Approximate counting in bounded arithmetic

Emil Jeřábek

jerabek@math.cas.cz
http://math.cas.cz/~jerabek/

Institute of Mathematics of the Academy of Sciences, Prague

The counting problem

Work in a theory of arithmetic.

Problem: Given a finite (= bounded) definable set X, determine its cardinality $|X|$.

Applications:

- proofs using counting arguments or probabilistic reasoning
- formalization of randomized algorithms

Example 1: the pigeonhole principle

Theorem: If $a < b$, there is no surjection $f\colon [0,a) \twoheadrightarrow [0,b)$.

Proof: By induction on $k \le b$, show that

$$\bigl|\{x < a \mid f(x) < k\}\bigr| \ge k.$$

Since the LHS is at most a, we obtain a contradiction for $k = b > a$. QED

Notation: $a = [0,a)$, e.g., $f\colon a \to b$

Example 2: Ramsey's theorem

Theorem: An undirected graph $G = \langle V, E\rangle$ on n vertices contains a clique or independent set of size $\geq \frac{1}{2}\log n$.

Proof: For $u \neq v \in V$, define $c(u,v) \in \{0,1\}$ by

$$c(u,v) = 1 \Leftrightarrow \{u,v\} \in E.$$

By induction on $k \leq \lceil \log n \rceil$, show that there exist $c_0, \dots, c_{k-1} < 2$ and distinct vertices $u_0, \dots, u_{k-1}$ such that

$$\forall i < j < k\; c(u_i, u_j) = c_i,$$

$$\left|\{v \in V \mid \forall i < k\; c(u_i, v) = c_i\}\right| \geq \frac{n+1}{2^k} - 1.$$

Denote the set on the LHS by $S(u_0, \dots, u_{k-1}; c_0, \dots, c_{k-1})$.

Example 2: Ramsey's theorem (cont'd)

The induction step: pick $u_k \in S(\vec{u};\vec{c})$. Since

$$S(\vec{u};\vec{c}) = \{u_k\} \cup S(\vec{u},u_k;\vec{c},0) \cup S(\vec{u},u_k;\vec{c},1),$$

we can choose $c_k < 2$ so that

$$|S(\vec{u},u_k;\vec{c},c_k)| \ge \frac{|S(\vec{u};\vec{c})|-1}{2} \ge \frac{n+1}{2^{k+1}} - 1.$$

Let $k = \lceil \log n \rceil$. If $c < 2$ is the more populous colour among $c_0,\dots,c_{k-1}$, then $H = \{u_i \mid c_i = c\}$ is a homogeneous set of size $\ge k/2$. QED

Example 3: the tournament principle

A tournament is a directed graph where any two vertices are joined by exactly one edge.

IOW: tournament = choice of orientation of edges of K_n.

If there is an edge $a \to b$, player a beats player b.

A dominating set is a set D of players such that any other player is beaten by some member of D.

Example 3: the tournament principle (cont'd)

Theorem: A tournament G with n players has a dominating set of size $\leq \log(n+1)$.

Proof: By induction on n. There are $n(n-1)/2$ matches in total, hence there exists a player v who wins $\geq (n-1)/2$ matches. By the induction hypothesis, the subtournament consisting of the $\leq (n-1)/2$ players who beat v has a dominating set D of size $\leq \log((n-1)/2+1) = \log(n+1)-1$, thus $D \cup \{v\}$ is a dominating set in the original tournament of size $\leq \log(n+1)$. QED

Example 4: the "probabilistic method"

Theorem: For any $n > 2$, there exists a graph G on n vertices with no clique or independent set of size $\geq 2\log n$.

Proof: Consider a random G. If $X \subseteq V$ has size k, then X is a homogeneous set for G with probability $2^{1-\binom{k}{2}}$, hence G contains a homogeneous set of size k with probability at most

$$\binom{n}{k} 2^{1-\binom{k}{2}} \leq \frac{n^k}{k!} 2^{1-\binom{k}{2}} \leq \left(\frac{ne}{k2^{(k-1)/2}}\right)^k < \left(\frac{n}{2^{k/2}}\right)^k \leq 1$$

as long as $k \geq 2\log n$, $k > e\sqrt{2}$. QED

Bounded arithmetic

Buss' theories

Language: 0, S, $+$, $\cdot$, $\leq$, $|x|$, $\#$, $\lfloor x/2^y \rfloor$

Intended meaning $|x| = \lceil \log(x+1) \rceil$, $x \# y = 2^{|x| \cdot |y|}$

Sharply bounded quantifiers: $\exists x \leq |t| \, \varphi$, $\forall x \leq |t| \, \varphi$

$\hat{\Sigma}^b_i$-formulas: i blocks of bounded quantifiers, starting with existential, followed by a sharply bounded kernel

Σ^b_i-formulas: ignore sharply bounded quantifiers anywhere

$\hat{\Pi}^b_i$, Π^b_i: dually

$i > 0 \Rightarrow \Sigma^b_i(\mathbb{N}) = \Sigma^P_i$, $\Pi^b_i(\mathbb{N}) = \Pi^P_i$

$BASIC$: finite list of open axioms, mostly recursive definitions of the function symbols

Buss' theories: T^i_2

$T^i_2 = BASIC + \Sigma^b_i\text{-}IND = BASIC + \Pi^b_i\text{-}IND$

(φ-IND) $\qquad \varphi(0) \land \forall x\,(\varphi(x) \to \varphi(x+1)) \to \varphi(u)$

For $i > 0$: $\qquad T^i_2 = BASIC + \Sigma^b_i\text{-}MIN = BASIC + \Sigma^b_i\text{-}MAX$

$$= BASIC + \Pi^b_{i-1}\text{-}MIN = BASIC + \Pi^b_{i-1}\text{-}MAX$$

(φ-MIN) $\qquad \varphi(u) \to \exists x\,(\varphi(x) \land \forall y < x\,\neg\varphi(y))$

(φ-MAX) $\qquad \varphi(0) \to \exists x \le a\,(\varphi(x) \land \forall y \le a\,(\varphi(y) \to y \le x))$

Buss' theories: S_2^i

For $i > 0$: $S_2^i = BASIC +$ any of the following:

Σ_i^b-$PIND$, Π_i^b-$PIND$, Σ_i^b-$LIND$, Π_i^b-$LIND$,
Σ_i^b-$LMIN$, Π_{i-1}^b-$LMIN$, Σ_i^b-$LMAX$, Π_{i-1}^b-$LMAX$,
Σ_i^b-$COMP$, Π_i^b-$COMP$

(φ-$PIND$) $$\varphi(0) \wedge \forall x\,(\varphi(\lfloor x/2 \rfloor) \to \varphi(x)) \to \varphi(u)$$

(φ-$LIND$) $$\varphi(0) \wedge \forall x\,(\varphi(x) \to \varphi(x+1)) \to \varphi(|u|)$$

(φ-$LMIN$) $$\varphi(u) \to \exists x\,(\varphi(x) \wedge \forall y\,(\varphi(y) \to |x| \le |y|))$$

(φ-$LMAX$) $$\varphi(0) \to \exists x \le a\,(\varphi(x) \wedge \forall y \le a\,(\varphi(y) \to |y| \le |x|))$$

(φ-$COMP$) $$\exists x < a \# 1\, \forall u < |a|\,(\underbrace{u \in x}_{\lfloor x/2^u \rfloor = 2\lfloor x/2^{u+1} \rfloor + 1} \leftrightarrow \varphi(u))$$

Buss' theories: basic properties

- $T^0_2 \subseteq S^1_2 \subseteq T^1_2 \subseteq S^2_2 \subseteq \cdots \subseteq T^i_2 \subseteq S^{i+1}_2 \subseteq T^{i+1}_2 \subseteq \cdots \subseteq T_2 = S_2$
- S^{i+1}_2 is a $\forall\Sigma^b_{i+1}$-conservative extension of T^i_2
- poly-time functions have well-behaved Σ^b_1-definitions in T^0_2 $\Rightarrow$ expansion by PV-functions
- T^i_2/S^i_2 proves the relevant $(P|L)IND$, $(L)MIN$, ... schemata in the expanded language $\Rightarrow$ we can use PV-functions freely
- more generally, T^i_2 has Σ^b_{i+1}-definitions for $FP^{\Sigma^P_i}$ $\Rightarrow PV_{i+1}$-functions
- Buss' witnessing theorem: if $S^{i+1}_2 \vdash \exists y\, \varphi(\vec{x}, y)$, $\varphi \in \Sigma^b_{i+1}$, then there exists $f \in PV_{i+1}$ s.t. $T^i_2 \vdash \varphi(\vec{x}, f(\vec{x}))$

Buss' theories: relativization

We can relativize the theories by adding an "oracle"

$S^i_2(\alpha)$, $T^i_2(\alpha)$: include a new predicate $\alpha(x)$,* expand schemas to the new language, no other axioms about α

- in $\langle \mathbb{N}, A\rangle$: $\Sigma^b_i(\alpha)$ defines $(\Sigma^P_i)^A$, $PV(\alpha)$ defines FP^A
- unconditional independence and separation results
- if $T^i_2(\alpha)$ proves stuff about $\Sigma^b_j(\alpha)$-formulas, then T^{i+k}_2 proves the same about Σ^b_{j+k}-formulas for any k

We will work in the relativized theories, but will omit α to keep the notation compact

---

*and the $x \bmod 2^y$ (LSP) function in the case of Σ^b_0-schemas

Exact counting in formal arithmetic

We can count using sequence encoding:

$$|X| \le k \Leftrightarrow \exists w \, \forall x \, [x \in X \to \exists i < k \, (w)_i = x]$$

$$|X| \ge k \Leftrightarrow \exists w \, \forall i < k \, [(w)_i \in X \wedge \forall j < i \, (w)_j \neq (w)_i]$$

- $I\Sigma_i$ can count $\Sigma^0_0(\Sigma^0_i)$-sets ($i > 0$)
- $I\Delta_0 + \exp$ can count $\Delta^0_0(\exp)$-sets
- S^i_2 can count small Σ^b_i-sets ($i > 0$)
- T^0_2 can count sets given explicitly by a sequence

Small = of size $\le \log a$ for some a.

What about larger sets?

Toda's theorem

In bounded arithmetic, we need $|X|$ to be definable by a bounded formula. This is impossible even for poly-time X:

$\#P$ = class of functions of the form $f(x) = \bigl|\{y \mid R(x,y)\}\bigr|$, where $R \in P$ and $R(x,y) \Rightarrow |y| \le |x|^c$

Theorem [Toda '89]: $PH \subseteq P^{\#P}$

Corollary: If $\#P \subseteq FP^{PH}$, then $PH = \Sigma^P_k$ for some k.

If exact counting of poly-time sets is expressible by a bounded formula, then the polynomial hierarchy collapses

$\Rightarrow$ can use only approximate counting

Weak pigeonhole principle

Weak pigeonhole principle

The multifunction (relation) pigeonhole principle:

$$mPHP^b_a(R) = \forall y < b\,\exists x < a\,R(y,x)$$
$$\to \exists y < y' < b\,\exists x < a\,(R(y,x) \wedge R(y',x))$$

Weak pigeonhole principle: b “much” larger than a

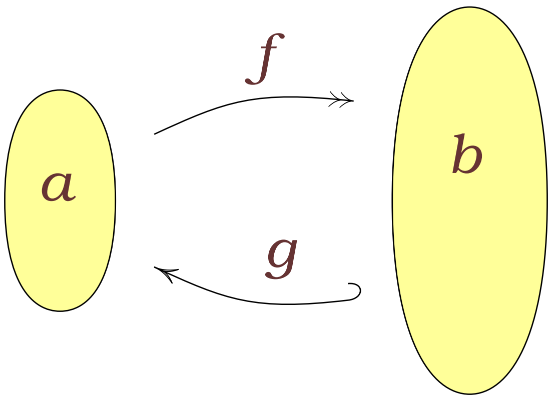
Popular choices: $mPHP^{a^2}_a$, $mPHP^{2a}_a$. For us:

$$mWPHP(R) = mPHP^{a(|b|+1)}_{a\,|b|}(R)$$

Theorem [PWW ’88, MPW ’02]: $T^2_2 \vdash mWPHP(\Sigma^b_1)$

Variants of WPHP

Special cases where R or R^{-1} is a function:



surjective WPHP

$$sPHP^b_a(f) = \exists y < b\, \forall x < a\; f(x) \neq y$$

injective WPHP

$$iPHP^b_a(g) = \forall y < b\; g(y) < a \to \exists y < y' < b\; g(y) = g(y')$$

retraction-pair WPHP

$$rPHP^b_a(f, g) = \forall y < b\; g(y) < a \to \exists y < b\; f(g(y)) \neq y$$

Variants of WPHP (cont'd)

$$\begin{tikzcd}
 & & sWPHP(PV) \arrow[dr, shift left] & \\
T^2_2 \arrow[r] & mWPHP(\Sigma^b_1) \arrow[ur] \arrow[dr] & & rWPHP(PV) \arrow[ul, dashed, shift left, "\Sigma^b_1"'] \\
 & & iWPHP(PV) \arrow[ur] &
\end{tikzcd}$$

$S^1_2 + sWPHP(PV)$ is $\forall\Sigma^b_1$-conservative over $T^0_2 + rWPHP(PV)$

Wilkie's witnessing theorem: If $S^1_2 + sWPHP(PV) \vdash \exists y\, \varphi(\vec{x}, y)$, $\varphi \in \Sigma^b_1$, then there exists a randomized poly-time algorithm f such that $\varphi(\vec{x}, f(\vec{x}))$ for every $\vec{x}$.

False for $iWPHP$, if factoring is hard!
$\Rightarrow$ our variant of choice is $rWPHP$ or $sWPHP$

Applications of WPHP

WPHP can replace counting arguments in bounded arithmetic.

Already in the paper which introduced it:

Theorem [PWW '88]: $I\Delta_0 + \Omega_1 \vdash \forall x\, \exists p > x\, (p$ is prime$)$.

Proof outline: Assume that there is no prime between a and a^{11}. By manipulating prime factorizations, stitch an injection from $9a \log a$ to $8a \log a$. QED

(In our setting: it goes through in $S^1_2 + rWPHP(\Gamma) \subseteq T^3_2$, where $\Gamma = FP^{NP[\mathrm{wit},\log n]}$ is the class of provably total Σ^b_2-definable functions of S^1_2.)

Approximate counting with WPHP

Basic idea: witness that $|X| \leq a$ by exhibiting a function f such that $f\colon a \twoheadrightarrow X$ (for $sWPHP$) or $f\colon X \hookrightarrow a$ (for $iWPHP$).

Trouble: Where do we get these functions from?

On the face of it, WPHP is a passive counting principle: it tells us that something is impossible, it does not supply any counting functions.

Example: Ramsey's theorem reloaded

Theorem [Pudlák '90]: $T_2(E)$ proves Ramsey's theorem: a graph $\langle V = n, E\rangle$ has a homogeneous set of size $\geq \frac{1}{2}\log n$.

Proof: Recall: if $u_0, \dots, u_{k-1} < n$ are pairwise distinct and $c_0, \dots, c_{k-1} < 2$ are such that $\forall i < j\ c(u_i, u_j) = c_j$, we put

$$S(\vec{u}; \vec{c}) = \{v < n \mid \forall i < k\,(u_i \neq v \wedge c(u_i, v) = c_i)\}.$$

We have

$$u \in S(\vec{u}; \vec{c}) \Rightarrow S(\vec{u}; \vec{c}) = \{u\} \cup S(\vec{u}, u; \vec{c}, 0) \cup S(\vec{u}, u; \vec{c}, 1).$$

This translates into a straightforward manipulation of counting functions:

Example: Ramsey's theorem (cont'd)

If $f_c\colon \{0,1\}^{<r} \twoheadrightarrow S(\vec{u},u;\vec{c},c)$, $c<2$, then $f\colon \{0,1\}^{<r+1} \twoheadrightarrow S(\vec{u};\vec{c})$, where

$$(*) \qquad \begin{aligned} f(\langle\rangle) &= u, \\ f(w \frown \langle c\rangle) &= f_c(w). \end{aligned}$$

Assuming for contradiction $S(u_0,\dots,u_{k-1};c_0,\dots,c_{k-1}) = \varnothing$ whenever $k = K := \lfloor \log n \rfloor - 1$, we have trivially an $f\colon \{0,1\}^{<0} \twoheadrightarrow S(\vec{u};\vec{c})$, and iterating $(*)$ we get

$$f_{\vec{u};\vec{c}}\colon \{0,1\}^{<K-k} \twoheadrightarrow S(u_0,\dots,u_{k-1};c_0,\dots,c_{k-1}).$$

We can likewise construct its coretraction

$$g_{\vec{u};\vec{c}}\colon S(\vec{u};\vec{c}) \hookrightarrow \{0,1\}^{<K-k}.$$

Example: Ramsey's theorem (still cont'd)

The complete definition ($*=$ "undefined"):

$$f_{\vec{u};\vec{c}}(w)=\begin{cases} * & \text{if } S(\vec{u};\vec{c})=\varnothing \\ u & \text{if } w=\langle\rangle \\ f_{\vec{u},u;\vec{c},c}(w') & \text{if } w=w'\frown\langle c\rangle \end{cases}$$

$$g_{\vec{u};\vec{c}}(x)=\begin{cases} \langle\rangle & \text{if } x=u \\ g_{\vec{u},u;\vec{c},c}(x)\frown\langle c\rangle & \text{where } c=c(u,x) \end{cases}$$

$$\text{where } u=\min S(\vec{u};\vec{c})$$

$f(\vec{u},\vec{c},w)=f_{\vec{u};\vec{c}}(w)$ and $g(\vec{u},\vec{c},x)=g_{\vec{u};\vec{c}}(x)$ are in FP^{NP}

Example: Ramsey's theorem (f'shed)

By induction on $K - k$, we prove

$$x \in S(\vec{u};\vec{c}) \Rightarrow f_{\vec{u};\vec{c}}(g_{\vec{u};\vec{c}}(x)) = x.$$

For $k = 0$: a retraction pair from $\{0,1\}^{<K} \approx 2^K - 1$ onto $S(;) = n \geq 2^{K+1}$, contradicts $WPHP$.

Thus there exist $c_0, \dots, c_{K-1}$, $u_0, \dots, u_K$, from which we pick a homogeneous set of size $\geq 1 + \lceil K/2 \rceil \geq 1 + \lfloor \frac{1}{2} \log n \rfloor$. QED

We actually got

Theorem: Ramsey's theorem is provable in $T^1_2(E) + rWPHP(PV_2(E)) \subseteq T^3_2(E)$.

Morals to draw

This worked. However:

- The definition of f, g is messy
  (even leading to miscalculation of its complexity)
  $\Rightarrow$ want a general theory of counting so that we do not need to resort to *ad hoc* functions.
- We have an obvious way of combining witnesses for $|X| \le a$ and $|Y| \le b$ into a witness for $|X \cup Y| \le a + b$.
  What about the dual principle

  $$|X \,\dot\cup\, Y| < a + b \Rightarrow |X| < a \text{ or } |Y| < b\,?$$

  Needed for the tournament principle, for example.

General theory of counting

Rest of the talk: two general setups

Approximate probabilities:

- estimate the size of $X \subseteq 2^n$ within error $2^n/poly(m)$
  = estimate $\Pr_{x<a}(x \in X)$ within error $1/poly(m)$
- $P/poly$ sets can be counted in $T^0_2 + sWPHP(PV) \subseteq T^2_2$
- based on pseudorandom generators

Proper approximate counting:

- estimate the size of $X \subseteq 2^n$ within error $|X|/poly(m)$
- $\Sigma^b_1/poly$ sets can be counted in $T^1_2 + sWPHP(PV_2) \subseteq T^3_2$
  (often $rWPHP$ suffices)
- based on hashing

Approximate probabilities

Approximate probabilities: intro

Basic strategy:

- we can estimate $\Pr_{x<a}(x \in X)$ with error ε by drawing $O(1/\varepsilon)$ independent random samples
  $\Rightarrow$ randomized poly-time algorithm
- derandomize using the Nisan–Wigderson pseudorandom generator
- analysis of the generator can be carried out in T^0_2, it provides explicit “counting functions” for X

Nisan–Wigderson generator

- intended for derandomization of poly-time algorithms (BPP)
- $NW_f \colon 2^{O(\log n)} \to 2^n$ fools poly-size circuits $C \colon 2^n \to 2$
- computable in time $poly(n)$ (= exponential in the size of the input)
- needs access to the truth table of an exponentially hard Boolean function $f \colon 2^{O(\log n)} \to 2$

Hard Boolean functions

Hardness of a function $f\colon 2^k \to 2$:
$H(f) \le s$ iff there exists a circuit C of size $\le s$ such that

$$\Pr_{x\in 2^k}(C(x) = f(x)) \ge \frac{1}{2} + \frac{1}{s}$$

f is (average-case) ε-hard if $H(f) \ge 2^{\varepsilon k}$

- by a simple counting argument, most Boolean functions are $(\frac{1}{3} - o(1))$-hard
- we can easily enumerate the easy functions
$\Rightarrow T^0_2 + sWPHP(PV) \vdash (\frac{1}{3} - o(1))$-hard functions exist
- (in fact: over S^1_2, this is equivalent to $sWPHP(PV)$)

Nisan–Wigderson generator (cont'd)

Theorem [NW '94]: For every $\varepsilon > 0$, there exist $c, d > 0$ and a setting of parameters of the Nisan–Wigderson generator so that $NW_f \colon 2^{c \log n} \to 2^n$ satisfies:

Whenever $f \colon 2^{d \log n} \to 2$ is ε-hard and $C \colon 2^n \to 2$ is a circuit of size at most n, we have

$$\left|\Pr_{x \in 2^n}(C(x)) - \Pr_{y \in 2^{c \log n}}(C(NW_f(y)))\right| \le \frac{1}{n}.$$

(If we need bigger $|C|$ or smaller error, we can pad C with dummy variables.)

NW in bounded arithmetic

Idea: Estimate $\Pr_{x \in 2^n}(C(x))$ by sampling it on the output of NW_f.

Problem: How does the theory know that the result is not just a meaningless number? Need some witness to ensure that the definition is well-behaved.

Solution: The NW generator can be analyzed in a very constructive way, ensuring the existence of suitable retraction pairs witnessing correctness of the computed size.

NW in bounded arithmetic (cont'd)

Theorem: $T^0_2 + sWPHP(PV)$ proves:
Let $X \subseteq 2^n$ be defined by a circuit C, and $\varepsilon^{-1} \in \mathrm{Log}$. There exist $s \leq 2^n$, $0 < v \leq poly(n\varepsilon^{-1}|C|)$, and functions

$$v(s + \varepsilon 2^n) \underset{g_0}{\overset{f_0}{\rightleftarrows}} v \times X \qquad v \times (X \mathbin{\dot\cup} \varepsilon 2^n) \underset{g_1}{\overset{f_1}{\rightleftarrows}} vs$$

defined by circuits of size $poly(n\varepsilon^{-1}|C|)$ such that $f_i \circ g_i = \mathrm{id}$.

Notation:

- $n \in \mathrm{Log} \Leftrightarrow \exists a\, n = |a|$
- ε rational: $\varepsilon^{-1} \in \mathrm{Log} \Leftrightarrow \varepsilon > 0 \wedge \exists a\, \varepsilon^{-1} \leq |a|$

Size comparison with error

Definition: $X, Y \subseteq 2^n$ definable sets, $\varepsilon \geq 0$, $n = |a|$:

- $X \preceq_\varepsilon Y$ iff there exist $v > 0$ and a circuit

$$C : v \times (Y \mathbin{\dot\cup} \varepsilon 2^n) \twoheadrightarrow v \times X$$

- $X \approx_\varepsilon Y$ iff $X \preceq_\varepsilon Y \wedge Y \preceq_\varepsilon X$
- $\Pr_{x<a}(x \in X) \preceq_\varepsilon p$ iff $X \cap a \preceq_\varepsilon pa$, and similarly for $\succeq$, $\approx$

Corollary: $T^0_2 + sWPHP(PV)$ proves: If X is defined by a circuit and $\varepsilon^{-1} \in \mathrm{Log}$, there exists s such that $X \approx_\varepsilon s$.

Complexity of $\preceq_\varepsilon$

- As it stands: $X \preceq_\varepsilon Y$ is an unbounded $\exists\Pi^b_2$-formula
- If $\varepsilon^{-1} \in \mathrm{Log}$ and X, Y are defined by circuits, it is (essentially) Σ^b_2 by the Theorem
- In fact, it is $P/poly$: given $\varepsilon^{-1} \in \mathrm{Log}$ and a family $\{X_u \mid u < a\}$ of subsets of 2^n defined by a circuit $C(u, x) \colon a \times 2^n \to 2$, there is a circuit s such that $X_u \approx_\varepsilon s(u)$, and circuits giving similarly the witnessing functions f_i, g_i
  $\Rightarrow$ can appear in induction formulas even in T^0_2

Elementary properties of $\preceq_\varepsilon$

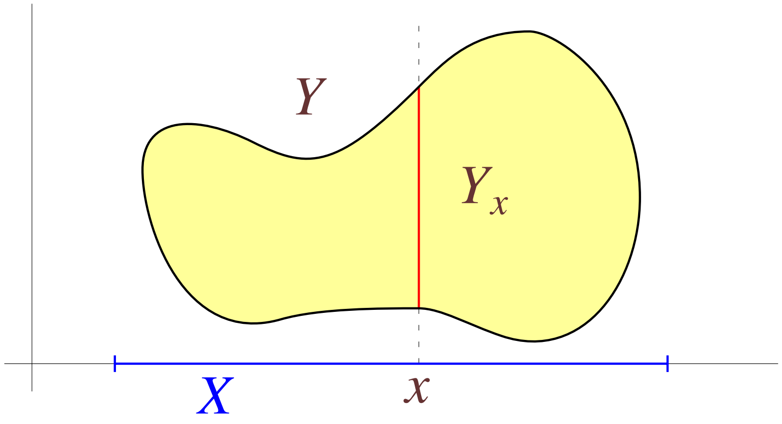
$T^0_2 + sWPHP(PV)$ proves (for sets defined by circuits and Greeks in inverse Log):

- $X \preceq_\varepsilon Y \preceq_\delta Z \Rightarrow X \preceq_{\varepsilon+\delta} Z$
- $X \preceq_\varepsilon X', Y \preceq_\delta Y' \Rightarrow X \times Y \preceq_{\varepsilon+\delta+\varepsilon\delta} X' \times Y'$
- $X \preceq_\varepsilon X', Y \preceq_\delta Y', X' \cap Y' = \varnothing \Rightarrow X \cup Y \preceq_{\varepsilon+\delta} X' \cup Y'$
- $s \preceq_\varepsilon X \preceq_\delta t \Rightarrow s \leq t + (\varepsilon + \delta + \eta)2^n$
- $X \preceq_\varepsilon Y$ or $Y \preceq_\varepsilon X$
- $X \preceq_\varepsilon Y \Rightarrow 2^n \smallsetminus Y \preceq_{\varepsilon+\eta} 2^n \smallsetminus X$
- $X \approx_\varepsilon s, Y \approx_\delta t, X \cap Y \approx_\eta u \Rightarrow X \cup Y \approx_{\varepsilon+\delta+\eta+\xi} s + t - u$
- …

Averaging

Theorem: $T^0_2 + sWPHP(PV)$ proves: if $X \subseteq 2^m$ and $Y \subseteq X \times 2^n$ are definable by circuits, $X \preceq_\delta t$, and $Y_x := \{y \mid \langle x, y\rangle \in Y\} \preceq_\varepsilon s$ for every $x \in X$, then $Y \preceq_{\varepsilon+\delta+\varepsilon\delta+\xi} st$ for any $\xi^{-1} \in \mathrm{Log}$.

Read contrapositively, this gives a formalization of the averaging principle: if $|X| \leq t$ and $|\bigcup_{x\in X} Y_x| > u$, then there exists $x \in X$ such that $|Y_x| > u/t$.



Chernoff–Hoeffding inequality

Theorem: $T^0_2 + sWPHP(PV)$ proves: if $X \subseteq a$ is defined by a circuit, $m \in \mathrm{Log}$, $p, \varepsilon, \delta \in [0,1]$, and $\Pr_{x<a}(x \in X) \succeq_\delta p$, then

$$\Pr_{w \in a^m}\big(|\{i < m \mid (w)_i \in X\}| \le m(p-\varepsilon)\big) \preceq_0 c4^{m(c\delta-\varepsilon^2)}$$

for some standard constant c.

Inclusion-exclusion principle

Theorem: $T^0_2 + sWPHP(PV)$ proves: let $X_i \subseteq 2^n$ ($i < m$) be defined by a sequence of circuits. Let $k \le m$, $(2m/k)^k \in \mathrm{Log}$. Assume $\bigcap_{i\in I} X_i \approx_{\varepsilon_I} s_I$ for every $I \subseteq m$ of size at most k, and put

$$s = \sum_{\substack{I\subseteq m \\ 0<|I|\le k}} (-1)^{|I|+1} s_I, \qquad \varepsilon = \sum_{\substack{I\subseteq m \\ 0<|I|\le k}} \varepsilon_I .$$

Then for any $\xi^{-1} \in \mathrm{Log}$,

$$\bigcup_{i<m} X_i \succeq_{\varepsilon+\xi} s \qquad \text{or} \qquad \bigcup_{i<m} X_i \preceq_{\varepsilon+\xi} s$$

if k is even or odd, respectively.

Randomized algorithms

Main application: formalization of classes of randomized algorithms ($TFRP$, BPP, APP, MA, AM, $\dots$)

- straightforward to define using approximate probabilities
- can't expect all of them to be "provably total": mostly semantic classes, no known complete problems
- instead, show that the definition is "well-behaved":
  - amplification of probability of success
  - closure properties (e.g., composition)
  - trading randomness for nonuniformity
  - inclusions between the randomized classes and levels of PH

Approximate counting

Approximate counting: intro

Proper approximate counting: error relative to size of X, not size of the ambient universe

- witness that $|X| \leq s$ using linear hash functions (Sipser's coding lemma)
- again, equivalent to existence of suitable surjective "counting functions"
- asymmetric: no witness for $|X| \geq s$
- can meaningfully count "sparse" sets
  $\Rightarrow$ useful for inductive counting arguments:
  Ramsey's theorem, tournament principle

Linear hashing: basic idea

Let $X \subseteq 2^n = F^n$, $F = GF(2)$, $|X| = s$.

If $x \neq y \in F^n$ and $a \in F^n$ is a random vector,

$$\Pr_a(a^\intercal x = a^\intercal y) = \Pr_a(a^\intercal(x - y) = 0) = \frac{1}{2}.$$

Thus, if $A \in F^{t \times n}$ is a random matrix,

$$\Pr_A(Ax = Ay) = 2^{-t},$$

$$\mathrm{E}_A \big| \{ \langle x, y \rangle \mid x, y \in X, x < y, Ax = Ay \} \big| = 2^{-t} \binom{s}{2}.$$

If $2^t > \binom{s}{2}$, there exists an injective linear function $A \colon X \hookrightarrow 2^t$

$\Rightarrow$ we can distinguish sets of size $\leq s$ and roughly $\geq s^2$!

Sipser's coding lemma

- $A \in F^{t\times n}$ **separates** x from $X \subseteq F^n$ if $Ax \neq Ay$ for every $y \in X \smallsetminus \{x\}$
- $\{A_i \mid i < k\}$ **isolates** X if every $x \in X$ is separated from X by some A_i

Take $k = \lceil \log s \rceil$, $t = k + 1$. We have

$$\Pr_A(A \text{ does not separate } x \text{ from } X) < \frac{s}{2^t} \leq \frac{1}{2},$$

$$\Pr_{A_0,\dots,A_{k-1}}(\text{no } A_i \text{ separates } x \text{ from } X) < \frac{1}{2^k},$$

$$\Pr_{A_0,\dots,A_{k-1}}(X \text{ not isolated by } A_0,\dots,A_{k-1}) < \frac{s}{2^k} \leq 1.$$

Sipser's coding lemma (cont'd)

Theorem [Sipser '83]: Let $X \subseteq 2^n$, $|X| \le s$, $k = \lceil \log s \rceil$, $t = k + 1$. Then there exists $\{A_i \mid i < k\}$, $A_i \in F^{t \times n}$, which isolates X.

OTOH: If such a sequence exists, each A_i can only separate 2^t points, hence $|X| \le 2^t k \le 4s(\log s + 1)$
$\Rightarrow$ we can distinguish sets of size s and about $4s \log s$

We want: distinguish s from $s(1+\varepsilon)$ for polynomially small ε

Apply to X^c: distinguish $|X^c| \le s^c$ from $4s^c \log s^c = 4s^c c \log s$
$\Rightarrow$ distinguish $|X| \le s$ from $s(4c \log s)^{1/c} \le s(1+\varepsilon)$ for suitably chosen $c = poly(\varepsilon^{-1}, \log \log s)$

Formalized approximate counting

Definition: Let $X \subseteq 2^n$ be a definable set and $\varepsilon^{-1} \in \mathrm{Log}$.

- if $s > 0$: $X \precsim_\varepsilon s$ iff there exists $0 < s' \le s$ and a sequence $\{A_i \mid i < t\}$, $A_i \in F^{t \times n}$, which isolates X^c, where $c = 12|s'|\lceil\varepsilon^{-1}\rceil^2$ and $t = |s'^c| + 1$
- $X \precsim_\varepsilon 0$ iff X is empty
- $X \precsim s$ iff $X \precsim_\varepsilon s$ for all $\varepsilon^{-1} \in \mathrm{Log}$

Basic properties:

- the definition is monotone and independent of n
- if $X \in \Sigma^b_1$, then $\precsim_\varepsilon$ is Σ^b_2; we can make it $\Pi^b_1/poly$

Reformulation with surjections

Theorem: $T^1_2 + sWPHP(PV_2)$ proves: let $X \in \Sigma^b_1$, $f \in PV_2$, $r, d > 0$, $d \in \mathrm{Log}$, and assume $f\colon rs^d \twoheadrightarrow^{*} r \times X^d$. Then $X \precsim s$. Moreover,

$$\Pr(\{A_i \mid i < t\} \text{ does not isolate } X^c) \preceq_0^{\Sigma^b_1} 2/3,$$

where c, t are as in the definition.

Theorem: $T^1_2 + rWPHP(PV_2)$ proves: if $X \in \Sigma^b_1$ and $X \precsim_\varepsilon s$, there exists a PV_2-retraction pair $\lfloor s(1+\varepsilon)\rfloor^c \underset{\longleftarrow}{\overset{\longrightarrow\!\!\!\!\!\rightarrow}{}} X^c$, where c is as in the definition.

---

* I'm cheating a bit

Agreement with other counting setups

Theorem: $T^1_2 + rWPHP(PV_2)$ proves: if $X \in \Sigma^b_1$ and $s \le \varepsilon^{-1} \in \mathrm{Log}$, then $X \precsim_\varepsilon s$ iff there exists a sequence of length at most s which includes all elements of X.

Theorem: $T^1_2 + sWPHP(PV_2)$ proves: let $X, Y \in \Sigma^b_1$, $f \in PV_2$, $d, r > 0$, $d, \varepsilon^{-1} \in \mathrm{Log}$. If $f\colon r \times X^d \twoheadrightarrow r \times Y^d$ and $X \precsim_\varepsilon s$, then $Y \precsim \lfloor s(1+\varepsilon) \rfloor$.
In particular: if $Y \preceq_\delta X$ and $X \precsim_\varepsilon s$, then $Y \precsim s(1+\varepsilon) + \delta 2^n$.

Unions and products

Theorem: $T^1_2 + rWPHP(PV_2)$ proves for $X, Y \in \Sigma^b_1$:

- if $X \precsim_\varepsilon s$ and $Y \precsim_\varepsilon t$, then $X \cup Y \precsim \lfloor (s+t)(1+2\varepsilon) \rfloor$
- if $X \precsim_\varepsilon s$ and $Y \precsim_\varepsilon t$, then $X \times Y \precsim \lfloor st(1+\varepsilon)^2 \rfloor$
- if $X \mathbin{\dot\cup} Y \precsim_\varepsilon s + t + 1$, then $X \precsim \lfloor s(1+2\varepsilon) \rfloor$ or $Y \precsim \lfloor t(1+2\varepsilon) \rfloor$
- if $X \times Y \precsim_\varepsilon st$, then $X \precsim \lfloor s(1+\varepsilon) \rfloor$ or $Y \precsim \lfloor t(1+\varepsilon) \rfloor$

Similar properties also hold for sums and products of logarithmically many sets rather than just two.

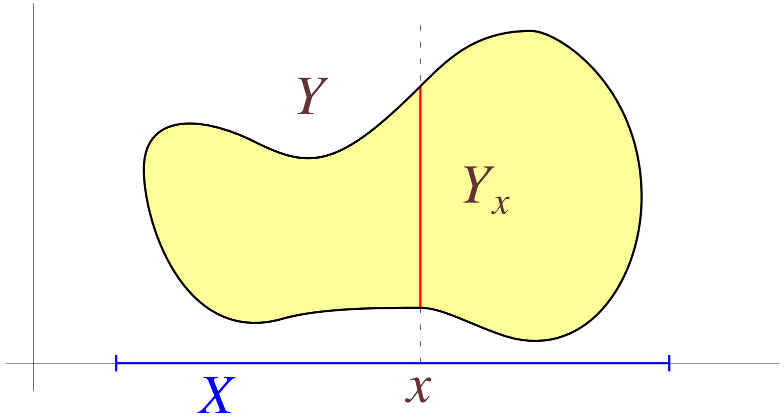
Averaging

Or: sums of many sets. Let $X, Y \in \Sigma^b_1$, $Y \subseteq X \times 2^n$, and denote $Y_x = \{y \mid \langle x, y\rangle \in Y\}$.

Theorem: $T^1_2 + sWPHP(PV_2)$ proves: if

- $X \precsim_\varepsilon s$ and
- $Y_x \precsim_\varepsilon t$ for all $x \in X$,

then $Y \precsim \lfloor st(1+4\varepsilon)\rfloor$.



Theorem: $T^1_2 + rWPHP(PV_2)$ proves: if $Y \precsim_\varepsilon st$, then

- $X \precsim s - 1$ or
- there exists $x \in X$ such that $Y_x \precsim \lfloor t(1+2\varepsilon)\rfloor$.

Approximate enumeration

Theorem: $T^1_2 + rWPHP(PV_2)$ proves: let $X \in \Sigma^b_1$, and $\varepsilon^{-1} \in \mathrm{Log}$. There exist t, s such that $s \le t \le \lfloor s(1+\varepsilon) \rfloor$, and non-decreasing PV_2-retraction pairs

$$t \underset{f'}{\overset{f}{\rightleftarrows}} X \underset{g'}{\overset{g}{\rightleftarrows}} s$$

such that f, g are ≤ 2-to-1, and

$$\left\lfloor \frac{s}{t} u \right\rfloor \le g(f(u)) \le \left\lceil \frac{s}{t} u \right\rceil$$

for every $u < t$.

Example: the tournament principle

Recall the proof from slide #6:

Theorem: A tournament G with n players has a dominating set of size $\leq \log(n+1)$.

Proof: By induction on n. There are $n(n-1)/2$ matches in total, hence there exists a player v who wins $\geq (n-1)/2$ matches. By the induction hypothesis, the subtournament consisting of the $\leq (n-1)/2$ players who beat v has a dominating set D of size $\leq \log((n-1)/2+1) = \log(n+1)-1$, thus $D \cup \{v\}$ is a dominating set in the original tournament of size $\leq \log(n+1)$. QED

Let's translate it to bounded arithmetic.

Example: the tournament principle (cont'd)

Theorem: $T^1_2(G) + rWPHP(PV_2(G)) \subseteq T^3_2(G)$ proves the tournament principle.

Proof: We can work in $S^2_2(G) + sWPHP(PV_2(G))$ by conservativity. Notation: if $\langle a_i \mid i < k\rangle$ is a sequence of players, let $G(\vec{a}) = \{x < n \mid \forall i < k\; x \to a_i\}$.

Fix $\varepsilon^{-1} \in \mathrm{Log}$ such that $(1+\varepsilon)^{8(|n|+1)} < 2$. By Σ^b_2-$LIND$ on $k \le |n| + 1$, prove

$$(*) \qquad \exists \langle a_i \mid i < k\rangle \text{ such that } G(\vec{a}) \precsim_\varepsilon \left\lfloor \frac{n}{2^k}(1+\varepsilon)^{8k} \right\rfloor .$$

For $k = |n| + 1$, we get $G(\vec{a}) = \varnothing$, i.e., $\vec{a}$ is a dominating set of size $\le |n| + 1$. (We can remove the "$+1$" using shameless trickery.)

Example: the tournament principle (cont'd)

Assume $(*)$ for k. Find $s \le n2^{-k}(1+\varepsilon)^{8k}$ s.t. $G(\vec{a}) \precsim_\varepsilon \lfloor s(1+\varepsilon) \rfloor$, $G(\vec{a}) \not\precsim_\varepsilon s-1$. We have

$$\{\langle x,y\rangle \in G(\vec{a})^2 \mid x \ne y\} \precsim_\varepsilon \lfloor s^2(1+\varepsilon)^4 \rfloor,$$

thus (omitting the "$\in G(\vec{a})^2$")

$$\{\langle x,y\rangle \mid y \to x\} \precsim_\varepsilon \left\lfloor \frac{s^2}{2}(1+\varepsilon)^6 \right\rfloor \text{ or } \{\langle x,y\rangle \mid x \to y\} \precsim_\varepsilon \left\lfloor \frac{s^2}{2}(1+\varepsilon)^6 \right\rfloor.$$

WLOG the former. Then there exists $x \in G(\vec{a})$ s.t.

$$G(\vec{a},x) = \{y \in G(\vec{a}) \mid y \to x\} \precsim_\varepsilon \left\lfloor \frac{s}{2}(1+\varepsilon)^8 \right\rfloor \le \left\lfloor \frac{N}{2^{k+1}}(1+\varepsilon)^{8(k+1)} \right\rfloor.$$

QED

Application: collapse of hierarchies

A variant of the tournament principle is used in the proof by [KPT '91] that collapse of the T^i_2 hierarchy implies collapse of the polynomial hierarchy.

Previously known: $T^i_2 = S^{i+1}_2$ iff $T^i_2 = T_2$, and implies

- $\Sigma^P_{i+1} \subseteq \Delta^P_{i+1}/poly$, thus $PH = \Sigma^P_{i+2} = \Pi^P_{i+2}$ [KPT '91]
- T^i_2 proves $\Sigma^b_{i+1} \subseteq \Pi^b_{i+1}/poly$ and $\Sigma^b_\infty = \mathcal{B}(\Sigma^b_{i+2})$ [Buss '95, Zambella '96]

Approximate counting gives:

- T^i_2 proves $\Sigma^b_{i+1} \subseteq \Delta^b_{i+1}/poly$ and $\Sigma^b_\infty = \mathcal{B}(\Sigma^b_{i+1})$

(using also [CK '07])

Other applications

- intervals on models of T_2 admit nontrivial totally ordered approximate Euler characteristic (in the sense of [Krajíček '04])
- $T^1_2 + rWPHP(PV_2)$ proves Ramsey's theorem (but we should have already known that)
- $T^1_2 + rWPHP(PV_2)$ proves $S^P_2 \subseteq ZPP^{NP}$
- $T^1_2 + rWPHP(PV_2)$ proves $GI \in coAM$

Thank you for attention!

References

S. Buss, *Bounded arithmetic*, Bibliopolis, Naples, 1986.

———, *Relating the bounded arithmetic and polynomial time hierarchies*, APAL 75 (1995), 67–77.

S. Cook, J. Krajíček, *Consequences of the provability of* $\mathbf{NP} \subseteq \mathbf{P}/\mathbf{poly}$, JSL 72 (2007), 1353–1371.

E. Jeřábek, *Dual weak pigeonhole principle, Boolean complexity, and derandomization*, APAL 129 (2004), 1–37.

———, *Approximate counting in bounded arithmetic*, JSL 72 (2007), 959–993.

———, *Approximate counting by hashing in bounded arithmetic*, JSL 74 (2009), 829–860.

References (cont'd)

J. Krajíček, *Bounded arithmetic, propositional logic, and complexity theory*, Cambridge University Press, 1995.

———, *Approximate Euler characteristic, dimension, and weak pigeonhole principles*, JSL 69 (2004), 201–214.

J. Krajíček, P. Pudlák, G. Takeuti, *Bounded arithmetic and the polynomial hierarchy*, APAL 52 (1991), 143–153.

A. Maciel, T. Pitassi, A. Woods, *A new proof of the weak pigeonhole principle*, JCSS 64 (2002), 843–872.

N. Nisan, A. Wigderson, *Hardness vs. randomness*, JCSS 49 (1994), 149–167.

J. Paris, A. Wilkie, A. Woods, *Provability of the pigeonhole principle and the existence of infinitely many primes*, JSL 53 (1988), 1235–1244.

References (cont'd)

P. Pudlák, *Ramsey's theorem in bounded arithmetic*, Proc. CSL '90, LNCS 533, Springer, 1991, 308–317.

M. Sipser, *A complexity theoretic approach to randomness*, Proc. 15th STOC, 1983, 330–335.

N. Thapen, *The weak pigeonhole principle in models of bounded arithmetic*, Ph.D. thesis, Oxford University, 2002.

S. Toda, *On the computational power of PP and* $\oplus P$, Proc. 30th FOCS, 1989, 514–519.

D. Zambella, *Notes on polynomially bounded arithmetic*, JSL 61 (1996), 942–966.