell)\} \quad \text{and} \quad \rho(C_{j'}) \subseteq \rho(C_k) \cup \{\rho(\overline{\ell})\}. \tag{1}$$

First we show that not both $\rho(C_j)$ and $\rho(C_{j'})$ can be tautological. Suppose to the contrary that there are literals $a, b \in C_j$, $a', b' \in C_{j'}$, such that $\rho(a) = \rho(\overline{b})$, and $\rho(a') = \rho(\overline{b'})$. Since $\rho(C_k)$ is non-tautological, $\rho(\ell) \in \{\rho(a), \rho(b)\}$ and $\rho(\overline{\ell}) \in \{\rho(a'), \rho(b')\}$. W.l.o.g., we assume $\rho(\ell) = \rho(a) = \rho(\overline{a'})$. By (1) we have $\rho(b), \rho(b') \in \rho(C_k)$; however, since $\rho(b) = \rho(\overline{b'})$, it follows that $\rho(C_k)$ is tautological, a contradiction.

Hence at least one of the clauses $\rho(C_j)$ and $\rho(C_{j'})$ is non-tautological. If both $\rho(C_j)$ and $\rho(C_{j'})$ are non-tautological, then evidently $\rho(C_j) \cap \rho(\overline{C_{j'}}) = \{\rho(\ell)\}$, and so $\rho(C_k)$ is the resolvent of $\rho(C_j)$ and $\rho(C_{j'})$. It remains to consider the case that exactly one of $\rho(C_j)$ and $\rho(C_{j'})$ is tautological, say $\rho(C_j)$. Thus, assume that there are literals $a, b \in C_j$ such that $\rho(a) = \rho(\overline{b})$. As above we conclude that $\rho(\ell) \in \{\rho(a), \rho(b)\}$, say $\rho(\ell) = \rho(a)$. From $\rho(b) \ne \rho(\ell)$ and the first inclusion of (1) we conclude $\rho(\overline{\ell}) \in \rho(C_k)$. Hence $\rho(C_{j'}) \subseteq \rho(C_k)$ follows from the second inclusion of (1). Thus $\rho(C_k)$ can be obtained from $\rho(C_{j'})$ by weakening.

The lemma now follows by induction on the length of S. ☐

Let F_1, F_2 be formulas and $\varphi : \mathsf{lit}(F_1) \to \mathsf{lit}(F_2)$ a renaming. We call φ a *homomorphism from F_1 to F_2* if $\varphi(F_1) \subseteq F_2$ (thus, for every $C \in F_1$, $\varphi(C)$ is a clause and belongs to F_2). The set of all homomorphisms from F_1 to F_2 is denoted by $\mathsf{Hom}(F_1, F_2)$. A homomorphism $\varphi \in \mathsf{Hom}(F_1, F_2)$ is a *monomorphism* if the map $\varphi : \mathsf{lit}(F_1) \to \mathsf{lit}(F_2)$ is injective. Homomorphisms from a formula to itself are called *endomorphisms*; an endomorphism φ of F is called *automorphism* (or *symmetry*) if $\varphi(F) = F$; otherwise it is a *proper endomorphism*. We denote by id_F the automorphism of F which maps every literal of F to itself. Finally, we call a homomorphism $\varphi \in \mathsf{Hom}(F_1, F_2)$ *positive* if $\varphi(\mathsf{var}(F_1)) \subseteq \mathsf{var}(F_2)$ (i.e., literals are mapped to literals of the same polarity), and we call φ *width preserving* if $|\varphi(C)| = |C|$ holds for all clauses $C \in F_1$.

We state some direct consequences of Lemma 5.

Lemma 6. *Let F_1 and F_2 be formulas.*

1. *If $C_1, \ldots, C_k$ is a resolution derivation from F_1, $\varphi \in \mathsf{Hom}(F_1, F_2)$, and $\varphi(C_k)$ is a clause, then $\varphi(C_1), \ldots, \varphi(C_k)$ contains a subsequence which is a resolution derivation of $\varphi(C_k)$ from F_2.*

2. *If* $\mathsf{Hom}(F_1, F_2) \neq \emptyset$*, then* $\mathsf{Comp}_{\mathrm{R}}(F_2) \leq \mathsf{Comp}_{\mathrm{R}}(F_1)$.

3. *If* $\mathsf{Hom}(F_1, F_2) \neq \emptyset$ *and* F_1 *is unsatisfiable, then* F_2 *is unsatisfiable.*

4. *Let* φ *be an endomorphism of* F_1*. Then* F_1 *is satisfiable if and only if* $\varphi(F_1)$ *is satisfiable.*

Parts 3 and 4 of the previous lemma have short semantic proofs as well, see [10]. In view of part 4 we can reduce a formula F by endomorphisms until we end up with a subset F' of F for which every endomorphism is an automorphism. We call such F' a *core* of F, and we call F a core if it is a core of itself. In general, there may be different ways of reducing F by endomorphisms, and we may end up with different cores. However, in [10] it is shown that all cores of a formula are isomorphic; thus, in a certain sense, these reductions are confluent. In the quoted paper it is also shown that recognition of cores (i.e., of formulas without proper endomorphisms) is co-NP-complete. The following is a direct consequence of the last part of Lemma 6.

Lemma 7. *Minimally unsatisfiable formulas are cores.*

4 The homomorphism rule

Consider a derivation S from a formula F and a subsequence S' of S which is a derivation of a clause C from a subset $F' \subseteq F$. If there is a homomorphism $\varphi \in \mathsf{Hom}(F', F)$ such that $\varphi(C)$ is non-tautological, then the *local homomorphism rule* allows the derivation of $\varphi(C)$. We call the restricted form of this rule which can only be applied if $F' = F$ the *global homomorphism rule*. The systems **HR-I** and **HR-II** arise from the resolution system by addition of the global and local homomorphism rule, respectively.

We illustrate the new rules by the following simple example. Consider the formula $F = \{C_1, \dots, C_5\}$ with $C_1 = \{a, x\}$, $C_2 = \{\neg v, \neg x, y\}$, $C_3 = \{a, \neg y\}$, $C_4 = \{b, \neg z\}$, $C_5 = \{\neg v, z\}$, and assume that we have obtained the clause $\{a, v\}$ from F by the resolution derivation S consisting of the following 5 clauses:

C_1	axiom;
C_2	axiom;
$\{a, \neg v, y\}$	by resolution from C_1 and C_2;
C_3	axiom;
$\{a, \neg v\}$	from $\{a, \neg v, y\}$ and C_3 by resolution.

Consider the non-injective renaming φ defined by $\varphi(x) = \varphi(\neg y) = \neg z$, $\varphi(a) = b$, and $\varphi(v) = v$ (by definition of a renaming, we need not specify the values for $\neg x$, y, $\neg a$, and $\neg v$). For $F' = \{C_1, C_2, C_3\}$, we have $\varphi(F') = \{C_4, C_5\} \subseteq F$; thus $\varphi \in \mathsf{Hom}(F', F)$. Since the axioms used in the derivation S belong to F', S is actually a derivation of $\{a, \neg v\}$ from F'. Thus we can obtain the clause $\varphi(\{a, \neg v\}) = \{b, \neg v\}$ by the local homomorphism rule, and we can add it as sixth clause to S. Actually, φ can be extended to an endomorphism φ' of F by setting $\varphi'(b) = b$, and $\varphi'(z) = z$, yielding $\varphi'(F) = \{C_4, C_5\}$. Thus, the inference of $\{b, \neg v\}$ can also be justified by the global homomorphism rule.

Now we consider $F^* = \{C_1, \ldots, C_6\}$ with $C_6 = \{\neg a\}$ instead of F. Clearly $\varphi \in \mathsf{Hom}(F', F^*)$ and so we can still derive $\{b, \neg v\}$ by the local homomorphism rule. However, φ cannot be extended to an endomorphism of F^* since $\varphi(\{\neg a\}) = \{\neg b\} \notin F^*$; thus $\{b, \neg v\}$ cannot be obtained by the global homomorphism rule in this case.

Lemma 8. *The homomorphism rule is sound; i.e., formulas having an HR-II refutation are unsatisfiable.*

Proof. Let F be a formula, $S = C_1, \ldots, C_k$ an HR-II refutation of F, and $n(S)$ the number of applications of the homomorphism rule. We show by induction on $n(S)$ that S can be transformed into a resolution refutation S' of F.

If $n(S) = 0$, then this holds vacuously. Assume $n(S) > 0$ and choose $i \in \{1, \ldots, k\}$ minimal such that C_i is obtained from some C_j, $1 \leq j < i$, using the homomorphism rule. Thus, there is some $F' \subseteq F$ and a homomorphism $\varphi \in \mathsf{Hom}(F', F)$ such that $\varphi(C_j) = C_i$, and $C_1, \ldots, C_j$ contains a subsequence S' which is a derivation of C_j from F'. By the choice of i, S' is a resolution derivation. Applying Lemma 6(1), we conclude that $\varphi(C_1), \ldots, \varphi(C_j)$ contains a subsequence S'' which is a resolution derivation of $\varphi(C_j)$ from $\varphi(F') \subseteq F$. By juxtaposition of S'' and S we get an HR-II refutation S^*; since $n(S'') = 0$, and since we replaced one application of the homomorphism rule by a weakening, we have $n(S^*) = n(S) - 1$. By induction hypothesis, S^* can be transformed into a resolution refutation of F. □

The proof of Lemma 8 gives a reason for considering HR-II refutations as *succinct representations of resolution refutations*. Note that the transformation defined in this proof may cause an exponential growth of refutation length (this is the case for the formulas constructed in Section 7).

Krishnamurthy's systems of *symmetric resolution* **SR**-λ and **SRC**-λ, $\lambda \in \{\mathrm{I}, \mathrm{II}\}$, arise as special cases of HR-λ: In SRC-λ, applications of the homomorphism rule are restricted to cases where φ is a monomorphism (for $\lambda = \mathrm{I}$, φ is an automorphism of the refuted formula); SR-λ arises from SRC-λ by considering only positive monomorphisms (variables are mapped to variables). In the context of SR-λ and SRC-λ we refer to the homomorphism rule as the *symmetry rule*.

In terms of informal proofs the homomorphism rule can be considered as the strategy of proving only a *hardest* case out of several prevailing cases; the symmetry rule says that it suffices to prove one of several *equivalent* cases.

Next we show that Lemma 1 extends to all the above systems.

Lemma 9. *For every HR-II derivation $S = C_1, \ldots, C_k$ from a formula F there is a weakening-free HR-II derivation $S' = D_1, \ldots, D_k$ from F with $D_i \subseteq C_i$, $i = 1, \ldots, k$; consequently, the length of a shortest weakening-free HR-II refutation of an unsatisfiable formula F is not greater than the length of a shortest HR-II refutation of F. Analogous statements hold for the systems R, SR-λ, SRC-λ, HR-λ ($\lambda \in \{I,II\}$).*

Proof. We obtain S' inductively as follows. If C_k is an axiom, then we put $D_k := C_k$, and if C_k is obtained by the weakening rule from some C_j, $1 \leq j < k$, then we put $D_k := D_j$.

Now assume that C_k is obtained by the resolution rule from clauses $C_j, C_{j'}$, $1 \leq j < j' < k$. Thus, there is a literal ℓ with $C_j \cap \overline{C_{j'}} = \{\ell\}$. If $\ell \notin D_j$, then we put $D_k := D_j \subseteq C_k$; otherwise, if $\overline{\ell} \notin D_{j'}$, then we put $D_k := D_{j'} \subseteq C_k$. If, however, $\ell \in D_j \cap \overline{D_{j'}}$, then $D_k := (D_j \cup D_{j'}) \setminus \{\ell, \overline{\ell}\} \subseteq C_k$ is the resolvent of D_j and $D_{j'}$.

It remains to consider the case that C_k is obtained by the homomorphism rule from some C_j, $1 \leq j < k$. That is, $\varphi(C_j) = C_k$ for $\varphi \in \mathsf{Hom}(F', F)$, and F' is a subset of F containing all axioms used to derive C_j. We put $D_k := \varphi(D_i)$. Evidently, D_k can be obtained from D_i using φ (observe that the axioms used to derive D_j belong to F' as well). Since $D_j \subseteq C_j$ by induction hypothesis, we have $D_k = \varphi(D_j) \subseteq \varphi(C_j) = C_k$. Hence the lemma holds for HR-II; it also holds for the other claimed systems since the respective restrictions to applications of the homomorphism rule in S translates to the same restrictions in S'. ☐

Borrowing a notion from category theory, we call a formula *rigid* if it has no automorphism except the identity map (cf. [9]). Since an SRC-I refutation of a rigid formula is nothing but a resolution refutation, we have the following.

Lemma 10. *If a formula F is rigid, then* $\mathsf{Comp}_{\text{SRC-I}}(F) = \mathsf{Comp}_{\text{R}}(F)$.

We say that F is *locally rigid* if for every integer $n \geq 2$ there is at most one clause $C \in F$ with $|C| = n$. The next result is due to Arai and Urquhart [4].

Lemma 11. *If F is locally rigid, then* $\mathsf{Comp}_{\text{R}}(F) = \mathsf{Comp}_{\text{SRC-II}}(F)$.

5 Separating HR-I from SRC-II

For this section, F denotes some arbitrary but fixed unsatisfiable formula and $S = C_1, \ldots, C_k$ a weakening-free SRC-I refutation of F. Let $h(1) < \cdots < h(n)$ be the indexes $h(i) \in \{1, \ldots, k\}$ such that $C_{h(i)}$ is obtained by the symmetry rule, and let $\alpha_{h(i)}$ denote the automorphism used to obtain $C_{h(i)}$.

We construct a formula $F^\times$ as follows. For each $i = 1, \ldots, n$ we take a variable-disjoint copy F_i of F, using a new variable $\langle x, i\rangle$ for each $x \in \mathsf{var}(F)$. To unify notation, we write $\langle x, 0\rangle := x$ and $F_0 := F$. By disjoint union we obtain the formula

$$F^\times := \bigcup_{i=0}^{n} F_i;$$

we observe that $\|F^\times\| \leq |S| \cdot \|F\|$.

Next we define two special endomorphisms ψ and π of $F^\times$.

ψ denotes the endomorphism of $F^\times$ which increments the level of variables, i.e., we put $\psi(\langle x, i\rangle) = \langle x, i+1\rangle$ for $i < n$ and $\psi(\langle x, n\rangle) = \langle x, n\rangle$. For a clause C with $\mathsf{var}(C) \subseteq \mathsf{var}(F^\times)$ we write $C^+ = \psi(C)$.

π denotes the endomorphism of $F^\times$ which projects $F^\times$ to F; i.e., $\psi(\langle x, j\rangle) = \langle x, 0\rangle$, fort any $j = 0, \ldots, n$.

We call an HR-I derivation $C_1, \ldots, C_t$ from $F^\times$ *decreasing* if for each $i \in \{1, \ldots, t\}$, there is some $j \in \{1, \ldots, n\}$ such that $\mathsf{var}(C_i) \subseteq \mathsf{var}(F_j)$, and whenever $C_{i'}$ is obtained from C_i by the homomorphism rule, $i' \in \{i+1, \ldots, t\}$, we have $\mathsf{var}(C_{i'}) \subseteq \mathsf{var}(F_{j-1})$.

Lemma 12. *There is a decreasing and weakening-free HR-I refutation $S^\times$ of $F^\times$ with $|S^\times| \leq |S|^2$.*

Proof. We construct inductively a sequence $S_0, \ldots, S_n$ of weakening-free HR-I refutations of $F^\times$ such that for each $i \in \{0, \ldots, n\}$ and

$$h^*(i) := \begin{cases} h(i+1) - 1 & \text{for } i < n, \\ k & \text{for } i = n \end{cases}$$

the following holds:

(*) S_i can be written as $D_1, \ldots, D_t, C_1, \ldots, C_k$ such that the initial part $S_i^* := D_1, \ldots, D_t, C_1 \ldots, C_{h^*(i)}$ is decreasing, and for every variable $\langle x, j\rangle$ occurring in S_i we have $j \leq i$.

Evidently, $S_0 := S$ satisfies (*), since every automorphism α of F gives rise to an automorphism $\alpha^\times of F^\times$, defined by $\alpha^\times(\langle x, j\rangle) = \langle \alpha(x), j\rangle$.

Now consider $0 < i \leq n$ and assume that we have already constructed

$$S_{i-1} = \underbrace{D_1, \ldots, D_t, C_1, \ldots, C_{h^*(i-1)}}_{S^*_{i-1}}, C_{h(i)}, \ldots, C_k,$$

satisfying (*). We define

$$S_i := \underbrace{D_1^+, \ldots, D_t^+, C_1^+, \ldots, C^+_{h^*(i-1)}, C_1, \ldots, C_{h^*(i)}}_{S^*_i}, \ldots, C_k.$$

Clearly S_i is an HR-I refutation of $F^\times$, since $D_1^+, \ldots, C^+_{h^*(i-1)}$ is just the initial part S^*_{i-1} of S_{i-1} shifted one level up; the remaining part $C_1, \ldots, C_k$ is an HR-I refutation of $F^\times$ by assumption. Moreover, for every variable $\langle x, j\rangle$ occurring in S_i, either $\langle x, j\rangle$ or $\langle x, j-1\rangle$ occurs in S_{i-1}, but not $\langle x, j'\rangle$ for any $j' > j$. Hence, for every variable $\langle x, j\rangle$ occurring in S_i we have $j \leq i$. It remains to show that S_i^* is decreasing.

- $S^*_{i-1} = D_1, \ldots, C_{h^*(i-1)}$ is decreasing by induction hypothesis, hence so is $D_1^+, \ldots, C^+_{h^*(i-1)}$.
- The clauses $C_1, \ldots, C_{h^*(i)-1}$ can be obtained from $C_1^+, \ldots, C^+_{h^*(i)-1}$ by projection π, and we have $\mathsf{var}(C_j^+) \subseteq \mathsf{var}(F_1)$ for $j = 1, \ldots, h^*(i-1)$.

- Recall that $C_{h(i)} = \alpha_{h(i)}(C_j)$ for some $1 \le j < i$. Since $C_j = \pi(C_j^+)$, $C_{h(i)}$ can be obtained from C_j^+ by the endomorphism $\alpha_{h(i)} \circ \pi$.

It follows now by induction that S_n satisfies (*); thus $S^\times := S_n$ is a decreasing and weakening-free HR-I refutation of $F^\times$. By construction, the length of $S^\times$ is at most $nk \le |S|^2$. Whence the lemma is shown true. □

Next we modify $F^\times$ so that it becomes a locally rigid formula $F^\sharp$, deploying a similar construction as used by Arai and Urquhart [4]. Let $E_1, \dots E_m$ be a sequence of all the clauses of $F^\times$ such that for any $E_j \in F_i$ and $E_{j'} \in F_{i'}$ we have

$$i < i' \text{ implies } j < j';$$
$$i = i' \text{ and } |E_j| < |E_{j'}| \text{ implies } j < j';$$

that is, for $i < i'$, clauses of F_i precede clauses of F_i', and clauses belonging to the same F_i are ordered by increasing size.

For each clause E_j we take new variables $y_{j,1}, \dots, y_{j,j}$, and we put

$$Q_j := \{E_j \cup \{y_{j,1}, \dots, y_{j,j}\}, \{\neg y_{j,1}\}, \dots, \{\neg y_{j,j}\}\}.$$

Finally we define $F^\sharp := \bigcup_{j=1}^m Q_j$, observing that $\|F^\sharp\| \le \|F^\times\| + 2|F^\times|^2$. We state a direct consequence of the above definitions.

Lemma 13. *$F^\sharp$ is locally rigid and can be reduced to $F^\times$ by unit resolution.*

Consider an endomorphism $\varphi^\times$ of $F^\times$ for which $\varphi^\times(E_j) = E_{j'}$ implies $j \ge j'$, $j, j' \in \{1, \dots, m\}$ (this holds for all endomorphisms used in $S^\times$, since $S^\times$ is decreasing). We extend $\varphi^\times$ to an endomorphism of $F^\sharp$ by setting

$$\varphi^\sharp(y_{j,i}) := y_{j',\min(i,j')}.$$

Observe that $\varphi^\times(E_j) = E_{j'}$ implies $\varphi^\sharp(Q_j) = Q_{j'}$.

Lemma 14. $\mathsf{Comp}_{\text{HR-I}}(F^\sharp) \le |S^\times| + |F^\sharp|$.

Proof. Let $S^\times$ be the HR-I refutation of $F^\times$ as provided by Lemma 12, and let Y denote the set of variables of the form $y_{j,i}$. We replace each clause C of $S^\times$ by some clause C', $C \subseteq C' \cup Y$, such that the resulting sequence $S^\sharp$ is an HR-I derivation from $F^\sharp$: If C is an axiom, i.e., $C = E_j \in F^\times$, then we put $C' := E_j \cup \{y_{j,1}, \dots, y_{j,j}\} \in F^\sharp$. If C is obtained by resolving clauses C_1, C_2, then we let C' be the resolvent of C_1' and C_2'. Finally, if C is obtained by the homomorphism rule, say $C = \varphi^\times(C_1)$, then we put $C' := \varphi^\sharp(C_1)$ where $\varphi^\sharp$ is the extension of $\varphi^\times$ as defined above.

Since the last clause of $S^\times$ is empty, the last clause of $S^\sharp$ is a subset of Y; hence we can use unit clauses $\{\neg y\}$, $y \in Y$, to extend $S^\sharp$ to an HR-I refutation of $F^\sharp$, increasing its length at most by $|Y| + 1 \le |F^\sharp|$. □

The following lemma is due to Urquhart [12], see also Krishnamurthy [8]. (In [12], the lemma is formulated for certain formulas PHC_n with $\mathrm{PH}_n \subseteq \mathrm{PHC}_n$; its proof, however, does not rely on the clauses in $\mathrm{PHC}_n \setminus \mathrm{PH}_n$.)

Lemma 15. *There are SR-I refutations of length* $(3n + 1)n/2$ *for the pigeon hole formulas* PH_n.

Theorem 2. *There is an infinite sequence of formulas* F_n, $n = 1, 2, \dots$ *such that the size of* F_n *is* $\mathcal{O}(n^{10})$, F_n *has HR-I refutations of length* $\mathcal{O}(n^{10})$, *but shortest SRC-II refutations have length* $2^{\Omega(n)}$.

Proof. By Lemma 15, pigeon hole formulas PH_n have SRC-I refutations S_n of length $\mathcal{O}(n^2)$. We apply the above constructions and consider $\mathrm{PH}_n^\times$, $\mathrm{PH}_n^\sharp$ and the corresponding HR-I refutations $S_n^\times$, $S_n^\sharp$, respectively. We put $F_n := \mathrm{PH}_n^\sharp$. Lemmas 12, 15, and 14 yield $|S_n^\sharp| = \mathcal{O}(n^{10})$. Putting $\varphi(\langle x, i\rangle) := x$ defines a homomorphism from $F^\times$ to F. Thus, by Lemmas 6(2), 2, 13, and 11, respectively, we have

$$\mathsf{Comp}_{\mathrm{R}}(\mathrm{PH}_n) \leq \mathsf{Comp}_{\mathrm{R}}(\mathrm{PH}_n^\times) \leq \mathsf{Comp}_{\mathrm{R}}(\mathrm{PH}_n^\sharp) = \mathsf{Comp}_{\mathrm{SRC\text{-}II}}(\mathrm{PH}_n^\sharp).$$

The result now follows from Theorem 1. ☐

Corollary 1. *SR-II (and so SR-I) p-simulates neither HR-I nor HR-II.*

6 Separating HR-I from HR-II

In [4] it is shown that SR-II has an exponential speed up over SR-I. We show an analogous result for HR-II and HR-I, using a similar construction.

Consider the pigeon hole formula $\mathrm{PH}_n = \{E_1, \dots, E_t\}$. For each clause E_j we take new variables $y_{j,1}, \dots, y_{j,j}$, and we define

$$Q_j := \{E_j \cup \{y_{j,1}\}, \{\neg y_{j,1}, y_{j,2}\}, \dots, \{\neg y_{j,j-1}, y_{j,j}\}, \{\neg y_{j,j}\}\},$$

and put $\mathrm{PH}_n^\sim := \bigcup_{j=1}^{t} Q_j$. Note that $\|\mathrm{PH}_n^\sim\| \leq \|\mathrm{PH}_n\| + 2|\mathrm{PH}_n|^2 = \mathcal{O}(n^6)$.

Lemma 16. $\mathrm{PH}_n^\sim$ *is a rigid core, for every* $n \geq 1$.

Proof. Let α be an automorphism of $\mathrm{PH}_n^\sim$. We show that $\alpha = id_{\mathrm{PH}_n^\sim}$. Choose $j \in \{1, \dots, t\}$ arbitrarily. Since $|\alpha(C)| = |C|$ for every clause C, it follows that $\alpha(\{\neg y_{j,j}\}) = \{\neg y_{j',j'}\}$ for some $j' \in \{1, \dots, t\}$, i.e., $\alpha(y_{j,j}) = y_{j',j'}$. Consequently, $\alpha(\{\neg y_{j,j-1}, y_{j,j}\}) = \{\neg y_{j',j'-1}, y_{j',j'}\}$ and so $\alpha(y_{j,j-1}) = y_{j',j'-1}$. Repeated application of this argument yields $j = j'$ and $\alpha(y_{j,i}) = y_{j,i}$ for all $i \in \{1, \dots, j\}$. Hence we have $y_{j,1} \in \alpha(E_j \cup \{y_{j,1}\})$; since $E_j \cup \{y_{j,1}\}$ is the only clause in $\mathrm{PH}_n^\sim$ which contains $y_{j,1}$, we have $\alpha(E_j \cup \{y_{j,1}\}) = E_j \cup \{y_{j,1}\}$, and so $\alpha(E_j) = E_j$. For $n = 1$ it is now easy to see that α is the identity map; hence assume $n \geq 2$. For every variable $x \in \mathsf{var}(\mathrm{PH}_n)$ there are clauses $\{\neg x, \neg x'\}, \{\neg x, \neg x''\} \in \mathrm{PH}_n$ with $x' \neq x''$. We have $\alpha(\{\neg x, \neg x'\}) = \{\neg x, \neg x'\}$ and $\alpha(\{\neg x, \neg x''\}) = \{\neg x, \neg x''\}$, thus $\alpha(x) \in \{x, x'\} \cap \{x, x''\} = \{x\}$. Hence $\alpha = id_{\mathrm{PH}_n^\sim}$, and so $\mathrm{PH}_n^\sim$ is rigid.

It follows from Lemma 3 that $\mathrm{PH}_n^\sim$ is minimally unsatisfiable. Thus it is a core by Lemma 7. ☐

We get the following separation of SR-II (resp. HR-II) from HR-I .

Theorem 3. *There is an infinite sequence of formulas F_n, $n = 1, 2, \dots$ such that the size of F_n is $\mathcal{O}(n^6)$, F_n has SR-II refutations (and so HR-II refutations) of length $\mathcal{O}(n^6)$, but shortest HR-I refutations have length $2^{\Omega(n)}$.*

Proof. By means of Lemma 2 we conclude from Theorem 1 that

$$\mathsf{Comp}_{\mathrm{R}}(\mathrm{PH}_n^{\sim}) = 2^{\Omega(n)}.$$

Since PH_n is minimally unsatisfiable, so is $\mathrm{PH}_n^{\sim}$; thus $\mathrm{PH}_n^{\sim}$ is a core by Lemma 7. It is not difficult to show that $\mathrm{PH}_n^{\sim}$ is rigid. Thus every HR-I refutation of $\mathrm{PH}_n^{\sim}$ is nothing but a resolution refutation, and we get

$$\mathsf{Comp}_{\mathrm{HR\text{-}I}}(\mathrm{PH}_n^{\sim}) = \mathsf{Comp}_{\mathrm{R}}(\mathrm{PH}_n^{\sim}) = 2^{\Omega(n)}.$$

By a straightforward construction, an SR-I refutation of PH_n can be transformed into an SR-II refutation of $\mathrm{PH}_n^{\sim}$ adding less than $2|\mathrm{PH}_n|^2$ steps of unit resolution. Hence, the Theorem follows by Lemma 15. ☐

Corollary 2. *HR-I p-simulates neither SR-II nor HR-II.*

In view of Corollary 1 we also have the following.

Corollary 3. *HR-I and SR-II are incomparable in terms of p-simulation.*

7 An exponential lower bound for HR-II

In this section, F denotes some arbitrarily chosen formula without unit clauses. We assume a fixed ordering $E_1, \dots, E_m$ of the clauses of F, and a fixed ordering of the literals in each clause, so that we can write

$$F = \{\{\ell_1, \dots, \ell_{i_1}\}, \{\ell_{i_1+1}, \dots, \ell_{i_2}\}, \dots, \{\ell_{i_{m-1}+1}, \dots, \ell_s\}\};\ s = \|F\|.$$

From F we construct a formula F° as follows. For every $j \in \{1, \dots, s\}$ we take new variables $y_{j,1}, \dots, y_{j,j+2}$ and z_j. We define the formula

$$L'_j = \{\{\neg y_{j,1}, y_{j,2}\}, \{\neg y_{j,2}, y_{j,3}\}, \dots, \{\neg y_{j,j+5}, y_{j,j+6}\}, \{\neg y_{j,j+7}, \ell_j\}\}$$

and obtain from it the formula L_j by adding the variable z_j to all clauses except the 4th and $j+5$th one; we call the formula L_j a *link*. The clause widths of a link L_j yield the unique sequence

$$3\ \ 3\ \ 3\ \ 2\ \ \underbrace{3\ \dots\ 3}_{j \text{ times}}\ \ 2\ \ 3\ \ 3. \tag{2}$$

A link L_j cannot be mapped by some homomorphism to a link $L_{j'}$ with $j \neq j'$, since the respective sequences of clause widths are different for L_j and L'_j. Moreover, since one end of a link has three clauses of width 3, and the other end has two clauses of width 3, one link cannot be mapped to itself by a homomorphism which maps one end to the other. The proof of the next lemma is elementary, but lengthy since several cases must be considered. Therefore we postpone it to the appendix.

Lemma 17. $\mathsf{Hom}(L_j, F^\circ) = \{id_{L_j}\}$ *for any* $1 \le j \le s$.

For every clause $E_i = \{\ell_j, \dots, \ell_{j+|E_i|}\}$ of F we define a corresponding clause

$$E_i^\circ := \{y_{j,1}, \dots, y_{j+|E_i|,1}\}.$$

Finally, we put the above definitions together and obtain

$$F^\circ := \{E_1^\circ, \dots, E_m^\circ\} \cup \bigcup_{j=1}^{s} (L_j \cup \{\neg z_j\}).$$

The size of $L_j \cup \{\neg z_j\}$ is less than $3(s+7)+1$, thus $\|F^\circ\| \le 3s^2 + 23s$.

We will refer to clauses E_i° as *main clauses*, to clauses in L_j as *link clauses*, and to unit clauses $\{z_j\}$ as *auxiliary clauses*.

For each link L_j there is exactly one main clause E_i° with $y_{j,1} \in E_i^\circ$; we put $L_j^* := L_j \cup E_i^\circ$. For a subset $F' \subseteq F^\circ$ we define its *body* $b(F')$ to be the union of all $L_j^* \subseteq F'$. Informally speaking, $b(F')$ can be obtained from F' by removing incomplete links, links which are not adjacent with a main clause in F', and isolated main clauses.

Lemma 18. *For any* $F' \subseteq F^\circ$ *and* $\varphi \in \mathsf{Hom}(F', F^\circ)$ *we have the following.*

1. *If* $\ell \in \mathsf{lit}(b(F))$ *is not a pure literal of* $b(F')$*, then* $\varphi(\ell) = \ell$*;*
2. $\varphi(C) = C$ *for all* $C \in b(F')$*;*
3. *if there is a weakening-free resolution derivation of a clause* D *from* $b(F')$*, then* $\varphi(D) = D$*.*

Proof. If $\ell \in \mathsf{lit}(b(F'))$ is not a pure literal of $b(F')$, then $\ell \in \mathsf{lit}(L_j)$ for some $L_j \subseteq b(F')$. Hence Part 1 follows from Lemma 17.

To show Part 2, choose a clause $C \in b(F')$ arbitrarily. If C is a link clause or an auxiliary clause, then $\varphi(C) = C$ follows from Part 1; hence assume that C is a main clause. By definition of $b(F')$, C contains at least one literal ℓ such that $\overline{\ell}$ belongs to some link clause of $b(F')$; consequently $\varphi(\ell) = \ell$. Since main clauses are mutually disjoint, we conclude $\varphi(C) = C$; thus Part 2 follows.

Part 3 follows from Parts 1 and 2 by induction on the length of the resolution derivation. ☐

We take a new variable z and define a renaming $\rho : \mathsf{lit}(F^\circ) \to \mathsf{lit}(F) \cup \{z, \neg z\}$ by setting

$$\begin{aligned} \rho(y_{j,i}) &:= \ell_j && (j = 1, \dots, s;\ i = 1, \dots, j+7), \\ \rho(\ell_j) &:= \ell_j && (j = 1, \dots, s), \\ \rho(z_j) &:= z && (j = 1, \dots, s). \end{aligned}$$

Consequently, for link clauses C we have $\{\ell_j, \overline{\ell_j}\} \subseteq \rho(C)$ for some $j \in \{1, \dots, s\}$; for auxiliary clauses C we have $\varphi(C) = \{\neg z\}$; for main clauses C° we have $\rho(C^\circ) = C$. Hence $\rho_{\mathsf{cls}}(F^\circ)$ is nothing but $F \cup \{\{\neg z\}\}$, and $\neg z$ is a pure literal of $\rho_{\mathsf{cls}}(F^\circ)$.

Lemma 19. *Let $S = C_1, \dots, C_n$ be a resolution derivation from $F' \subseteq F^\circ$. If $\rho(C_n)$ is non-tautological, then either some subsequence S' of $\rho(C_1), \dots, \rho(C_n)$ is a resolution derivation of $\rho(C_n)$ from $\rho_{\mathsf{cls}}(b(F'))$, or there is some $D \in F'$ with $\rho(D) \subseteq \rho(C_n)$.*

Proof. We assume, w.l.o.g., that no proper subsequence of S is a resolution derivation of C_n from $F' \subseteq F^\circ$. Hence, if ℓ is a literal of some axiom of S, and if no clause of S is obtained by resolving on ℓ, then the last clause of S contains ℓ as well.

By Lemma 5 some subsequence S' of $\rho(C_1), \dots, \rho(C_n)$ is a resolution derivation of $\rho(C_n)$ from $\rho_{\mathsf{cls}}(F')$.

Assume that S' is not a resolution derivation of $\rho(C_n)$ from $\rho_{\mathsf{cls}}(b(F'))$. That is, some axiom D' of S' belongs to $\rho_{\mathsf{cls}}(F') \setminus \rho_{\mathsf{cls}}(b(F'))$. Consequently, there is an axiom $D \in F' \setminus b(F')$ of S with $\rho(D) = D'$. We will show that $D' = \rho(D) \subseteq \rho(C_n)$.

As observed above, $\rho_{\mathsf{cls}}(F^\circ) = F \cup \{\{\neg z\}\}$, and $z \notin C$ for any $C \in F$. Since $\rho(D)$ is tautological for link clauses, D is either a main clause or an auxiliary clause.

First assume that D is a main clause. Consequently $D' \in F$; thus, for some $j \in \{1, \dots, s\}$,

$$D = \{y_{j,1}, \dots, y_{j+|D|,1}\} \text{ and } D' = \{\ell_j, \dots, \ell_{j+|D|}\}.$$

Consider any $j' \in \{j, \dots, j + |D|\}$. Since $D \notin b(F')$, $L_{j'} \nsubseteq F'$ by definition of $b(F')$. Then, however, some $y_{j',i'}$, $i' \in \{1, \dots, j' + 2\}$, is a pure literal of F'. Hence no clause of S is obtained by resolving on $y_{j',i'}$, and since S is assumed to be minimal, $y_{j',i'} \in C_n$ follows. Thus $\rho(y_{j',i'}) = \ell_{j'} \in \rho(C_n)$. This holds for any $j' \in \{j, \dots, j + |D|\}$, and so $\rho(D) \subseteq \rho(C_n)$ follows.

Now assume that D is an auxiliary clause; thus $D = \{\{\neg z_j\}\}$ and $D' = \{\{\neg z\}\}$. Since $\neg z$ is a pure literal of F', we conclude as in the previous case that $\neg z \in \rho(C_n)$. Thus $D' \subseteq \rho(C_n)$ follows. Whence the lemma is shown true. □

Lemma 20. $\mathsf{Comp}_{\mathrm{R}}(F) \leq \mathsf{Comp}_{\text{HR-II}}(F^\circ) + |F|$.

Proof. Let $S = C_1, \dots, C_n$ be a weakening-free HR-II resolution refutation of F°, and let C_i be the first clause which is obtained from some clause C_j, $j < i$, by the homomorphism rule; say $\varphi \in \mathsf{Hom}(F', F^\circ)$ and $C_i = \varphi(C_j)$. If $\rho(C_j)$ is non-tautological, then it follows from Lemma 19 that either some subsequence of $\rho(C_1), \dots, \rho(C_j)$ is a resolution derivation of $\rho(C_j)$ from $\rho_{\mathsf{cls}}(b(F'))$, or $\rho(E_k) \subseteq \rho(C_j)$ for some $k \in \{1, \dots, m\}$ (recall that $F = \{E_1, \dots, E_m\}$). In the first case, Lemma 18 yields $\varphi(b(F')) = b(F')$ and $\varphi(C_j) = C_j = C_i$; thus $\rho(C_i) = \rho(C_j)$. In the second case we can obtain $\rho(C_i)$ by weakening from E_k.

By multiple applications of this argument we can successively eliminate applications of the homomorphism rule, and we end up with a resolution refutation of F which is a subsequence of $E_1, \dots, E_m, \rho(C_1), \dots, \rho(C_n)$. □

Theorem 4. *There is an infinite sequence of unsatisfiable formulas F_n, $n = 1, 2, \ldots$ such that the size of F_n is $\mathcal{O}(n^6)$, and shortest HR-II refutations of F_n have length $2^{\Omega(n)}$.*

Proof. Again we use the pigeon hole formulas and put $F_n = \mathrm{PH}^{\circ}_{n+1}$ (we avoid PH_1 since it contains unit clauses). By construction, we have $\|\mathrm{PH}^{\circ}_{n+1}\| \leq \mathcal{O}(\|\mathrm{PH}_{n+1}\|^2) = \mathcal{O}(n^6)$. The theorem follows by Lemma 20 and Theorem 1. ☐

Corollary 4. *SR-II cannot p-simulate HR-I or HR-II; SR-I cannot p-simulate HR-I or HR-II.*

8 Discussion and further generalizations

The Achilles' heel of HR-II appears to be the fact that the local homomorphism rule cannot take advantage of structural properties of the input formula if these properties are slightly "disguised;" that is, if the properties are not explicitly present in the input formula, but can be made explicit by a simple preprocessing using resolution. We used this observation for showing the exponential lower bound for HR-II: though pigeon hole formulas PH_n have short HR-II refutations, disguised as PH°_n they require HR-II refutations of exponential length.

Other proof systems like *cutting plane proofs (CP)* and *simple combinatorial reasoning (SCR)* (see [6] and [2], respectively), which also allow short refutations of the pigeon hole formulas, are more robust with respect to such disguise. This was observed in [4], where it is shown that SRC-II cannot p-simulate CP or SCR (CP cannot p-simulate SR-I neither). Using a similar argument, it can be shown that HR-II cannot p-simulate CP or SCR. Thus we conclude that HR-II and CP are incomparable in terms of p-simulation.

However, the described flaw of HR-II can be fixed; inspection of the soundness proof (Lemma 8) yields that we can generalize the local homomorphism rule as follows, without loosing soundness.

> Consider a derivation $S = C_1, \ldots, C_k$ from F and a subsequence S' of S which is a derivation of a clause C from some formula F'. If there is a homomorphism $\varphi \in \mathsf{Hom}(F', \{C_1, \ldots, C_k\})$ such that $\varphi(C)$ is non-tautological, then the *dynamic homomorphism rule* allows the derivation of $\varphi(C)$.

Note that we have released two constraints of the local homomorphisms rule: F' is not necessarily a subset of the input formula F, and φ is not necessarily a homomorphism from F' to F (but a homomorphism from F' to the set of clauses appearing in S). Let SR-III, SRC-III, and HR-III denote the proof systems arising from the respective systems using the dynamic homomorphism rule. The formulas which are used to show exponential lower bounds for the global and local systems (see [4, 12] and Theorems 3 and 4 of the present paper) have evidently refutations of polynomial length even in the weakest dynamic system SR-III.

The complexities of SR-III, SRC-III, and HR-III, and their relations to CP and SCR remain as interesting open problems (it seems to be feasible to defeat SR-III by formulas obtained from the pigeon hole formulas by suitable flipping of polarities of literals).

9 Appendix: Proof of Lemma 17

This appendix is devoted to a proof of Lemma 17: the identity map is the only homomorphism which maps a link L_j, $j \in \{1, \dots s\}$, into F°.

Choose $j \in \{1, \dots s\}$ arbitrarily and consider $\varphi \in \mathsf{Hom}(L_j, F^\circ)$. To simplify notation we write $y_i := y_{j,i}$, $y_{j+7} := \ell_j$, and $z := z_j$.

Claim 1. *φ is width preserving, i.e., $|\varphi(C)| = |C|$ holds for all $C \in L_j$.*

Proof. Observe that a clause $C \in L_j$ has width 3 if and only if there is some clause $D \in L_j$ such that C and D clash and overlap. By Lemma 4, $\varphi(C)$ and $\varphi(D)$ clash and overlap as well, hence $|\varphi(C)| = 3$. Thus $|\varphi(C)| = |C|$ holds for all clauses $C \in L_j$ of width 3.

Now consider a clause $C \in L_j$ of width 2; i.e., $C = \{\neg y_i, y_{i+1}\}$. Consequently, L_j contains clauses $A = \{\neg y_{i-1}, y_i, z\}$ and $B = \{\neg y_{i+1}, y_{i+2}, z\}$. Assume to the contrary that $|\varphi(C)| < |C|$; that is, $\varphi(\neg y_i) = \varphi(y_{i+1})$. Consequently $\varphi(y_i) \in \varphi(A) \cap \varphi(B)$. Since also $\varphi(z) \in \varphi(A) \cap \varphi(B)$, but any distinct clauses of F° share at most one literal, it follows that either $\varphi(A) = \varphi(B)$ or $\varphi(z) = \varphi(y_i)$. The latter is impossible, since $|\varphi(A)| = |A| = 3$ as shown above. Hence $\varphi(A) = \varphi(B)$ follows of necessity. By definition of L_j it contains a clause $A' = \{\neg y_{i-2}, y_{i-1}, z\}$. Since A and A' clash and overlap, we conclude by Lemma 4 that also $\varphi(A)$ and $\varphi(A')$ clash and overlap. In particular $\varphi(A) \neq \varphi(A')$ follows. Observe that for any two clauses $X, Y \in F^\circ$ which clash and overlap, if X and some unit clause $Z \in F^\circ$ clash, then also Z and Y clash. Hence, putting $X = \varphi(A) = \varphi(B)$, $Y = \varphi(A')$, and $Z = \{\varphi(\neg y_i)\} = \{\varphi(y_{i+1})\}$, we conclude that $\varphi(y_i) \in \varphi(A')$. Thus $\{\varphi(y_i), \varphi(z)\} \subseteq \varphi(A) \cap \varphi(A')$ and, as shown above, $\varphi(z) \neq \varphi(y_i)$. However, any distinct clauses of F° share at most one literal; thus we have a contradiction. Whence $|\varphi(C)| = |C|$ holds for all clauses $C \in L_j$ and the claim is shown true. □

Claim 2. *$\varphi(L_j) \subseteq L_{j'}$ for some $j' \in \{1, \dots, s\}$.*

Proof. Consider a clause $C \in L_j$ of width 3. There is a clause $C' \in L_j$ such that C and C' clash and overlap. Since main clauses do not overlap with other clauses, and since φ is width preserving by Claim 1, it follows that $\varphi(C)$ is a link clause. Since overlapping link clauses belong to the same link, it follows that there is some link $L_{j'}$, $1 \leq j' \leq s$, which contains all $\varphi(C)$ for $C \in L_j$ and $|C| = 3$. It is now obvious that for $C \in L_j$ with $|C| = 2$, $\varphi(C)$ belongs to $L_{j'}$ as well. □

Claim 3. *φ is a monomorphism.*

Proof. We assume to the contrary that $\varphi(\ell') = \varphi(\ell'')$ holds for distinct literals $\ell', \ell'' \in \mathsf{lit}(L_j)$; w.l.o.g., ℓ' is a variable. Since φ is width preserving, it maps the only unit clause of L_j to itself, hence $\varphi(z) = z$. Thus $\ell' \neq z$ and we are left with the following two cases.

Case 1: $\varphi(y_{i'}) = \varphi(y_i)$ for some $1 \leq i < i' \leq j + 7$. We choose such pair i, i' with minimal i'. Let A denote the (unique) clause of F° that contains y_i (A is possibly a main clause), and let B denote the (unique) clause of L_j that contains $y_{i'}$ and $\neg y_{i'-1}$. If $i = 1$ then A is a main clause, and so $\varphi(A) \neq \varphi(B)$; hence $\varphi(y_i) \in \varphi(A) \cap \varphi(B)$ contradicts the fact that main clauses do not overlap with other clauses. Hence $i > 1$ follows. Consequently A is a link clause and $\neg y_{i-1} \in A$. By Claim 2 $\varphi(A)$ and $\varphi(B)$ belong to the same link $L_{j'}$. Since i' is chosen minimal, $\varphi(y_{i-1}) \neq \varphi(y_{i'-1})$. Thus $\varphi(\neg y_{i-1}) \in \varphi(A)$ and $\varphi(\neg y_{i'-1}) \in \varphi(B)$ implies $\varphi(A) \neq \varphi(B)$. Since $\varphi(A)$ and $\varphi(B)$ overlap, $|A| = |B| = 3$ follows (any two overlapping link clauses have width 3). Hence $\varphi(z) \in \varphi(A) \cap \varphi(B)$. As two link clauses share at most one literal, we infer $\varphi(z) = \varphi(y_{i'})$ and so $|\varphi(A)| < |A|$. This contradicts the fact that φ is width preserving.

Case 2: $\varphi(y_{i'}) = \varphi(\neg y_i)$ for some $1 \leq i < i' \leq j + 7$. We choose such pair i, i' with maximal i'. Let A and B denote the (unique) clauses in L_j that contain $\neg y_i, y_{i+1}$ and $y_{i'}, \neg y_{i'-1}$, respectively. Since i' is chosen maximal, $\varphi(y_{i+1}) \neq \varphi(y_{i'-1})$ and so $\varphi(A) \neq \varphi(B)$ follows. If any two link clauses overlap, then their width is 3; therefore $|A| = |\varphi(A)| = |B| = |\varphi(B)| = 3$ and so $\varphi(z) \in \varphi(A) \cap \varphi(B)$. However, since $|\varphi(A) \cap \varphi(B)| \leq 1$ (this holds for any two link clauses), $\varphi(z) = \varphi(\neg y_i)$ follows. Hence $|\varphi(A)| < |A|$, a contradiction. □

Since each link yields a unique sequence of clause widths (cf. (2)), Claims 2 and 3 imply $\mathsf{Hom}(L_j, F^\circ) = \{id_{L_j}\}$. Hence Lemma 17 is shown true.

References

[1] N. H. Arai. Tractability of cut-free Gentzen type propositional calculus with permutation inference. *Theoret. Comput. Sci.*, 170(1-2):129–144, 1996.

[2] N. H. Arai. No feasible monotone interpolation for simple combinatorial reasoning. *Theoret. Comput. Sci.*, 238(1-2):477–482, 2000.

[3] N. H. Arai. Tractability of cut-free Gentzen-type propositional calculus with permutation inference. II. *Theoret. Comput. Sci.*, 243(1-2):185–197, 2000.

[4] N. H. Arai and A. Urquhart. Local symmetries in propositional logic. In R. Dyckhoff, editor, *Automated Reasoning with Analytic Tableaux and Related Methods (Proc. TABLEAUX 2000)*, volume 1847 of *Lecture Notes in Computer Science*, pages 40–51. Springer Verlag, 2000.

[5] E. Ben-Sasson and A. Wigderson. Short proofs are narrow—resolution made simple. *Journal of the ACM*, 48(2):149–169, 2001.

[6] W. Cook, C. R. Coullard, and G. Turán. On the complexity of cutting-plane proofs. *Discr. Appl. Math.*, 18(1):25–38, 1987.

[7] A. Haken. The intractability of resolution. *Theoret. Comput. Sci.*, 39:297–308, 1985.

[8] B. Krishnamurthy. Short proofs for tricky formulas. *Acta Informatica*, 22:253–275, 1985.

[9] A. Pultr and V. Trnková. *Combinatorial, Algebraic and Topological Representations of Groups, Semigroups and Categories.* North-Holland Publishing Co., Amsterdam, 1980.

[10] S. Szeider. Homomorphisms of conjunctive normal forms. *Discr. Appl. Math.*, 130(2):351–365, 2003.

[11] A. Urquhart. The complexity of propositional proofs. *Bull. of Symbolic Logic*, 1(4):425–467, 1995.

[12] A. Urquhart. The symmetry rule in propositional logic. *Discr. Appl. Math.*, 96/97:177–193, 1999.