On the Proof Complexity of Paris-Harrington and Off-diagonal Ramsey Tautologies*†

Lorenzo Carlucci
carlucci@di.uniroma1.it

Nicola Galesi
galesi@di.uniroma1.it

Massimo Lauria
lauria@cs.upc.edu

March 11, 2016

Abstract

We study the proof complexity of Paris-Harrington's Large Ramsey Theorem for bi-colorings of graphs and of off-diagonal Ramsey's Theorem. For Paris-Harrington we prove a non-trivial conditional lower bound in Resolution and a non-trivial 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 off-diagonal Ramsey principle is established. This is obtained by adapting some constructions due to Erdős and Mills. We prove a non-trivial Resolution lower bound for a family of such off-diagonal Ramsey principles.

1 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

*The second and third authors have been supported by grant N. 20517 by the John Templeton Foundation, as part of the project "Limits of Theorem Proving"

†A preliminary version of the present paper has been presented at the IEEE Conference on Computational Complexity, 2011

cannot be proved in strong theories like Peano Arithmetic, as shown by Harrington and Paris in [9].

It has been sometimes proposed (e.g., by Clote in [4]) that propositional encoding of logically strong combinatorial principles could produce hard tautologies for propositional proof systems. Krajíček [15] recently dismissed this idea as impracticable. Since the functions witnessing the truth of such principles have an extremely fast growth, the corresponding tautologies are so large that there is no room for non-trivial lower and upper bounds on the proof length. This is true to a lesser extent if one focuses on suitably weak instances of the strong principles, as exemplified in this paper by focusing on the Paris-Harrington Theorem for bi-colorings of graphs.

Our first result is that for the known upper bound $u(k)$ on $R(k,k)$ (due to Erdős and Mills [7, 19]) the natural propositional translation of the statement "$R(k,k) \leq u(k)$" has efficient bounded-depth Frege proofs. The upper bound is $O(|F|^{\log\log\log|F|})$ where $|F|$ is the size of the formula. This improves over the trivial quasi-polynomial upper bound $O(|F|)^{\log|F|}$. The proof combines a combinatorial argument by Mills [19] with a proof in bounded-depth Frege of a Paris-Harrington principle for triangles. To obtain the latter we adapt Pudlák's [21] proof of Ramsey Theorem in Bounded Arithmetic: since we focus on an off-diagonal Ramsey principle, 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 in this case very large compared to the number of variables ($2^{\Theta(u(k))}$ clauses vs. $u(k)^2$ variables, see *infra* for details).

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 [14] 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 [7] that has never been applied in proof complexity before. The overall proof-scheme significantly extends Pudlák's [21] and Krajíček's [14] methods.

We further investigate the proof complexity of a family of off-diagonal Ramsey principles that played a significant role in the analysis of Paris-Harrington tautologies, as mentioned above. We establish a non-trivial lower bound in Resolution for a family of tautologies encoding a quadratic upper bound for very unbalanced Ramsey principles, where one of the two parameters is fixed to be 3 in to order exclude triangles.

Our results on Paris-Harrington tautologies 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 numbers 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 construction of a graph with neither cliques nor independent sets of size k. So far all attempts to build such graph explicitly have failed. 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 established by Krajíček [14] 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 tight the known 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 a (new) good candidate for separating bounded-depth from low-depth (e.g. depth 2) Frege systems. This separation is a recurrent and notable open problem in propositional proof complexity showing the big difference with Boolean circuit complexity, where a separation between bounded-depth circuits and low-depth circuits (e.g. depth 3) is known since the early work in the area (see, e.g., [10]). By contrast, only a few good candidates and some partial results are known for the proof complexity separation [13, 2].

The plan of the paper is a follows. In Section 2 we introduce the propositional versions of Ramsey and Paris-Harrington principles and discuss the proof scheme of our main results; in Section 3 we give a non-trivial quasi-polynomial upper bound for the Paris-Harrington principle in bounded-depth Frege systems; in Section 4 we give a conditional lower bound for the Paris-Harrington principle in Resolution. The proof of the upper bound depends on a theorem which is proved in Section 5. In Section 5.3 we establish a lower bound in Resolution for a family of off-diagonal Ramsey principles.

2 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 an independent set of arbitrarily prescribed size.

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 an independent set of size s.*

The conclusion of the above theorem is obviously satisfied by any $n \geq r(k,s)$, and we 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 [9] in the context of the incompleteness of formal theories of arithmetic. This theorem is the first example of a mathematically natural statement which is unprovable in arithmetic. The general version is unprovable in first-order Peano Arithmetic [9], and the same still holds if one just considers bi-colorings of hypergraphs [17]. 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 of integer numbers 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 with respect to prescribed parameters k and m, then any graph with vertices labeled by the integers $[k, n]$ either contains a clique of size m or contains an independent 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 independent 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 $R(a; b) \geq r(a, b)$ 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 claim "$n < r(k, s)$" 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. For large enough k we have $\frac{n}{3} \geq \frac{R(k;m)}{3} > k$ (see equation (3)). For small k we get that $\frac{n}{3} > k$ eventually, as n grows. In both cases there is a clause of type (2) corresponding to each subset of size $\lfloor n/3 \rfloor$ having $\lfloor n/3 \rfloor$ as minimum element. □

While general Paris-Harrington principles (for arbitrary colorings of hypergraphs) have enormously growing lower bounds [11], 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 [7] and later

improved by Mills [19]. The best known bounds are as follows: 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 [6, 25, 1, 12]. 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 present paper it is often sufficient to use the following weaker bound [8]. 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 independent sets of the same size k. Krishnamurty and Moll [16] proved a $r(k,k)/2$ width lower bound in Resolution and an exponential lower bound for the Davis-Putnam procedure for $\textsc{Ram}(r(k,k);k,k)$. Recently Krajíček [15] established an exponential size lower bound in Resolution for the same principle. Pudlák proved in [21] that the formula $\textsc{Ram}(4^k;k,k)$ has a proof in bounded-depth Frege system of size $2^{k^{O(1)}}$ (note that such proof is polynomial in the size of the Ramsey principle and is quasi-polynomial in the number of variables). Krajíček [14] proved a conditional lower bound for the same formula: a lower bound for $\textsc{Ram}(4^k;k,k)$ in Resolution follows from a lower bound for $\textsc{Php}_n^{n^4}$ in $\textsc{Res}(2)$. The idea is the following: assume the existence of an injective mapping from $[n^4]$ into $[n]$, and pick a graph with $2^{k/2}$ vertices and neither cliques nor independent sets of size k. The injective mapping allows to blow-up the graph into a graph of 4^k vertices with the same properties, but this is of course impossible. In this way a proof for the Ramsey Theorem can be used as a proof for some Pigeonhole Principle. This can be seen as a reversal of Pudlák's [21] approach. The proof of our conditional lower bound in Section 4 can be seen as an extension of these ideas to the case of the Paris-Harrington principle. Recently an unconditional lower bound of $2^{n^{\frac{1}{4}-o(1)}}$ for the size of Resolution refutations of $\textsc{Ram}(4^k;k,k)$ has been proved by Pudlák [22].

We now give a brief overview of our proofs for the upper bound and for the lower bound for the Paris-Harrington tautologies. 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 [19]) to reduce the Paris-Harrington principle to a Paris-Harrington principle for triangles. Then we reduce the latter to the off-diagonal Ramsey principle for triangles. Finally we use Pudlák's [21]

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 for triangles, as in [7], and we relate the latter to a weak quasi-polynomial Pigeonhole principle.

3 Bounded-depth Frege proof of Paris-Harrington

For $\beta = 1.471$ (see equation (3)) and $N = k^{2^{2\beta k}}$ we prove that the Paris-Harrington principle $\text{PH}(N; k, k)$ has proofs of size $2^{O(N \log\log N)}$ in bounded-depth Frege systems.

We start by recalling the details of bounded-depth Frege systems [3]. Lines of a proof are unbounded fan-in formulas over the language $\{\neg, \vee, \wedge\}$. The proof system has the following inference rules.

$$\frac{}{A \vee \neg A} \qquad \text{Axiom}$$

$$\frac{A}{A \vee B} \qquad \text{Weakening}$$

$$\frac{\bigvee(\{\vee_i \Gamma_i\} \cup \Delta)}{\bigvee_i(\Gamma_i \cup \Delta)} \qquad \text{Merging}$$

$$\frac{\bigvee_i(\Gamma_i \cup \Delta)}{\bigvee(\{\vee_i \Gamma_i\} \cup \Delta)} \qquad \text{Unmerging}$$

$$\frac{A \vee B \qquad \neg A \vee C}{B \vee C} \qquad \text{Cut}$$

The *depth of a formula* is the maximal number of alternation of connectives in the formula. The depth of a literal is 0. The *size of a formula* is the number of occurrences of connectives in the formula. A Frege proof of depth d for formula F is a sequence $D_1, \ldots, D_n$ of formulas of depth at most d such that each D_i is either an Axiom or else is derived from previous formulas in the sequence by applying one of the other inference rules, and D_n is F. The *depth of a proof* is the maximal depth of formulas occurring in the proof and *the size of a proof* is the sum of the sizes of the formulas occurring in the proof.

We introduce the sequent notation $A_1, A_2, \ldots, A_m \vdash B_1, \ldots, B_\ell$ which is an alternative notation for the formula $\bigvee_{i=1}^{m} \neg A_i \vee \bigvee_{j=1}^{\ell} B_j$.

The argument for our upper bound has two main ingredients: (1) We simulate a combinatorial upper bound construction by Mills [19]. 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 Section 5).

Theorem 1. $\text{PH}(k^2; k, 3)$ *has polynomial-size proofs (w.r.t. the size of the formula) in bounded-depth Frege.*

To prove point (1) we translate Mills' [19] proof-method into 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 independent set. Such a procedure is guaranteed to succeed,

and is essentially a decision tree, with the notable exception of the base cases. The well-known isomorphism between decision trees and tree-like Resolution refutations gives the refutation of $\mathrm{PH}(k^{2^{2\beta k}}; k, k)$. More precisely, Mills' construction defines a decision tree and thus a tree-like Resolution refutation. The leaves of this tree are either tautologies or else are clauses that can be derived in bounded-depth Frege using Theorem 1. The desired proof of $Ph(k^{2^{(2\beta k)}}; k, k)$ in bounded-depth Frege is obtained by composing these derivations and the tree-like Resolution refutation corresponding to the decision tree. [1]

Theorem 2. *Let $N = k^{2^{2\beta k}}$. Then $\mathrm{PH}(N; k, k)$ has a proof of size $2^{O(N \log\log N)}$ in bounded-depth Frege.*

Proof. Mills [19, 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.

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

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

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.

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

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

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

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.

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

[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 $\mathrm{PH}(k^{2^{\beta k}}; k, k)$ with a slightly more involved construction, thus matching the best known upper bound on Paris-Harrington numbers.

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 $\mathrm{PH}(N;k,m)$ which is falsified. Since $N \geq R(k;m)$ (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 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 independent set is found, then the procedure outputs such a set and terminates. 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 $t \in [1, \frac{m}{2}-1]$, $A_t = \{i \big| E_{i,v_1} \wedge E_{i,v_2} \wedge \ldots \wedge E_{i,v_t} = 1 \text{ and } E_{i,v_{t+1}} = 0\}$, 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 i such that $0 \leq i < \frac{m}{2}$ and $|A_i| \geq r(m-i, v_{i+1}-1)$.

(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 an A_i to find either a clique C of size $m-i$ or an independent 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 independent 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 $A_{m/2}$. To estimate the size of $A_{m/2}$ we need the following lemma.

Lemma (Mills [19])**.** *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 and 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 and m. □

The previous lemma guarantees that the size of $A_{m/2}$ is at least

$$N\left(N(k, m/2)^{m-1}, \frac{m}{2}\right) - N(k, m/2)^{m-1} + 1,$$

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 a clique of size $m/2$ or a relatively large independent 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 independent set S. We can do this because either (i) $m/2 = 3$, or else (ii) $m/2$ and $N(k, m/2)^{m-1} = (k^{B(m/2)})^{m-1}$ 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 independent 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 proof of the 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 independent 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 cliques of size $m/2$ or large independent 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

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

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

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

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 values $k_0, k_1, \ldots, k_\ell$, where $k_0 = k$, and, for $0 \leq i < \ell$

$$k_{i+1} = N(k_i, m/2^{i+1})^{m/2^i - 1},$$

where $\ell = \log m - \log 3$, so that $m/2^\ell = 3$. The k_is are the successive values of k in the recursive calls. 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 level $i \in [0, \ell - 1]$ 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 level 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 on 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

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

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 $0 \leq i < \ell$,

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

We now observe that 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.

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

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 trivial tree-like refutation is 2^{N^2} which is far greater than our upper bound $2^{O(N \log\log N)}$. 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 $\textsc{Ph}(N;k,k)$ 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 [23]). A natural open question is whether the upper bound in Theorem 2 can be improved to polynomial with respect to formula size.

4 A conditional Resolution lower bound for Paris-Harrington

We prove a conditional lower bound on the Paris-Harrington principle $\textsc{Ph}(k^{2^{\beta k}};k,k)$ in Resolution. The lower bound is conditional on a lower bound for a quasi-polynomial Pigeonhole principle in $\textsc{Res}(2)$. The technique can be seen as an extension of Krajíček's [14, 15] 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 independent sets and how to blow it up—using a suitable Pigeonhole principle—to a large graph on $[k,N]$ without k-cliques and large independent 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 [7] 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 [19] (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 [14] to reduce a refutation of $\textsc{Php}_n^{2^{(\log n)^c}}$, for some c,n depending on the parameters k,β, to a refutation of $\textsc{Ph}(k^{2^{\beta k}};k,k)$. Note that Krajíček [14] uses $\textsc{Php}_n^{n^4}$ 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.

We first recall the details of the proof systems Res and Res(2). Both are refutational systems. A *refutation of size S* of a formula F in CNF form $\bigwedge_{i=1}^{m} C_i$ is a sequence of formulas $D_1, \ldots, D_S$ such that $D_i = C_i$ for $1 \leq i \leq m$, for $i > m$ the formula D_i is either an axiom or is logically inferred from two previous formulas in the sequence, and D_S is the empty formula.

In Res every line in the refutation is a disjunction of literals and there is only one inference rule, the resolution rule:

$$\frac{A \vee \ \ell \qquad B \vee \ \neg\ell}{A \vee \ B} \qquad \text{Resolution}$$

The propositional proof-system Res(2) has been first defined by Krajíček [14] as an extension of Resolution. Res(2) is a refutational system working with 2-DNFs, i.e., clauses C of the form $\bigvee_i D_i$ where each D_i is a conjunction of at most two literals. There are the following basic rules:

$$\frac{}{\ell \vee \ \neg\ell} \qquad \text{Axiom}$$

$$\frac{A \vee \ \ell_1 \qquad B \vee \ \ell_2}{A \vee \ B \vee \ell_1\ell_2} \qquad \wedge\text{-Introduction}$$

$$\frac{A \vee \ \ell_1\ell_2 \qquad B \vee \ \neg\ell_1 \vee \ \neg\ell_2}{A \vee \ B} \qquad \text{Resolution}$$

$$\frac{A \vee \ \ell_1\ell_2}{A \vee \ \ell_1} \qquad \text{Weakening 1}$$

$$\frac{A}{A \vee \ \ell_1\ell_2} \qquad \text{Weakening 2}$$

It is easy to see that also the following rules are admissible.

$$\frac{A \vee \ \ell_1\ell_2 \qquad B \vee \ \neg\ell_1}{A \vee \ B} \qquad \text{Resolution 2}$$

$$\frac{A}{A \vee \ \ell} \qquad \text{Weakening 3}$$

Since we consider Res(2) as a refutational system, thus we include as axioms also the clauses of the CNF we want to refute.

Theorem 3. *Let $N \geq k^{2^{\beta k}}$ where β is the constant from equation (3). There exists $M = M(k)$ such that*

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

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

Proof. We assume even $k \geq 6$. Consider any refutation for $\textsc{Ph}(N;k,k)$ 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 [7], note that we are essentially carrying over Erdős-Mills' construction up to the penultimate step inside a suitably large interval given in advance.

Now we prove point (i). The RHS of (i) can be obtained by the following calculations (see [7]). Let a be such that for all sufficiently large s, $r(3,s) \geq as^2/(\log s)^2$ (cfr. [6]). 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 $c\sqrt{k}/\log k > 2$.[2]

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

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

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 prove point (ii) in the statement of the theorem. We define a restriction ρ on the variables of $\textsc{Ph}(N;k,k)$. First of all we fix $E_{a,b}$ to 1 for every choice of a and b in different intervals. For all $i \leq k/2-3$, $|I_i| = r(3,n_i) - 1$. Therefore there exists a

[2] The lower bound on M can be slightly improved using the bounds on Ramsey numbers from equation (4) but this is irrelevant for our purposes.

graph G_i of size $|I_i|$ with no independent 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 an independent set 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 $\text{RAM}(N-M+1; 3, M)$. □

Theorem 4. *Let $T < r(k, s)$. If $\text{RAM}(U; k, s)$ has a Resolution refutation of size S then PHP^U_T 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-size independent 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-independent set, 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 encodings for each 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^U_T.

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^U_T. 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^U_T.

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. 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-independent set.

Inference simulation. 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 formulas is essentially a 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 $\text{RES}(2)$ 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

$$A \vee \ \neg p_{i,c} \vee \ \neg p_{j,d} \tag{9}$$

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

$$A \vee \bigvee_{(a,b) \in \ \Delta} p_{i,a} \wedge \ p_{j,b} \tag{10}$$

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 (10) 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 (10), 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 (9) requires $O(T^4)$ steps.

Now we have all formulas of the form (9) 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 (9).

Axiom deduction. We show how to deduce the disjunctive encoding of an axiom of $\textsc{Ram}(U; k, s)$ from the $\textsc{Php}_T^U$ axioms. We focus on the axioms that claim that no independent set 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.

$$\bigvee_{i \neq j \in [s]} \bigvee_{(a,b) \in \Delta} p_{i,a} \wedge p_{j,b}. \tag{11}$$

The deduction of such an axiom is equivalent to proving that there is no independent set of size s in the model graph G (indeed formula (11) 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.

Lemma 1. *Let G be a graph with T vertices and no independent 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 $T^{O(s)}$.*

$$\bigvee_v p_{i,v} \qquad i \in [s] \tag{12}$$

$$\neg p_{i,v} \vee \neg p_{j,v} \qquad i \neq j \in [s] \text{ and } v \in V(G) \tag{13}$$

$$\neg p_{i,v} \vee \neg p_{j,v'} \qquad i \neq j \in [s] \text{ and } \{v, v'\} \in E(G) \tag{14}$$

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 independent 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 (13) or (14).

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 (12)) 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 $T^{O(s)}$. □

Lemma 1 immediately implies that formula (11) is deducible in $T^{O(s)}$ steps. The refutation of (11) is obtained by simulating the refutation given by Lemma 1 using the initial clauses of $\textsc{Php}_T^U$. Clauses (12) and (13) are also initial clauses of $\textsc{Php}_T^U$; clauses

(14) 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 (11).

If a Resolution refutation of $\textsc{Ram}(U; k, s)$ has length S, then the corresponding $\textsc{Res}(2)$ refutation of $\textsc{Php}_T^U$ 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* $\textsc{Ph}(N; k, k)$ *has a refutation of size* S *in Resolution, then* $\textsc{Php}_L^{N-M+1}$ *has a refutation of size* $2^{O(M \log M)} \cdot S$ *in* $\textsc{Res}(2)$.

Proof. By Theorem 3 if the Paris-Harrington principle $\textsc{Ph}(N; k, k)$ has a Resolution refutation of size S, then $\textsc{Ram}(N - M + 1; 3, M)$ also has such a refutation. By Theorem 4 if $\textsc{Ram}(N - M + 1; 3, M)$ has a size S refutation in Resolution then the Pigeonhole principle $\textsc{Php}_L^{N-M+1}$ has a $\textsc{Res}(2)$-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 $\textsc{Php}_L^{N-M+1}$ 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

$$2^{2^{k/2-1}} < M < \sqrt{k^{2^{\beta k}}}. \tag{15}$$

For $L = r(3, M) - 1$ we have ([12], see equation (4)) that $L \approx \frac{M^2}{\log M}$.

If M is close to the upper bound in (15), 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 (15), 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 $\textsc{Php}_L^{N-M+1}$ in $\textsc{Res}(2)$. 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 $\textsc{Ph}(N; k, k)$ 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* $\textsc{Res}(2)$ *refutations of* $\textsc{Php}_L^{N-M+1}$ *is at least* $2^{L^{\frac{1}{2}+\epsilon}}$ *for some* $\epsilon > 0$, *then any Resolution refutation of* $\textsc{Ph}(N; k, k)$ *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 15) 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.

5 The case of triangle-free graphs

In this Section we prove Theorem 1, used as the base case of the recursive construction in the proof of Theorem 2. To achieve this we follow an argument by Mills [19] that reduces Paris-Harrington principle for triangles to an off-diagonal Ramsey principle. In Section 5.2 we formalize such reduction, but first in Section 5.1 we prove efficiently such off-diagonal Ramsey Theorem in bounded-depth Frege systems. The latter proof is a rather straightforward generalization of Pudlák's [21] proof for the diagonal Ramsey Theorem, but we avoid using the language of Bounded Arithmetic. In Section 5.3 we prove a lower bound in Resolution for the off-diagonal Ramsey Theorem.

5.1 Off-diagonal Ramsey Theorem in bounded depth

We adapt Pudlák's [21] 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 $\textsc{Ram}(s^2 - 5s + 2; 3, s - 1)$ 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 $\textsc{Ph}(s^2; s, 3)$. We will show how to obtain such proofs by a reduction to $\textsc{Ram}(s^2 - 5s + 2; 3, s - 1)$. 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 this 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 sufficient for our purposes.

Lemma 2. *The Pigeonhole principle* $\textsc{Php}_n^{2n-6\sqrt{n}}$ *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 the Pigeonhole Principle. 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 $\textsc{Php}_{n-6\sqrt{n}}^{2(n-6\sqrt{n})}$.

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 [20, 18]), 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 0'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. $\textsc{Ram}((s+1)(s-2)-4(s-1); 3, s-1)$ *has polynomial-size bounded-depth Frege proofs.*

Proof. The proof is by reduction to $\textsc{Php}_{(s+1)(s-2)/2}^{(s+1)(s-2)-4(s-1)}$. 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.

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

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,

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

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.

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 fix x_0 to be an arbitrary, but fixed, vertex (e.g. $x_0 = 1$), and 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 independent 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, the truth of $C_x(x_0, \ldots, x_\ell; \alpha_0, \ldots, \alpha_{\ell-1})$ implies

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

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 $A \wedge E_{x_\ell,x} = 0$.

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

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 an independent 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.

Injectivity Axioms Deduction For the simulation of the inferences it is sufficient to show that $p_{x,\vec{\alpha}} \vdash \overline{p_{y,\vec{\alpha}}}$ (i.e., that $p_{x,\vec{\alpha}} \wedge p_{y,\vec{\alpha}}$ is contradictory) 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 $\textsc{Php}^{(s+1)(s-2)-4(s-1)}_{(s+1)(s-2)/2}$. 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). □

5.2 Small Paris-Harrington numbers

Paris-Harrington numbers for the case of forbidding a triangle and a large independent set have the same asymptotic as the corresponding off-diagonal Ramsey numbers. In particular, Mills [19] 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. $\textsc{Ph}(k^2; k, 3)$ *has polynomial-size bounded-depth Frege proofs.*

Proof. In the previous subsection we showed how to prove efficiently $\textsc{Ram}((k+1)(k-2)-4(k-1);3,k-1)$ in bounded-depth Frege. We will show how to mimic efficiently Mills' proof [19] 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 $\textsc{Ph}((k+1)(k-2)-4(k-1)+5k-7;k,3)$, i.e., of $\textsc{Ph}(k^2-5;k,3)$, to a proof of $\textsc{Ram}((k+1)(k-2)-4(k-1);3,k-1)$. *A fortiori* this gives a small proof of $\textsc{Ph}(k^2;k,3)$. 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 triangle and no large independent 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 an independent set. This produces at most $|A|^2$ branches. In case A is not an independent set, then a triangle is found and we are done. On the remaining branches the set A is independent. If $|A|\geq \min(A)$ then we have found a large independent set and we are done.

If $|B|\geq (k+1)(k-2)-4(k-1)$ then we know how to prove $\textsc{Ram}(|B|;3,k-1)$ 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 an independent set $X\subseteq B$ of size $k-1$. In the latter case $\{k\}\cup X$ is a large independent 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.

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

(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 independent 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 independent set. Analogously for q and $q-2$. 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 $2^{n-k} \cdot 2^{O(k \log k)} \cdot 2^{2n} \leq 2^{4n} = 2^{3n+O(k \log k)} = 2^{O(n)}$. □

5.3 Off-diagonal Ramsey Theorem in Resolution

We study the Resolution proof complexity for the propositional formula which claims that $r(3,t) > t^2$.

The known bounds on off-diagonal Ramsey numbers for graphs has been given in the sequence of papers [6, 1, 12]. In particular it is known that

$$r(3,t) = \Theta\left(\frac{t^2}{\log t}\right). \tag{16}$$

The main result of this section is a lower bound on the refutation length of $\textsc{Ram}(n; 3, \sqrt{n})$ and its proof is similar to the one used in [6] to show a lower bound to Ramsey number $r(3,t)$. That proof consisted in a probabilistic construction of a triangle-free graph with no independent sets of size t. Our proof would try to construct a triangle-free graph such that a *particular family* of independent sets are forbidden.

Theorem 6. $\textsc{Ram}(n; 3, \sqrt{n})$ *is an unsatisfiable CNF of* $2^{\Theta(\sqrt{n} \log n)}$ *clauses and width* $\Theta(n)$ *which requires Resolution refutations of length* $2^{c\sqrt{n}}$ *for some constant* $c > 0$.

Proof. We fix $t = \sqrt{n}$. W.l.o.g. we assume it is integer. The size and the width of the formula are clear by its definition.

Assignments for this formulas corresponds to graph of t^2 vertices. The initial clauses of the formula enforce forbidden triangles and forbidden independent sets of size t. We are going to prove that if just forbid less than 2^{ct} independent sets, then there exists an assignment encoding a graph G which is triangle-free and such that none of the forbidden independent sets is independent in G. That would immediately imply the theorem, since any Resolution refutation of length smaller that 2^{ct} would use less than 2^{ct} initial clauses of the form Ind. Some graph G would satisfy simultaneously all such initial clauses and all clauses which forbid triangles, thus satisfying all clauses of a Resolution refutation. That is impossible.

Let us consider a generic Resolution refutation. We call $\mathcal{F} \subseteq \binom{[t^2]}{t}$ the family of forbidden independent sets induced such refutation (i.e. which corresponds to the clauses Ind used in it). We assume $|\mathcal{F}| < 2^{ct}$, with $c > 0$ to be fixed later.

We now want to find G which is triangle-free and such that no set of vertices in $\mathcal{F}$ is independent. To construct G we start by choosing I to be a random graph in the model $\mathcal{G}(t^2, \frac{1}{10t})$: the graph has t^2 vertices and edges are independently distributed according to a Bernoulli distribution with parameter $\frac{1}{10t}$ (I stands for "independently distributed"). The random graph G is obtained from I by removing a minimal set of edges such that G is triangle-free. Notice that the edges of graph G are not distributed independently anymore. We will show that for this probabilistic construction any set of t vertices contains an edge with probability at least $1 - 2^{-ct}$. Graph G is triangle-free

by construction and with probability $1 - \frac{|\mathcal{F}|}{2^{ct}} > 0$ none of the sets in $\mathcal{F}$ is independent. Thus we can fix the random choices to obtain the desired graph.

For the rest of the proof we focus on a particular set X of t vertices. We also fix notation Y for the set of the $t^2 - t$ remaining vertices. Our goal is to show that X is independent in G with probability at most 2^{-ct}. To do this it is *sufficient* to upper bound the probability of the following event A_X:

> for all pairs $\{i,j\} \in \binom{X}{2}$, if $\{i,j\} \in E(I)$ then there is a vertex $w \in Y$ such that edges $\{i,w\}$ and $\{j,w\}$ are both in $E(I)$.

Lemma 3. $\Pr[X \textit{ is an independent set in } G] \leq \Pr[A_X]$

Proof. Let G_X and I_X to be the graphs G and I respectively, restricted to vertices in X. Let E be the set of edges which have been deleted in the cancellation step of the random construction. More precisely $E := E(I) \setminus E(G)$.

Assume by contradiction that X is independent in G and that A_X does not hold. We partition E in three classes. The set of "bad" edges E_b is the set of all $\{i,j\} \in E(I_X)$ such that there is a vertex $w \in Y$ and $\{i,w\}$ and $\{j,w\}$ in $E(I)$. $E_g := E(I_X)/E_b \cup E(G_X)$ are the "good" edges removed from I_X but not involved in a triangle with Y (so in particular they must be in a triangle involving just vertices in X). E_o are the deleted edges which are not in I_X at all. Clearly E_o, E_g, E_b form a partition of E.

After removing from I all edges in E_o and E_b, all triangles survived so far are contained in X. We know that G_X is the empty graph, so all edges in $\binom{X}{2}$ survived so far must be eventually deleted and are exactly E_g. E_g is non-empty because we assumed A_X does not hold. To make the graph (X, E_g) triangle-free it is sufficient to remove $E'_g \subsetneq E_g$. It follows that removing $E_o \cup E_b \cup E'_g$ from I makes it triangle-free. Since E was defined to be minimal we have reached a contradiction. □

Studying the event A_X instead of studying directly the independence of X in graph G allows us to focus on graph I. The edges in the latter are independently distributed, so the analysis is facilitated.

To conclude the proof we need to show that $\Pr[A_X] \leq \frac{1}{2^{ct}}$. Let B to be number of unordered pairs of vertices in X which are connected in I to a common vertex $w \in Y$. By independence

$$\Pr[A_X] \leq (1-p)^{\binom{t^2}{2}-B} = \left(1 - \frac{1}{10t}\right)^{\binom{t^2}{2}-B}.$$

We need to bound the value of B from above: let n_d be the number of elements of Y with at least d neighbors in X. Clearly $B \leq \sum_{d=2}^{t} (n_d - n_{d+1})\binom{d}{2}$, a bound that in principle can be larger than B and even larger than $\binom{t^2}{2}$. Nevertheless with high probability such bound is small. In particular we use the following lemma to control the values n_d.

Lemma 4. *Let* $d_L = \lfloor \frac{\log t}{\log 10} \rfloor$ *and* $d_H = \lceil 3 \log t \rceil$. *Let the event* Good *be the event that the following conditions are satisfied:*

- *for all* $2 \leq d \leq d_L$ *it holds that* $n_d \leq \frac{t^2}{10^d}$;
- *for all* $d_H < d \leq \frac{t}{10}$ *it holds that* $n_d < \frac{t}{10d}$;

- *for* $d > \frac{t}{10}$ *it holds that* $n_d = 0$.

Then the probability that Good *is false is at most* $2^{-\Omega(t)}$.

Proof. To simplify counting we consider $|Y| = t^2$. This can only increase the value of n_d so it is without loss of generality. We also focus on $d \geq 2$. The probability that a vertex in Y has degree $\geq d$ is at most $\binom{t}{d} \cdot \frac{1}{10^d t^d} \leq \frac{1}{d! 10^d} \leq \frac{1}{2 \cdot 10^d}$.

The expected degree of each vertex in Y is less than $\frac{t^2}{2 \cdot 10^d}$ so the probability of n_d being more than twice the expected value is $2^{-\Omega\left(\frac{t^2}{10^d}\right)}$ by Chernoff Bound [5, Theorem 1.1]. For $d \leq d_L$ that is $2^{-\Omega(t)}$.

For $d \geq d_H$ fix $m = \frac{t}{10d}$, and notice that $md = \frac{t}{10}$. The probability that at least m vertices of Y have at least d neighbors in X is at most

$$\binom{t^2}{m} \cdot \left(\frac{1}{10}\right)^{md} \leq \left(\frac{et^2}{m}\right)^m \cdot \left(\frac{1}{10}\right)^{md} \leq \left(\sqrt[d]{edt}\right)^{t/10} \cdot \left(\frac{1}{10}\right)^{t/10} = 2^{-\Omega(t)}.$$

In the last inequality we used that $d \geq 3 \log t$. □

Assuming the event Good we can control the magnitude of B.

$$\begin{aligned} B \leq \sum_{d=2}^{t} (n_d - n_{d+1}) \cdot \binom{d}{2} = \sum_{d=2}^{t} n_d (d-1) \leq \\ \leq \left(t^2 \cdot \sum_{d=2}^{d_L} \frac{d-1}{10^d} \right) + d_H (d_H - d_L) n_{d_L} + \sum_{d=d_H+1}^{t/10} n_d \cdot d \leq \\ \leq \left(\frac{t^2}{100} \cdot \sum_{d=0}^{\infty} \frac{1}{5^d} \right) + O(t(\log t)^2) + \frac{t^2}{100} \leq \frac{t^2}{40} + o(t^2). \quad (17) \end{aligned}$$

Assuming B is small, it is easy to show that event A_X occur with small probability. More formally:

$$\begin{aligned} \Pr[A_X] \leq \Pr[A_X | \text{Good}] + \Pr[\neg \text{Good}] \leq \\ \leq \left(1 - \frac{1}{10t}\right)^{\binom{t^2}{2} - B} + 2^{-\Omega(t)} = \left(1 - \frac{1}{10t}\right)^{\Omega(t^2)} + 2^{-\Omega(t)} = 2^{-\Omega(t)}. \quad (18) \end{aligned}$$

We just proved that there is a constant c such that $\Pr[A_X] \leq 2^{-ct}$. By union bound all vertex sets in any family $\mathcal{F} \subset \binom{t^2}{t}$ of size less than 2^{ct} can be made independent in some graph with no triangles. That concludes the proof of the theorem.

□

It is a legitimate question to ask why we focus on an off-diagonal Ramsey statement which is weaker than the state of the art. Our lower bound is indeed non-trivial, while a (weaker) lower bound for the harder statement "$r(3,t) > c\frac{t^2}{\log t}$" is a simple corollary of the following two theorems. The first theorem is just our Theorem 4 rephrased for $r(3,t)$.

Theorem 7. *Let $L < r(3,t) < U$. If claim "$r(3,t) > U$" has a Resolution refutation of size S then PHP_T^U has a $\text{RES}(2)$ refutation of size $S \cdot 2^{O(t \log t)}$.*

Theorem 8 (Theorem 6.2 in [24], rephrased for $\text{RES}(2)$)**.** *For every $c > 1$, there exists $\epsilon > 0$ so that for all n sufficiently large, every $\text{RES}(2)$ refutation of PHP_n^{cn} has size at least 2^{n^ϵ}*

Unfortunately our lower bound is sub-polynomial with respect to the size of the CNF to be refuted. Our lower bound is a non-trivial result for such a big formula like $\text{RAM}(n; 3, \sqrt{n})$, nevertheless it is natural to ask whether it is possible obtain lower bounds that are super-linear with respect to the size of the formula. Our proof technique cannot work in such direction, since it is based on finding the size of the smallest unsatisfiable sub-formula.

We further observe that that Theorem 6 and Theorem 3 have the following corollary. $M(k)$ is as in Theorem 3.

Corollary 3. *Let $N = k^{2^{\beta k}}$. If $M(k) = (1 + o(1))\sqrt{N}$, then the CNF encoding the claim "$R(k,k) > N$" is an unsatisfiable propositional formula of size $2^{\Theta(N)}$ which requires Resolution refutations of size $2^{\Omega(\sqrt{N})}$.*

The problem here is that we do not know if such $M(k)$ (which comes from the constructions in [19]) is close to $\sqrt{N}$. In particular if $M \equiv \sqrt{N}$ the lower bound transfer from off-diagonal Ramsey to Paris-Harrington. The authors must admit that the condition on $M(k)$ in the previous Corollary does not seem very plausible. Nevertheless it is important to notice that any lower bound of type $2^{\Omega(N^\gamma)}$ for constant $\gamma > 0$ would implies a breakthrough in lower bounding $R(k,k)$. Thus it is quite natural for actual proof complexity lower bound to be conditioned on the quality of actual constructions employed to prove lower on $R(k,k)$, which in turn are notoriously hard to find.

6 Conclusion

We briefly comment on the significance of our results. 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 (15)) that for some c, $N = 2^{O((\log L)^c)}$. Thus our conditional $2^{L^{\frac{1}{2}+\epsilon}}$ lower bound 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. On the other hand, 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 [23]).

Furthermore notice that when $\text{PH}(N; k, k)$ is unsatisfiable, then $N \geq R(k; k)$ and the clauses of $\text{PH}(R(k; k); k, k)$ are contained in $\text{PH}(N; k, k)$. This means that $2^{R(k;k)^2}$

steps are always sufficient for a tree-like refutation of $\textsc{Ph}(N;k,k)$. Thus, any lower bound of the form $2^{h(k)}$ even for simple tree-like resolution implies $\sqrt{h(k)} \leq R(k;k)$. Proving a non-trivial lower bound requires a better understanding of the value of $R(k;k)$ itself. Indeed, the strength of our conditional lower bound from Section 4 depends on how close the lower and upper bound for $R(k;k)$ are.

Besides the problem of turning our lower bound into an unconditional one, a natural open question is whether the upper bound in Theorem 2 can be improved to polynomial with respect to formula size.

7 Acknowledgement

We thank the anonymous referees for comments that 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. 5, 23

[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

[3] Stephen Bellantoni, Toniann Pitassi, and Alasdair Urquhart. Approximation and small-depth Frege proofs. *Siam Journal of Computing*, 21:1161–1179, 1992. 6

[4] Peter Clote. Cutting planes and Frege proofs. *Information and Computation*, 121(1):103–122, 1995. 2

[5] Devdatt P. Dubhashi and Alessandro Panconesi. *Concentration of measure for the Analysis of Randomized Algorithms*. Cambridge University Press, 2009. 25

[6] Paul Erdős. Graph theory and probability II. *Canadian Journal of Mathematics*, 13:346–352, 1961. 5, 13, 23

[7] Paul Erdős and George Mills. Some bounds for the Ramsey-Paris-Harrington numbers. *Journal of Combinatorial Theory, Series A*, 30(1):53–70, 1981. 2, 4, 6, 11, 13

[8] Jack E. Graver and James Yackel. Some graph theoretic results associated with Ramsey's theorem. *Journal of Combinatorial Theory*, 4(2):125–175, 1968. 5

[9] 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. 2, 3

[10] Johan Håstad. Almost optimal lower bounds for small depth circuits. In *Proceedings of the 18th ACM Symposium on Theory of Computing*, pages 6–20. ACM, 1986. 3

[11] Jussi Ketonen and Robert M. Solovay. Rapidly growing Ramsey functions. *Annals of Mathematics*, 113:267–314, 1981. 4

[12] 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. 5, 17, 23

[13] Jan Krajíček. Lower bounds to the size of constant-depth propositional proofs. *Journal of Symbolic Logic*, 59(1):73–86, 1994. 3

[14] Jan Krajíček. On the weak pigeonhole principle. *Fundamenta Mathematicae*, 170(1-3):123–140, 2001. 2, 3, 5, 11, 12

[15] Jan Krajíček. A note on propositional proof complexity of some Ramsey-type statements. *Archive for Mathematical Logic*, 50:245–255, 2011. 10.1007/s00153-010-0212-9. 2, 5, 11

[16] Balakrishnan Krishnamurthy and Robert N. Moll. Examples of hard tautologies in the propositional calculus. In *STOC 1981, 13th ACM Symposium on Th. of Computing*, pages 28–37, 1981. 5

[17] Martin Loebl and Jaroslav Nešetřil. An unprovable Ramsey-type theorem. *Proceedings of the American Mathematical Society*, 116(3):819–824, 1992. 3

[18] 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. 19

[19] George Mills. Ramsey-Paris-Harrington numbers for graphs. *Journal of Combinatorial Theory, Series A*, 38(1):30 – 37, 1985. 2, 5, 6, 7, 8, 11, 18, 21, 22, 26

[20] 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. 19

[21] Pavel Pudlák. Ramsey's theorem in Bounded Arithmetic. In *Proceedings of Computer Science Logic 1990*, pages 308–317, 1991. 2, 5, 18

[22] Pavel Pudlák. A lower bound on the size of resolution proofs of the Ramsey theorem. *Information Processing Letters*, 14–15(112):610–611, 2013. 5

[23] 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. 11, 26

[24] Nathan Segerlind, Samuel R. Buss, and Russell Impagliazzo. A switching lemma for small restrictions and lower bounds for k-DNF resolution. *SIAM J. Comput.*, 33(5):1171–1200, 2004. 26

[25] Joel Spencer. Asymptotic lower bounds for Ramsey functions. *Discrete Mathematics*, 20:69–76, 1977. 5