Bounded Arithmetic

A survey of (some) themes

Arnold Beckmann

ICMS, July 2022

Themes

I) The Heritage

II) The Thing

III) Computational Complexity

IV) Propositional Proof Systems

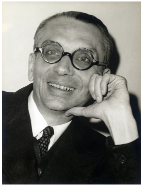
V) Total NP Search Problems

VI) Some Things missed

The Heritage

G. Peano (1858–1932)

A. Turing (1912 – 1954)



K. Gödel (1906 – 1978)

G. Gentzen (1909 – 1945)

Peano Arithmetic (PA)

- domain : $\mathbb{N}$
- language : $0, 1, +, \cdot, \leq$
- axioms : defining equations

  schema of full induction for all formulas

  $$A(0) \wedge \forall x\,(A(x) \to A(Sx)) \to \forall x\, A(x)$$

Gödel 2nd Incompl. Thm: $\quad PA \nvdash Con_{PA}$

Gentzen's Consistency Proof: $\quad PA + TI(\varepsilon_0) \vdash Con_{PA}$

Fragments of PA

- Kirby & Paris end of 1970's

  $I\Sigma_n$ $\qquad \Sigma_n : \exists x_1 \forall x_2 \ldots Q x_n \underbrace{\varphi(\vec{x})}_{\text{"simple"}}$

  e.g. bounded quantifiers

- Parsons beginning of 1970's

  provable recursive fcts of $I\Sigma_1$ = prim. rec. fcts.

- Wainer, Ono & Kadota 1970 - 1980

  provable recursive fcts of PA = $< \varepsilon_0$ - rec. fct.

Themes

I) The Heritage

II) The Thing

III) Computational Complexity

IV) Propositional Proof Systems

V) Total NP Search Problems

VI) Some Things missed

The Thing: Bounded Arithmetic

Cook 1975 : equational theory PV

Buss 1985: aligned to PA

Zambella, Cook-Nguyen : language with sorts for indices and strings

Bounded Arithmetic à la Sam

- similar to PA
- domain $\mathbb{N}$
- language: $0, 1, +, \cdot, \leq$ plus $|.|$, $\#$, ...

$|x|$ = binary length of x

$x \# y = 2^{|x| \cdot |y|}$ polynomial growth rate

- bounded formulas

Σ^b_1: $\exists x_1 \leq s_1 \; \forall y \leq |t| \; A(x_1, y)$ $\qquad NP = \Sigma^p_1$

Σ^b_2: $\exists x_1 \leq s_1 \; \forall x_2 \leq s_2 \; \exists y \leq |t| \; A(x_1, x_2, y)$ $\qquad NP^{NP} = \Sigma^p_2$

$\vdots$

s_1, s_2, t terms, A quantifier-free

Theories

- BASIC = set of open fmlas defining non-logical symbols
- Induction

Σ^b_i-Ind : $A(0) \wedge \forall x\,(A(x) \to A(Sx)) \to \forall x\, A(x)$

Σ^b_i-LInd : $A(0) \wedge \forall x\,(A(x) \to A(Sx)) \to \forall x\, A(|x|)$

where $A \in \Sigma^b_i$

- Theories

S^1_2 = BASIC + Σ^b_1-LInd $\qquad$ T^1_2 = BASIC + Σ^b_1-Ind

S^2_2 = BASIC + Σ^b_2-LInd $\qquad$ T^2_2 = BASIC + Σ^b_2-Ind

$\vdots \qquad \vdots$

Themes

I) The Heritage

II) The Thing

III) Computational Complexity

IV) Propositional Proof Systems

V) Total NP Search Problems

VI) Some Things missed

III Computational Complexity

Main result for S^1_2:

Σ^b_1-def'ble fcts in S^1_2 = poly time fcts =: $\mathcal{FP}$

Main methods:

- version of Gentzen's LK
- cut-elimination
- Witnessing

Σ^b_1-def'ble fcts in S^1_2

f Σ^b_1-def'ble in S^1_2 iff ex. Σ^b_1-fmla $A_f(x,y)$ st.

1) A_f defines graph of f over $\mathbb{N}$

2) $S^1_2 \vdash \forall x\, \exists y \leq t\ A_f(x,y)$ for some term t

3) $S^1_2 \vdash \forall x,y,y' \left(A_f(x,y) \wedge A_f(x,y') \rightarrow y = y' \right)$

Thm [Buss '85]

S^1_2 can Σ^b_1-define all fcts in FP

Converse needs Witnessing

Witnessing

A **witness** of $\exists y \le t\ \varphi(a,y)$ is some $w \le t$ with $\varphi(a,w)$

Given LK proof in S^1_2 of

$$A_1, \dots, A_k \longrightarrow B_1, \dots, B_\ell$$

$$\Sigma^b_1$$

$\Rightarrow$ exists $f \in FP$

f

$$\overset{\text{witnesses}}{A_1, \dots, A_k} \longrightarrow B_1, \dots, \overset{\text{witness}}{B_i}, \dots, B_\ell$$

$$\Sigma^b_1$$

Then $S^1_2 \vdash \exists y \le t\ \varphi(a,y) \Rightarrow$ ex. $f \in FP$ $\mathbb{N} \models \forall x\ \varphi(x, f(x))$

Other characterisations

Theories	Induction	Graph Definability	Computational Complexity
S^1_2	Σ^b_1-LInd	Σ^b_1	FP
S^2_2	Σ^b_2-LInd	Σ^b_2	FP^{NP}
S^{k+1}_2	Σ^b_{k+1}-LInd	Σ^b_{k+1}	$FP^{\Sigma^p_k}$
U^1_2	$\Sigma^{1,b}_1$-LInd	$\Sigma^{1,b}_1$	FPSPACE
V^1_2	$\Sigma^{1,b}_1$-Ind	$\Sigma^{1,b}_1$	FEXPTIME

Further Results

Thm [Buss '85]

$$S^1_2 \subseteq T^1_2 \preccurlyeq_{\forall\Sigma^b_2} S^2_2 \subseteq T^2_2 \preccurlyeq_{\forall\Sigma^b_3} S^3_2 \subseteq \dots$$

Thm [KPT, B, Z, J]

If $T^i_2 = S^{i+1}_2$, then PH collapses to $\Delta^p_{i+1}/\text{poly}$

and $\mathcal{B}(\Sigma^b_{i+1})$, provably in BA

Boolean combinations

Prf introduces KPT witnessing thm

KPT witnessing

universal version

Suppose $\varphi(a,x,y) \in \Sigma^b_{i+1}$ and $T^i_2 \vdash \exists x \forall y \, \varphi(a,x,y)$

Then ex. $FP^{\Sigma^p_i}$-fcts $f_1(a), f_2(a,b_1), \ldots, f_k(a,b_1,\ldots,b_{k-1})$

such that $T^i_2 \vdash \varphi(a,f_1(a),b_1) \vee \varphi(a,f_2(a,b_1),b_2) \vee \ldots$

$\ldots \vee \varphi(a,f_k(a,b_1,\ldots,b_{k-1}),b_k)$

Relativisation – link to type 2

- Add 2nd order variables α, β, γ ranging over sets of integers
- new atomic formula $t \in \alpha$ or $\alpha(t)$
- $\Sigma^b_i(\alpha)$: allow $\alpha(t)$ as atomic fmla
- $S^i_2(\alpha)$, $T^i_2(\alpha)$

• Results relativize

$$\Sigma^b_1(\alpha)\text{-def'ble fcts in } S^1_2(\alpha) \quad = \quad \text{polytime fcts } FP^\alpha$$

$$S^1_2(\alpha) \subseteq T^1_2(\alpha) \preccurlyeq_{\forall\Sigma^b_2(\alpha)} S^2_2(\alpha) \subseteq T^2_2(\alpha) \preccurlyeq_{\forall\Sigma^b_3(\alpha)} S^3_2(\alpha) \subseteq \dots$$

Comment: α in theories completely unspecified.

Using a specific oracle to separate complexity classes will separate theories.
However, a specific oracle collapsing complexity classes will <u>not</u> collapse theories.

Thm [KPT]

$$T^i_2(\alpha) \neq S^{i+1}_2(\alpha)$$

Prf idea:

- "=" implies a finite round student – teacher game for some property in PH
- construct oracle that falsifies this game.

$\square$

Themes

I) The Heritage

II) The Thing

III) Computational Complexity

IV) Propositional Proof Systems

V) Total NP Search Problems

VI) Some Things missed

IV) Propositional Proof Systems — Aims

Correspondence between theory T and proof system P:

- $T \vdash \forall x\, \varphi(x) \Rightarrow$ translation of $\varphi(b)$ has small P-proofs
- T proves soundness of P
- Q any other proof system:

T proves soundness of $Q \Rightarrow P$ polynomially simulates Q

Prime example: $T = PV \quad P = EF \qquad$ [Cook]

Also: Upper bounds / simulation easier

Paris – Wilkie – Translation

PW: bounded fmlas, relativised $\longrightarrow$ propositional fmlas

- $\alpha(t)$, $t^{\mathbb{N}} = n \quad \mapsto \quad p_n$
- $s = t \quad \mapsto \quad \begin{cases} \top & \text{if } s^{\mathbb{N}} = t^{\mathbb{N}} \\ \bot & \text{o/w} \end{cases}$
- translation commutes over Boolean connectives $\wedge, \vee, \neg$
- $\forall x \le t\ \varphi(x) \quad \mapsto \quad \bigwedge_{i \le t^{\mathbb{N}}} \varphi(i)^{PW}$
- $\exists x \le t\ \varphi(x) \quad \mapsto \quad \bigvee_{i \le t^{\mathbb{N}}} \varphi(i)^{PW}$

Then: $\varphi(n)^{PW}$ is const. depth prop formula of size $(\varphi)\mathrm{poly}(n)$

Example:

PHP(α): $\forall x \le a\ \exists y < a\ \alpha(x,y) \to \exists x < x' \le a\ \exists y < a\ (\alpha(x,y) \wedge \alpha(x',y))$

$\overset{PW}{\underset{a/n}{\longmapsto}}$

PHP_n: $\bigwedge_{i=0}^{n} \bigvee_{j=0}^{n-1} p_{ij} \to \bigvee_{i=0}^{n-1} \bigvee_{i'=i+1}^{n} \bigvee_{j=0}^{n-1} (p_{ij} \wedge p_{i'j})$

Thus: $T_2(\alpha) \nvdash PHP(a)$

because $T_2(\alpha) \vdash PHP(a)$

$\Rightarrow$ PHP_n AC_0-Frege proofs of (q)poly size

which contradicts [A, BPI, KPW]

Paris – Wilkie – Translation of Provability

Theory	PPS
$T^1_2(\alpha)$	$Res^*(\log)$ / tree-like $\frac{1}{2}$-PK
$T^2_2(\alpha)$	$Res(\log)$ / $\frac{1}{2}$ - PK
$T^3_2(\alpha)$	$1\frac{1}{2}$ - PK
$\vdots$	$\vdots$
U^1_2	F
V^1_2	EF

PK propositional version of Gentzen's LK

Cook-Translation of Provability

Theory	PPS
PV, S^1_2, VPV	EF, G^*_1
T^1_2, S^2_2	G_1, G^*_2
T^2_2, S^3_2	G_2, G^*_3
$\vdots$	$\vdots$
U^1_2	G
V^1_2	—

Themes

I) The Heritage

II) The Thing

III) Computational Complexity

IV) Propositional Proof Systems

V) Total NP Search Problems

VI) Some Things missed

V) Total NP Search Problems

TFNP: set of ptime $R(x,y)$ s.t.

- R polynomially bounded: $R(x,y) \Rightarrow |y| \le |x|^{O(1)}$
- R total: $\forall x \exists y\, R(x,y)$

Search task: Given x find y s.t. $R(x,y)$.

Provably Total NP Search Problems

TFNP(T): set of provably total TFNPs in T

Observe:

$$FP = TFNP(S^1_2) \subseteq TFNP(T^1_2) \subseteq TFNP(T^2_2) \subseteq \dots$$
$$\subseteq TFNP(I\Sigma_1) \subseteq \dots \subseteq TFNP(PA) \subseteq TFNP(ZFC)$$

Thm [Buss, Krajicek '94]

$$TFNP(T^1_2) = \leq(PLS)$$

Results

Theory	Complete Problem	
T^1_2	PLS	BK
T^2_2	CPLS	KST
T^k_2	LLI_k	KNT
U^1_2	LLI, RLI_1	KNT, BB
V^1_2	LI, RLI_{log}	KNT, BB
PA	α-BLS, $\alpha < \varepsilon_0$	B

Separations revisited

- $S_2^{i+1}(\alpha) \not\equiv_{\forall\Sigma_{i+1}^b(\alpha)} T_2^{i+1}(\alpha)$
- $S_2^2(\alpha) \not\equiv_{\forall\Sigma_1^b(\alpha)} T_2^2(\alpha)$ [CK]

Open Problem:

$$\exists k \ \forall i \quad T_2^i(\alpha) \not\equiv_{\forall\Sigma_k^b(\alpha)} T_2(\alpha)$$

$$\forall i \quad T_2^i(\alpha) \not\equiv_{\forall\Sigma_1^b(\alpha)} T_2(\alpha)$$

Approximate Counting

APC$_1$: $S^1_2 + sWPHP(PV_1)$ [Jeřábek]

APC$_2$: $T^1_2 + sWPHP(PV_2)$

Can count size of P/NP set up to polynomial error.

Thm [BKT, AT]

$$\left.\begin{array}{l} PV_1(\alpha) + sWPHP(PV_2(\alpha)) \\ T^1_2(\alpha) + sWPHP(PV_1(\alpha)) \\ T^1_2(\alpha) + iWPHP(PV_1(\alpha)) \end{array}\right\} \forall\Sigma^b_1(\alpha)\text{-separated from } \begin{array}{l} APC_2(\alpha) \\ T^2_2(\alpha) \end{array} \subseteq T^3_2(\alpha)$$

Also [KT] $APC_2(\alpha) \neq_{\forall\Sigma^b_1(\alpha)} T^2_2(\alpha)$

Themes

I) The Heritage

II) The Thing

III) Computational Complexity

IV) Propositional Proof Systems

V) Total NP Search Problems

VI) Some Things missed

Missed

- 2-sorted BA below P
- non-standard models, forcing
- formalisations of lower bounds
- other forms of Gödel's consistency statements

etc etc etc

Thanks