क्वांटम गणना: एक ट्यूटोरियल

सैमुअल एल.ब्रूनस्टीन

सार:

एक कंप्यूटर की कल्पना करें जिसका स्मृति अपने स्पष्ट भौतिक आकार की तुलना में तेजी से बड़ा है; एक कंप्यूटर जो एक साथ इनपुट के घातीय सेट में हेरफेर कर सकता है; एक कंप्यूटर जो हिल्बर्ट अंतरिक्ष के सांप क्षेत्र में गणना करता है। आप क्वांटम कंप्यूटर के बारे में सोच रहे होंगे। क्वांटम कंप्यूटर्स को एक संभावना बनाने के लिए क्वांटम यांत्रिकी से अपेक्षाकृत कुछ और सरल अवधारणाओं की आवश्यकता होती है। सूक्ष्मता इन अवधारणाओं में हेरफेर करने के लिए सीख रहा है। क्या ऐसा कंप्यूटर एक अनिवार्यता है या इसे बनाना मुश्किल होगा?

इस पेपर में हम एक ट्यूटोरियल देते हैं कि गणना को बेहतर बनाने के लिए क्वांटम यांत्रिकी का उपयोग कैसे किया जा सकता है। हमारी चुनौती: एक पारंपरिक कंप्यूटर के लिए एक बेहद मुश्किल समस्या को हल करना — एक बड़ी संख्या फैक्टरिंग की। एक प्रस्ताव के रूप में, हम गणना, सार्वभौमिक द्वार और मशीनों के मानक उपकरणों की समीक्षा करते हैं। इन विचारों को पहले शास्त्रीय, अपव्यय कंप्यूटर और फिर क्वांटम कंप्यूटर पर लागू किया जाता है। क्वांटम कंप्यूटर का एक योजनाबद्ध मॉडल इसके प्रोग्रामिंग में कुछ सूक्ष्मताओं के साथ-साथ वर्णित है। क्वांटम कंप्यूटर पर कुशलतापूर्वक फैक्टरिंग संख्याओं के लिए शोर एल्गोरिदम [1,2] दो भागों में प्रस्तुत किया जाता है: एल्गोरिदम के भीतर क्वांटम प्रक्रिया और क्लासिकल एल्गोरिदम जो क्वांटम प्रक्रिया को कॉल करता है। फैक्टरिंग में गणितीय संरचना जो शोर एल्गोरिदम संभव बनाता है, पर चर्चा की जाती है। हम आगामी वर्षों में क्वांटम गणना के लिए व्यवहार्यता और संभावनाओं के दृष्टिकोण के साथ निष्कर्ष निकाला है।

आइए हम समस्या को हाथ से वर्णन करके शुरू करें: अपने प्रमुख कारकों में एक संख्या एन को फैक्टर करना (उदा, संख्या 51688 को विघटित किया जा सकता है $2^3 \times 7 \times 13 \times 71$). एक विशेष एल्गोरिदम किसी समस्या को हल करने में कितनी तेज़ी से मापने का एक सुविधाजनक तरीका यह पूछना है कि 'इनपुट' के आकार के साथ एल्गोरिदम स्केल को पूरा करने के चरणों की संख्या कैसे एल्गोरिदम खिलाया जाता है। फैक्टरिंग समस्या के लिए, यह इनपुट केवल संख्या N है जिसे हम कारक बनाना चाहते हैं; इसलिए इनपुट की लंबाई है logN। (लॉगरिदम का आधार हमारी संख्या प्रणाली द्वारा निर्धारित किया जाता है। इस प्रकार 2 का आधार बाइनरी में लंबाई देता है; दशमलव में 10 का आधार।) 'उचित' एल्गोरिदम वे हैं जो इनपुट आकार में कुछ छोटे-डिग्री बहुपद के रूप में स्केल करते हैं (शायद 2 या 3 की डिग्री के साथ)।

पारंपरिक कंप्यूटरों पर सबसे अच्छी तरह से ज्ञात फैक्टरिंग एल्गोरिदम चलता है O(exp[(64/9)1/3(ln N)1/3(ln ln N)2/3]) कदम [3] इसलिए, यह एल्गोरिदम इनपुट आकार के साथ तेजी से स्केल करता है log N. उदाहरण के लिए, 1994 में 129

दुनिया भर में फैले लगभग 1600 कार्यस्थानों पर इस एल्गोरिदम का उपयोग करके फैक्टर किया गया; पूरे कारक में आठ महीने लगे [4]। उपर्युक्त घातीय स्केलिंग के प्रीफैक्टर का अनुमान लगाने के लिए इसका उपयोग करके, हम पाते हैं कि एक ही कंप्यूटर पावर के साथ 250 अंकों की संख्या को कारक करने में लगभग 800,000 साल लगेंगे; इसी प्रकार, एक 1000 अंक संख्या के लिए वर्षों की आवश्यकता होगी (ब्रह्मांड की उम्र से काफी हद तक लोन जीर)। बड़ी संख्या में फैक्टरिंग की कठिनाई सार्वजनिक कुंजी क्रिप्टोसिस्टम के लिए महत्वपूर्ण है, जैसे कि बैंकों द्वारा उपयोग किए जाने वाले। वहां, ऐसे कोड लगभग 250 अंकों के साथ फैक्टरिंग संख्याओं की कठिनाई पर भरोसा करते हैं।

हाल ही में, एक एल्गोरिदम एक क्वांटम कंप्यूटर पर फैक्टरिंग संख्याओं के लिए विकसित किया गया था। जो चलता है, O((log N)2+∈) कदम जहा ∈ छोटा है[1] । यह इनपुट आकार में मोटे तौर पर वर्गबद्ध है, इसलिए इस तरह के एल्गोरिदम के साथ 1000 अंकों की संख्या को फैक्टर करने के लिए केवल कुछ मिलियन चरणों की आवश्यकता होगी। निहितार्थ यह है कि फैक्टरिंग के आधार पर सार्वजनिक कुंजी क्रिप्टोसिस्टम टूटने योग्य हो सकते हैं।

आपको यह पता लगाने के लिए कि यह घातीय सुधार कैसे संभव हो सकता है, हम एक प्राथमिक क्वांटम यांत्रिक प्रयोग की समीक्षा करते हैं जो दर्शाता है कि ऐसी शक्ति कहां छिपी हुई है [5] दो-स्लिट प्रयोग क्वांटम यांत्रिक व्यवहार को देखने के लिए प्रोटोटाइपिक है: एक स्रोत फोटॉन, इलेक्ट्रॉन या अन्य कणों को उत्सर्जित करता है जो स्लिट की एक जोड़ी पर पहुंचते हैं। ये कण एकतापूर्ण विकास और अंततः माप से गुजरते हैं। हम एक हस्तक्षेप पैटर्न देखते हैं, दोनों स्लिट खुले होते हैं, जो स्लिट कवर होने पर पूरी तरह गायब हो जाते हैं। कुछ अर्थ में, कण समानांतर में दोनों स्लिट के माध्यम से गुजरते हैं। यदि ऐसा एकतात्मक विकास गणना (या गणना के भीतर एक ऑपरेशन) का प्रतिनिधित्व करना था तो क्वांटम सिस्टम समांतर में कंप्यूटेशंस कर रहा होगा। क्वांटम समांतरता मुफ्त में आता है। इस प्रणाली का उत्पादन समानांतर गणनाओं के बीच रचनात्मक हस्तक्षेप द्वारा दिया जाएगा।

- संदर्भ
- इस दस्तावेज़ के बारे में ...

Source: http://www-users.cs.york.ac.uk/~schmuel/comp/comp.html

May 13, 2018 1:29 pm