A feasible interpolation for random resolution

Jan Krajíček

Faculty of Mathematics and Physics
Charles University in Prague

Abstract

Random resolution, defined by Buss, Kolodziejczyk and Thapen (JSL, 2014), is a sound propositional proof system that extends the resolution proof system by the possibility to augment any set of initial clauses by a set of randomly chosen clauses (modulo a technical condition). We show how to apply the general feasible interpolation theorem for semantic derivations of Krajíček (JSL, 1997) to random resolution. As a consequence we get a lower bound for random resolution refutations of the clique-coloring formulas.

Assume $A_1, \dots, A_m, B_1, \dots, B_\ell$ is an unsatisfiable set of clauses in variables partitioned into three disjoint sets $\mathbf{p}$, $\mathbf{q}$ and $\mathbf{r}$, with clauses A_i containing only variables from $\mathbf{p}$ and $\mathbf{q}$ while clauses B_j contain only variables from $\mathbf{p}$ or $\mathbf{r}$.

Feasible interpolation for resolution [6, Thm.6.1] says that if the set has a resolution refutation with k clauses then there is a circuit of size[1] $kn^{O(1)}$, where n is the number of variables $\mathbf{p}$, with inputs $\mathbf{p}$ that outputs 1 on all $\mathbf{p} := \mathbf{a} \in \{0,1\}^n$ for which $\bigwedge_i A_i(\mathbf{a}, \mathbf{q})$ is satisfiable and 0 on all $\mathbf{a}$ for which $\bigwedge_j B_j(\mathbf{a}, \mathbf{r})$ is satisfiable. Moreover, if variables $\mathbf{p}$ occur only positively in clauses A_i then the interpolating circuit can be required to be monotone.

The monotone version can then be applied to the clique-coloring clauses [6, Def.7.1] where there are $\binom{n}{2}$ variables $\mathbf{p}$ indexed by unordered pairs i, j of different elements from $[n] := \{1, \dots, n\}$, $\omega \cdot n$ variables $\mathbf{q}$ indexed by elements of $[\omega] \times [n]$ and $n \cdot \xi$ variables $\mathbf{r}$ indexed by elements of $[n] \times [\xi]$, with $n \geq \omega > \xi \geq 1$:

1. $\{q_{u1}, \dots, q_{un}\}$, for each $u \in [\omega]$
2. $\{\neg q_{ui}, \neg q_{vi}\}$, for $u \neq v \in [\omega]$ and $i \in [n]$
3. $\{\neg q_{ui}, \neg q_{vj}, p_{ij}\}$, for $u \neq v \in [\omega]$ and $i \neq j \in [n]$
4. $\{r_{i1}, \dots, r_{i\xi}\}$, for each $i \in [n]$
5. $\{\neg r_{iu}, \neg r_{iv}\}$, for each $u \neq v \in [\xi]$ and $i \in [n]$

[1] The bound $kn^{O(1)}$ is derived from a general interpolation theorem for semantic derivations whose framework we also use below; a bit better bound (proportional to the size of the refutation and hence $O(kn)$) can be proved by resolution specific arguments.

6. $\{\neg r_{iv}, \neg r_{jv}, \neg p_{ij}\}$, for $v \in [\xi]$ and $i \neq j \in [n]$

The clauses in the first three items comprise the set $Clique_{n,\omega}$ and the clauses in the last three items comprise the set $Color_{n,\xi}$, They have only variables $\mathbf{p}$ in common and these occur only positively in $Clique_{n,\omega}$. The assignments $\mathbf{a}$ to $\mathbf{p}$ for which $Clique_n, \omega(\mathbf{a}, \mathbf{q})$ is satisfiable can be identified with undirected graphs on $[n]$ without loops and having a clique of size at least ω while those $\mathbf{a}$ for which $Color_{n,\xi}(\mathbf{a}, \mathbf{r})$ is satisfiable are ξ-colorable graphs. Hence $Clique_{n,\omega} \cup Color_{n,\xi}$ is unsatisfiable as $\xi < \omega$ and the monotone feasible interpolation combined with the Alon-Boppana [1] exponential lower for monotone circuits separating the two classes of graphs implies that all resolution refutations of the set must have an exponential number of clauses, cf.[6, Sec.7].

Buss, Kolodziejczyk and Thapen [3, Sec.5.2] defined the notion of δ-random resolution (the definition is attributed in [3] to S. Dantchev). The motivation for introducing the proof system came from bounded arithmetic; the proof system simulates an interesting theory. A *δ-random resolution refutation distribution* of a set of clauses Ψ ([3] considers only narrow clauses because of the specific problem studied there) is a random distribution $(\pi_{\mathbf{s}}, \Delta_{\mathbf{s}})_{\mathbf{s}}$ such that $\pi_{\mathbf{s}}$ is a resolution refutation of $\Psi \cup \Delta_{\mathbf{s}}$, and where the following technical condition is satisfied:

- any fixed truth assignment to all variables satisfies the set of clauses $\Delta_{\mathbf{s}}$ with probability at least $1 - \delta$.

The number of clauses in such a random refutation is the maximal number of clauses among all $\pi_{\mathbf{s}}$. Note that it is a sound proof system in the sense that any refutable set Ψ is indeed unsatisfiable: if $\mathbf{a}$ would be a satisfying assignment for Ψ then, by the condition above, $\mathbf{a}$ would satisfy also some $\Delta_{\mathbf{s}}$ and hence $\pi_{\mathbf{s}}$ would be a resolution refutation of a satisfiable set of clauses which is impossible. Variants of the definition of this proof system and its properties are studied in [10].

The presence of the clauses $\Delta_{\mathbf{s}}$ spoils the separation of the $\mathbf{q}$ and $\mathbf{r}$ variables in initial clauses and this seems to prohibit any application of the feasible interpolation method. The point of this note is to show that, in fact, the construction behind the general feasible interpolation theorem [6] for semantic derivations based on communication complexity does apply here fairly straightforwardly.

We recall some feasible interpolation preliminaries from [6] in Section 1. In Section 2 we prove monotone feasible interpolation for random resolution and this will yield the following lower bound for random resolution refutations of the clique-coloring clauses.

Theorem 0.1 *Let $n \geq \omega > \xi \geq 1$ and $\xi^{1/2}\omega \leq 8n/\log n$. Assume $\delta < 1$ and let $(\pi_{\mathbf{s}}, \Delta_{\mathbf{s}})_{\mathbf{s}}$ be a δ-random resolution refutation distribution of $Clique_{n,\omega} \cup Color_{n,\xi}$ with k clauses. Put $d := \max_{\mathbf{s}} |\Delta_{\mathbf{s}}|$.*

Then:

1. *If $d\delta < 1$ then $k \geq (1 - d\delta^{1/2})n^{\Omega(\xi^{1/2})}$.*

2. $k \geq \min(1/(2\delta^{1/2}), n^{\Omega(\xi^{1/2})})$.

The proof of this theorem will be given at the end of Section 2. We only remark that for tree-like refutations a feasible interpolation via ordinary randomized Karchmer-Wigderson protocols follows from [6] immediately and it yields an exponential lower bound for formulas formalizing Hall's theorem as described in [7, Sec.4].

We will give below a detailed formulation of constructions from [6] needed here but we will not repeat the arguments from that paper. For more general background on proof complexity the reader may consult [5, 9].

1 Feasible interpolation via protocols

We review the needed material from [6] just for the case of monotone interpolation and the clique-coloring clauses (but it is quite representative). Identify undirected graphs without loops on $[n]$ with strings from $\{0,1\}^{\binom{n}{2}}$. Note that indices of $\mathbf{p}$ variables correspond to pairs of different vertices and hence the truth value an assignment $\mathbf{a}$ gives to a particular $\mathbf{p}$-variable indicates whether or not the edge corresponding to the variable is in the graph $\mathbf{a}$.

Let $U \subseteq \{0,1\}^{\binom{n}{2}}$ be the set of graphs having a clique of size at least ω and let $V \subseteq \{0,1\}^{\binom{n}{2}}$ be the set of ξ-colorable graphs. Let the monotone Karchmer-Wigderson function $KW^m(u,v)$ be a multi-function defined on $U \times V$ whose valid value on a pair $(u,v) \in U \times V$ is any edge (i.e. unordered pair $i \neq j \in [n]$) that is present in u but not in v.

The method in [6] extracts from a resolution refutation of $Clique_{n,\omega} \cup Color_{n,\xi}$ a protocol for a communication between two players, one holding u and the other one v, who want to find a valid value for $KW^m(u,v)$. The protocols in [6] are, however, more complex than just binary trees as in the ordinary communication complexity set-up of [4].

A monotone protocol for computing KW^m in the sense of [6, Def.2.2] is a 4-tuple (G, lab, F, S) satisfying the following conditions:

1. G is a directed acyclic graph that has one root (the in-degree 0 node) denoted $\emptyset$.

2. The nodes with the out-degree 0 are leaves and they are labelled by the mapping lab. The mapping lab assigns an element of $[\binom{n}{2}]$ (i.e., a potential edge) to each leaf in G.

3. $S(u,v,x)$ is a function (called the strategy) that assigns to a node $x \in G$ and a pair $u \in U$ and $v \in V$ a node $S(u,v,x)$ reachable from the node x by one edge.

4. For every $u \in U$ and $v \in V$, $F(u,v) \subseteq G$ is a set (called the consistency condition) satisfying:

    (a) $\emptyset \in F(u,v)$,

(b) $x \in F(u,v) \longrightarrow S(u,v,x) \in F(u,v)$,

(c) if $x \in F(u,v)$ is a leaf and $\mathsf{lab}(x) = \{i,j\}$, then $u_{i,j} = 1 \wedge v_{i,j} = 0$ holds.

The *size* of (G, lab, F, S) is the cardinality of G and its *communication complexity* is the minimal t such that for every $x \in G$ the communication complexity for the players (one knowing u and x, the other one v and x) to decide $x \in_? F(u,v)$ or to compute $S(u,v,x)$ is at most t.

Put $s := n \cdot \omega$ and identify strings from $\{0,1\}^s$ with assignments to $\mathbf{q}$-variables, and similarly put $t := n \cdot \xi$ and identify strings from $\{0,1\}^t$ with assignments to $\mathbf{r}$-variables. For any $u \in U$ fix $q^u \in \{0,1\}^s$ such that (u, q^u) satisfies all clauses from $Clique_{n,\omega}$ and for $v \in V$ fix $r^v \in \{0,1\}^t$ such that (v, r^v) satisfies all clauses of $Color_{n,\xi}$.

The protocol (G, lab, F, S) for KW^m constructed in [6, Thm.5.1 and Thm.6.1] from a resolution refutation π of $Clique_{n,\omega} \cup Color_{n,\xi}$ having k steps has $k + \binom{n}{2}$ nodes: k nodes corresponding to the clauses of π are the inner nodes and $\binom{n}{2}$ other nodes are the leaves and these are labelled by the $\binom{n}{2}$ possible values of the multi-function KW^m. The consistency condition $x \in F(u,v)$ for a node x corresponding to a clause C of π is defined by the condition that the assignment (v, q^u, r^v) falsifies C, and for a leaf by the condition that the label is a valid value of KW^m for the pair (u,v). The strategy S (whose exact definition we do not need) navigates from the root (the end-clause of π) through π towards the initial clauses and the construction shows that sooner or later it encounters a situation that allows it to compute a valid value of KW^m and move to the leaf with the appropriate label. The construction is fairly general and we shall formulate in Theorem 1.1 its one particular feature.

For a set Δ of clauses in variables $\mathbf{p}, \mathbf{q}$ and $\mathbf{r}$ define a multifunction F_Δ on $U \times V$ whose valid value on a pair (u,v) is any valid value of $KW^m(u,v)$ and also a new value $\bot$ *provided* that (v, q^u, r^v) falsifies some clause in Δ. Note the similarity of the condition permitting the value $\bot$ with the consistency condition in the protocol just discussed.

Now we recall a particular fact about the existence of protocols provided by the constructions in the proofs of [6, Thm.5.1 and Thm.6.1] (again we restrict ourselves to the clique-coloring formulas and the monotone case).

Theorem 1.1 ([6])

Assume that Δ is a set of clauses in variables $\mathbf{p}, \mathbf{q}$ and $\mathbf{r}$ and that π is a resolution refutation of the set $Clique_{n,\omega} \cup Color_{n,\xi} \cup \Delta$ and that π has k steps.

Then there is a protocol (G, lab, F, S) for F_Δ of size $k + \binom{n}{2}$ whose strategy has the communication complexity at most $2 + 2\log n$ and whose consistency condition has the communication complexity 2.

Further, the existence of a protocol for KW^m on $U' \times V' \subseteq U \times V$ of size k' and monotone communication complexity $O(\log n)$ implies the existence of a monotone circuit of size at most $k' \cdot n^{O(1)}$ separating U' from V'.

The part about the existence of a circuit is in [6] proved using a result from [11]; a stand alone proof can be found in [8, Sec.2.4].

2 The lower bound

For $(u,v) \in U \times V$ define $w(u,v) := (v, q^u, r^v)$ and for $X \subseteq U$ and $Y \subseteq V$ define $W(X,Y) \subseteq \{0,1\}^{\binom{n}{2}} \times \{0,1\}^s \times \{0,1\}^t$ to be the set of all tuples $w(u,v)$ for $(u,v) \in X \times Y$.

Assume $(\pi_{\mathbf{s}}, \Delta_{\mathbf{s}})_{\mathbf{s}}$ is a δ-random resolution refutation distribution of clauses $Clique_{n,\omega} \cup Color_{n,\xi}$ having k steps. For a sample $\mathbf{s}$ define the set $Bad_{\mathbf{s}} \subseteq U \times V$ to be the set of all pairs $(u,v) \in U \times V$ such that the assignment $w(u,v)$ falsifies some clause in $\Delta_{\mathbf{s}}$. An averaging argument implies the following statement.

Lemma 2.1 *There exists sample* $\mathbf{s}$ *such that* $|Bad_{\mathbf{s}}| < \delta |U \times V|$.

Fix for the rest of the paper one such $\mathbf{s}$. Denote by (G, lab, F, S) the protocol for $F_{\Delta_{\mathbf{s}}}$ constructed from $\pi_{\mathbf{s}}$ as described in Theorem 1.1. Put $d := |\Delta_{\mathbf{s}}|$.

Lemma 2.2 *There exists* $U' \subseteq U$ *and* $V' \subseteq V$ *such that:*

1. $(U' \times V') \cap Bad_{\mathbf{s}} = \emptyset$.
2. $|U'| \geq (1 - d\delta^{1/2})|U|$ *and* $|V'| \geq (1 - d\delta^{1/2})|V|$.

Proof :

Claim 1: *The set* $Bad_{\mathbf{s}}$ *is a union of at most* d' *rectangles* $U_i \times V_i \subseteq U \times V$, *for* $1 \leq d' \leq d$.

For a clause D let $False(D)$ is the set of all $(u,v) \in U \times V$ such that $w(u,v)$ falsifies D. We have that

$$Bad_{\mathbf{s}} = \bigcup_{D \in \Delta_{\mathbf{s}}} False(D) \ .$$

But for each of at most d possible D the set $False(D)$ is a combinatorial rectangle as it consists of all pairs $(u,v) \in U \times V$ satisfying two separate conditions for u and v: that q^u makes all **q**-literals in D false and that v, r^v makes all **p**- and **r**-literals in D false.

Let μ_i be the measure of $U_i \times V_i$ in $U \times V$ (and so $\mu_i < \delta$). The following is obvious.

Claim 2: *For each* $i \leq d'$, *either* $|U_i| \leq \mu_i^{1/2}|U|$ *or* $|V_i| \leq \mu_i^{1/2}|V|$.

We are now ready to prove the lemma. Consider the following process. For $i = 1, \ldots, d'$ delete from U all elements in U_i, if $|U_i| \leq \mu_i^{1/2}|U|$, otherwise delete from V all elements of V_i. Let U' and V' be what remains of U and V, respectively. Because we deleted one side of every rectangle $U_i \times V_i$, all of them have the empty intersection with $U' \times V'$.

The measure of $U \setminus U'$ in U, as well as the measure of $V \setminus V'$ in V, is bounded above by $\sum_{i \leq d'} \mu_i^{1/2} < d\delta^{1/2}$.

q.e.d.

Lemma 2.3 *There exists a monotone protocol for KW^m on $U' \times V'$ of size at most $k + \binom{n}{2}$ and of communication complexity at most $O(\log n)$.*

Proof :

Take the protocol (G, lab, F, S) for $F_{\Delta_{\mathbf{s}}}$ described before Lemma 2.2. By the definition of the sets U' and V' the multifunction $F_{\Delta_{\mathbf{s}}}$ restricted to $U' \times V'$ is just KW^m (the condition permitting the extra value $\perp$ is never satisfied).

q.e.d.

Proof of Theorem 0.1:

The proof of the $n^{\Omega(\xi^{1/2})}$ lower bound from [1] for monotone circuits separating U from V culminates by comparing two quantities with the sizes of U and V, respectively (see the elementary presentation in [2, Sec.4.3]). The same argument applies also to separations of any $U' \subseteq U$ from any $V' \subseteq V$ and the resulting lower bound just gets multiplied by the smaller of the two measures $|U'|/|U|$ and $|V'|/|V|$.

By Lemmas 2.2 and 2.3 we have two sets U', V' of relative measures at least $(1 - d\delta^{1/2})$ and a monotone protocol for KW^m on them of the size at most $k + \binom{n}{2}$ and communication complexity $O(\log n)$. By Theorem 1.1 this yields a monotone circuit separating U' from V' of size $kn^{O(1)}$. Hence it must hold:

$$kn^{O(1)} \ \geq (1 - d\delta^{1/2}) n^{\Omega(\xi^{1/2})}$$

which entails the first inequality in Theorem 0.1. The second follows from the first one by estimating $d \leq k$: if $k \leq 1/(2\delta^{1/2})$ then the factor $(1 - d\delta^{1/2})$ is at least $1/2$ and the lower bound $n^{\Omega(\xi^{1/2})}$ follows.

q.e.d.

Acknowledgements: I thank E. Jeřábek, P. Pudlák and N. Thapen for comments on early versions of this paper, and the anonymous referee for suggestions improving the presentation.

References

[1] N. Alon and R. Boppana, The monotone circuit complexity of Boolean functions, *Combinatorica*, **7(1)**, (1987), pp.1-22.

[2] R. Boppana and M. Sipser, The complexity of finite functions, in: Handbook of Theoretical Computer Science, (1990), pp.759–804. Elsevier Science Publishers.

[3] S. R. Buss, L. Kolodziejczyk and N. Thapen, Fragments of approximate counting, *J. of Symbolic Logic*, Vol **79:2**, (2014), pp.496-525.

[4] M. Karchmer and A. Wigderson, Monotone circuits for connectivity require super - logarithmic depth, in: *Proc. 20^{th} Annual ACM Symp. on Theory of Computing*, (1988), pp.539-550. ACM Press.

[5] J. Krajíček, *Bounded arithmetic, propositional logic, and complexity theory*, Encyclopedia of Mathematics and Its Applications, Vol. **60**, Cambridge University Press, (1995).

[6] J. Krajíček, Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic, *J. Symbolic Logic*, **62(2)**, (1997), pp. 457-486.

[7] J. Krajíček, Interpolation by a game, *Mathematical Logic Quarterly*, **44(4)**, (1998), pp.450-458.

[8] Krajíček, J., *Propositional proof complexity I.*, lecture notes, (2003), Charles University.
Available at `http://www.karlin.mff.cuni.cz/krajicek/ds1.ps`

[9] P. Pudlák, The lengths of proofs, in: Handbook of Proof Theory, S.R. Buss ed., Elsevier, (1998), pp.547-637.

[10] P. Pudlák and N. Thapen, Random resolution refutations, preprint, (2016).

[11] A. A. Razborov, Unprovability of lower bounds on the circuit size in certain fragments of bounded arithmetic, *Izvestiya of the R.A.N.*, **59(1)**, (1995), pp.201-224.

Mailing address:

Department of Algebra
Faculty of Mathematics and Physics
Charles University
Sokolovská 83, Prague 8, CZ - 186 75
The Czech Republic
`krajicek@karlin.mff.cuni.cz`