Separating quantum and classical computing: rigorous proof and practical application

Marshall, S.C.

Samenvatting

Dit proefschrift onderzoekt en bewijst waar mogelijk de veronderstelde voordelen van quantum computing, eerst door te analyseren onder welke omstandigheden een voordeel theoretisch aanwezig kan zijn, en vervolgens door technieken te ontwikkelen en te onderzoeken om een praktisch voordeel te produceren.

Het inleidende hoofdstuk introduceert de kernconcepten die nodig zijn om te begrijpen wat quantum computing is, hoe het zich verhoudt tot concepten zoals complexiteitstheorie en machine learning, evenals geavanceerdere onderwerpen binnen quantum computing, zoals circuit cutting.

Het tweede hoofdstuk ontwikkelt het sterkste bewijs tot nu toe dat quantumcomputers kunnen bemonsteren uit verdelingen of functies kunnen berekenen die klassieke computers niet kunnen, wat we formaliseren als $\mathsf{SampP} \stackrel{?}{=} \mathsf{SampBQP}$ of $\mathsf{FBQP} \stackrel{?}{=} \mathsf{FBPP}$. Dit hoofdstuk herhaalt bestaande voorwaarden voor de scheiding van quantum en klassieke computing, vindt sterkere voorwaarden dan eerder bereikt en suggereert dat als quantumcomputers geen snelheidsvoordelen bieden ten opzichte van klassieke computers, zouden wijdverbreide overtuigingen over de complexiteitstheorie onjuist zijn. Deze vooruitgang wordt geboekt door aan te tonen dat exacte telling en benaderende telling verschillend moeten zijn, tenzij de polynomiale hiërarchie instort tot het tweede niveau.

Hoofdstuk 3 bouwt voort op Hoofdstuk 2 door te onderzoeken of advies de scheiding tussen klassieke en kwantumberekeningen kan beïnvloeden. Geïnspireerd door artikelen die taken identificeren die waarschijnlijk een kwantumvoordeel hebben, hebben ze alleen een kwantumvoordeel nodig

om samples voor te bereiden, zoals [38]. Dit hoofdstuk generaliseerde deze vraag eerst naar een adviesgenererende Turing-machine en een adviesontvangende machine. Deze generalisatie stond algemene regels toe, met name $\mathsf{P}/\mathsf{poly}^{\mathsf{B}} = \mathsf{P}^{\mathsf{Un(B)}}$. Dit resultaat laat zien dat advies van kwantumcomputers klassieke computers kan versterken, tenzij BQEXP=BPEXP (als kwantum- en klassieke machines even nuttig zijn als ze beide exponentieel lang mogen draaien). Dit hoofdstuk benadrukt de praktische implicaties van kwantumadviesgevers. Aangezien kwantumcomputers in eerste instantie erg duur zullen zijn, zal het belangrijk zijn om ze te kunnen gebruiken voor een klein deel van de totale berekening van een kwantumverbeterde taak.

Hoofdstukken 4 en 6 kunnen worden gezien als voortbouwend op het praktische gebruiksvoorbeeld van het vorige hoofdstuk, door beide te proberen beperkte moderne machines te verbeteren. Hoofdstuk 6 doet dit rechtstreeks door een model te ontwikkelen waarin een kwantummachine wordt gebruikt om een model voor te bereiden en te trainen dat vervolgens kan worden geïmplementeerd met alleen klassieke hardware. Het model blijkt universeel te zijn voor modellen die kwantum zijn voorbereid en klassiek zijn geïmplementeerd, daarom impliceren de resultaten van hoofdstuk 3 dat het krachtiger is dan klassieke modellen, tenzij BQEXP=BPEXP. Hoofdstuk 4 verbetert beperkte moderne machines door circuitsnijden toe te passen, waarbij een model wordt ontwikkeld dat uiteindelijk de opgeknipte versie van een geparametriseerd kwantumcircuit wordt, maar ook kan worden ingesteld om veel minder bronnen te gebruiken dan perfect circuitsnijden zou vereisen. Door experimenten wordt aangetoond dat dit model in staat is om distributies te leren die niet triviaal zijn voor een quantummachine (zoals handschrift), terwijl het nog steeds voordelen van de quantummachine behoudt (zoals het kunnen passen van quantumcircuits). Beide hoofdstukken onderzoeken de kracht van quantumcomputing door ons de mogelijkheid te bieden om quantumalgoritmen te bestuderen die we anders niet op moderne machines zouden kunnen bestuderen.

Hoofdstuk 5 heeft een andere toon dan de vorige hoofdstukken: in plaats van een onderzoekslijn voort te zetten om aan te tonen dat quantumcomputing krachtiger is dan klassieke computing, suggereert het dat een onderzoeksrichting, circuitsnijden, nooit een significante snelheidsverbetering kan opleveren. Dit wordt bereikt door aan te tonen dat als circuit cutting efficiënt zou kunnen worden gedaan, dan $\mathsf{BQP} = \mathsf{BPP}$. Dit heeft directe implicaties voor de resultaten van hoofdstuk 4, en laat zien dat dit model nooit zo goed kan zijn als een model op ware grootte voor alle taken. Het helpt ook om een aantal verbeteringen aan snijschema's te beperken en te sturen.

Al deze hoofdstukken laten kwantum-klassieke scheidingen zien of verschaffen informatieve resultaten voor degenen die een dergelijk verband proberen aan te tonen.