Proveravanje modela kvantnih programa korišćenjem kvantnih Markovljevih lanaca

Uroš Ševkušić
2007/2024

28. avgust 2025.

1 Uvod

Kvantno računarstvo je jedna od novijih oblasti računarstva čije prednosti u odnosu na klasično računarstvo su počele da se otkrivaju 90-tih godina prošlog veka kroz radove Dojča i Jože [5], Bernštajna i Vaziranija [4], Sajmona [12], Grovera [7] i Šora [10] i [11].

Iako su kvantno i klasično računarstvo ekvivalentni u smislu da je ista klasa problema rešiva na oba modela računarstva, postoje neke suštinske razlike u radu kvantnih računara u odnosu na klasične:

1. Klasična stanja su bitovi 0 i 1.

   Kvantna stanja su vektori $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ i $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ i bilo koja linearna kombinacija $\alpha\,|0\rangle + \beta\,|1\rangle$ sa kompleksnim koeficijentima α, β, gde je $||\alpha||^2 + ||\beta||^2 = 1$. Dakle, kvantni računar dozvoljava i stanja *između* 0 i 1. Kvantna stanja se nazivaju *kubiti*. Vektori v koji određuju kvantna stanja se beleže $|v\rangle$, a konjugovani transponat od $|v\rangle$ se obeležava sa $\langle v|$.

2. Na klasičnom računaru su operacije logička kola, a na kvantnom su unitarne transformacije [1].

[1] Unitarna transformacija je određena unitarnom matricom. Unitarna matrica M je ona za koju važi $MM^\dagger = I$ i $M^\dagger M = I$, gde je $M^\dagger$ konjugovani transponat matrice M, a I je jedinična matrica $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

3. Čitanje podataka na klasičnom računaru je deterministička operacija koja vraća trenutno stanje i trenutno stanje se ne menja posle čitanja.

   Na kvantnom računaru se jedino mogu pročitati osnovna stanja $|0\rangle$ i $|1\rangle$: $|0\rangle$ sa verovatnoćom $||\alpha||^2$, $|1\rangle$ sa verovatnoćom $||\beta||^2$. Nakon čitanja će kubit završiti u pročitanom stanju.

4. Sistem od više bitova se uvek može zapisati kao konkatenacija stanja pojedinačnih bitova na klasičnom računaru.

   Na kvantnom računaru, konkatenacija stanja je primena operacije tenzorskog proizvoda $\otimes$ nad pojedinačnim kubitima [2]. Postoje sistemi od više kubita koji se ne mogu predstaviti kao tenzorski proizvod pojedinačnih kubita. Glavni primer je stanje $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$. Za bilo koji izbor vektora $|v\rangle = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$ i $|w\rangle = \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}$, jednačina $|\Phi^+\rangle = |v\rangle \otimes |w\rangle$ nema rešenja. Pojava da se kvantno stanje sistema od više kubita ne može predstaviti kao tenzorski proizvod pojedinačnih kubita se naziva *kvantno sprezanje* (eng. *quantum entanglement*).

5. Na klasičnom računaru je moguće kopirati stanje nekog sistema.

   Na kvantnom računaru nije moguće napraviti kopiju nepoznatih kvantnih stanja. Intuitivno, to je zato što bismo morali da pročitamo kvantno stanje sistema, a time dobijamo samo deo informacije. Nakon čitanja, sistem se menja i dalje nije moguće izvući korisne informacije o prethodnom stanju sistema. Formalan dokaz za nemogućnost kloniranja se nalazi u radu [14].

Kvantna informatika je oblast kvantnog računarstva koja se bavi slanjem informacija korišćenjem kvantnih i klasičnih kanala. Klasični kanal je onaj koji prosleđuje bitove, a kvantni onaj koji prosleđuje kubite. Jedan od najpoznatijih algoritama iz kvantne informatike je algoritam kvantnog teleportovanja [3]. Takođe, poznati su i neki protokoli iz kvantne kriptografije, od kojih je protokol $BB84$ [2] jedan od najstarijih.

Zbog pojave kvantne spregnutosti i potrebe da se barem neka informacija dobije o stanjima pojedinačnih kubita u spregnutim stanjima, u kvantnoj informatici se koristi drugačija formalizacija kvantnih stanja. Umesto vektora,

[2] Za definiciju tenzorskog proizvoda, pogledati ubženike iz linearne algebre, na primer [9]

stanje kvantnog sistema od jednog ili više kubita se zapisuje kao ermitska[3] matrica A dimenzija $2^n \times 2^n$ (n je broj kubita u sistemu) čiji je trag 1 i za koju važi osobina pozitivnosti: za sve $|v\rangle$ važi $\langle v| A |v\rangle \geq 0$. Matrica A se naziva matricom gustine (eng. *density matrix*). Više o matricama gustine se može naći u relevantnim udžbenicima iz kvantnog računarstva, na primer [8].

Ovde ćemo prikazati kako se, imajući u vidu razlike između kvantnog i klasičnog računarstva, i reprezentaciju kvantnih stanja pomoću matrica gustine, mogu preurediti tehnike proveravanja modela zasnovanih na Markovljevim lancima za verifikaciju protokola iz kvantne informatike. Jedan od glavnih radova iz te oblasti je rad [6] autora Juana Fenga, Nengkuna Jua i Mingšeng Jinga.

2 Markovljevi lanci

Markovljevi lanci su detaljno izučavana oblast koja je, osim u verifikaciji probabilističkih sistema, našla primenu i u drugim oblastima računarstva. Jedan od poznatih primera primene Markovljevih lanaca je derandomizacija probabilističkih algoritama i generisanje efikasnijih procedura za poboljšanje verovatnoće uspeha kod takvih algoritama. Za te primene Markovljevih lanaca, pogledati pregled [13] koji je dao profesor Salil Vadan.

Markovljev lanac karakterišu naredni elementi:

- skup stanja: to mogu biti stanja nekog programa. Na primer, stanje programa može biti definisano kao skup promenljivih sa njihovim trenutnim vrednostima, zajedno sa narednom naredbom koja se izvršava na računaru.

- prelazi između stanja obeleženi nekim brojem $0 \leq p \leq 1$: opisuju kako se iz jednog stanja sistema prelazi u drugo. Broj p ovde označava verovatnoću da se prelaz desi. Recimo, bacanjem novčića odlučujemo da li je naredna naredba $x+ = 1$ ili je to $x- = 1$ sa verovatnoćom 0.8 za prvi događaj i 0.2 za drugi.

- skup inicijalnih stanja sa dodeljenim verovatnoćama da sistem počne u tom stanju

[3] Matrica M je ermitska ako je $M^\dagger = M$.

- skup atomskih logičkih formula: to su prosti iskazi koji mogu da važe ili da ne važe u stanjima. Recimo, $x \neq 0$ je atomska formula i ona ne važi u stanju gde je $x = 0$, a važi u stanju gde je $x = 2$.

- funkcija koja mapira skup stanja u podskup atomskih formula koje u njemu važe.

Jedno lepo svojstvo Markovljevih lanaca, a koje važi u velikom broju situacija, jeste činjenica da oni *ne pamte* prethodna stanja. To znači da na verovatnoću prelaza iz stanja s u stanje q ne utiču prethodni prelazi koji su doveli do stanja s. To znači da su ti događaji zapravo nezavisni, što olakšava računanje verovatnoća složenijih događaja, kao što je "da li je skup stanja B dostižan iz početnog stanja".

Za verifikaciju sistema zasnovanim na Markoljevim lancima, postoji logički jezik PCTL. Jezik PCTL je skraćenica za Probabilistic Computational Tree Logic, odnosno Probabilistic CTL. On predstavlja ekstenziju jezika CTL koja obuhvata i iskaze vezane za verovatnoću da se neki događaj dogodi (ili ne dogodi) tokom izvršavanja. Jezik PCTL se zasniva na *formulama stanja* i *formulama puta*. Formule stanja Φ mogu biti oblika:

- a, gde je a atomska formula,

- $\Phi_1 \wedge \Phi_2$, gde su Φ_i formule stanja,

- $\neg\Phi$, gde je Φ formula stanja,

- $P_J(\phi)$, gde je ϕ formula puta i J je neki podinterval od $[0, 1]$.

Formule puta mogu biti oblika:

- $\bigcirc\Phi$, za formulu stanja Φ,

- $\Phi_1 \mathcal{U} \Phi_2$, za formule stanja Φ_i,

- $\Phi_1 \mathcal{U}^{\leq n} \Phi_2$, za formule stanja Φ_i.

Da li formula stanja Φ važi u stanju s se definiše rekurzivno:

- a važi u s ako atomska formula a važi u s,

- $\Phi_1 \wedge \Phi_2$ važi u s ako Φ_i važe u s,

- $\neg\Phi$ važi u s ako Φ ne važi u s,

- $P_J(\phi)$ važi u s ako je verovatnoća da formula ϕ važi na proizvoljnom beskonačnom putu koji počinje u s i ide kroz Markovljev lanac u intervalu J. Da bi verovatnoće ovakvih događaja mogle da se mere, potrebno je zadati sigma algebru skupova, počevši od nekih elementarnih događaja i kvantnifikovanjem verovatnoća da se oni dogode. Elementarni događaji su "beskonačan put počinje sa $s_1, s_2, \ldots, s_n$", za sve $n \in \mathbb{N}$, odnosno skupovi $Cyl(s_1 s_2 \ldots s_n) = \{\pi \in \text{Paths} | \pi[j] = s_j, 1 \leq j \leq n\}$ su elementarni događaji za sve $n \in \mathbb{N}$ i proizvoljne $s_1, s_2, \ldots, s_n$. Ovakvi skupovi se nazivaju i *cilindrični skupovi*. Verovatnoća elementarnih događaja se računa tako što se pomnože verovatnoće odgovarajućih grana na tom putu sa verovatnoćom da put počinje u s_1. Dakle, to bi bio proizvod $p_{s_{n-1} \to s_n} \ldots p_{s_1 \to s_2} p_{init(s_1)}$. Ostali događaji se definišu na osnovu ovih i postoje detaljno opisane procedure za izračunavanje tih verovatnoća u knjizi [1].

Da li formula puta ϕ važi na beksonačnom putu π se definiše rekurzivno:

- $\bigcirc\Phi$ važi na π ako formula Φ važi na drugom stanju tog puta. Dakle, ako je put $\pi = s_1, s_2, \ldots$, onda formula $\bigcirc\Phi$ važi na π ako Φ važi u stanju s_2. Ova formula je bez izmena preuzeta iz jezika CTL i naziva se *next operator*.

- $\Phi_1 \mathcal{U} \Phi_2$ važi na π ako postoji neko stanje s_j na tom putu na kom važi Φ_2, a na stanjima pre s_j na tom putu uvek važi Φ_1. Ova formula je bez izmena preuzeta iz jezika CTL i naziva se *until operator*.

- $\Phi_1 \mathcal{U}^{\leq n} \Phi_2$ važi na π važi na π ako postoji stanje s_j, za $j \leq n$, na tom putu na kom važi Φ_2, a na stanjima pre s_j na tom putu uvek važi Φ_1.

Postoje poznati algoritmi koji proveravaju da li formula iz jezika PCTL važi. Osnovna ideja je da se koristi rekurzivna struktura PCTL formula stanja i formula puta tako što se prvo izračunaju skupovi stanja na kojima važe potformule, nakon čega se potformule zamene atomskim formulama koje važe na stanjima na kojima važe te potformule. Na primer, ako formula Φ_1 važi u stanjima p, q, r, onda možemo formulu Φ_1 zameniti atomskom formulom a_1 i Markovljev lanac preurediti tako što se stanjima p, q, r dodaje formula a_1. Tako se postepeno problem računanja formule olakšava. Na primer, lakše je odrediti koji skup zadovoljava formulu $a_1 \wedge a_2$ nego $\Phi_1 \wedge \Phi_2$.

3 Kvantni Markovljevi lanci

Da bi se ispoštovale razlike koje kvantno računarstvo ima u odnosu na klasično, osmišljen je kvantni Markovljev lanac i logički jezik QCTL. Intuicija iza kvantnih Markovljevih lanaca je ista kao i kod običnih Markovljevih lanaca. Štaviše, kvantni Markovljev lanac može da se posmatra kao uopštenje Markovljevih lanaca.

Ključna izmena Markovljevog lanca je to što na granama između stanja nije broj p, već se na granama nalaze linearna preslikavanja koja preslikavaju prostor matrica u prostor matrica. Takva preslikavanja se zovu nadoperatori (eng. *superoperator*), jer matrica se posmatra kao linearni operator, a onda operator koji slika operator u operator je nadoperator. Biraju se nadoperatori, jer kvatna stanja nisu vektori kolona, već su matrice. Zato operacije množenja unitarnom transformacijom i kvantno merenje ne mogu više biti obične matrične operacije kao do sada, već se podižu na nivo nadoperatora.

Ako sistem polazi iz stanja Q, njegovu evoluciju možemo opisati kao sukcesivnu primenu nadoperatora. Dakle, svaki put u kvantnom Markovljevom lancu odgovara sukcesivnoj primeni nadoperatora $\mathcal{Q}_n\mathcal{Q}_{n-1}\ldots\mathcal{Q}_1Q$. [4] Glavna ideja je da trag matrice $\mathcal{Q}_n\mathcal{Q}_{n-1}\ldots\mathcal{Q}_1Q$ opisuje verovatnoću da beskonačan put počinje u stanju Q i da u prvih n koraka primenimo operatore $\mathcal{Q}_i$. Elementarni događaji su isti kao i kod Markovljevih lanaca, samo što sada nemamo proizvod verovatnoća na granama kao meru verovatnoće, već imamo proizvod nadoperatora sa početnim stanjem. Dakle, umesto da verovatnoća nekog događaja bude broj, ona će biti operator. Ovo se može primeniti u verifikaciji tako što se definiše jezik QCTL (Quantum CTL), koji predstavlja ekstenziju jezika CTL.

Jezik QCTL je jako sličan jeziku PCTL: jedina izmena je što se u QCTL-u $P_J(\phi)$ menja sa $Q_{\lesssim\mathcal{E}}(\phi)$ i $Q_{\gtrsim\mathcal{E}}(\phi)$, gde je $\mathcal{E}$ proizvoljni nadoperator. Relacija $\mathcal{Q} \lesssim \mathcal{E}$ se definiše tako da važi ako, za sva kvantna stanja q, $Tr(\mathcal{Q}(q)) \leq Tr(\mathcal{E}(q))$. Slično se definiše $\gtrsim$, a ako važe obe relacije, onda pišemo $\mathcal{Q} \simeq \mathcal{E}$. Dakle, $Q_{\lesssim\mathcal{E}}(\phi)$ kaže "verovatnoća da na proizvoljnom putu π koji počinje sa kvantnim stanjem q važi formula puta ϕ nije veća od $Tr(\mathcal{E}(q))$". Na primer, formula ϕ može da tvrdi "ovaj protokol se nikada neće prekinuti" ili "desiće se da ćemo se nekada u budućnosti naći u stanju gde je kubit q u stanju ψ". Formula $Q_{\lesssim\mathcal{E}}(\phi)$ onda tvrdi "ovaj protokol se neće prekinuti sa verovatnoćom

[4] Kompoziciju nadoperatora pišemo kao proizvod, jer su i nadoperatori linearni operatori, pa imaju svoju matričnu reprezentaciju.

manjom od $Tr(\mathcal{E}(q))$" ili "sa verovatnoćom manjom od $Tr(\mathcal{E}(q))$, desiće se nekada u budućnosti da će stanje kubita q biti ψ". Razlog zašto umesto konkretnog intervala stoji nadoperator $\mathcal{E}$ je što je moguće porediti nadoperator putanje $\mathcal{Q}_n\mathcal{Q}_{n-1}\ldots\mathcal{Q}_1$ sa $\mathcal{E}$. Ovde je trag matrice ključan, a izbor nadoperatora $\mathcal{E}$ nije bitan. Može se, bez narušavanja cele ove strukture, $\mathcal{E}$ zameniti bilo kojim drugim nadoperatorom čiji je trag u počenim stanjima sistema onaj koji tražimo.

Da bi se proverilo da li QCTL formula važi za neko početno stanje, koriste se slične tehnike kao i u proveravanju modela u PCTL jeziku. Razlike koje dolaze iz činjenice da koristimo nadoperatore umesto konkretnih brojeva za verovatnoće se mogu uskladiti korišćenjem tehnika iz [6]. Glavni problem je bio izračunavanje nadoperatora koji opisuju događaje $\bigcirc\Phi$, $\Phi_1\mathcal{U}\Phi_2$ i $\Phi_1\mathcal{U}^{\leq n}\Phi_2$ u kvantnom Markovljevom lancu. Autori su našli proceduru za izračunavanje jednostavnijeg nadoperatora koji je $\simeq$-ekvivalentan sa nadoperatorom događaja. To znači da se računanje verovatnoće može rešiti sada tako što se nađe vrednost početnog stanja kvantnog programa u tom jednostavnijem operatoru, pa se od rezultata uzme trag matrice. Ostalo je sve isto kao u PCTL-u.

Ovaj pristup je implementiran u alatu IscasMC. Alat je dostupan na linku https://tis.ios.ac.cn/tool/qmc/. U alatu je definisan poseban jezik za opisivanje kvantnih programa, odgovarajućih nadoperatora i zahteva u vidu logičkih iskaza u jeziku QCTL.

4 Zaključak

U ovom radu smo videli kako se tehnike modelovanja i proveravanja modela pomoću Markovljevih lanaca i jezika PCTL mogu preraditi da bi se dobile efikasne procedure za proveravanje kvantnih programa. Prikazan je kvantni Markovljev lanac i objašnjene su sličnosti sa klasičnim Markovljevim lancima. Takođe je obrađen jezik QCTL i dat je opis tehnika korišćenih da se proveri da li formula u tom jeziku važi.

Literatura

[1] Christel Baier and Joost-Pieter Katoen. *Principles of Model Checking (Representation and Mind Series)*. The MIT Press, 2008.

[2] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, 2014. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[3] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, Mar 1993.

[4] Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. In *Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing*, STOC '93, page 11–20, New York, NY, USA, 1993. Association for Computing Machinery.

[5] David Deutsch and Richard Jozsa. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences*, 439:553 – 558, 1992.

[6] Yuan Feng, Nengkun Yu, and Mingsheng Ying. Model checking quantum markov chains. *Journal of Computer and System Sciences*, 79(7):1181–1198, 2013.

[7] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '96, page 212–219, New York, NY, USA, 1996. Association for Computing Machinery.

[8] David McMahon. *Quantum Computing Explained*. Wiley-IEEE Computer Society Pr, 2007.

[9] Steven Roman. *Advanced Linear Algebra*. Springer-Verlag, New York, NY, third edition, 2007.

[10] Peter W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[11] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.*, 41:303–332, 1995.

[12] Daniel R. Simon. On the power of quantum computation. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 116–123, 1994.

[13] Salil P. Vadhan. *Pseudorandomness*. Now Publishers Inc., Hanover, MA, USA, 2012.

[14] William K. Wootters, William K. Wootters, and Wojciech H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.