HIIT FOUNDATIONS FRIDAY

ON COUNTING PROPOSITIONAL LOGIC AND WAGNER'S HIERARCHY

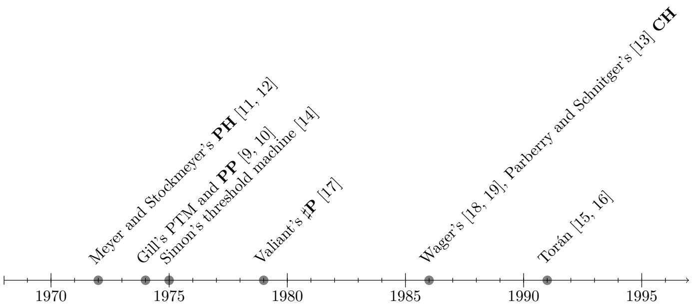
melissa.antonelli@helsinki.fi

Contents

1. On Wagner's Hierarchy

A *counting Turing machine* is a standard nondeterministic TM with an auxiliary output device that (magically) prints in binary notation on a special tape the number of accepting computations induced by the input [17, p. 191]

Probabilistic and Counting Computational Models and Classes



...there are many natural computational problems whose complexity cannot be modelized in terms of existential and universal quantifiers; on the other hand this complexity is captured by other complexity classes, more adapted to the idea of counting. [15, p. 213]

Definition 1 (Counting Hierarchy, Oracle Characterization [15, 16, 1]). *Let $n \geq 0$,*

$$\mathbf{CH}_0 = \mathbf{P}$$

$$\mathbf{CH}_{n+1} = \mathbf{PP}^{\mathbf{CH}_n}.$$

Date: April 21, 2023.

2. On (Univariate) Counting Propositional Logic

Definition 2 (Formulas of $\mathbb{CPL}_0$)**.** Formulas of $\mathbb{CPL}_0$ *are defined by the grammar below:*

$$F ::= \mathbf{i} \mid \neg F \mid F \wedge F \mid F \vee F \mid \mathbf{C}^q F \mid \mathbf{D}^q F$$

where $i \in \mathbb{N}$ *and* $q \in \mathbb{Q}_{[0,1]}$*.*

Let $\sigma(\mathscr{C})$ be the σ-algebra generated by $\mathscr{C}$, namely the set of all cylinders, (i.e. the smallest σ-algebra containing $\mathscr{C}$ and which is Borel), and μ denote the standard cylinder measure over $\sigma(\mathscr{C})$ (i.e. the unique measure on $\sigma(\mathscr{C})$ such that $\mu(\mathrm{Cyl}(i)) = \frac{1}{2}$), see [8].

Definition 3 (Semantics of $\mathbb{CPL}_0$)**.** *For each* $\mathbb{CPL}_0$*-formula,* F*, its interpretation is the* measurable *set,* $[\![F]\!] \in \mathscr{B}(2^{\mathbb{N}})$ *inductively defined as follows:*

$$[\![\mathbf{i}]\!] := \mathrm{Cyl}(i) \qquad [\![\mathbf{C}^q F]\!] := \begin{cases} 2^{\mathbb{N}} & \text{if } \mu([\![A]\!]) \geq q \\ \emptyset & \text{otherwise} \end{cases}$$

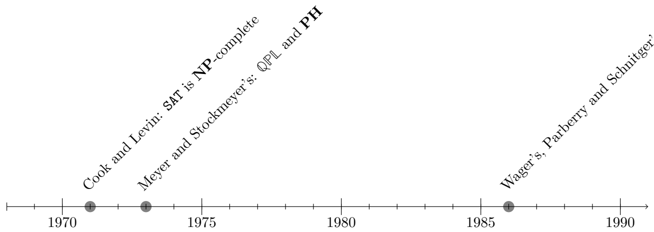
$$[\![\neg F]\!] := 2^{\mathbb{N}} - [\![F]\!]$$

$$[\![F \wedge G]\!] := [\![F]\!] \cap [\![G]\!] \qquad [\![\mathbf{D}^q F]\!] := \begin{cases} 2^{\mathbb{N}} & \text{if } \mu([\![A]\!]) < q \\ \emptyset & \text{otherwise.} \end{cases}$$

$$[\![F \vee G]\!] := [\![F]\!] \cup [\![G]\!]$$

3. Characterizing the Counting Hierarchy

Complete Problems and Classical Logic



Is there a logical system characterizing **CH** *in the same way*?

1. [19, Theorem 7]: For each level $\mathbf{CH}_k$ there is a complete problem W^k defined due to *counting operators over languages.*
2. From univariate $\mathbb{CPL}_0$ to multivariate $\mathbb{CPL}$:

$$\begin{array}{rcl} \mathbf{i} & \rightsquigarrow & \mathbf{i}_a \\ \mathbf{C}^q F & \rightsquigarrow & \mathbf{C}^q_a F. \end{array}$$

3. Every formula of $\mathbb{CPL}$ can be converted into *positive prenex normal form* (PPNF), where a formula of $\mathbb{CPL}$ is in PPNF if it is both in PNF and **D**-free.

Theorem 1 ([4, 7])**.** *The validity problem for formulas of* $\mathbb{CPL}$ *with* k *nested quantifiers is complete for* $\mathbf{CH}_k$*.*

4. Interested in Further Details?

On what partially introduced today,

- Counting propositional logics and Wagner's hierarchy [4, 7].
- Preliminary study on the expressive power of $\mathbb{CPL}_0$ as a model for stochastic experiments [2].

Other studies we are conducting on measure-quantified logics and probabilsitic computation:

- Probabilistic Curry-Howard correspondence: intuitionistic $\mathbf{i}\mathbb{CPL}_0$ and counting-typed randomized λ-calculus [6].
- Extended measure-quantified language for arithmetic and its relations with randomized computation [5].
- A randomized bounded theory to capture **BPP** (under review, abstract available [3]).

References

[1] E.W. Allender and K.W. Wagner. Counting Hierarchies: Polynomial Time and Constant Depth Circuits. In *Current Trends in Theoretical Computer Science*, pages 469–483, 1993.

[2] M. Antonelli. Two Remarks on Counting Propositional Logic. In *Proc. BEWARE*, AIxIA Conference, pages 20–32, 2023.

[3] M. Antonelli, U. Dal Lago, D. Davoli, I. Oitavem, and P. Pistone. Towards Randomized Bounded Arithmetic. In *Proc. AILA (Book of Abstract)*, 2022.

[4] M. Antonelli, U. Dal Lago, and P. Pistone. On Counting Propositional Logic and Wagner's Hierarchy. In *Proc. ICTCS*, pages 107–121, 2021.

[5] M. Antonelli, U. Dal Lago, and P. Pistone. On Measure Quantifiers in First-Order Arithmetic. In *Proc. CiE*, pages 12–24, 2021.

[6] M. Antonelli, U. Dal Lago, and P. Pistone. Curry and Howard Meet Borel. In *Proc. LICS*, pages 1–13, 2022.

[7] M. Antonelli, U. Dal Lago, and P. Pistone. Towards Logical Foudations for Probabilistic Computation. *Annals of Pure and Applied Logic*, to appear (we hope).

[8] P. Billingsley. *Probability and Measure*. Wiley, 1995.

[9] J.T. Gill. Computational Complexity of Probabilistic Turing Machines. In *Proc. STOC*, pages 91–95, 1974.

[10] J.T. Gill. Computational Complexity of Probabilistic Turing Machines. *SIAM Journal on Computing*, 6(4):675–695, 1977.

[11] A.R. Meyer and L.J. Stockmeyer. The Equivalence Problem for Regular Expressions with Squaring Requires Exponential Space. In *Proc. SWAT*, pages 125–129, 1972.

[12] A.R. Meyer and L.J. Stockmeyer. Word Problems Requiring Exponential Time (Preliminary Report). In *Proc. STOC*, pages 1–9, 1973.

[13] I. Parberry and G. Schnitger. Parallel Computation with Threshold Functions. *JCSS*, 36:278–302, 1988.

[14] J. Simon. *On Some Central Problems in Computational Complexity*. PhD thesis, Cornell University, 1975.

[15] J. Torán. An Oracle Characterization of the Counting Hierarchy. In *Proc. Structure in Complexity Theory Third Annual Conference*, pages 213–223, 1988.

[16] J. Torán. Complexity Classes defined by Counting Quantifiers. *Journal of the ACM*, 38(3):753–774, 1991.

[17] L.G. Valiant. The Complexity of Computing the Permanent. *TCS*, 8(2):189–201, 1979.

[18] K.W. Wagner. Compact Descriptions and the Counting Polynomial-Time Hierarchy. In *Frege Conference 1984: Proc. International Conference held at Schwerin*, pages 383–392, 1984.

[19] K.W. Wagner. The Complexity of Combinatorial Problems with Succinct Input Representation. *Acta Informatica*, 23:325–356, 1986.

5. Additional Material

5.1. Proof Theory of $\mathbb{CPL}_0$.

Definition 4 (Boolean Formula)**.** *The grammar of* Boolean formulas *is as below:*

$$\mathtt{b} ::= \mathtt{x}_i \mid \top \mid \bot \mid \neg \mathtt{b} \mid \mathtt{b} \wedge \mathtt{b} \mid \mathtt{b} \vee \mathtt{b},$$

where $i \in \mathbb{N}$. The interpretation *of a Boolean formula* $\mathtt{b}$ *is defined in an inductive way:*

$$[\![\mathtt{x}_i]\!] = Cyl i \qquad [\![\neg \mathtt{b}]\!] = 2^{\mathbb{N}} - [\![\mathtt{b}]\!]$$
$$[\![\top]\!] = 2^{\mathbb{N}} \qquad [\![\mathtt{b} \wedge \mathtt{c}]\!] = [\![\mathtt{b}]\!] \cap [\![\mathtt{c}]\!]$$
$$[\![\bot]\!] = \emptyset \qquad [\![\mathtt{b} \vee \mathtt{c}]\!] = [\![\mathtt{b}]\!] \cup [\![\mathtt{c}]\!].$$

Definition 5 (Labelled Formula)**.** *A* labelled formula *is an expression of one of the forms* $\mathtt{b} \rightarrowtail F$ *and* $\mathtt{b} \leftarrowtail F$*, where* $\mathtt{b}$ *is a Boolean formula and F is a counting one. A* labelled sequent *is a sequent of the form* $\vdash L$*, where L is a labelled formula.*

The proof system $\mathbf{LK}_{\mathbb{CPL}_0}$ is defined by the rules illustrated in Figure 1.

Initial Sequents

$$\frac{\mathtt{b} \models \mathtt{x}_n}{\vdash \mathtt{b} \rightarrowtail \mathbf{n}}\ Ax1 \qquad \frac{\mathtt{x}_n \models \mathtt{b}}{\vdash \mathtt{b} \leftarrowtail \mathbf{n}}\ Ax2$$

Set Rules

$$\frac{\vdash \mathtt{c} \rightarrowtail F \qquad \vdash \mathtt{d} \rightarrowtail F \qquad \mathtt{b} \models \mathtt{c} \vee \mathtt{d}}{\vdash \mathtt{b} \rightarrowtail F}\ R_{\cup}^{\rightarrowtail}$$

$$\frac{\vdash \mathtt{c} \leftarrowtail F \qquad \vdash \mathtt{d} \leftarrowtail F \qquad \mathtt{c} \wedge \mathtt{d} \models \mathtt{b}}{\vdash \mathtt{b} \leftarrowtail F}\ R_{\cap}^{\leftarrowtail}$$

Logical Rules

$$\frac{\vdash \mathtt{c} \leftarrowtail F \qquad \mathtt{b} \models \neg \mathtt{c}}{\vdash \mathtt{b} \rightarrowtail \neg F}\ R_{\neg}^{\rightarrowtail} \qquad \frac{\vdash \mathtt{c} \rightarrowtail F \qquad \neg \mathtt{c} \models \mathtt{b}}{\vdash \mathtt{b} \leftarrowtail \neg F}\ R_{\neg}^{\leftarrowtail}$$

$$\frac{\vdash \mathtt{b} \rightarrowtail F}{\vdash \mathtt{b} \rightarrowtail F \vee G}\ R1_{\vee}^{\rightarrowtail} \qquad \frac{\vdash \mathtt{b} \rightarrowtail G}{\vdash \mathtt{b} \rightarrowtail F \vee G}\ R2_{\vee}^{\rightarrowtail}$$

$$\frac{\vdash \mathtt{b} \leftarrowtail F \qquad \vdash \mathtt{b} \leftarrowtail G}{\vdash \mathtt{b} \leftarrowtail F \vee G}\ R_{\vee}^{\leftarrowtail} \qquad \frac{\vdash \mathtt{b} \rightarrowtail F \qquad \vdash \mathtt{b} \rightarrowtail G}{\vdash \mathtt{b} \rightarrowtail F \wedge G}\ R_{\wedge}^{\rightarrowtail}$$

$$\frac{\vdash \mathtt{b} \leftarrowtail F}{\vdash \mathtt{b} \leftarrowtail F \wedge G}\ R1_{\wedge}^{\leftarrowtail} \qquad \frac{\vdash \mathtt{b} \leftarrowtail G}{\vdash \mathtt{b} \leftarrowtail F \wedge G}\ R2_{\wedge}^{\leftarrowtail}$$

Counting Rules

$$\frac{\mu([\![\mathtt{b}]\!]) = 0}{\vdash \mathtt{b} \rightarrowtail F}\ R_{\mu}^{\rightarrowtail} \qquad \frac{\mu([\![\mathtt{b}]\!]) = 1}{\vdash \mathtt{b} \leftarrowtail F}\ R_{\mu}^{\leftarrowtail}$$

$$\frac{\vdash \mathtt{c} \rightarrowtail F \qquad \mu([\![\mathtt{c}]\!]) \geq q}{\vdash \mathtt{b} \rightarrowtail \mathbf{C}^q F}\ R_{\mathbf{C}}^{\rightarrowtail} \qquad \frac{\vdash \mathtt{c} \leftarrowtail F \qquad \mu([\![\mathtt{c}]\!]) < q}{\vdash \mathtt{b} \leftarrowtail \mathbf{C}^q F}\ R_{\mathbf{C}}^{\leftarrowtail}$$

$$\frac{\vdash \mathtt{c} \leftarrowtail F \qquad \mu([\![\mathtt{c}]\!]) < q}{\vdash \mathtt{b} \rightarrowtail \mathbf{D}^q F}\ R_{\mathbf{D}}^{\rightarrowtail} \qquad \frac{\vdash \mathtt{c} \rightarrowtail F \qquad \mu([\![\mathtt{c}]\!]) \geq q}{\vdash \mathtt{b} \leftarrowtail \mathbf{D}^q F}\ R_{\mathbf{D}}^{\leftarrowtail}$$

Figure 1. Sequent Calculus $\mathbf{LK}_{\mathbb{CPL}_0}$

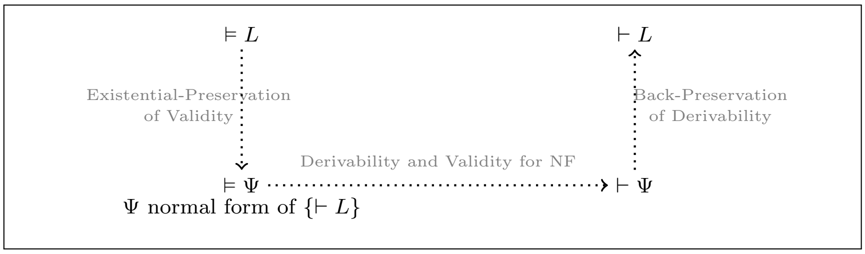


FIGURE 2. Skeleton of $\mathbf{LK}_{\mathbb{CPL}_0}$-Completeness Proof

5.2. **Multivariate $\mathbb{CPL}$.**
Language of $\mathbb{CPL}$.

Definition 6 (Formulas of $\mathbb{CPL}$)**.** Formulas of $\mathbb{CPL}$ *are defined by the grammar below:*

$$F ::= \mathbf{i}_a \mid \neg F \mid F \wedge F \mid F \vee F \mid \mathbf{C}^q_a F \mid \mathbf{D}^q_a F$$

where $i \in \mathbb{N}$*,* a *is a name, and* $q \in \mathbb{Q}_{[0,1]}$*.*

The intuitive meaning of *named* quantifiers is that they count models *relative* to the corresponding bounded variables. Named quantifiers, $\mathbf{C}^q_a, \mathbf{D}^q_a$, bind the occurrences of name a in A. Given a formula A, $\mathrm{FN}(A)$ denotes the set of names occurring *free* in A. Names can be used to distinguish between distinct groups of propositional variables.
Semantics of $\mathbb{CPL}$. The interpretation of a formula A now depends on the choice of a finite set of names $X \supseteq \mathrm{FN}(A)$ and is a measurable set $[\![A]\!]_X$ belonging to the Borel algebra, $\mathscr{B}((2^{\mathbb{N}})^X)$. The quantifiers $\mathbf{C}^q_a, \mathbf{D}^q_a$ correspond to operations allowing one to pass from $\mathscr{B}((2^{\mathbb{N}})^{X\cup\{a\}})$ to $\mathscr{B}((2^{\mathbb{N}})^X)$. To define such operations we need the following technical notation:

Definition 7 (f-projection)**.** *Let* X, Y *be two disjoint finite sets of names and* $f \in (2^{\mathbb{N}})^X$*. For all* $\mathcal{X} \subseteq (2^{\mathbb{N}})^{X\cup Y}$*, the* f-projection of $\mathcal{X}$ *is the set:*

$$\Pi_f(\mathcal{X}) = \{g \in (2^{\mathbb{N}})^Y \mid f + g \in \mathcal{X}\} \subseteq (2^{\mathbb{N}})^Y,$$

where $(f+g)(\alpha)$ *is* $f(\alpha)$*, if* $\alpha \in X$ *and* $g(\alpha)$ *if* $\alpha \in Y$*.*

Suppose X, Y are disjoint sets of names, with $FN(A) \subseteq X \cup Y$. Then, if we fix a valuation $f \in (2^{\mathbb{N}})^X$ of the variables of A with names in X, the set $\Pi_f\big([\![A]\!]_{X\cup Y}\big)$ describes the set of valuations of the variables of A with names in Y which extend f.

Definition 8 (Semantics of $\mathbb{CPL}$)**.** *For each formula* A *of* $\mathbb{CPL}$*, and finite set of names such that* $X \supset FN(A)$*, the* interpretation of A, $[\![A]\!]_X \subseteq (2^{\mathbb{N}})^X$*, is inductively defined as follows:*

$$\begin{aligned}
[\![\mathbf{i}_a]\!]_X &= \{f \mid f(a)(i) = 1\} & [\![\neg A]\!]_X &= (2^{\mathbb{N}})^X - [\![A]\!]_X \\
[\![A \wedge B]\!]_X &= [\![A]\!]_X \cap [\![B]\!]_X & [\![\mathbf{C}^q_a A]\!]_X &= \{f \mid \mu(\Pi_f([\![A]\!]_{X\cup\{a\}})) \geq q\} \\
[\![A \vee B]\!]_X &= [\![A]\!]_X \cup [\![B]\!]_X & [\![\mathbf{D}^q_a A]\!]_X &= \{f \mid \mu(\Pi_f([\![A]\!]_{X\cup\{a\}})) < q\}.
\end{aligned}$$

Example 1. *Let* F *be the formula of* $\mathbb{CPL}$*:*

$$F : \big(\mathbf{2}_a \wedge (\neg\mathbf{2}_b \wedge \mathbf{3}_b)\big) \wedge \big(\neg\mathbf{2}_a \wedge (\mathbf{2}_b \wedge \neg\mathbf{3}_b)\big) \vee \big((\neg\mathbf{2}_a \wedge \mathbf{3}_a) \wedge \mathbf{3}_b\big)$$

The valuations $f \in (2^{\mathbb{N}})^{\{b\}}$ *belonging to* $[\![\mathbf{C}^{1/2}_a F]\!]_{\{b\}}$ *are those which can be extended to valuations of all Boolean variables in* F*, satisfying in at least half of the cases. Let us list all possible cases:*

(1) $f(b)(2) = f(b)(3) = 1$*, then* F *has* $\frac{1}{4}$ *chances of being true, as both* $\neg\mathbf{2}_a$ *and* $\mathbf{3}_a$ *must be true.*

(2) $f(b)(2) = 1$ *and* $f(b)(3) = 0$*, then* F *has* $\frac{1}{2}$ *chances of being true, as* $\neg \mathbf{2}_a$ *must be true.*
(3) $f(b)(2) = 0$ *and* $f(b)(3) = 1$*, then* F *has* $\frac{3}{4}$ *chances of being true, as either* $\mathbf{2}_a$ *or both* $\neg \mathbf{2}_a$ *and* $\mathbf{3}_a$ *must be true.*
(4) $f(b)(2) = f(b)(3) = 0$*, then* F *has no chances of being true.*

Clearly, $[\![\mathbf{C}^{1/2}_a F]\!]_{\{b\}}$ *only contains the valuations which agree with cases 2. and 3. Therefore* $[\![\mathbf{C}^{1/2}\mathbf{C}^{1/2}_a F]\!]_{\emptyset} = 2^{\mathbb{N}}$ *– that is* $\mathbf{C}1/2_b \mathbf{C}^{1/2}_a F$ *is valid – since half of the valuations of* b *has at least* $\frac{1}{2}$ *chances of being extended to a model for* F*.*