Interpolation and approximate semantic derivations

Jan Krajíček*

Mathematical Institute†
Academy of Sciences, Prague

Abstract

We show that the feasible interpolation property is robust for some proof systems but not for other.

Let $A_1, \ldots, A_m \subseteq \{0,1\}^n$. A *semantic derivation*, defined in [6], of $B \subseteq \{0,1\}^n$ from A_i's is a sequence $C_1, \ldots, C_k$ of subsets of $\{0,1\}^n$ such that $C_k = B$ and each C_j is either one of A_i's or derived from some earlier C_{j_1}, C_{j_2}, $j_1, j_2 < j$ by the semantic rule: E, F infer G iff $G \supseteq E \cap F$.

Of course, B can be derived from A_i's iff $B \supseteq \bigcap_i A_i$, in which case $k-1$ steps suffice. However, if we add a condition that all C_j's are from some class $\mathcal{X} \subseteq \exp(\{0,1\}^n)$ (tacitly assuming that A_i's and B are in $\mathcal{X}$) then this trivial derivation may not be possible anymore. We call derivations restricted to $\mathcal{X}$ $\mathcal{X}$-derivations.

Example 1: Let $\mathcal{R} \subseteq \exp(\{0,1\}^n)$ be the class of sets definable by a clause. The $\mathcal{R}$-derivations are a semantic version of resolution.

Example 2: Let $\mathcal{CP}_M \subseteq \exp(\{0,1\}^n)$ be the class of sets definable by an integer linear inequality with all coefficients bounded in absolute value by M. This is a semantic version of cutting planes proof system with bounded coefficients.[1]

---

*Partially supported by grant # A 101 99 01 of the Academy of Sciences of the Czech Republic and by project LN00A056 of The Ministry of Education of the Czech Republic.

†Also member of the Institute for Theoretical Computer Science of the Charles University. A part of this work was done while visiting the Mathematical Institute, Oxford.

[1]The restriction to bounded coefficients is just for convenience, allowing as to talk only about boolean communication complexity later on. The general case can be treated similarly using the real communication complexity, cf. [8].

Example 3: Let $\mathcal{PC}_d \subseteq \exp(\{0,1\}^n)$ be the class of sets definable by a polynomial of degree at most d over some fixed finite prime field $\mathbf{F}_p$. This is a semantic version of polynomial calculus.

The reason for introduction of semantic derivations in [6] was that for some proof systems (those suspectable to an approach to feasible interpolation via communication complexity) feasible interpolation can be derived for the semantic version of the system (we use this term informally only). In particular, both $\mathcal{R}$-derivations and $\mathcal{CP}_M$-derivations admit monotone feasible interpolation (and hence also exponential lower bounds to the size of proofs can be proved) and this can be extended to their various generalizations, cf. [7, 6, 8]. Feasible interpolation, albeit not monotone, holds also for $\mathcal{PC}_d$. This is because one inference using the semantic rule for $\mathcal{PC}_d$ can be simulated in polynomial calculus of degree at most $2(p-1)d$ (cf. [3, Thm.2.6]), and polynomial calculus admits feasible interpolation by [4]. However, the feasible interpolation for polynomial calculus does not come from properties of sets definable by low degree polynomials (such as the low communication complexity in the sense of Definition 2) but from a global property of the proof system; namely, the set of polynomials derivable in a fixed degree forms a vector space with particular properties. We shall show that the feasible interpolation is a robust property for $\mathcal{X}$-derivations, if it is proved via communication complexity method of [6]. The qualification *robust* is formalized be the following notion.

Definition 1 *Let $\epsilon \geq 0$ be arbitrary and let $\mathcal{X} \subseteq \exp(\{0,1\}^n)$ be a class of sets. An ϵ-approximate $\mathcal{X}$-derivation is a semantic derivation using sets $C \subseteq \{0,1\}^n$ such that there is $D \in \mathcal{X}$ for which $|C \triangle D| \leq \epsilon 2^n$ ($C \triangle D$ is the symmetric difference).*

Let U, V be two NP sets of x's from $\{0,1\}^n$. We assume that U and V are defined by 3CNF formulas α and β in variables $x_1, \ldots, x_n$ and $y_1, \ldots, y_s$, and $x_1, \ldots, x_n$ and $z_1, \ldots, z_t$ respectively. That is, $\overline{x} \in U$ iff there is $\overline{y}$ such that $(\overline{x}, \overline{y})$ satisfies α, and similarly for V, $(\overline{x}, \overline{z})$ and β.

To formulate the theorem and its proof we need to recall a notion from [6] related to this situation.

Definition 2 ([6, Def.4.3]) *Let $A \subseteq \{0,1\}^{n+s+t}$, and let $u, v \in \{0,1\}^n$, $q^u \in \{0,1\}^s$ and $r^v \in \{0,1\}^t$. Consider three tasks:*

1. *Decide whether $(u, q^u, r^v) \in A$.*

2. *Decide whether* $(v, q^u, r^v) \in A$.

3. *If* $(u, q^u, r^v) \in A \not\equiv (v, q^u, r^v) \in A$ *find* $i \leq n$ *such that* $u_i \neq v_i$.

These tasks can be solved by two players, one knowing u, q^u *and the other one knowing* v, r^v. *The communication complexity of* A, $CC(A)$, *is the minimal number of bits they need to exchange in the worst case in solving any of these three tasks.*

Consider one task:

4. *If* $(u, q^u, r^v) \in A$ *and* $(v, q^u, r^v) \notin A$ *either find* $i \leq n$ *such that* $u_i = 1 \wedge v_i = 0$, *or learn that there is some* u' *satisfying* $u' \geq u$ *(i.e. every bit satisfies* $u'_i \geq u_i$*) and* $(u', q^u, r^v) \notin A$.

(Note that the two players are not supposed to find such u', *and that the two cases in 4. are not necessarily exclusive.)*

The monotone communication complexity of A *w.r.t.* U, $MCC_U(A)$, *is the minimal* $t \geq CC(A)$ *such that the task 4. can be solved communicating at most* t *bits in the worst case.*

Now we can give an interpolation theorem for approximate derivations. If the two NP sets U and V are disjoint, a proof of the disjointness is a proof of simultaneous unsatisfiability of the two 3CNFs defining the sets. In particular, a semantic derivation of $U \cap V = \emptyset$ is the derivation of $\emptyset$ from the sets defined by the 3-clauses of the two 3CNFs.

Theorem 3 *Let* $\epsilon \geq 0$ *be arbitrary and let* $\mathcal{X} \subseteq \exp(\{0,1\}^n)$ *be a class of sets. Assume that* U *and* V *are two disjoint NP sets, and that there is an* ϵ*-approximate* $\mathcal{X}$*-derivation of* $U \cap V = \emptyset$ *with* k *steps.*

1. *Assume that* $CC(C) \leq t$ *for any* $C \in \mathcal{X}$. *Then there exists a boolean circuit* D *of size at most* $(k + 2n)2^{O(t)}$, *and a set* $W \subseteq \{0,1\}^n$ *such that* $|W| \leq \epsilon k 2^n$ *and such that* D *separates* $U \setminus W$ *and* $V \setminus W$.

2. *Assume that* U *satisfies the following monotonicity condition: if* (u, q^u) *satisfies* α *and* $u' \geq u$ *then* (u', q^u) *satisfies* α. *Further assume that* $MCC_U(C) \leq t$ *for all* $C \in \mathcal{X}$. *Then there is a monotone boolean circuit* D *of size at most* $(k+n)2^{O(t)}$, *and a set* $W \subseteq \{0,1\}^n$ *such that* $|W| \leq \epsilon k 2^n$ *and such that* D *is constantly* 1 *on* $U \setminus W$ *and is constantly* 0 *on* $V \setminus W$.

Proof :

We shall assume that the reader is familiar with the argument in [6, Sec.5] proving the feasible interpolation for semantic derivations, and we only describe where it needs to be appended.

Two players, one given $u \in U$ and the other one $v \in V$, search for bit i such that $u_i \neq v_i$. They use a derivation of $U \cap V = \emptyset$ for this purpose, building a path through the derivation from the end line (set $\emptyset$) back to one of the initial sets, always progressing from the conclusion of an inference to one of its two hypotheses. Every set A on the path should have the property that $(u, q^u, r^v) \notin A$ as well as $(v, q^u, r^v) \notin A$ (this the players can decide using $CC(A)$ bits of communication).

As none of the initial sets has this property, sooner or later the players find A such that $(u, q^u, r^v) \in A \not\equiv (v, q^u, r^v) \in A$, and they find i such that $u_i \neq v_i$ using $CC(A)$ bits (via clause 3. of Definition 2). This strategy of the players can be turned into a boolean circuit of size $(k + 2n)^{O(t)}$ separating sets U and V, cf. [6, Thm.2.3].

Assume now that the derivation is not an $\mathcal{X}$-derivation but only ϵ-approximate $\mathcal{X}$-derivation. For any set A in the derivation let A^* be a canonically chosen set from $\mathcal{X}$ such that $|A \triangle A^*| \leq \epsilon 2^n$. Further assume that $\emptyset^* = \emptyset$ and that $A = A^*$ for all initial sets. The players proceed as before, but using sets A^* in place of A.

As long as both u, v are outside $W := \bigcup_A (A \triangle A^*)$, A runs over the k sets in the derivation, the players will find A^* such that $(u, q^u, r^v) \in A^* \not\equiv (v, q^u, r^v) \in A^*$ and consequently a bit i with $u_i \neq v_i$. Hence one gets a circuit separating $U \setminus W$ from $V \setminus W$.

The argument from [6, Sec.5] in the monotone case can be modified completely analogously.

q.e.d.

The monotone version is considered because there are exponential lower bounds for monotone circuits separating the set of graphs with a k-clique from $(k-1)$-colorable graphs (cf. [1]), while lower bounds for general circuits are known only under some unproven conjectures.

The hypothesis about the monotone communication complexity of sets in $\mathcal{X}$ is satisfied for $\mathcal{R}$ and $\mathcal{CP}_M$ (cf. [6]) and hence the theorem applies to ϵ-approximate versions of theses derivations. In particular, one gets lower bounds for such derivations. This is because the exponential circuit lower bound for monotone circuits separating the set of graphs with a clique of size

$k := \lfloor\sqrt{n}\rfloor + 1$ from the set of graphs that are k-colorable holds also if the circuit is allowed small error (the argument as presented in [2] literally says that no small monotone circuit can separate a lot of graphs from the first set from a lot of graphs from the second set). Hence, by an argument analogous to the lower bound proof in [6, Sec.7], one gets the following proposition.

Corollary 4 *Let U be the set of graphs on n vertices having a clique of size $\lfloor\sqrt{n}\rfloor + 1$, and let V be the set of $\lfloor\sqrt{n}\rfloor$-colorable graphs.*

Assume that $\epsilon \leq 2^{n^{(1/2-\Omega(1))}}$. Then:

1. *Every ϵ-approximate $\mathcal{R}$-derivation of $U \cap V = \emptyset$ must have at least $2^{\Omega(n^{1/4})}$ steps.*
2. *Every ϵ-approximate $\mathcal{CP}_M$-derivation of $U \cap V = \emptyset$ must have at least $\frac{2^{\Omega(n^{1/4})}}{M^{O(\log n)}}$ steps.*

Proof :

If $\epsilon \leq 2^{n^{(1/2-\Omega(1))}}$ and let W be a set of at most $\epsilon 2^{\binom{n}{2}}$ graphs on n vertices, then $\frac{|U \setminus W|}{|U|} = |U|^{(1-o(1))}$ and similarly for V. The argument in [2] then straightforwardly yields that every monotone circuit separating $U \setminus W$ from $V \setminus W$ must have size at least $2^{\Omega(n^{1/4})}$.

The MCC of $\mathcal{R}$-sets is $O(\log n)$ and of $\mathcal{CP}_M$-sets it is $O(\log(Mn) + \log(n)\log(Mn))$, by [6, Thms.6.1 and 6.4]. Using this in Theorem 3 yields upper bounds on the sizes of the separating circuits in terms of k, and comparing these with the lower bound $2^{\Omega(n^{1/4})}$ entails the lower bounds on k.

q.e.d.

Feasible interpolation of polynomial calculus does not transfer to feasible interpolation of approximate $\mathcal{PC}_d$-derivations. This can be seen as follows. Let $\alpha_1, \ldots, \alpha_k$ be any clauses that are unsatisfiable, and let $A_1, \ldots, A_k \subseteq \{0,1\}^n$ are the sets defined by these clauses. So $\bigcap_i A_i = \emptyset$. Take the trivial derivation: $A_1, A_1 \cap A_2, \ldots, A_1 \cap \ldots \cap A_k$. Each of the $k-1$ sets in this derivations are definable by a depth two formula of small size (there are $2k-1$ different subformulas other than literals in total). By the approximation method of [10, 11] there are polynomials f_i over $\mathbf{F}_p$ of degree at most $(p-1)^2\ell^2$ such that each set $V(f_i) := \{\overline{x} \in \{0,1\}^n \mid f_i(\overline{x}) = 0\}$ differs from $A_1 \cap \ldots \cap A_i$ in at most $2ke^{-\frac{\ell}{p}}2^n$ points, with $\ell \geq 1$ any parameter. In particular, the trivial derivation is ϵ-approximate $\mathcal{PC}_d$-derivation, if $\epsilon \geq 2ke^{-\frac{\sqrt{d}}{p(p-1)}}$.

A more general way of defining approximate derivations is as follows. Let $\mathcal{J} \subseteq \exp(\{0,1\}^n)$ be a non-empty class of sets closed downwards, i.e. $D \subseteq C \in \mathcal{J}$ implies $D \in \mathcal{J}$. In particular, $\emptyset \in \mathcal{J}$. A $\mathcal{J}$-approximate $\mathcal{X}$ derivation can use sets C such that there is $D \in \mathcal{X}$ for which $C \triangle D \in \mathcal{J}$. In the ϵ-approximate derivations one just takes for $\mathcal{J}$ sets of size at most $\epsilon 2^n$. It would be interesting to know if for some $\mathcal{J}$ the $\mathcal{J}$-approximate $\mathcal{PC}_d$-derivations have super-polynomial speed-up over $\mathcal{PC}_d$-derivations but still admit feasible interpolation. For example, if we take for $\mathcal{J}$ the sets that can be included in a degree d' hypersurface, then the $\mathcal{J}$-approximate $\mathcal{PC}_d$-derivations admit feasible interpolation as they are included in $\mathcal{PC}_{dd'}$-derivations (same argument as after Example 3).

If $\mathcal{X}$-derivations admit non-monotone feasible interpolation only rather than monotone, one gets at least a conditional lower bound for the number of steps in the derivations of the disjointness of two sets based on RSA as in [9]. The condition is then the conjectured security of RSA.

References

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

[2] Boppana, R., and Sipser, M., Complexity of finite functions. in:*Handbook of Theoretical Computer Science*, ed.J. van Leeuwen, (1990), pp.758-804.

[3] S. Buss, R. Impagliazzo, J. Krajíček, P. Pudlák, J. Sgall, and A. A. Razborov, Proof complexity in algebraic systems and bounded depth Frege systems with modular counting, *Computational Complexity*, **6**, (1996/1997), pp.256-298.

[4] M. Clegg, J. Edmonds, and R. Impagliazzo, Using the Groebner basis algorithm to find proofs of unsatisfiability, in: *Proceedings of the 28th ACM Symposium on Theory of Computing*, ACM Press. (1996), pp.174-183.

[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*, Vol.**62(2)**, (1997), pp.457-486.

[7] J. Krajíček, Discretely ordered modules as a first-order extension of the cutting planes proof system, *J. Symbolic Logic*, Vol.**63(4)**, (1998), pp.1582-1596.

[8] J. Krajíček, Interpolation by a game, *Mathematical Logic Quarterly*, Vol.**44(40)**, (1998), pp.450-458.

[9] J. Krajíček and P. Pudlák, Some consequences of cryptographical conjectures for S^1_2 and EF", *Information and Computation*, Vol. **140 (1)**, (January 10, 1998), pp.82-94.

[10] Razborov, A. A., Lower bounds on the size of bounded depth networks over a complete basis with logical addition, *Matem. Zametki*, **41(4)**, (1987), pp.598-607.

[11] Smolensky, R., Algebraic methods in the theory of lower bounds for Boolean circuit complexity, in: *Proc. 19th Ann. ACM Symp. on Th. of Computing*, (1987), pp. 77-82.

Mailing address:
Mathematical Institute
Academy of Sciences
Žitná 25
Prague 1, CZ - 115 67
The Czech Republic
`krajicek@math.cas.cz`