Computational Flows in Arithmetic

Amir Akbar Tabatabai

Institute of Mathematics
Academy of Sciences of the Czech Republic

November 16, 2017

Motivation

A proof is a flow of information from the assumptions to the conclusion!

Motivation

A proof is a flow of information from the assumptions to the conclusion! But what do we mean by information in this rough definition? There are different many interpretations. The minimal one is just the truth value which gets preserved by usual sound proofs. But there are more useful interpretations, as well.

Motivation

A proof is a flow of information from the assumptions to the conclusion! But what do we mean by information in this rough definition? There are different many interpretations. The minimal one is just the truth value which gets preserved by usual sound proofs. But there are more useful interpretations, as well.
The main one in the realm of proof theory is *the computational content* of a sentence.

Motivation

A proof is a flow of information from the assumptions to the conclusion! But what do we mean by information in this rough definition? There are different many interpretations. The minimal one is just the truth value which gets preserved by usual sound proofs. But there are more useful interpretations, as well.
The main one in the realm of proof theory is *the computational content* of a sentence. But what is the meaning of this computational content? We will interpret more formally the computational content of a sentence as the computational problem associated to the sentence and by *flowing*, we just mean the computational reductions.

Bounded Arithmetic

Let us define the minimum language and the minimum theory that we will use.

Definition

Let $\mathcal{L}$ be a first order language of arithmetic extending $\{0, 1, +, -, \cdot, \lfloor \frac{\cdot}{\cdot} \rfloor, \leq\}$. By $\mathcal{R}$ we mean the first order theory consisting of the axioms of commutative discrete ordered semirings (the usual axioms of commutative rings minus the existence of additive inverse plus the axioms to state that $\leq$ is a total discrete order such that $<$ is compatible with addition and multiplication with non-zero elements), plus the following defining axioms for $-$ and $\lfloor \frac{\cdot}{\cdot} \rfloor$:

$$(x \geq y \rightarrow (x - y) + y = x) \wedge (x < y \rightarrow x - y = 0)$$

$$((y + 1) \cdot \lfloor \frac{x}{y} \rfloor \leq x) \wedge (x - (y + 1) \cdot \lfloor \frac{x}{y} \rfloor < y + 1)$$

Bounded Arithmetic

Definition

Let Φ be a class that includes all quantifier-free formulas and is closed under all boolean operations. The hierarchy $\{\Sigma_k(\Phi), \Pi_k(\Phi)\}_{k=0}^{\infty}$ is defined as the following:

(*i*) $\Pi_0(\Phi) = \Sigma_0(\Phi)$ is the class Φ.

(*ii*) If $B(x) \in \Sigma_k(\Phi)$ then $\exists x \leq t\ B(x) \in \Sigma_k(\Phi)$ and $\forall x \leq t\ B(x) \in \Pi_{k+1}(\Phi)$.

(*iii*) If $B(x) \in \Pi_k(\Phi)$ then $\forall x \leq t\ B(x) \in \Pi_k(\Phi)$ and $\forall x \leq t\ B(x) \in \Sigma_{k+1}(\Phi)$.

Bounded Arithmetic

Definition

Let $\mathcal{A}$ be a set of quantifier-free axioms and Φ be a class of bounded formulas closed under substitution and subformulas. By the first order bounded arithmetic, $\mathfrak{B}(\Pi_k(\Phi), \mathcal{A})$ we mean the theory in the language $\mathcal{L}$ which consists of axioms $\mathcal{A}$, and the $\Pi_k(\Phi)$-induction axiom, i.e.

$$A(0) \wedge \forall x(A(x) \to A(x+1)) \to \forall x A(x)$$

where $A \in \Pi_k(\Phi)$.

Bounded Arithmetic

Definition

Let $\mathcal{A}$ be a set of quantifier-free axioms and Φ be a class of bounded formulas closed under substitution and subformulas. By the first order bounded arithmetic, $\mathfrak{B}(\Pi_k(\Phi), \mathcal{A})$ we mean the theory in the language $\mathcal{L}$ which consists of axioms $\mathcal{A}$, and the $\Pi_k(\Phi)$-induction axiom, i.e.

$$A(0) \wedge \forall x(A(x) \rightarrow A(x+1)) \rightarrow \forall x A(x)$$

where $A \in \Pi_k(\Phi)$.

Example

With our definition of bounded arithmetic, different kinds of theories can be considered as bounded theories of arithmetic, for instance $I\Delta_0$, S^k_n, T^k_n, $I\Delta_0 + \mathrm{EXP}$ and PRA are just some of the well-known examples.

Computational Reductions

Definition

Let $A(\vec{x})$ and $B(\vec{x})$ be some formulas in $\Pi_k(\Phi)$ and $\{F_i\}_{i=1}^k$ be a sequence of terms. By recursion on k, we will define $F = \{F_i\}_{i=1}^k$ as a deterministic $\Pi_k(\Phi)$-reduction from $B(\vec{x})$ to $A(\vec{x})$ and we will denote it by $A(\vec{x}) \leq_d^{F,k} B(\vec{x})$ when:

(*i*) If $A(\vec{x}), B(\vec{x})$ are in $\Pi_0(\Phi)$, we say that the empty sequence of functions is a deterministic reduction from B to A iff $\mathcal{B} \vdash A(\vec{x}) \to B(\vec{x})$.

(*ii*) If $A = \forall \vec{u} \leq \vec{p}(\vec{x}) C(\vec{x}, \vec{u})$, $B = \forall \vec{v} \leq \vec{q}(\vec{x}) D(\vec{x}, \vec{v})$ and $F = \{F_i\}_{i=1}^{k+1}$ is a sequence of terms, then $A(\vec{x}) \leq_d^{F,k+1} B(\vec{x})$ iff

$$\mathcal{B} \vdash \vec{v} \leq \vec{q}(\vec{x}) \to F_{k+1}(\vec{x}, \vec{v}) \leq \vec{p}(\vec{x})$$

Definition

$$F_{k+1}(\vec{x},\vec{v}) \leq \vec{p}(\vec{x}) \to C(\vec{x}, F_{k+1}(\vec{x},\vec{v})) \leq_d^{\hat{F},k} \vec{v} \leq \vec{q}(\vec{x}) \to D(\vec{x},\vec{v})$$

where $\hat{F} = \{F_i\}_{i=1}^k$.

(iii) If $A = \exists \vec{u} \leq \vec{p}(\vec{x}) C(\vec{x},\vec{u})$, $B = \exists \vec{v} \leq \vec{q}(\vec{x}) D(\vec{x},\vec{v})$ and $F = \{F_i\}_{i=1}^{k+1}$ is a sequence of terms, then $A(\vec{x}) \leq_d^{F,k+1} B(\vec{x})$ iff

$$\mathcal{B} \vdash \vec{u} \leq \vec{p}(\vec{x}) \to F_{k+1}(\vec{x},\vec{u}) \leq \vec{q}(\vec{x})$$

and

$$\vec{y} \leq \vec{p}(\vec{x}) \wedge C(\vec{x},u) \leq_d^{\hat{F},k} F_{k+1}(\vec{x},\vec{u}) \leq \vec{q}(\vec{x}) \wedge D(\vec{x}, F_{k+1}(\vec{x},\vec{u}))$$

where $\hat{F} = \{F_i\}_{i=1}^k$.

We say B is $(\Pi_k(\Phi), \mathcal{B})$-deterministicly reducible to A and we write $A \leq_d^{\Pi_k(\Phi)} B$, when there exists a sequence of terms F such that $A \leq_d^{F,k} B$.

Computational Flows

Definition

Let $A(\vec{x}), B(\vec{x}) \in \Pi_k(\Phi)$. A $(\Pi_k(\Phi), \mathcal{B})$-deterministic flow from $A(\vec{x})$ to $B(\vec{x})$ is the following data: A term $t(\vec{x})$, a formula $H(u, \vec{x}) \in \Pi_k(\Phi)$ and sequences of terms E_0, E_1, G_0, G_1 and $F(u)$ such that the following statements are provable in $\mathcal{B}$:

(*i*) $H(0, \vec{x}) \equiv_d^{(E_0, E_1)} A(\vec{x})$.

(*ii*) $H(t(x), \vec{x}) \equiv_d^{(G_0, G_1)} B(\vec{x})$.

(*iii*) $\forall u < t(x) H(u, \vec{x}) \leq_d^{F(u)} H(u+1, \vec{x})$.

If there exists a deterministic $(\Pi_k(\Phi), \mathcal{B})$-flow from $A(\vec{x})$ to $B(\vec{x})$ we will write $A(\vec{x}) \rhd_d^{(\Pi_k(\Phi), \mathcal{B})} B(\vec{x})$. Moreover, if Γ and Δ are sequents of formulas in $\Pi_k(\Phi)$, by $\Gamma \rhd_d^{(\Pi_k(\Phi), \mathcal{B})} \Delta$ we mean $\bigwedge \Gamma \rhd_d^{(\Pi_k(\Phi), \mathcal{B})} \bigvee \Delta$.

Theorem (Soundness-Completeness)

Let $\Gamma(\vec{x}) \cup \Delta(\vec{x}) \subseteq \Pi_k(\Phi)$ and $\mathcal{A} \subseteq \mathcal{B} \subseteq \mathfrak{B}(\Pi_k(\Phi), \mathcal{A})$. Then $\mathfrak{B}(\Pi_k(\Phi), \mathcal{A}) \vdash \Gamma(\vec{x}) \Rightarrow \Delta(\vec{x})$ iff $\Gamma \rhd_d^{(\Pi_k(\Phi), \mathcal{B})} \Delta$.

Theorem (Soundness-Completeness)

Let $\Gamma(\vec{x}) \cup \Delta(\vec{x}) \subseteq \Pi_k(\Phi)$ and $\mathcal{A} \subseteq \mathcal{B} \subseteq \mathfrak{B}(\Pi_k(\Phi), \mathcal{A})$. Then $\mathfrak{B}(\Pi_k(\Phi), \mathcal{A}) \vdash \Gamma(\vec{x}) \Rightarrow \Delta(\vec{x})$ iff $\Gamma \rhd_d^{(\Pi_k(\Phi), \mathcal{B})} \Delta$.

Proof Sketch

The completeness part is an easy consequence of the induction axiom in $\mathfrak{B}(\Pi_k(\Phi), \mathcal{A})$ and the fact that $\mathcal{B} \subseteq \mathfrak{B}(\Pi_k(\Phi), \mathcal{A})$.

Theorem (Soundness-Completeness)

Let $\Gamma(\vec{x}) \cup \Delta(\vec{x}) \subseteq \Pi_k(\Phi)$ and $\mathcal{A} \subseteq \mathcal{B} \subseteq \mathfrak{B}(\Pi_k(\Phi), \mathcal{A})$. Then $\mathfrak{B}(\Pi_k(\Phi), \mathcal{A}) \vdash \Gamma(\vec{x}) \Rightarrow \Delta(\vec{x})$ iff $\Gamma \rhd_d^{(\Pi_k(\Phi), \mathcal{B})} \Delta$.

Proof Sketch

The completeness part is an easy consequence of the induction axiom in $\mathfrak{B}(\Pi_k(\Phi), \mathcal{A})$ and the fact that $\mathcal{B} \subseteq \mathfrak{B}(\Pi_k(\Phi), \mathcal{A})$. For the soundness, we have to show that flows admit all rules. The crucial cases are $\exists L$ and the contraction rules.

Theorem (Soundness-Completeness)

Let $\Gamma(\vec{x}) \cup \Delta(\vec{x}) \subseteq \Pi_k(\Phi)$ and $\mathcal{A} \subseteq \mathcal{B} \subseteq \mathfrak{B}(\Pi_k(\Phi), \mathcal{A})$. Then $\mathfrak{B}(\Pi_k(\Phi), \mathcal{A}) \vdash \Gamma(\vec{x}) \Rightarrow \Delta(\vec{x})$ iff $\Gamma \rhd_d^{(\Pi_k(\Phi), \mathcal{B})} \Delta$.

Proof Sketch

The completeness part is an easy consequence of the induction axiom in $\mathfrak{B}(\Pi_k(\Phi), \mathcal{A})$ and the fact that $\mathcal{B} \subseteq \mathfrak{B}(\Pi_k(\Phi), \mathcal{A})$. For the soundness, we have to show that flows admit all rules. The crucial cases are $\exists L$ and the contraction rules. To have an idea, let us think about the contraction rule

$$cL\ \frac{\Gamma \Rightarrow \exists y \leq tA(y), \exists y \leq tA(y)}{\Gamma \Rightarrow \exists y \leq tA(y)}$$

To admit this rule it seems reasonable to reduce $\exists y \leq tA(y) \vee \exists y \leq tA(y)$ to $\exists y \leq tA(y)$ but this means that we have to choose between two witnesses which is not obvious without knowing the value of $A(y)$.

Computability of Characteristic Functions

To solve this problem and also the other ones, we will simulate the decision problem of A by a flow of reductions:

Computability of Characteristic Functions

To solve this problem and also the other ones, we will simulate the decision problem of A by a flow of reductions:

Theorem (Computability of Characteristic Functions)

Let $\{\Sigma_k(\Phi), \Pi_k(\Phi)\}_{k=0}^{\infty}$ be a hierarchy and $\mathcal{B}$ has characteristic terms for all $\phi \in \Phi$, then for any $\Psi \in \{\Pi_k(\Phi), \Sigma_k(\Phi)\}$ if $A(\vec{x}) \in \Psi$ then

$$\rhd_d^{(\Sigma_{k+1}(\Phi),\mathcal{B})} \exists i \leq 1 \left[(i = 0 \to A) \wedge (i = 1 \to \neg A)\right]$$

Computability of Characteristic Functions

To solve this problem and also the other ones, we will simulate the decision problem of A by a flow of reductions:

Theorem (Computability of Characteristic Functions)

Let $\{\Sigma_k(\Phi), \Pi_k(\Phi)\}_{k=0}^{\infty}$ be a hierarchy and $\mathcal{B}$ has characteristic terms for all $\phi \in \Phi$, then for any $\Psi \in \{\Pi_k(\Phi), \Sigma_k(\Phi)\}$ if $A(\vec{x}) \in \Psi$ then

$$\rhd_d^{(\Sigma_{k+1}(\Phi),\mathcal{B})} \exists i \leq 1 \left[(i = 0 \to A) \wedge (i = 1 \to \neg A)\right]$$

It reduces the problem of deciding A to the problem of deciding the value i which is definitely much easier to solve.

Applications

Let us apply the theorem to some familiar cases:

Theorem

Let $\Gamma(\vec{x}) \cup \Delta(\vec{x}) \subseteq \hat{U}_k$, *then* $I\hat{U}_k \vdash \Gamma(\vec{x}) \Rightarrow \Delta(\vec{x})$ *iff* $\Gamma \rhd_d^{(\hat{U}_k, \mathcal{R})} \Delta$.

Applications

Let us apply the theorem to some familiar cases:

Theorem

Let $\Gamma(\vec{x}) \cup \Delta(\vec{x}) \subseteq \hat{U}_k$, *then* $I\hat{U}_k \vdash \Gamma(\vec{x}) \Rightarrow \Delta(\vec{x})$ *iff* $\Gamma \rhd_d^{(\hat{U}_k, \mathcal{R})} \Delta$.

Theorem

Let $\Gamma(\vec{x}) \cup \Delta(\vec{x}) \subseteq \hat{\Pi}^b_k(\#_n)$, *then* $T^k_n \vdash \Gamma(\vec{x}) \Rightarrow \Delta(\vec{x})$ *iff* $\Gamma \rhd_d^{(\hat{\Pi}^b_k(\#_n), \mathrm{PV}(\#_n))} \Delta$. *Specifically, for* $n = 2$, $T^k_2 \vdash \Gamma(\vec{x}) \Rightarrow \Delta(\vec{x})$ *iff* $\Gamma \rhd_d^{(\hat{\Pi}^b_k, \mathrm{PV})} \Delta$.

Therefore, it is possible to decompose any proof of $A \in \hat{\Pi}^b_k$ in T^k_2, to an exponential-length sequence of polytime reductions provable in PV.

Generalized Local Search Problems

Define a generalized local search problem in the following way:

Definition

A formalized $(\Psi, \Lambda, \mathcal{B}, \prec, t)$-GLS problem consists of the following data:

(*i*) A term $N(x, s) \in \mathcal{L}_{\mathcal{B}}$.

(*ii*) A term $c(x, s) \in \mathcal{L}_{\mathcal{B}}$.

(*iii*) A predicate $F(x, s) \in \Psi$ which intuitively means that s is a feasible solution for the input x.

(*iv*) An initial term $i(x) \in \mathcal{L}_{\mathcal{B}}$.

(*v*) A goal predicate $G(x, s) \in \Lambda$.

(*vi*) An atomic predicate $\prec \in \mathcal{L}_{\mathcal{B}}$ as a well-ordering.

(*vii*) A bounding term $t(x)$.

Definition

such that $\mathcal{B}$ proves that $\prec$ is a total order and

$$\mathcal{B} \vdash \forall x\ F(x, i(x))$$

$$\mathcal{B} \vdash \forall xs\ (F(x, s) \to F(x, N(x, s)))$$

$$\mathcal{B} \vdash \forall xs\ (N(x, s) = s \vee c(x, N(x, s)) \prec c(x, s))$$

$$\mathcal{B} \vdash \forall xs\ (G(x, s) \leftrightarrow (N(x, s) = s \wedge F(x, s)))$$

$$\mathcal{B} \vdash \forall xs\ (G(x, s) \to s \leq t(x))$$

for some term t.
Moreover, if $\mathcal{L}_{\mathrm{PV}} \subseteq \mathcal{L}_{\mathcal{B}}$ and $t(x) = 2^{p(|x|)}$ for some polynomial p we show the GLS problem by $\mathrm{PLS}(\Psi, \Lambda, \prec, \mathcal{B})$ and if F is quantifier-free in the language of $\mathcal{B}$, G is quantifier-free in the language of PV we show the GLS problem by $\mathrm{PLS}(\prec, \mathcal{B})$. Finally if $\mathcal{B} = \mathrm{PV}$, then we write $\mathrm{PLS}(\prec)$.

GLS and Bounded Arithmetic

Using the soundness-completeness of the flow interpretation we will have:

Theorem

If $A \in \Pi_k(\Phi)$ *then* $\mathfrak{B}(\Pi_{k+1}(\Phi), \mathcal{B}) \vdash \forall x \exists y \leq t(x) A(x, y)$ *iff the search problem of finding* y *by* x *is reducible by a projection to an instance of a* $\mathrm{GLS}(\Pi_k(\Phi), \{A\}, \mathcal{B}, \leq, t)$ *provably in* $\mathcal{B}$.

GLS and Bounded Arithmetic

Using the soundness-completeness of the flow interpretation we will have:

Theorem

If $A \in \Pi_k(\Phi)$ *then* $\mathfrak{B}(\Pi_{k+1}(\Phi), \mathcal{B}) \vdash \forall x \exists y \leq t(x) A(x, y)$ *iff the search problem of finding* y *by* x *is reducible by a projection to an instance of a* $\mathrm{GLS}(\Pi_k(\Phi), \{A\}, \mathcal{B}, \leq, t)$ *provably in* $\mathcal{B}$.

This characterization just unwinds one quantifier and puts the rest into the feasibility condition.

GLS and Bounded Arithmetic

Using the soundness-completeness of the flow interpretation we will have:

Theorem

If $A \in \Pi_k(\Phi)$ *then* $\mathfrak{B}(\Pi_{k+1}(\Phi), \mathcal{B}) \vdash \forall x \exists y \leq t(x) A(x, y)$ *iff the search problem of finding* y *by* x *is reducible by a projection to an instance of a* $\mathrm{GLS}(\Pi_k(\Phi), \{A\}, \mathcal{B}, \leq, t)$ *provably in* $\mathcal{B}$.

This characterization just unwinds one quantifier and puts the rest into the feasibility condition.
We can also reprove the following characterization:

Corollary. [BB]

For all $l \leq k$, $\forall\Sigma^b_{l+1}(T_2^{k+1}) \equiv \mathrm{PLS}(\Pi^b_k, \Pi^b_l, \mathrm{PV}, \leq)$.

Game Induction

Definition

Fix a language $\mathcal{L}$. An instance of the (j,k)-game induction principle $GI^j_k(\mathcal{L})$ is given by size parameters a and b, a uniform sequence $G_0,\ldots,G_{a-1}$ of open (quantifier-free) relations, a term V and a uniform sequence $W_0,\ldots,W_{a-2}$ of terms. The instance $GI(G,V,W,a,b)$ states that, interpreting $G_0,\ldots,G_{a-1}$ as k-turn games in which all moves are bounded by b, the following cannot all be true:

(*i*) Deciding the winner of game G_0 depends only on the first j moves,

(*ii*) Player B can always win G_0 (expressed as a $\Pi_j(open)$ property.)

(*iii*) For $i=0,\ldots,a-2$, W_i gives a deterministic reduction of G_{i+1} to G_i,

(*iv*) V is an explicit winning strategy for Player A in G_{a-1}.

Game Induction and Bounded Arithmetic

Using the soundness-completeness again, we can prove the following characterization:

Theorem

Let $\mathcal{B}$ be a sound theory and $j \leq k$. Then

$$\forall \Sigma_j(\mathfrak{B}(\Pi_k, \mathcal{B})) \equiv^{\mathcal{B}} GI^j_k(\mathcal{L})$$

Game Induction and Bounded Arithmetic

Using the soundness-completeness again, we can prove the following characterization:

Theorem

Let $\mathcal{B}$ be a sound theory and $j \leq k$. Then

$$\forall\Sigma_j(\mathfrak{B}(\Pi_k, \mathcal{B})) \equiv^{\mathcal{B}} GI_k^j(\mathcal{L})$$

Corollary. [ST], [Th]

For all $j \leq k$, $\forall\hat{\Sigma}_j^b(T_2^k) \equiv GI_k^j$.

Game Induction and Bounded Arithmetic

Using the soundness-completeness again, we can prove the following characterization:

Theorem

Let $\mathcal{B}$ be a sound theory and $j \leq k$. Then

$$\forall\Sigma_j(\mathfrak{B}(\Pi_k, \mathcal{B})) \equiv^{\mathcal{B}} GI_k^j(\mathcal{L})$$

Corollary. [ST], [Th]

For all $j \leq k$, $\forall\hat{\Sigma}_j^b(T_2^k) \equiv GI_k^j$.

The Game Induction characterization is also weaker than the flow characterization, simply because it relaxes the condition of provability of the reductions in the base theory.

Generalizations

There are some generalizations of these results to the cases that the length of the flow is essentially less than the length of the terms. We call these flows non-deterministic as opposed to the deterministic reductions that we introduced here. These non-deterministic reductions play a crucial role in the case of second order bounded arithmetic.

Generalizations

There are some generalizations of these results to the cases that the length of the flow is essentially less than the length of the terms. We call these flows non-deterministic as opposed to the deterministic reductions that we introduced here. These non-deterministic reductions play a crucial role in the case of second order bounded arithmetic.
It is also possible to develop the same theory for unbounded theories of arithmetic such as $I\Sigma_n$ or $\mathrm{PA} + \mathrm{TI}(\alpha)$. The idea is first using continuous cut elimination to reduce the theory to its corresponding simplified arithmetic augmented with some transfinite induction and then by using ordinal-length flows we can decompose the new proofs in the new theory.

Thank you for your attention!