Bounded Arithmetic and Randomized Computation

Riassunto

Davide Davoli

2 luglio 2022

Da novembre 2021 faccio parte di un progetto di ricerca che coinvolge assieme a me il Prof. Ugo Dal Lago, il Dott. Paolo Pistone, la Dott.ssa Melissa Antonelli dell'Università di Bologna e la Prof.ssa Isabel Oitavem dell'Università di Lisbona.

Il nostro lavoro di ricerca verte sull'estensione della teoria S_2^1 introdotta da S. Buss [3] per caratterizzare la classe **FP** [5] verso una nuova teoria, detta RS_2^1, in grado di catturare classi di complessità probabilistiche mediante lo sviluppo di una randomized bounded arithmetic. Un tale risultato permetterebbe, per esempio, di sviluppare caratterizzazioni puramente logiche di classi di complessità probabilistiche e, dunque, di studiare tali oggetti ed i problemi aperti ad essi legati senza impiegare metodi solamente combinatorici, ma anche quelli logici.

Preliminaries. In questo capitalo vengono introdotte alcune nozioni fondamentali per lo sviluppo dei capitoti successivi. In particolare, viene definita in modo formale la nozione di spazio di probabilità, assieme a quella di σ-algebra, e di misura. Nella sezione successiva, viene brevemente descritto il paradigma di computazione probabilistico e vengono definite le principali classi di complessità probabilistiche che catturano il concetto di *feasibility* in tale ambito. Infine, vengono introdotti alcuni risultati preliminari del lavoro di S. Buss per lo sviluppo di una bounded arithmetic in grado di catturare la classe di complessità **FP**.

A Randomized Bounded Arithmetic. Questo capitolo descrive come, partendo dal lavoro di Ferreira [6], sia possibile sviluppare una bounded arithmetic per catturare un'algebra di funzioni ivi introdotta e detta $\mathcal{POR}$. In primo luogo, viene definita tale algebra di funzioni e, assieme ad essa, il linguaggio al prim'ordine $\mathcal{L}$ assieme ad una semantica quantitativa che associa ad ogni formula un insieme misurabile anziché un valore binario di verità. Successivamente, viene definita una nozione di Σ_1^b-rappresentabilità sul modello di quella definita da Buss in []. Infine, viene descritto come è possibile provare che tutte le funzioni Σ_1^b-rappresentabili all'interno della teoria RS_2^1 appartengono a $\mathcal{POR}$. Nella sezione successiva, viene delineata la prova dell'inclusione inversa, seguendo [].

On the equivalence between PPT and $\mathcal{POR}$. Questo capitolo si occupa di studiare l'espressività delle funzioni che si trovano all'interno di $\mathcal{POR}$. In particolare, all'inizio del capitolo si congettura che tale classe di funzioni sia equivalente alla classe **PPT**, ossia l'insieme delle distribuzioni di stringhe che sono calcolabili da macchine di Turing probabilistiche in tempo al più polinomiale. Per provare tale congettura, vengono introdotti numerose classi di funzione, fondate

su diversi paradigmi di computazione, le quali le quali si dimostrano essere equivalenti l'una alle altre. La più importante di queste classi di funzioni è **SFP**. Essa contiene tutte le funzioni che sono calcolabili in tempo polinomiale da macchine di Turing dotate di un nastro aggiuntivo da cui leggono una sequenza infinita di bit casuali. In una prima parte del capitolo, viene provata un'equivalenza fra $\mathcal{POR}$ e **SFP**, passivamente viene provata l'equivalenza fra **SFP** e $\mathcal{POR}$, infine, l'equivalenza fra $\mathcal{POR}$ e **PPT**.

On the equivalence between FP and Cobham's Algebra. In questo capitolo vengono sfruttati i risultati del corollario precedente per derivare, come corollario, l'equivalenza fra la classe di funzioni computabili da una macchina di Turing in tempo polinomiale, detta **FP**, e le funzioni descritte da un'algebra di funzioni $\mathcal{F}_{\mathsf{Cob}}$ definita sul modello di quella proposta da Cobham, [5]. Infatti, questo risultato, per quanto ne siamo a conoscenza, non possiede alcuna prova sufficientemente esaustiva ed auto-contenuta, nonostante sia vastamente condiviso in letteratura. Dunque, dal momento che il modelli di calcolo su cui abbiamo definito **SFP** è molto simile a quello delle macchine di Turing così come l'algebra di funzioni $\mathcal{POR}$ è molto simile a $\mathcal{F}_{\mathsf{Cob}}$, abbiamo deciso di provare tale risultato. L'equivalenza fra **FP** e $\mathcal{F}_{\mathsf{Cob}}$ si ottiene dall'equivalenza fra $\mathcal{POR}$ e **SFP** mediante alcune semplici trasformazioni fra macchine di Turing.

Characterizing complexity classes. All'interno di quest'ultimo capitolo, studiamo come è possibile estendere ulteriormente il linguaggio $\mathcal{L}$ in modo da fare uso della nozione di Σ_1^b-rappresentabilità per caratterizzare note classi di complessità probabilistiche. A tal fine, prendendo ispirazione dall'aritmetica MQPA descritta in [2, 1], definiamo un'estensione di $\mathcal{L}$ mediante un quantificatore $\mathbf{C}^{s/t}F$ il cui valore di verità dipende direttamente dalla misura dell'insieme descritto dalla semantica F, ottenendo linguaggio $\mathcal{L}^{\mathsf{MQ}}$. Successivamente, sulla base delle definizioni delle classi di complessità probabilistiche date in precedenza, definiamo le caratterizzazioni di **BPP**, **RP**, co-**RP** e **ZPP** all'interno di $\mathcal{L}^{\mathsf{MQ}}$, provandone la correttezza.

Future Work. In questa sezione, congetturiamo la possibilità di ridurre il linguaggio $\mathcal{L}^{\mathsf{MQ}}$ al linguaggio della logica al prim'ordine. Questo processo richiederebbe la riduzione del quantificatore $\mathbf{C}^{s/t}$ ad un quantificatore a soglia su modello di [7], contestualmente a questa riduzione, tutto il linguaggio delle formule di $\mathcal{L}^{\mathsf{MQ}}$ sarebbe ridotto a quello standard della logica del prim'ordine, ad eccezione del quantificatore a soglia. Successivamente, sulla base di alcuni lavori simili [8, 4] ma su aritmetiche meno espressive, congetturiamo che, quantomeno nel contesto delle caratterizzazioni di classi di complessità probabilistiche, anche quest'ultimo quantificatore possa a sua volta essere ridotto ad un quantificatore al prim'ordine standard. Si potrebbe dunque identificare un sottoinsieme di **BPP** ricorsivamente enumerabile contenente tutti i problemi di quest'ultima classe che sono descritti da formule al prim'ordine provabili all'interno di un sistema come PA. Sarebbe dunque interessante studiare quali problemi che si congetturano essere in $\mathbf{BPP} \setminus \mathbf{P}$ si trovino in questa classe.

Riferimenti bibliografici

[1] M. Antonelli, U. Dal Lago e P. Pistone. "On Counting Propositional Logic and Wagner's Hierarchy". In: *Proc. ICTCS '21*. A cura di CEUR Workshop Proceedings. Vol. 3072. 2021, pp. 107–121.

[2] M. Antonelli, U. Del Lago e P. Pistone. "On Measure Quantifiers in First-Order Arithmetic". In: *Connecting with Computabiliy*. A cura di L. De Mol et al. Springer, 2021, pp. 12–24.

[3] S.R. Buss. "Bounded Arithmetic". Tesi di dott. Princeton University, 1986.

[4] Dmitry Chistikov, Christoph Haase e Alessio Mansutti. "Presburger arithmetic with threshold counting quantifiers is easy". In: *ArXiv* abs/2103.05087 (2021).

[5] Alan Cobham. "The Intrinsic Computational Difficulty of Functions". In: *Logic, Methodology and Philosophy of Science: Proceedings of the 1964 International Congress (Studies in Logic and the Foundations of Mathematics)*. A cura di Yehoshua Bar-Hillel. North-Holland Publishing, 1965, pp. 24–30.

[6] F. Ferreira. "Polyonmial Time Computable Arithmetic and Conservative Extesions". Ph.D. Dissertation. Dic. 1988.

[7] E. Gradel, M. Otto e E. Rosen. "Two-variable logic with counting is decidable". In: *Proceedings of Twelfth Annual IEEE Symposium on Logic in Computer Science*. 1997, pp. 306–317. DOI: 10.1109/LICS.1997.614957.

[8] Nicole Schweikardt. "Arithmetic, First-Order Logic, and Counting Quantifiers". In: *ACM Transactions on Computational Logic* 6 (dic. 2002). DOI: 10.1145/1071596.1071602.