2011 26th Annual IEEE Conference on Computational Complexity

Paris-Harrington tautologies

Lorenzo Carlucci, Nicola Galesi* and Massimo Lauria
Dipartimento di Informatica
Università di Roma "La Sapienza"
Roma, Italia
Email: {carlucci,galesi,lauria}@di.uniroma1.it

***Abstract*—We study the proof complexity of Paris-Harrington's Large Ramsey Theorem for bi-colorings of graphs. We prove a non-trivial conditional lower bound in Resolution and a quasi-polynomial upper bound in bounded-depth Frege. The lower bound is conditional on a (very reasonable) hardness assumption for a weak (quasi-polynomial) Pigeonhole principle in RES(2). We show that under such assumption, there is no refutation of the Paris-Harrington formulas of size quasi-polynomial in the number of propositional variables. The proof technique for the lower bound extends the idea of using a combinatorial principle to blow-up a counterexample for another combinatorial principle beyond the threshold of inconsistency. A strong link with the proof complexity of an unbalanced Ramsey principle for triangles is established. This is obtained by adapting some constructions due to Erdős and Mills.**

***Keywords*-proof complexity; bounded-depth frege; resolution; ramsey.**

I. Introduction and Motivation

The Paris-Harrington Theorem for graphs says that for every k and m, there exists an integer $R(k,m)$ such that every graph on the vertices $\{k,\ldots,R(k,m)\}$ contains either a clique with m vertices or an independent set with at least as many vertices as its minimum member (and therefore with at least k vertices). The general version (for arbitrary colorings of hypergraphs) of this seemingly innocent variant of Ramsey Theorem is the most famous example of a natural mathematical finitary theorem that cannot be proved in strong theories like Peano arithmetic, as shown by Harrington and Paris in [8].

It has been sometimes proposed (e.g., by Clote in [3]) that propositional encoding of logically strong combinatorial principles could produce hard tautologies for propositional proof systems. Krajíček [14] recently dismissed this idea as impracticable. The involved functions have an extremely fast growth, and this translates to tautologies so large that there is no room for non-trivial lower and upper bounds on the proof length. This is no longer true if one focuses on suitably weak instances of the strong principles, as exemplified in this paper.

Our first result is that for the known upper bound $u(k)$ on $R(k,k)$ (due to Erdős and Mills [5], [18]) the natural propositional translation of the statement "$R(k,k) \leq u(k)$" has efficient bounded-depth Frege proofs. The proof combines a combinatorial argument by Mills [18] with a proof of a Paris-Harrington principle for triangles. To obtain the latter we adapt Pudlák's [20] proof of Ramsey Theorem in Bounded Arithmetic: since we focus on an off-diagonal Ramsey, the argument requires careful and non-trivial analysis to succeed. This is basically the only part in which we really need the strength of bounded-depth Frege. Note that our upper bound is quasi-polynomial in the *size of the formula*, which is very large compared to the number of variables.

Our second result is that the natural propositional encoding of "$R(k,k) \leq u(k)$" does not have polynomial-size Resolution proofs, unless the weak Pigeonhole principle with quasi-polynomially many more pigeons than holes has small proofs in RES(2). This is a very plausible assumption, perhaps not far beyond the reach of current methods. Our method of proof builds on a technique due to Krajíček [13] who showed how to reduce a proof of the Pigeonhole principle to a proof of Ramsey Theorem. We show how to lift examples witnessing the known lower bounds on the Paris-Harrington numbers $R(k,k)$ to counterexamples to a weak Pigeonhole principle. To do this we employ a construction by Erdős and Mills [5] that has never been applied in proof complexity before. The overall proof-scheme significantly extends Pudlák's [20] and Krajíček's [13] methods.

Our results stress an interesting connection between: (a) constructing witnesses to lower bounds on combinatorial quantities such as $R(k,k)$ or $r(k,k)$, and (b) proving complexity-theoretic lower bounds (in this case, conditional lower bounds for Resolution). Proving lower bounds on Ramsey-like quantities is a notable open-ended problem in combinatorics. The most famous example is the best known lower bound on $r(k,k)$, based on the probabilistic method, that eludes so far all attempts to a constructive proof. Other famous examples include Ramsey numbers for k-uniform hypergraphs for $k > 2$. The method of proof in our second result hints at a computational complexity lower bound being hidden under the problem of narrowing the interval in which $R(k,k)$ lays. This remarkable connection was originally made by Krajíček [13] for Ramsey numbers and we push it further to Paris-Harrington numbers. In our case, the quality of the lower bound on the proof length strongly depends on how good the combinatorial bounds are. In the worst case we are able to (conditionally) exclude proofs of quasi-polynomial length with respect to the number of propositional variables. We believe that the connection is inspiring and worth of further study.

Another point of interest it that the proposed encoding of Paris-Harrington formulas can be considered as (new) good candidates for separating bounded-depth from low-depth (e.g. depth 2) Frege systems. The corresponding problem in circuit

* Partly supported by Sapienza Research Project: "Complessità e Rappresentabilità Compatta di Strutture Discrete".

1093-0159/11 $26.00 © 2011 IEEE
DOI 10.1109/CCC.2011.17

complexity has long been solved (see [9]), but in proof complexity only partial results are known [12], [2].

II. Ramsey and Paris-Harrington principles

We introduce the combinatorial principles of interest for the present paper and their propositional formalizations. We consider the following formulation of Ramsey Theorem for bi-colorings of graphs. The principle states that any large enough graph contains either a clique or a stable set of arbitrary size. Of course "large enough" is relative to the size of the clique and of the stable set.

Theorem (Ramsey Theorem)**.** *There exists a number $r(k,s)$ which is the smallest number such that any graph with at least $r(k,s)$ vertices contains either a clique of size k or a stable set of size s.*

The conclusion of the above theorem is obviously satisfied by any $n \geq r(k,s)$. We occasionally say that such an n satisfies the Ramsey principle for parameters k and s.

In this paper we are mainly concerned with Paris-Harrington principles. The general Paris-Harrington Theorem (for arbitrary colorings of hypergraphs) was introduced in [8] as the first example of a mathematically natural witness of the incompleteness phenomenon for formal theories of arithmetic. The general version is known to be unprovable in first-order Peano arithmetic [8], and this is already the case if one considers bi-colorings of hypergraphs only [16]. We focus instead on the restriction of the theorem to bi-colorings of graphs, which is known to be well in the realm of standard combinatorics (see *infra*). We now state the principle.

A set is called *relatively large* (or just *large*, for brevity) if its cardinality is not smaller than its minimum element. The principle claims that if n is big enough then any graph with vertices labeled by the integers $[k,n]$ either contains a clique of size m or contains a stable set such that the labels of the vertices are a large set. A large set is called *exactly large* if the minimum of the set is equal to the cardinality of the set.

Theorem (Paris-Harrington Theorem for graphs)**.** *There exists a number $R(k;m)$ which is the smallest number such that any graph on the integers $[k,R(k;m)]$ contains either a clique of size m or a relatively large stable set.*

Obviously, the conclusion in the above principle is true for every number $n \geq R(k;m)$. We occasionally say that such an n satisfies the Paris-Harrington principle for parameters k and m. Obviously $R(a;b) \geq r(a,b)$ always holds.

We now encode the Ramsey and the Paris-Harrington principles in propositional logic. For any unordered pair of vertices we denote by $E_{i,j}$ a propositional variable whose intended meaning is that vertices i and j are connected. We use two types of clauses, where $X \subseteq [n]$.

$$\mathsf{Cli}(X) = \bigvee_{\{i,j\} \in \binom{X}{2}} \neg E_{i,j} \tag{1}$$

$$\mathsf{Ind}(X) = \bigvee_{\{i,j\} \in \binom{X}{2}} E_{i,j} \tag{2}$$

Clauses (1) express that X is not a clique, and clauses (2) express that X is not an independent set. The CNF encoding the fact that n does not satisfy the Ramsey principle for k and s consists of the clauses $\mathsf{Cli}(X)$, for any $X \subseteq [n]$ of size k and $\mathsf{Ind}(X)$, for any $X \subseteq [n]$ of size s. We denote this formula by $\textsc{Ram}(n;k,s)$ and we refer to it as the *Ramsey principle* when the parameters are clear from context. When n is larger than $r(k,s)$, $\textsc{Ram}(n;k,s)$ is unsatisfiable because of Ramsey Theorem. The size of $\textsc{Ram}(n;k,s)$ is $O(n^{\max(k,s)})$: the formula has $\binom{n}{k}$ clauses of size $\binom{k}{2}$ and $\binom{n}{s}$ clauses of size $\binom{s}{2}$.

The Paris-Harrington principle for n, k, m, consists of the clauses $\mathsf{Cli}(X)$ for any $X \subseteq [k,n]$ of size m and $\mathsf{Ind}(X)$ for any exactly large set $X \subseteq [k,n]$. We denote this CNF as $\textsc{Ph}(n;k,m)$ and we refer to it as the *Paris-Harrington principle* with parameters n, k, m. Note that we explicitly mention exactly large sets only. This is without loss of generality since any large set contains an exactly large subset. When $n \geq R(k;m)$ such CNF is unsatisfiable and we can study its refutations. As for Ramsey principles, the typical cases of interest are when n is the critical (but unknown) Paris-Harrington number $R(k;m)$, and when n is a known upper bound for the latter. The size of the Paris-Harrington principle is dominated by the number of clauses dealing with large sets. For our purposes the following Fact is sufficient.

Fact 1. *Formula $\textsc{Ph}(n;k,m)$ contains $2^{\Theta(n)}$ clauses, for $n \geq R(k;m)$.*

Proof: Since $\frac{n}{3} \geq \frac{R(k;m)}{3} > k$ (see equation (4)), there is a clause of type (2) corresponding to each subset of size $\lfloor n/3 \rfloor$ having $\lfloor n/3 \rfloor$ as the minimum. ∎

While general Paris-Harrington principles (for arbitrary colorings of hypergraphs) have enormously growing lower bounds [10], the above version for bi-colorings of graphs is only slightly stronger than Ramsey Theorem. Indeed, it is known to have double exponential upper bounds. This has been established by Erdős and Mills [5] and later improved by Mills [18]. There exist constants $\alpha, \beta, N > 0$ such that for all $m \geq 3$ and $k \geq N$

$$k^{2^{\alpha m}} < R(k;m) < k^{2^{\beta m}} \quad . \tag{3}$$

On the other hand, we recall the known bounds on Ramsey numbers [4], [22], [1], [11]. There are constants c_1, c_2, c_3, c_4 such that

$$\frac{c_1 \cdot m^2}{\log m} \leq \; r(3,m) \leq \; \frac{c_2 \cdot m^2}{\log m} \quad \text{and}$$
$$c_3 \left(\frac{m}{\log m} \right)^{\frac{k+1}{2}} \leq \; r(k,m) \leq \; \frac{c_4 \cdot m^{k-1}}{(\log m)^{k-2}} \quad , \tag{4}$$

for fixed $k > 3$. In the paper it is often sufficient to use the following weaker bound [7]. For $k, m \geq 2$

$$r(k,m) \leq \binom{k+m-2}{m-1}. \tag{5}$$

Thus, for $2 \leq m \leq k$, we have that $r(k-1,m) \leq k^{m-1} - k^{m-2}$.

We now briefly discuss what is known about the proof complexity of Ramsey principles. Note that all known results deal with the *diagonal* Ramsey theorem, where one forbids cliques

and stable sets of the same size k. Krishnamurty and Moll [15] proved a $r(k,k)/2$ width lower bound in Resolution and an exponential lower bound for the Davis-Putnam procedure for $\text{RAM}(r(k,k);k,k)$. Recently Krajíček [14] established an exponential size lower bound in Resolution for the same principle. Pudlák proved in [20] that the formula $\text{RAM}(4^k;k,k)$ has a quasi-polynomial size $2^{k^{O(1)}}$ proof in bounded-depth Frege systems (note that the proof is polynomial in the size of the Ramsey principle, which is quasi-polynomial in the number of variables). Krajíček [13] proved a conditional lower bound for the same formula: a lower bound for $\text{RAM}(4^k;k,k)$ in Resolution follows from a lower bound for $\text{PHP}_n^{n^4}$ in $\text{RES}(2)$. A suitable Pigeonhole principle is used to blow-up a given counterexample to a Ramsey-type statement, so as to obtain a counterexample that violates some known upper bound on the corresponding Ramsey numbers. This can be seen as a reversal of Pudlák's [20] approach. The proof of our conditional lower bound in Section IV can be seen as an extension of these ideas to the case of the Paris-Harrington principle.

We give a brief overview of our proofs for the upper bound and for the lower bound. Both rely on a two-steps reduction:

1) from the Paris-Harrington principle to an off-diagonal Ramsey principle,
2) from that off-diagonal Ramsey principle to a suitably weak Pigeonhole principle.

For the upper bound we give a recursive procedure (based on [18]) to reduce the Paris-Harrington principle to a Paris-Harrington principle for triangles. Then we reduce this to the off-diagonal Ramsey principle for triangles. Finally we use Pudlák's [20] method to reduce to a suitably weak Pigeonhole principle. For the lower bound we reduce the Paris-Harrington principle to a very unbalanced off-diagonal Ramsey principle on triangles, as in [5], and we relate the latter to a weak quasi-polynomial Pigeonhole principle.

III. An upper bound in bounded-depth Frege

We prove that the Paris-Harrington principle $\text{PH}(k^{2^{2\beta k}};k,k)$ has quasi-polynomial size proofs in bounded-depth Frege systems, where $\beta = 1.471$ is the constant from equation (3).

The argument has two main ingredients: (1) We simulate a combinatorial upper bound construction by Mills [18]. This construction recursively reduces the upper bound for the Paris-Harrington principle to upper bounds for very unbalanced Ramsey principles; (2) We deal with the base cases of the recursion using small bounded-depth Frege proofs of the Paris-Harrington principle for triangles which exist by the following theorem (proof is deferred to Appendix A).

Theorem 1. *$\text{PH}(k^2;k,3)$ has polynomial-size bounded-depth Frege proofs.*

To prove point (1) we translate Mills' [18] proof-method in a search procedure which takes any graph on integers in the interval $[k,k^{2^{2\beta k}}]$ and looks for either a clique or a relatively large stable set. Such a procedure is guaranteed to succeed, and it is essentially a decision tree, with the notable exception of the base cases. The well-known isomorphism between decision trees and tree-like refutations gives the refutation of $\text{PH}(k^{2^{2\beta k}};k,k)$.[1]

Theorem 2. *$\text{PH}(k^{2^{2\beta k}};k,k)$ has a quasi-polynomial size proofs in bounded-depth Frege.*

Proof: Mills [18, Theorem 4] defines a function B as follows: $B(1)=1$; $B(2t)=(2t-1)B(t)^2$ and $B(2t+1)=2tB(t)B(t+1)$. Mills shows that the following properties hold.

$$B(t) \le 2^{\beta t}, \text{ if } t = 3\cdot 2^r \text{ for some } r; \tag{6}$$

$$k^{B(m)} \ge R(k;m), \text{ for } m \ge 3 \text{ and sufficiently large } k. \tag{7}$$

While we are interested mostly in the case $k=m$, we need to keep the two parameters distinct in the proof of the present theorem. For any s there is an integer r such that $s \le 3\cdot 2^r < 2s$.

From a refutation of $\text{PH}(X;Y,Z)$ one can always obtain a refutation of $\text{PH}(X';Y,Z)$ for any $X' > X$. Similarly, from a refutation of $\text{PH}(X;Y,Z)$ one can always obtain a refutation of $\text{PH}(X;Y,Z')$ for any $Z' < Z$. Given k, choose r such that $k \le 3\cdot 2^r < 2k$. Property (6) implies that $k^{B(k)} \le k^{B(3\cdot 2^r)} \le k^{2^{\beta 3\cdot 2^r}} \le k^{2^{2\beta k}}$. Thus, from a refutation of $\text{PH}(k^{B(3\cdot 2^r)};k,3\cdot 2^r)$ we obtain a refutation of $\text{PH}(k^{2^{\beta 3\cdot 2^r}};k,3\cdot 2^r)$, from the latter we obtain a refutation of $\text{PH}(k^{2^{\beta 3\cdot 2^r}};k,k)$ and finally from the latter we obtain a refutation of $\text{PH}(k^{2^{2\beta k}};k,k)$.

We make the following assumptions without loss of generality: (a) $m = 3\cdot 2^r$ for some $r \ge 0$, and (b) k is so large that the condition of inequality (7) is met with respect to such m. Then the propositional formula $\text{PH}(k^{B(m)};k,m)$ is contradictory. For ease of notation we fix $N(k,m) = k^{B(m)}$. If $r=0$ then $N(k,m) = B(3) = 2$. For $r > 0$, and our choice of m the function $N(k,m)$ has the following property.

$$N(k,m) = N\left(N\Big(k,\frac{m}{2}\Big)^{m-1},\frac{m}{2}\right) \tag{8}$$

This follows from the properties of B and from the special form of m, as we now show in detail. On the one hand we have the following equalities.

$$N(k,m) = k^{B(m)} = k^{B(3\cdot 2^r)} = k^{(3\cdot 2^r-1)B(3\cdot 2^{r-1})^2}.$$

On the other hand we have the following equality.

$$N\left(N\Big(k,\frac{m}{2}\Big)^{m-1},\frac{m}{2}\right) = k^{B(3\cdot 2^{r-1})(3\cdot 2^r-1)B(3\cdot 2^{r-1})}.$$

Proof strategy. Fix $N = N(k,m)$. We describe a search procedure that defines a decision tree for the following problem: given a graph on integers $[k,N]$, find a clause in $\text{PH}(N;k,m)$ which is falsified. Since $N \ge R(k;m)$ (by equation (7)) this decision problem has always an answer. The leaves of the decision tree will be either initial clauses of the Paris-Harrington principle or points at which a small proof of a suitable Paris-Harrington principle for triangles can be

[1] A comment is in order here. The best known upper bound on $R(k;k)$ is $k^{2^{\beta k}}$ while we deal with the weaker $k^{2^{2\beta k}}$. The reason for this is technical and has to do with the details of Mills' original proof. We believe that the result can be strengthen to $\text{PH}(k^{2^{\beta k}};k,k)$ with a slightly more involved construction, thus matching the best known upper bound on Paris-Harrington numbers.

plugged-in. These exist by Theorem 1. The decision tree can thus be easily formalized as a bounded-depth Frege proof.

We recall that $E_{i,j}$ indicates if $\{i,j\}$ is an edge in the graph.

The first step of the procedure is to read all edges between integers from k to $R(k,m/2)$. This costs at most $R(k,m/2)^2$ queries. If a relatively large stable set is found, then the procedure outputs such a set and quits. Otherwise the graph explored so far contains a clique of $m/2$ vertices. Let these vertices be $P=\{v_1,\ldots,v_{m/2}\}$.

The second step is to read all edges with one vertex in P and the other outside P. This requires less than $\frac{m}{2}N$ queries.

For any outcome of the queries, we identify the following sets. $A_0=\{i\big|E_{i,v_1}=0\}$, and for $t\in[1,\frac{m}{2}-1]$, $A_t=\{i\big|E_{i,v_1}\wedge E_{i,v_2}\wedge\ \ldots\ \wedge E_{i,v_t}=1$ and $E_{i,v_{t+1}}=0\}$, and $A_{\frac{m}{2}}=\{i\big|E_{i,v_1}\wedge E_{i,v_2}\wedge\ \ldots\ \wedge E_{i,v_{\frac{m}{2}}}=1\}$.

The third step Each branch of the tree satisfies one of the following two cases:

(Case 1) There exists $0\leq\ i<\frac{m}{2}$ with $|A_i|\geq r(m-i,v_{i+1}-1)$.

(Case 2) For all $0\leq\ i<\frac{m}{2}$, $|A_i|<r(m-i,v_{i+1}-1)$.

If (Case 1) applies for some A_i, then we apply a brute force search procedure on the first $r(m-i,v_{i+1}-1)$ elements of such A_i to find either a clique C of size $m-i$ or a stable set S of size $v_{i+1}-1$. We know that all elements of A_i are connected with $v_1,\ldots,v_i$ and disconnected from v_{i+1}. Thus either we output the m-clique $\{v_1,\ldots,v_i\}\cup C$ or the stable set $\{v_{i+1}\}\cup S$ of size v_{i+1} and minimum less than or equal to v_{i+1}. The brute force search procedure requires at most $r(m-i,v_{i+1}-1)^2$ queries. Note that $v_{i+1}\leq R(k;m/2)$ and hence $r(m-i,v_{i+1}-1)\leq r(m,R(k;m/2)-1)$. Thus the cost of the procedure (i.e., the maximal depth of a branch) in this case is at most $R(k;m/2)^{2m}$, using equation (5).

In (Case 2) we focus on $A_{m/2}$. The size of $A_{m/2}$ is at least of $N\left(N(k,m/2)^{m-1},\frac{m}{2}\right)-N(k,m/2)^{m-1}+1$ because of the following Lemma.

Lemma (Mills [18]). *Let* $w=N\left(k,\frac{m}{2}\right)$. *If, for all* $0\leq\ i<\frac{m}{2}$, $|A_i|<r(m-i,v_{i+1}-1)$, *then* $|A_{m/2}|>N(w^{m-1},m/2)-w^{m-1}$.

Thus the graph induced by the elements of $A_{m/2}$ (preserving their order) on the interval $[N(k,m/2)^{m-1},N]$ either contains an $m/2$-clique or a relatively large stable set.

We then apply the search procedure recursively on this graph to find either a clique C of size $m/2$ or a relatively large stable set S. We can do this because either (i) $m/2=3$, or else (ii) $m/2$ and $N(k,m/2)^{m-1}=\left(k^{B(m/2)}\right)^{m-1}$ are such that the conditions for the validity of inequalities (6) and (7) are met, i.e., $B(m/2)\leq 2^{\beta m/2}$ and $k^{B(m/2)}\geq R(k;m/2)$. In case (i) we apply Theorem 1. Note that the relevant interval in this case is $[N(k,3)^5,N(N(k,3)^5,3)]$, which is $[(k^{B(3)})^5,((k^{B(3)})^5)^{B(3)}]$, i.e., $[k^{10},k^{20}]$, since $B(3)=2$. Now consider case (ii). If C is found then it maps to a clique of size $m/2$ in $A_{m/2}$ which is in turn completely connected with vertices in P. Thus we output $C\cup P$. If S is found, notice that mapping back S to $A_{m/2}$ preserves the size and never increases the indexes of vertices. This implies that S is a relatively large stable set in the original graph and a legitimate output. This concludes the description of the search procedure.

Depth of the procedure. We give an upper bound on the size of our the proof of Paris-Harrington principle.

Let $Q([a,b],c)$ denote the size of the proof that $[a,b]$ satisfies the Paris-Harrington principle for cliques of size c and large stable sets, i.e., of $\textsc{Ph}(b;a,c)$.

In the first and second steps the procedure does an exhaustive search on the value of the queried variables. Thus the number of branches required is at most $2^{R(k;m/2)^2+\frac{m}{2}N(k,m)}$.

An analogous search procedure takes place in the third step if (Case 1) occurs, requiring at most $2^{R(k;m/2)^{2m}}$ branches. If (Case 2) occurs then the procedure is applied recursively to the restriction of the input graph to the interval $[N(k,m/2)^{m-1},N]$ and the search looks for $m/2$-cliques or large stable sets. The recursion stops either when (Case 1) occurs or when the target clique size becomes 3.

We now have to evaluate the cost of this recursion. We have

$$Q([k,N],m)\leq R(k,m/2)^2+\frac{m\cdot N}{2}+M(k,m,N),$$

where $M(k,m,N)$ abbreviates

$$\max\{R(k,m/2)^{2m},Q([N(k,m/2)^{m-1},N],m/2)\}.$$

Note that $N=N(N(k,m/2)^{m-1},m/2)$. This is so because $N=N(k,m)$ and $N(k,m)$ satisfies equation (8). Therefore the term $Q([N(k,m/2)^{m-1},N],m/2)$ is of the correct form for the recursion to go through.

To simplify the estimate of the cost of the recursion we make the following observations. For $m=3\cdot 2^\ell$ for some ℓ, the base case of the recursion is $Q([a,b],3)$ for some a,b. The recursion determines the following values.

$$k_0=k,k_1=N(k,m/2)^{m-1},\ldots$$
$$\ldots,k_{i+1}=N(k_i,m/2^{i+1})^{m/2^i-1},\ldots,k_\ell$$

where $\ell=\log m-\log 3$ so that $m/2^\ell=3$. We observe that $k_\ell=\sqrt{N}$. This can be seen as follows: by repeated application of equation (8) we have that for every i, $N(k_i,m/2^i)=N$. In particular $N(k_\ell,3)=N$. By definition of $N(k_\ell,3)$ we get that $k_\ell^{B(3)}=N$. Thus $k_\ell=\sqrt{N}$, since $B(3)=2$.

We now show that the recursive call arising from (Case 2) always dominates the cost of the procedure in (Case 1). First note that $Q([k_{i+1},N],m/2^{i+1})$ costs at least as the cost of the execution of Step 1 and Step 2, for each step $i\in[0,\ell-1]$ of the recursion. Therefore

$$Q([k_{i+1},N],\frac{m}{2^{i+1}})\geq 2^{\frac{m}{2^{i+2}}\cdot(N-k_i)}\geq 2^{3(N-\sqrt{N})}\geq 2^{\frac{3}{2}N}.$$

We now evaluate the cost of (Case 1). Let us assume that we are at step i of the recursion. Let t be such that $0\leq t<m/2^{i+1}$ and $|A_t|\geq r(m/2^i-t,v_{t+1}-1)$. The cost of (Case 1) is then at most $2^{r(m/2^i-t,v_{t+1}-1)^2}$, since a search is performed only the first $r(m/2^i-t,v_{t+1}-1)$ elements of A_t. It is now sufficient to show that $r(m/2^i-t,v_{t+1}-1)\leq\sqrt{N}$. By construction $v_{t+1}\in[k_i,N(k_i,m/2^{i+1})]$ hence $v_{t+1}\leq N(k_i,m/2^{i+1})$ and therefore $r(m/2^i-t,v_{t+1}-1)$ is not

larger than $r(m/2^i - t, N(k_i, m/2^{i+1}))$ and we have

$$\begin{aligned} r(m/2^i - t, N(k_i, m/2^{i+1})) \leq \\ \leq\ N(k_i, m/2^{i+1})^{m/2^i - t - 1} \leq \\ \leq\ N(k_i, m/2^{i+1})^{m/2^i - 1} = k_{i+1}. \end{aligned}$$

The first inequality is by equation (5), the last equality is by definition of k_{i+1}. Finally we observe $k_{i+1} \leq \sqrt{N}$ since at worst $k_{i+1} \leq k_\ell$ and we have already proved that $k_\ell = \sqrt{N}$. Thus we have, for every $0 \leq i < \ell$,

$$\begin{aligned} Q([k_i, N], m/2^i) \leq \\ 2^{R(k_i; m/2^{i+1})^2 + \left(\frac{m}{2^{i+1}}\right)\cdot(N - k_i)} \cdot Q([k_{i+1}, N], m/2^{i+1}). \end{aligned}$$

We now observe that the for all steps of the recursion except the last, the term $R(k_i; m/2^{i+1})^2$ is asymptotically polynomially smaller than N. This can be seen as follows.

$$R(k_i; m/2^{i+1})^2 \leq \left(k_i^{B\left(\frac{m}{2^{i+1}}\right)}\right)^2 \leq \left(\sqrt[m/2^i - 1]{k_{i+1}}\right)^2$$

since $k_{i+1} = \left(k_i^{B\left(\frac{m}{2^{i+1}}\right)}\right)^{\frac{m}{2^i} - 1}$. The term $\left(\sqrt[m/2^i - 1]{k_{i+1}}\right)^2$ is polynomially smaller than N since $k_\ell = \sqrt{N}$. At the last step of the recursion the term $R(k_i; m/2^{i+1})^2$ *could* be of the order of N.

Therefore, since the recursion bottoms out after logarithmically many steps, we obtain the following bound on the size of the whole procedure.

$$\begin{aligned} Q([k, N], m) \leq \\ Q([\sqrt{N}, N], 3) \cdot 2^{\frac{m}{2}N + \frac{m}{4}N + \ldots + \frac{m}{2^\ell}N + O(N)} \leq \\ \leq\ 2^{cmN\left(\sum_{i=0}^{\ell} 1/2^i\right)} = q2^{O(mN)}. \end{aligned}$$

Note that for $m = k$ we have $m \approx \log\log N$. Note that the complexity of the base case accounts for the need of reasoning in bounded-depth Frege. ∎

Assessing the quality of the refutation in Theorem 2 is somehow more difficult than usual. For $N = k^{2^{\beta k}}$ the size of the worst tree-like refutation is 2^{N^2} which is far greater than our upper bound. Furthermore, such large refutations are only quasi-polynomial in the size of the formula itself, which is $2^{\Theta(N)}$. While the size of the formula and the number of variables are usually polynomially related, it is not the case here, since the number of variables in $\text{PH}(N; k, k)$ is $O(N^2)$. Thus, while our refutation is not much longer than the formula, there might be refutations that are smaller than the formula itself (as in very weak Pigeonhole principle formulations [21]). With respect to the problem of formula size vs. variable number, Ramsey-like statements defined in the recent work of Friedman [6] might be of some help. A natural open question is whether the quasi-polynomial upper bound in Theorem 2 can be improved to polynomial with respect to formula size.

IV. A conditional lower bound in Resolution

We prove a conditional lower bound on the Paris-Harrington principle $\text{PH}(k^{2^{\beta k}}; k, k)$ in Resolution. The lower bound is conditional on a lower bound for a quasi-polynomial Pigeonhole principle in $\text{RES}(2)$. The technique can be seen as generalizing Krajíček's [13], [14] approach to the Ramsey principle. We use a weak Pigeonhole principle to blow-up a counterexample to the Paris-Harrington principle so as to obtain a contradiction. More precisely we show how to start from a small graph on $[k, L]$ without k-cliques and large stable sets and to blow it up — using a suitable Pigeonhole principle — to a large graph on $[k, N]$ without k-cliques and large stable sets. This is contradictory as soon as N goes above the known upper bounds for $R(k; k)$.

The proof has two ingredients: (1) We show how to adapt a combinatorial lower bound construction for $R(k; k)$ by Erdős and Mills [5] to reduce the proof complexity of the Paris-Harrington principle to that of a very unbalanced off-diagonal Ramsey principle for triangles; (2) We use a suitable Pigeonhole principle to obtain conditional lower bounds on the off-diagonal Ramsey principle from part (1) of the proof.

Consider the bounds for $R(k; k)$ proved by Mills in [18] (see equation (3)). Any proof system that can prove an upper bound for $R(k; k)$ must be able to distinguish the upper bound from the lower bound in equation (3). Then it must be able to prove some kind of Pigeonhole principle.

We substantially extend the technique by Krajíček [13] to reduce a refutation of $\text{PHP}_n^{2^{(\log n)^c}}$, for some c, n depending on the parameters k, β, to a refutation of $\text{PH}(k^{2^{\beta k}}; k, k)$.

Note that Krajíček [13] uses $\text{PHP}_n^{n^4}$ to postulate a bijective mapping between a counterexample to Ramsey Theorem for small graphs and a big graph for which the theorem is true. This gives a contradiction. This technique does not apply immediately to the Paris-Harrington principle. The Pigeonhole mapping does not preserve the relative order of indexes, which is needed for Paris-Harrington. On the other hand a natural formulation of an order-preserving Pigeonhole principle is easy to refute. We get around this obstacle by going first from Paris-Harrington to Ramsey and only then to the Pigeonhole principle. The first step exploits a construction from Erdős-Mills [5].

We consider $\text{RES}(2)$ as a refutational system, thus we include as axioms also the clauses of the CNF we want to refute.

Theorem 3. *Let $N \geq k^{2^{\beta k}}$. There exists $M = M(k)$ such that*

i. $2^{2^{k/2-1}} < M < \sqrt{N}$, *and*

ii. if $\text{PH}(N; k, k)$ *has a Resolution refutation of size S then* $\text{RAM}(N - M + 1; 3, M)$ *has a Resolution refutation of size S.*

Proof: We assume even $k \geq 6$. Consider any refutation for $\text{PH}(N; k, k)$ of size S, and consider the interval $[k, N]$. We divide the interval in the following way: fix $n_0 = k$, $n_1 = k + r(3, k) - 1$, $n_{i+1} = n_i + r(3, n_i) - 1$, up to $M = M(k) = n_{k/2-2}$. The interval $[k, N]$ is divided as $[n_0, n_1 - 1]$, $[n_1, n_2 - 1]$, up to $[n_{k/2-2}, n_{k/2-3} - 1]$, plus another residual interval $[n_{k/2-2}, N]$. For $0 \leq\ i \leq k/2 - 3$ we call I_i the interval $[n_i, n_{i+1} - 1]$. The last interval is $[n_{k/2-2}, N] = [M, N]$. For those familiar with [5], note that

we are essentially carrying over Erdős-Mills' construction up to the penultimate step inside a suitably large interval given in advance.

Point (i) in the statement of the theorem can be proved by elementary calculations (see Appendix B for details).

We now prove point (ii) in the statement of the theorem. We define a restriction ρ on the variables of $\text{PH}(N;k,k)$. First of all we fix $E_{a,b}$ to 1 for every indices a and b in different intervals. For all $i \leq k/2-3$, $|I_i| = r(3,n_i)-1$. Therefore there exists a graph G_i of size $|I_i|$ with no stable set of size n_i and no triangle. G_i immediately defines an assignment ρ_i to all variable $E_{a,b}$ with $a,b \in I_i$. We restrict the variables in I_i according to ρ_i.

We observe that the only variables left unassigned are those of the form $E_{a,b}$ with $a,b \in [M,N]$. We now argue that a refutation of $\text{PH}(N;k,k)|_\rho$ induces a refutation of $\text{RAM}(N-M+1;3,M)$. In particular for any clause C in the refutation of $\text{PH}(N;k,k)$, we can deduce the clause $C|_\rho$ (or a subset of it) from $\text{RAM}(N-M+1;3,M)$. We prove it for initial clauses, the rest follows by induction on the Resolution inference process.

If C is an initial clause in $\text{PH}(N;k,k)$ then is either of type (1) or of type (2).

First suppose C is of type (1). If three or more elements mentioned in C are in the same I_i for some i, then the restriction ρ satisfies C because no triangles are in the assignment ρ_i associated to I_i. Therefore the clause is deducible, since it is true. Suppose now that C refers to at most two elements in any interval I_i. Then it must refer to at least 3 elements of interval $[M,N]$, since there are $k/2-2$ intervals I_i. The corresponding edges are not assigned by the restriction ρ. Thus, in this case, $C|_\rho$ is a superset of a clause of $\text{RAM}(N-M+1;3,M)$ of type (1).

Now suppose that C is of type (2). If C refers only to elements from different intervals then it is killed by the restriction ρ which set to 1 all edges across different intervals. Any clause of type (2) which refers to indexes in an interval I_i concerns a stable of size at least n_i, and is killed by the restriction ρ_i which set to 1 at least one edge in any set of n_i vertices in I_i. The only other clauses of type (2) of the Paris-Harrington principle that survive are the ones referring to vertices in the interval $[M,N]$. Such clauses refer to sets of vertices of size at least M, thus are subsumed by the clauses of type (2) of $\text{RAM}(N-M+1;3,M)$. We conclude that any refutation of size S for $\text{PH}(N;k,k)$ gives a refutation of the same size for $\text{RAM}(N-M+1;3,n(k))$. ∎

Theorem 4. *Let $T < r(k,s)$. If $\text{RAM}(U;k,s)$ has a Resolution refutation of size S then PHP_T^U has a $\text{RES}(2)$ refutation of size less than $S \cdot 2^{O(ks\cdot\max(\log s,\log k))}$.*

Proof: To refute $\text{RAM}(U;k,s)$ it is necessary to distinguish between numbers U and T with $U \geq r(k,s) > T$. The proof strategy is to encode a Resolution refutation of $\text{RAM}(U;k,s)$ as a Pigeonhole principle refutation in $\text{RES}(2)$. If there was an homomorphism between a graph of T vertices with neither a k-size clique nor a s-stable set and a graph of U vertices, then $\text{RAM}(U;k,s)$ would not be refutable. Thus any refutation of $\text{RAM}(U;k,s)$ could be used to refute the Pigeonhole principle.

Fix $G=(V,E)$ to be a graph with no k-clique and no s-stable, with $|V|=T$ vertices. We identify two sets Δ, Γ of edges and non-edges as follows.

$$\Delta = \{(a,b)\big|\{a,b\} \in E\},\ \Gamma = \{(a,b)\big|\{a,b\} \notin E \text{ and } a \neq b\}$$

Consider any pair $i,j \in \binom{[U]}{2}$. We give two different encoding for any literal. The disjunctive encoding is defined as follows.

$$E_{i,j} \mapsto \bigvee_{(a,b)\in\Delta} p_{i,a} \wedge p_{j,b}, \quad \neg E_{i,j} \mapsto \bigvee_{(a,b)\in\Gamma} p_{i,a} \wedge p_{j,b}$$

The conjunctive encoding is defined as follows.

$$E_{i,j} \mapsto \bigwedge_{(a,b)\in\Gamma} (\neg p_{i,a} \vee \neg p_{j,b}),\ \neg E_{i,j} \mapsto \bigwedge_{(a,b)\in\Delta} (\neg p_{i,a} \vee \neg p_{j,b})$$

In the above, the variables $p_{i,a}$ for $i \in U$ and $a \in T$ are the variables of PHP_T^U.

The disjunctive encoding allows to encode each clause in the refutation of $\text{RAM}(U;k,s)$ as a 2-DNF on the variables of PHP_T^U. To prove the theorem it is sufficient to show that in $\text{RES}(2)$ the following hold.

1) the disjunctive encoding of the empty clause is the empty clause.
2) the disjunctive encoding of $A \vee B$ is deducible from the disjunctive encoding of $A \vee E_{i,j}$ and $B \vee \neg E_{i,j}$ for any A, B clauses on the variables of $\text{RAM}(U;k,s)$.
3) the disjunctive encoding of the initial clauses of $\text{RAM}(U;k,s)$ is deducible from PHP_T^U.

Point (1) is trivial. To show point (2) we will use the conjunctive encoding. The conjunctive encoding is necessary to simulate the Resolution cut, but it requires $\Theta(T^2)$ clauses to represent a literal. To represent a clause of width w it would require up to T^{2w} clauses, which is too inefficient. Instead we use the disjunctive encoding for representing clauses, and we extract a mixed encoding to do the cut: all literals but one are in disjunctive form, while one of the literals involved in the cut is represented in conjunctive form. The details of the proof can be found in Appendix C. Proving point (3) requires more work, since deducing the encoding of an axiom of $\text{RAM}(U;k,s)$ is equivalent to showing that G has no k-clique and no s-stable set. We now show how this is done.

Axiom deduction. We show how to deduce the disjunctive encoding of an axiom of $\text{RAM}(U;k,s)$ from the PHP_T^U axioms. We focus on the axioms that claim that no stable of size s exists in the graph. The case of cliques is dual. Without loss of generality we assume that the axiom we want to deduce is exactly the following.

$$\bigvee_{i\neq j\in[s]} \bigvee_{(a,b)\in\Delta} p_{i,a} \wedge\ p_{j,b}. \tag{9}$$

The deduction of such an axiom is equivalent to proving that there is no stable set of size s in the model graph G (indeed formula (9) claims that any set of s vertices contains a pair with an edge of G between them). The deduction of the latter fact can be done in $T^{O(s)}$ steps, according to the following lemma whose straightforward proof we omit.

Lemma 1. *Let G be a graph with T vertices and no stable set of size s. Consider propositional variables $p_{i,v}$ for $i \in [s]$ and $v \in V(G)$. The following formula has Resolution refutation of size $T^{O(s)}$.*

$$\bigvee_v p_{i,v} \qquad i \in [s] \quad (10)$$

$$\neg p_{i,v} \vee \neg p_{j,v} \qquad i \neq j \in [s] \text{ and } v \in V(G) \quad (11)$$

$$\neg p_{i,v} \vee \neg p_{j,v'} \qquad i \neq j \in [s] \text{ and } \{v, v'\} \in E(G) \quad (12)$$

Lemma 1 immediately implies that formula (9) is deducible in $T^{O(s)}$ steps. The refutation of (9) is obtained by simulating the refutation given by Lemma 1 using the initial clauses of PHP_T^U. Clauses (14) and (15) are also initial clauses of PHP_T^U; clauses (16) are substituted by the corresponding 2-DNF tautologies $\neg p_{i,v} \vee \neg p_{j,v'} \vee (p_{i,v} \wedge p_{j,v'})$ which require 3 steps each to be deduced. The simulation of the refutation in Lemma 1 does not end with the empty clause, because of the weakening of the initial formulas. Instead it ends with the disjunction of all weakenings made at the beginning. Such a disjunction is a sub-formula of the desired axiom (9).

If a Resolution refutation of $\text{RAM}(U; k, s)$ has length S, then the corresponding $\text{RES}(2)$ refutation of PHP_T^U costs T^4 for each inference step, $T^{O(k)}$ for each axiom (1) and $T^{O(s)}$ for each axiom (2). Thus the length of the whole refutation is at most $T^{O(\max(s,k))}S$. By the choice of $T < r(k,s)$ and by equation (5), we have $T \leq (k+s-2)^{\min(k,s)} = 2^{O(\min(k,s)\max(\log k, \log s))}$. Thus the total length is $T^{O(\max(s,k))}S = 2^{O(ks \cdot \max(\log s, \log k))}S$. ∎

In the following discussion we fix $N = k^{2^{\beta k}}$, $M = n_{k/2-2}$ as in the proof of Theorem 4, and $L = r(3, M) - 1$. From Theorem 3 and Theorem 4 we immediately obtain the following corollary.

Corollary 1. *If $\text{PH}(N; k, k)$ has a refutation of size S in Resolution, then PHP_L^{N-M+1} has a refutation of size $2^{O(M \log M)} \cdot S$ in $\text{RES}(2)$.*

Proof: By Theorem 3 if the Paris-Harrington principle $\text{PH}(N; k, k)$ has a Resolution refutation of size S, then $\text{RAM}(N - M + 1; 3, M)$ also has such a refutation. By Theorem 4 if $\text{RAM}(N - M + 1; 3, M)$ has a size S refutation in Resolution then the Pigeonhole principle PHP_L^{N-M+1} has a $\text{RES}(2)$-refutation of size $M^{O(M)} \cdot S$. ∎

A conditional lower bound for the Paris-Harrington principle in Resolution can be gleaned from the above results as follows. First note that PHP_L^{N-M+1} is at best quasi-linear and at worst quasi-polynomial for the parameters N, M, and L in question. From (i) in Theorem 3 we know that

$$2^{2^{k/2-1}} < M < \sqrt{k^{2^{\beta k}}}. \quad (13)$$

For $L = r(3, M) - 1$ we have ([11], see equation (4)) that $L \approx \frac{M^2}{\log M}$.

If M is close to the upper bound in (13), then $L = \Theta\left(\frac{N}{\log N}\right)$, and we are dealing with a quasi-linear Pigeonhole principle. If M is close to the lower bound in (13), then $L = 2^{2^{\Theta(k)}}$ and we are dealing with a quasi-polynomial Pigeonhole principle (recall that $k \approx \log \log N$).

The strength of our result then depends on the lower bound we assume on the relevant Pigeonhole principle PHP_L^{N-M+1} in $\text{RES}(2)$. For the sake of concreteness, let us assume a lower bound of $2^{L^{\frac{1}{2}+\epsilon}}$ for some $\epsilon > 0$. Then $2^{L^{\frac{1}{2}+\epsilon}\left(2^{O(M \log M)}\right)^{-1}}$ is a lower bound for $\text{PH}(N; k, k)$ in Resolution. Since $L = \Omega\left(\frac{M^2}{\log M}\right)$, we have that $L^{1+\epsilon} \geq \frac{M^{1+\epsilon}}{(\log M)^d}$ for some d, and the latter term obviously dominates $M \log M$. Therefore we obtain a bound of $2^{\Omega\left(L^{\frac{1}{2}+\epsilon}\right)}$ for the Paris-Harrington principle in Resolution. We sum up the above observations in the following corollary.

Corollary 2. *If the length of any $\text{RES}(2)$ refutations of PHP_L^{N-M+1} is at least $2^{L^{\frac{1}{2}+\epsilon}}$ for some $\epsilon > 0$, then any Resolution refutations of $\text{PH}(N; k, k)$ has size $2^{\Omega\left(L^{\frac{1}{2}+\epsilon}\right)}$.*

In our conditional lower bound L could be very small when compared to N. Indeed, we could have (if M is close to the lower bound in 13) that for some c, $N = 2^{O((\log L)^c)}$. Thus our conditional $2^{L^{\frac{1}{2}+\epsilon}}$ lower bound in the worst case only excludes proofs of size quasi-polynomial in N but much smaller than the trivial 2^{N^2} upper bound in Resolution. Nevertheless, any progress seems unlikely without a serious improvement of the combinatorial upper and lower bounds.

V. Acknowledgement

We thank an anonymous referee for insightful comments, that significantly improved the presentation of the paper.

References

[1] Miklós Ajtai, János Komlós, and Endre Szemerédi. A note on Ramsey numbers. *Journal of Combinatorial Theory, Series A*, 29(3):354–360, 1980.

[2] Arnold Beckmann and Samuel R. Buss. Separation results for the size of constant-depth propositional proofs. *Annals of Pure and Applied Logic*, 136(1–2):30–55, 2005.

[3] Peter Clote. Cutting planes and Frege proofs. *Information and Computation*, 121(1):103–122, 1995.

[4] Paul Erdős. Graph theory and probability II. *Canadian Journal of Mathematics*, 13:346–352, 1961.

[5] Paul Erdős and George Mills. Some bounds for the Ramsey-Paris-Harrington numbers. *Journal of Combinatorial Theory, Series A*, 30(1):53–70, 1981.

[6] Harvey M. Friedman. Adjacent Ramsey theory, 2010. Unpublished.

[7] Jack E. Graver and James Yackel. Some graph theoretic results associated with Ramsey's Theorem. *Journal of Combinatorial Theory*, 4(2):125–175, 1968.

[8] Leo Harrington and Jeff Paris. A mathematical incompleteness in Peano Arithmetic. In John Barwise, editor, *Handbook of Mathematical Logic*, pages 1133–1142. North-Holland, 1977.

[9] Johan Håstad. Almost optimal lower bounds for small depth circuits. In *Proceedings of the 18th ACM Symposium on Theory of Computing*, pages 6–20, 1986.

[10] Jussi Ketonen and Robert M. Solovay. Rapidly growing Ramsey functions. *Annals of Mathematics*, 113(2):267–314, 1981.

[11] Jeong Han Kim. The Ramsey number $r(3,t)$ has order of magnitude $t^2/\log(t)$. *Random Structures and Algorithms*, 7(3):173–208, 1995.

[12] Jan Krajíček. Lower Bounds to the Size of Constant-Depth Propositional Proofs. *Journal of Symbolic Logic*, 59(1):73–86, 1994.

[13] Jan Krajíček. On the weak pigeonhole principle. *Fundamenta Mathematicae*, 170(1–3):123–140, 2001.

[14] Jan Krajíček. A note on propositional proof complexity of some Ramsey-type statements. *Archive for Mathematical Logic*, 50(1):245–255, 2011.

[15] Balakrishnan Krishnamurthy and Robert N. Moll. Examples of hard tautologies in the propositional calculus. In *Proceedings of the 13th ACM Symposium on Theory of Computing*, pages 28–37, 1981.

[16] Martin Loebl and Jaroslav Nešetřil. An unprovable Ramsey-type theorem. *Proceedings of the American Mathematical Society*, 116(3):819–824, 1992.
[17] Alexis Maciel, Toniann Pitassi, and Alan Woods. A new proof of the weak pigeonhole principle. *Journal of Computer and System Sciences*, 64(4):843–872, 2002.
[18] George Mills. Ramsey-Paris-Harrington numbers for graphs. *Journal of Combinatorial Theory, Series A*, 38(1):30–37, 1985.
[19] Jeff Paris, Alex Wilkie and Alan Woods. Provability of the pigeonhole principle and the existence of infinitely many primes. *Journal of Symbolic Logic*, 53(4):1235–1244, 1988.
[20] Pavel Pudlák. Ramsey's Theorem in Bounded Arithmetic. In *Proceedings of Computer Science Logic 1990*, pages 308–317, 1991.
[21] Alexander A. Razborov. Proof complexity of pigeonhole principles. In *Proceedings of the 5th Developments in Language Theory*, volume 2295 of *Lecture Notes in Computer Science*, pages 100–116. Springer-Verlag, 2002.
[22] Joel Spencer. Asymptotic lower bounds for Ramsey functions. *Discrete Mathematics*, 20:69–76, 1977.

APPENDIX

In this Appendix we prove Theorem 1, used as the base case of the recursive construction in the proof of Theorem 2. In Section A we give an upper bound on the size of proof of an off-diagonal Ramsey Theorem in bounded-depth Frege systems. This is a rather straightforward generalization of Pudlák's [20] proof for the diagonal Ramsey Theorem, but we avoid using the language of Bounded Arithmetic. In Section B we formalize an argument by Mills [18] that gives a reduction from a Paris-Harrington principle for triangles to an off-diagonal Ramsey principle.

A. Off-diagonal Ramsey Theorem in bounded depth

We adapt Pudlák's [20] treatment to the case of severely unbalanced off-diagonal Ramsey principles. We bypass the use of transfer principles from Bounded Arithmetic to propositional systems. In particular we show that $\text{RAM}(s^2-5s+2;3,s-1)$ has polynomial-size proofs in bounded-depth Frege systems. The choice of the parameters is dictated by the aim of eventually obtaining polynomial size proofs for $\text{PH}(s^2;s,3)$. We will show how to obtain such proofs by a reduction to $\text{RAM}(s^2-5s+2;3,s-1)$. Note that by equation (4) there exists a constant c such that $s^2-5+2 \geq c(s^2-2s+1)/(\log(s-1)) \geq r(3,s-1)$ for sufficiently large s. Small proofs for the Ramsey principles are obtained by reduction to a weak Pigeonhole principle of the form $(2n-6\sqrt{n}) \to n$. We start with a simple lemma concerning the latter principle. We do not make any attempt to strenghten the claim (e.g. by reducing to a stronger but still efficiently provable Pigeonhole principle), which is just sufficient for our present purposes.

Lemma 2. *The Pigeonhole principle* $\text{PHP}_n^{2n-6\sqrt{n}}$ *has bounded-depth Frege proofs of size* $n^{O(\sqrt{n})}$.

Proof: Consider the first $6\sqrt{n}$ pigeons. In the first part of the refutation we deduce the sequent $p_{1,h_1}, p_{2,h_2}, \ldots, p_{6\sqrt{n},h_{6\sqrt{n}}} \vdash \bot$ for any sequence $(h_1, h_2, \ldots, h_{6\sqrt{n}})$ of holes.

If a sequence contains a repetition then the corresponding sequent follows immediately from the injectivity axioms of PHP. Fix a sequence with no repetitions, and consider a restricted version of the principle, where the first $6\sqrt{n}$ pigeons are assigned to that sequence of holes.

We call such restricted formula F. It is easy to see that up to renaming variables, F is isomorphic to $PHP_{n-6\sqrt{n}}^{2(n-6\sqrt{n})}$.

By unit propagation of the partial assignment implied by the left part of the sequent, formula $p_{1,h_1}, p_{2,h_2}, \ldots, p_{6\sqrt{n},h_{6\sqrt{n}}} \vdash F$ can be deduced in polynomial time from the initial pigeon axioms. Furthermore F has a polynomial size refutation in bounded depth Frege (see [19], [17]), thus we can deduce the empty clause from the $p_{1,h_1}, p_{1,h_2}, \ldots, p_{6\sqrt{n},h_{6\sqrt{n}}}$ and the axioms of the Pigeonhole principle in polynomial size.

The second part of the refutation goes through by noticing that for any i and any formula A the collection of sequents $\{p_{i,j}, A \vdash \bot\}_{j=1}^{n}$ and the axiom $\vdash \vee_{j=1}^{n} p_{i,j}$ imply $A \vdash \bot$ with n cut operations. Thus for $6\sqrt{n}$ times we group sequents which are equal up to the last hole, and we deduce the sequent corresponding to the common part. By induction we obtain the empty sequence, i.e. the sequent $\emptyset \vdash \bot$.

The number of sequents to produce in the first part is $n^{6\sqrt{n}}$ and each one requires a polynomial number of steps. The second part has size roughly $n^{6\sqrt{n}+O(1)}$, since the deduction process mimics a tree of height $6\sqrt{n}$ and branch n and there is a $O(n)$ cost at each node to actually simulate the branching. ∎

Given $s \geq 3$, let $\Sigma = \Sigma(s)$ be the set of binary sequences containing at most one occurrence of 1 and at most $s-2$ occurrences of 0. The sequences in Σ are called *good sequences*. Note that good sequences have length at most $s-1$. The cardinality of Σ is $S = \frac{(s+2)(s-1)}{2}$. This can be seen as follows. Σ contains a single sequence consisting of all O's, for each of the possible lengths. This gives $s-1$ sequences (including the empty one). For each possible positive length up to $s-1$, Σ contains one sequence per choice of positioning a 1, which gives $\sum_{\ell=1}^{s-1} \ell$ many sequences. We use the cardinality of Σ as an upper bound to the off-diagonal Ramsey number $r(3,s)$ (see equation (4)).

Theorem 5. $\text{RAM}((s+1)(s-2)-4(s-1);3,s-1)$ *has polynomial-size bounded-depth Frege proofs.*

Proof: The proof is by reduction to $\text{PHP}_{(s+1)(s-2)/2}^{(s+1)(s-2)-4(s-1)}$. The latter has small bounded-depth Frege proofs by Lemma 2 and since

$$4(s-1) \leq 6\sqrt{(s+1)(s-2)/2}.$$

We introduce a crucial relation. For any sequence $x_0, \ldots, x_j$ of elements of $[1,(s+1)(s-2)-4(s-1)]$, and for any binary sequence $\alpha_0, \ldots, \alpha_{j-1}$, we denote by $R(x_0, \ldots, x_j; \alpha_0, \ldots, \alpha_{j-1})$ the following formula.

$$\Big(\bigwedge_{u\in[0,j-1]} \bigwedge_{v\in[u+1,j-1]} E_{x_u,x_v} = \alpha_u\Big) \wedge \Big(\bigwedge_{u\in[1,j]} \bigwedge_{x_{u-1}<y<x_u} \bigvee_{w\in[0,u-1]} E_{x_w,y} \neq \alpha_w\Big).$$

The first conjunct expresses a compatibility condition between the sequence of vertices $\vec{x}$ and the sequence of colors $\vec{\alpha}$; the second conjunct expresses a minimality condition.

We further set, for every sequence $\vec{\alpha}$ of length j,

$$p_{x,\vec{\alpha}} := \bigvee_{x_0<\cdots<x_{j-1}} R(x_0, \ldots, x_{j-1}, x; \vec{\alpha}).$$

a) Proof Strategy: We show how to deduce, given x in the domain, the disjunction $\bigvee_{\vec{\alpha}\in\Sigma} p_{x,\vec{\alpha}}$ from the negation of the Ramsey principle.

b) Completeness Axioms Deduction: We first give a sketch of the deduction of the Pigeonhole principle axioms in the form of a Branching Program. In this particular case the Branching Program is readily translatable in a bounded-depth Frege proof.

We branch on the value of $E_{x_0,x}$. This univocally determines the color of (x_0, x), be it α_0. We then branch on $E_{x_0,t} = \alpha_0$, for $t = 1, \ldots, x-1$. If all these queries have negative answer, then the program exits and $R(x_0, x; \alpha_0)$ holds. Else, let x_1 be the first value of t such that $E_{x_0,t} = \alpha_0$. We then branch on $E_{x_1,x}$, which determines color α_1. We then branch on $E_{x_0,t} = \alpha_0 \wedge E_{x_1,t} = \alpha_1$, for $t > x_1$. If no t satisfies the condition, then the program exits and the relation $R(x_0, x_1, x; \alpha_0, \alpha_1)$ is satisfied. Else, we proceed in a similar fashion chosing x_2 as the first value of t that satisfies the condition. We continue this process indefinitely.

The program either exits satisfying the relation $R(x_0, \ldots, x_{j-1}, x; \vec{\alpha})$ for some $x_0, \ldots, x_{j-1}$, and some $\alpha_0, \ldots, \alpha_{j-1}$, or else $\vec{\alpha}$ is not a good sequence. The corresponding branch then falsifies one of the initial clauses, since it implies the existence of either a triangle or a large stable set.

It is easy to see that the cost of the process for every vertex is $O((s^2)^s) = O(s^{2s})$.

We now show how to translate the above Branching Program into a derivation in a bounded-depth Frege system. We introduce a family of auxiliary relations, parametrized by x.

$$C_x(x_0, \ldots, x_\ell; \alpha_0, \ldots, \alpha_{\ell-1}) := \\ R(x_0, \ldots, x_\ell; \alpha_0, \ldots, \alpha_{\ell-1}) \wedge \bigwedge_{i=0}^{\ell-1} E_{x_i,x} = \alpha_i.$$

Observe that $C_x(x_0, \ldots, x_{\ell-1}, x; \alpha_0, \ldots, \alpha_{\ell-1})$ is $R(x_0, \ldots, x_{\ell-1}, x; \alpha_0, \ldots, \alpha_{\ell-1})$. We split the rest of the argument in two parts. First we show that, for all ℓ, $C_x(x_0, \ldots, x_\ell; \alpha_0, \ldots, \alpha_{\ell-1})$ implies

$$\bigvee_{x_\ell < z \leq x} C_x(x_0, \ldots, x_\ell, z; \alpha_0, \ldots, \alpha_\ell, 0) \vee \\ \vee \bigvee_{x_\ell < z \leq x} C_x(x_0, \ldots, x_\ell, z; \alpha_0, \ldots, \alpha_\ell, 1).$$

Second we show that all the formulas $C_x(x_0, \ldots, x_\ell, \vec{\alpha})$ generated by the just described inference process can be cut except those with $\vec{\alpha} \in \Sigma$ and that for all such formulas $x_\ell = x$.

For the rest of this proof we abbreviate by R (respectively A) the first (respectively the second) conjunct of $C_x(x_0, \ldots, x_\ell; \alpha_0, \ldots, \alpha_{\ell-1})$. First observe that

$$(R \wedge A \wedge E_{x_\ell,x} = 0) \vee (R \wedge A \wedge E_{x_\ell,x} = 1)$$

is obviously deducible. We now reason by cases. We treat the case $R \wedge A \wedge E_{x_\ell,x} = 0$ (the other case is symmetric).

First observe that the following formula is deducible from $A \wedge E_{x_\ell,x} = 0$.

$$\bigvee_{x_\ell < z \leq x} \left(\overbrace{\bigwedge_{i=0}^{\ell-1} E_{x_i,z} = \alpha_i \wedge \; E_{x_\ell,z} = 0}^{F(z)} \\ \vee \\ \underbrace{\bigwedge_{x_\ell < y < z} \left(\bigvee_{i=0}^{\ell-1} E_{x_i,y} \neq \; \alpha_i \vee \; E_{x_\ell,y} \neq \; 0 \right)}_{G(z)} \right)$$

For $z = x$, $F(z)$ is exactly $A \wedge E_{x_\ell,x} = 0$. We then reason by cases to either obtain $G(x)$ or to obtain $F(z) \wedge G(z)$ for some $x_\ell < z < x$. The reasoning by cases is on the minimality of the currently inspected z, i.e., on the axiom $G(z) \vee \neg G(z)$. Thus, we have that $R \wedge A \wedge E_{x_\ell,x} = 0$ implies

$$R \wedge \bigvee_{x_\ell < z \leq x} \big(\bigwedge_{i=0}^{\ell-1} E_{x_i,z} = \alpha_i \wedge \; E_{x_\ell,z} = 0 \big) \wedge \\ \bigwedge_{x_\ell < y < z} \big(\bigvee_{i=0}^{\ell-1} E_{x_i,y} \neq \; \alpha_i \vee \; E_{x_\ell,y} \neq \; 0 \big),$$

which is just $\bigvee_{x_\ell < z \leq x} C_x(x_0, \ldots, x_\ell, z; \alpha_0, \ldots, \alpha_\ell, 0)$ as needed.

If the sequence $\vec{\alpha}$ is not a good sequence, then the conjunct $R(\vec{x}, \vec{\alpha})$ in $C_x(\vec{x}, \vec{\alpha})$ induces a monochromatic triangle or a stable set of size $s-1$, thus violating one of the axioms of the Ramsey principle. The case that α is a good sequence but $x_\ell \neq x$ is impossible since the sequence would have been extended using the above described inference process.

c) Injectivity Axioms Deduction: For the simulation of the inferences it is sufficient to show that $p_{x,\vec{\alpha}} \to \overline{p_{y,\vec{\alpha}}}$, i.e., that $p_{x,\vec{\alpha}} \wedge p_{y,\vec{\alpha}} \to$, for every $x \neq y$ and every $\vec{\alpha}$.

Each of $p_{x,\vec{\alpha}}$ (resp. $p_{y,\vec{\alpha}}$) is a disjunction asserting the existence of a sequence of vertices of length $j-1$ that can be extended by x (resp. y) so that the relation R is satisfied with respect to $\vec{\alpha}$. For each such pair of sequences, σ and σ', the extensions $\sigma \cdot x$ and $\sigma' \cdot y$ are distinct (since $x \neq y$). Consider the first coordinate in which they differ, and let v, v' be the corresponding vertices. Suppose without loss of generality that $v < v'$. Then $R(\sigma \cdot x, \vec{\alpha})$ contains a clause asserting the compatibility of v while $R(\sigma \cdot y, \vec{\alpha})$ contains a clause asserting the non-compatibility of $v < v'$. These two clauses can be singled out using structural rules and then eliminated by a Cut.

The cost of the simulation is $O(s^{2s} \times s^{2s}) = O(s^{4s})$ steps.

The cost of the whole reduction is thus $O(s^{4s})$ times the size of a refutation of the formula $\text{PHP}^{(s+1)(s-2)-4(s-1)}_{(s+1)(s-2)/2}$. By Lemma 2 the latter quantity is bounded by $O(s^{12s})$. The size of the whole proof is thus bounded by $s^{O(s)}$, which is polynomial in the size of the Ramsey formula (hence quasi-polynomial in the number of variables). ■

B. Small Paris-Harrington numbers

Paris-Harrington numbers for the case of forbidding a triangle and a large stable set have the same asymptotic as

the corresponding off-diagonal Ramsey numbers. In particular, Mills [18] gives a direct proof of the following fact. For all $k \geq 3$,

$$R(k;3) \leq r(3,k-1) + 5k - 7.$$

Thus, $k^2 \geq R(3;k)$ for sufficiently large k, by equation (4). We analyze this proof to show that the complexity of proving a quadratic Paris-Harrington principle for forbidding triangles can be reduced to the complexity of the quadratic off-diagonal Ramsey principle from the previous subsection.

Theorem 1. $\text{PH}(k^2;k,3)$ *has polynomial-size bounded-depth Frege proofs.*

Proof: In the previous subsection we showed how to prove efficiently $\text{RAM}((k+1)(k-2)-4(k-1);3,k-1)$ in bounded-depth Frege. We will show how to mimic efficiently Mills' proof [18] by replacing the critical Ramsey number $r(3,k-1)$ by the upper bound $(k+1)(k-2)-4(k-1)$ used in our proof of Theorem 5. Thus we show how to efficiently reduce a proof of $\text{PH}((k+1)(k-2)-4(k-1)+5k-7;k,3)$, i.e., of $\text{PH}(k^2-5;k,3)$, to a proof of $\text{RAM}((k+1)(k-2)-4(k-1);3,k-1)$. *A fortiori* this gives a small proof of $\text{PH}(k^2;k,3)$. The reduction procedure can be achieved in tree-like Resolution with the exception of the use of small bounded-depth Frege proofs of Ramsey principles for triangles.

Let $n = k^2$ and suppose by way of contradiction that $G = (V,E)$ is given such that $V = [k,n]$ and G contains no triangles and no large stable set.

Let A denote the set of vertices connected to k in G and B denote the set of vertices disconnected from k in G. We branch exhaustively to determine A and B completely. This results in at most 2^{n-k} branches.

We then verify that A is a stable set. This produces at most $|A|^2$ branches. In case A is not stable, then a triangle is found and we are done. On the remaining branches the set A is stable. If $|A| \geq \min(A)$ then we have found a large stable set and we are done.

If $|B| \geq (k+1)(k-2)-4(k-1)$ then we know how to prove $\text{RAM}(|B|;3,k-1)$ in size $2^{O(k\log k)}$ (Theorem 5). Then either we find a triangle in B, in which case we are done immediately, or else we find a stable set $X \subseteq B$ of size $k-1$. In the latter case $\{k\} \cup X$ is a large stable set in G and we are done.

In the rest of the proof all the branches that are left open correspond to cases where $|A| < \min(A)$ and $|B| < (k+1)(k-2)-4(k-1)$. We prove that such cases are impossible. We distinguish two further cases.

(Case 1) $\min(A) < 2k$. Then $|A| \leq 2k-2$. Thus, since $n = |A|+|B|+k$, we have the following contradiction to the choice of n.

$$\begin{aligned} n &\leq k + 2k - 2 + (k+1)(k-2) - 4(k-1) \\ &= k + 2k - 2 + k^2 - k - 4k + 2 = k^2 - k < k^2. \end{aligned}$$

(Case 2) $\min(A) \geq 2k$. Then we have $I = [k+1, 2k-1] \subseteq B$. We explore all the pairs in I. This requires at most k^2 branches. If no positive edge is found, then G contains a large stable set and we are done. Otherwise, let $p < q$ be connected vertices in B.

We look for triangles involving vertices p, q in G. This search requires n branches.

With $2^{2|A|} \leq 2^{2n}$ steps we determine the set of all vertices in A independent from p and the set of all vertices in A independent from q. If more than $p-2$ vertices in A are independent from p, then we have found a large stable set. Analogously for q an $q-2$. We now assume that A contains at most $p-2$ vertices independent from p and $q-2$ vertices independent from q. But then we have that

$$|A| \geq |A \cap \{\text{neighbors of } p\}| + |A \cap \{\text{neighbors of } q\}|,$$

and thus

$$|A| \geq |A| - p + 2 + |A| - q + 2 = 2|A| - (p+q-4).$$

Hence, since $p, q \leq 2k-1$,

$$|A| \leq p + q - 4 \leq 2k - 1 + 2k - 2 - 4 \leq 4k - 7.$$

Finally then (recall $|B| \leq (k+1)(k-2)-4(k-1)-1$)

$$n = k + |A| + |B| \leq 4k - 7 + k + k^2 - k - 4k + 1 = k^2 - 6.$$

This is a contradiction to our choice of n.

In the worst case, the above procedure translates into a bounded-depth Frege proof of size at most $2^{n-k} \cdot 2^{O(k\log k)} \cdot 2^{2n} \leq 2^{4n} = 2^{3n+O(k\log k)} = 2^{O(n)}$. ∎

In the proof of Theorem 2 we use the following Lemma by Mills [18]. We give the proof here for completeness.

Lemma (Mills [18])**.** *Let* $w = N\left(k, \frac{m}{2}\right)$. *If, for all* $0 \leq i < \frac{m}{2}$, $|A_i| < r(m-i, v_{i+1}-1)$, *then* $|A_{m/2}| > N(w^{m-1}, m/2) - w^{m-1}$.

Proof: In this proof we use the bound $r(t,s) \leq (s+1)^{t-1} - (s+1)^{t-2}$ for $2 \leq s \leq t$ (see equation (5)). For all $i < \frac{m}{2}$ we have by construction that $v_i \leq w$, thus we have $|A_i| < r(m-i, v_{i+1}-1) \leq r(m-i, w-1) \leq w^{m-i-1} - w^{m-i-2}$.

The size of set $P \cup A_0 \cup \ldots \cup A_{m/2-1}$ is less than $m/2 + w^{m-1} - w^{m/2-1}$ thus

$$\begin{aligned} |A_{m/2}| \geq\ & N(k,m) - k - w^{m-1} + w^{m/2-1} - m/2 = \\ &= N(N(w^{m-1}, m/2), m/2) - k - w^{m-1} + w^{m/2-1} - m/2 = \\ &= N(w^{m-1}, m/2)^{B(m/2)} - k - w^{m-1} + w^{m/2-1} - m/2 > \\ &> N(w^{m-1}, m/2) - w^{m-1}, \end{aligned}$$

for sufficiently large k, m. The second line is because of equation (8), the third line is by definition of N, the last line is because $B(x) \geq 1$, and $w^{m/2-1} > k + m/2$ for large enough k, m. ∎

In the proof of Theorem 3 we omitted the proof of point (i).

Theorem 3. *Let* $N \geq k^{2^{\beta k}}$. *There exists* $M = M(k)$ *such that*

i. $2^{2^{k/2-1}} < M < \sqrt{N}$, *and*

ii. if $\text{PH}(N;k,k)$ *has a Resolution refutation of size* S *then* $\text{RAM}(N-M+1;3,M)$ *has a Resolution refutation of size* S.

Proof of (i): The RHS of (i) can be obtained by the following calculations (see [5]). Let a be such that for

all sufficiently large s, $r(3,s) \geq as^2/(\log s)^2$ (cfr. [4]). Let $b = a/(\log k)^2$ (we can assume that $b \leq 1$). One can show inductively for $i = 0, 1, \ldots, k/2-1$ that $n_i \geq (k^{2^i} b^{2^i-1})/(4^{2^i-i-1})$. Let now $c = \sqrt{a/4}$. For all sufficiently large k we have $n_{k/2-2} \geq (c\sqrt{k}/\log k)^{2^{k/2-1}}$ by the following calculation:

$$\begin{aligned} n_{k/2-2} &\geq \left(k^{2^{k/2-2}} b^{2^{k/2-2-1}}\right) / \left(4^{2^{k/2-2}-k/2+1}\right) \\ &\geq (kb/4)^{2^{k/2-2}} = (c\sqrt{k}/\log k)^{2^{k/2-1}}. \end{aligned}$$

The desired inequality follows for k so large that $c\sqrt{k}/\log k > 2$. The lower bound can be slightly improved using the bounds in equation (4) but this is irrelevant for our purposes.

For the LHS of (i), we give a very rough overestimation which is sufficient for our purposes (in particular we ignore the logarithmic factor in the denominator of equation (4)). Let $u(x) := x + r(3,x)$. Obviously then $n_{i+1} \leq u(n_i)$, by definition of n_{i+1}. Thus, $n_{i+1} \leq u^{i+1}(k)$ and thence $M \leq u^{k/2-2}(k)$. Also, $u^{i+1}(x) \leq 2 \cdot r(3, u^i(x))$, by monotonicity of $r(3,x)$. By the LHS of equation (4), $r(3,u^i(x)) < (u^i(x))^2$. By induction on i we easily prove $u^{i+1}(k) \leq 2^{2^{i+1}-1} \cdot k^{2^{i+1}}$: for $i = 0$, we have $u(k) = k + r(3,k) \leq 2 \cdot r(3,k) < 2 \cdot k^2$. For the inductive step we have

$$\begin{aligned} u^{i+1}(k) \leq\ & 2r(3,u^i(k)) \leq\ 2(u^i(k))^2 \leq \\ \leq\ & 2(2^{2^i-1} \cdot k^{2^i})^2 \leq\ 2 \cdot\ 2^{2^{i+1}-2} \cdot k^{2^{i+1}} \leq \\ & \leq\ 2^{2^{i+1}-1} \cdot k^{2^{i+1}}. \end{aligned}$$

Thus $M < 2^{2^{k/2-2}-1} \cdot k^{2^{k/2-2}}$ and $M^2 < 2^{2^{k/2-1}-2} \cdot k^{2^{k/2-1}}$, which is strictly smaller than $N = k^{2^{\beta k}}$, since

$$2^{k/2-1} - 2 + \log k 2^{k/2-1} < 2 \log k 2^{k/2-1} = \log k 2^{k/2}$$

which is smaller that $\log k 2^{\beta k}$ for $\beta > 1$. ∎

We now give the simple proof of Lemma 1 from Section IV.

Lemma 1. *Let G be a graph with T vertices and no stable set of size s. Consider propositional variables $p_{i,v}$ for $i \in [s]$ and $v \in V(G)$. The following formula has Resolution refutation of size $T^{O(s)}$.*

$$\bigvee_v p_{i,v} \qquad i \in [s] \quad (14)$$

$$\neg p_{i,v} \vee \neg p_{j,v} \qquad i \neq j \in [s] \text{ and } v \in V(G) \quad (15)$$

$$\neg p_{i,v} \vee \neg p_{j,v'} \qquad i \neq j \in [s] \text{ and } \{v,v'\} \in E(G) \quad (16)$$

Proof: Proof strategy is a brute force exploration of all possible assignments of the s indexes to T elements. For any sequence of vertices $(v_1, \ldots, v_w)$ of length $0 \leq w \leq s$ we are going to deduce the clause $\bigvee_{i=1}^{w} \neg p_{i,v_i}$.

We start with $w = s$ and we proceed downward to $w = 0$ which corresponds to the empty clause, i.e. the end of the refutation.

Since G has no stable set of size s, any sequence of $(v_1, \ldots, v_s)$ either has a repetition or there is an edge between v_i and v_j for some $1 \leq i < j \leq s$. In both cases the clause to deduce is a weakening of an initial clause of type (15) or (16).

Fix $w < s$ and $C = \bigvee_{i=1}^{w} \neg p_{i,v_i}$. For any $v \in V(G)$, clause $C \vee \neg p_{w+1,v}$ has been deduced at the previous step. We obtain clause C by doing resolution of the initial clause $\bigvee_v p_{w+1,v}$ (clause (14)) with all such T many clauses.

In this refutation we produce T^w clauses of witdh w for $0 \leq w \leq s$. The clauses of width s need an axiom download and a (not strictly necessary) weakening step to be deduced from initial clauses. Each clause of width less than s requires at most $T+1$ steps to be deduced from the corresponding clauses of larger width. The total size is then $T^{O(s)}$. ∎

C. Inference simulation

During the proof of Theorem 4, we claimed that the disjunctive encoding of $A \vee B$ is deducible from the disjunctive encoding of $A \vee E_{i,j}$ and $B \vee \neg E_{i,j}$ for any A, B clauses on the variables of $\textsc{Ram}(U; k, s)$. In this section we explain such inference simulation. For the definition of disjunctive and conjunctive encoding, we point back to the proof of Theorem 4.

Consider $A \vee E_{i,j}$ and $B \vee \neg E_{i,j}$ where we assume that A and B are already disjunctively encoded. We want to deduce $A \vee \neg p_{i,c} \vee \neg p_{j,d}$ for every pair $(c,d) \in \Gamma$. Such set of formula is essentially an mixed encoding for which A is encoded disjunctively, and $E_{i,j}$ is encoded conjunctively. Since we encode conjunctively just one literal, the size blow-up does not occur.

Once the mixed encoding of $A \vee E_{i,j}$ has been deduced, we then apply $\textsc{Res}(2)$ Cut to all such formulas and to the disjunctive encoding of $B \vee \neg E_{i,j}$ to obtain $A \vee B$. We now show how to obtain the set of $O(T^2)$ formulas

$$A \vee\ \neg p_{i,c} \vee\ \neg p_{j,d} \quad (17)$$

for each $(c,d) \in \Gamma$, from the 2-DNF disjunctive encoding of $A \vee E_{i,j}$, which is

$$A \vee \bigvee_{(a,b) \in\ \Delta} p_{i,a} \wedge\ p_{j,b} \quad (18)$$

Fix any $(c,d) \in \Gamma$. For any of $(a,b) \in \Delta$ either $a \neq c$ or $b \neq d$ because Δ and Γ are disjoint sets. Thus any term $p_{i,a} \wedge p_{j,b}$ can be eliminated from formula (18) by an application of resolution with either $\neg p_{i,a} \vee \neg p_{i,c}$ or $\neg p_{j,b} \vee \neg p_{j,d}$: at least one of these formulas is a Pigeonhole axiom. After removing all such terms from (18), we are left with a formula of the form $A \vee \neg p_{i,c} \vee \neg p_{j,d}$. The just described process costs $O(T^2)$ steps and must be repeated for any $(c,d) \in \Gamma$. Thus inferring the formulas in (17) requires $O(T^4)$ steps.

Now we have all formulas of the form (17) and $B \vee \bigvee_{(c,d) \in \Gamma} p_{i,c} \wedge p_{j,d}$, which is the disjunctive encoding of $B \vee \neg E_{i,j}$. To deduce the disjunctive encoding of $A \vee B$, we proceed as follows. Consider any $\Gamma' \subseteq \Gamma$. We have that for any $(c,d) \in \Gamma'$, one application of resolution to $A \vee\ \neg p_{i,c} \vee \neg p_{j,d}$ and

$$A \vee\ B \vee\ \Big(\bigvee_{(c',d') \in \Gamma' - \{(c,d)\}} p_{i,c'} \wedge p_{j,d'} \Big) \vee (p_{i,c} \wedge p_{j,d})$$

gives

$$A \vee B \vee \Big(\bigvee_{(c',d') \in \Gamma' - \{(c,d)\}} p_{i,c'} \wedge p_{j,d'} \Big).$$

The base case $A \vee B \vee E_{i,j}$ is obtained by weakening. We repeat this inference until $\Gamma' = \emptyset$, and we get $A \vee B$. The complete process is dominated by the $O(T^4)$ steps required to obtain the formulas in (17).