Um Algoritmo Quântico para um Problema de Distância Estatística*

Henrique Hepp[1], **Murilo V. G. da Silva**[1], **Leandro M. Zatesko**[2]

[1]Departamento de Informática, Universidade Federal do Paraná

[2]Departamento Acadêmico de Informática, Universidade Tecnológica Federal do Paraná

{hhepp,murilo}@inf.ufpr.br, zatesko@utfpr.edu.br

Abstract. *In the Statistical Distance to Uniform Distribution (SDU) problem, the aim is to compare a probability distribution over all n-bit strings with the uniform distribution. In this paper, we deal with the restriction of SDU in which the probabilities of the $2^n/2$ first strings (under the usual lexicographic ordering) are never smaller than the $2^n/2$ last strings. We prove that this restriction admits a polynomial-time quantum algorithm.*

Resumo. *No problema Distância Estatística para Distribuição Uniforme (SDU), o objetivo é comparar uma distribuição de probabilidade sobre as strings de n bits com a distribuição uniforme. Neste trabalho, lidamos com a restrição de SDU em que as probabilidades das $2^n/2$ primeiras strings (sob a ordenação lexicográfica usual) nunca são menores que as das $2^n/2$ últimas. Provamos que esta restrição admite um algoritmo quântico polinomial.*

1. Introdução

Distância Estatística para Distribuição Uniforme (*SDU*), conforme definido a seguir, é um problema de promessa em que precisamos comparar uma distribuição de probabilidade X com a distribuição uniforme U_n, ambas sobre todas as strings com n bits, perguntando-nos o quão próximo a *distância estatística* $\Delta(X, U_n)$ está de 0 ou de 1. Este problema é completo para NISZK, a classe dos problemas que admitem um protocolo não-interativo de conhecimento zero estatístico [Goldreich et al. 1999].

SDU

Dados:	um inteiro não-negativo n e um circuito booleano C de tamanho polinomial em n com n bits de saída, o qual codifica uma distribuição de probabilidade X sobre todas as strings com n bits;
decidir entre:	*instância positiva:* $\Delta(X, U_n) < 1/n$; *instância negativa:* $\Delta(X, U_n) > 1 - 1/n$;

prometido que vale um dos casos.

Não se sabe se SDU está em BQP, a classe dos problemas que admitem algoritmos quânticos polinomiais.

Distância Estatística entre Distribuição Biparticionada e Distribuição Uniforme (*BSDU*) é o problema SDU restrito a distribuições de probabilidade *biparticionadas*. No

*Realizado com apoio parcial de CAPES (código 001) e CNPQ (428941/2016-8).

nosso contexto, dizemos que uma distribuição de probabilidade Y sobre todas as strings com n bits, codificada por um circuito booleano C com n bits de saída, é *biparticionada* se, para qualquer string x dentre as $2^n/2$ *primeiras* (sob a ordenação lexicográfica usual $00\cdots00, \ldots, 11\cdots11$) e qualquer string y dentre as $2^n/2$ *últimas*, a probabilidade de se obter x como saída de C é não menor que a probabilidade de se obter y.

Neste trabalho, provamos que BSDU está em BQP, exibindo um algoritmo quântico polinomial para o problema. Em contrapartida, parece não haver uma maneira direta de se colocar o problema em BPP usando técnicas análogas, uma vez que nosso algoritmo trata todas as 2^n strings em sobreposição quântica.

Este trabalho está organizado do seguinte modo: na Seção 2, apresentamos alguns preliminares e, na Seção 3, a demonstração de que BSDU está em BQP.

2. Preliminares[1]

Sendo o estado de um sistema quântico um vetor unitário de números complexos representado por $|\psi\rangle$, seu transposto conjugado é representado por $\langle\psi|$. O produto interno entre dois vetores ψ_1, ψ_2 é representado por $\langle\psi_1|\psi_2\rangle$. O produto diádico entre ψ_1 e ψ_2 é representado por $|\psi_1\rangle\langle\psi_2|$. Um estado $|\psi\rangle$ em um espaço $\mathbb{C}^N$ pode ser descrito pela combinação linear de N estados linearmente independentes $|\psi\rangle = \alpha_1|1\rangle + \alpha_2|2\rangle + \cdots + \alpha_N|N\rangle$, para $\alpha_1, \cdots \alpha_N \in \mathbb{C}$, dizemos que esses N estados estão em *sobreposição*. Um *qubit* é um estado quântico $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, para $\alpha, \beta \in \mathbb{C}$ e $|\alpha|^2 + |\beta|^2 = 1$. Um estado quântico de n qubits é um produto tensorial entre n qubits.

Dado o estado $|\Psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle$, podemos fazer uma *medição quântica* de $|\Psi\rangle$ com relação à base $\{|0\rangle, |1\rangle, \cdots, |2^n-1\rangle\}$, obtendo um dos estados $|i\rangle$ com probabilidade $|\alpha_i|^2$. Um *circuito quântico* é um grafo dirigido acíclico em que cada vértice é ou uma transformação unitária (representada por uma matriz unitária), ou uma medição agindo sobre um qubit. O *tamanho do circuito* é o número de vértices do grafo.

Sendo $|\psi_1\rangle, \ldots, |\psi_k\rangle$ estados quânticos de n qubits, um *estado misto* de n qubits é representado por *um operador de densidade*, ou *matriz de densidade*, que é a matriz de $\mathbb{C}^{2^n\times 2^n}$ definida por $\rho \coloneqq \sum_{i=1}^{k} p_i |\psi_i\rangle\langle\psi_i|$, sendo p_i a probabilidade clássica de ocorrer o estado ψ_i, de modo que $\sum_{i=1}^{k} p_i = 1$. Se $k = 1$, o estado ρ é chamado de *estado puro*. O traço de uma matriz de densidade é sempre igual a 1 e os valores de sua diagonal são reais e não-negativos. Caso ρ seja uma matriz diagonal, representa uma distribuição de probabilidade, com cada uma das 2^n entradas da diagonal sendo a probabilidade referente a cada uma das strings de n bits. A matriz de densidade $\mathbb{1}/2^n$ é conhecida como *matriz de densidade maximalmente mista* e sua diagonal corresponde à distribuição uniforme.

Dada uma matriz de densidade de n qubits, as matrizes de densidade reduzidas referentes a $m < n$ qubits podem ser obtidas pelo descarte de $n - m$ qubits por meio da operação de traço parcial (*trace out*). Dada uma matriz de densidade ρ_{AB} que pode ser decomposta nas bases $\{|a_i\rangle\}$ e $\{|b_i\rangle\}$ como $\rho_{AB} = \sum_{ijk\ell} c_{ijk\ell} |a_i\rangle\langle a_j| \otimes |b_k\rangle\langle b_\ell|$, a matriz de densidade reduzida da parte A, obtida ao se fazer o *traço parcial* da parte B do sistema, é dada pela expressão $\mathrm{tr}_B\, \rho_{AB} \coloneqq \sum_{ijk\ell} c_{ijk\ell} |a_i\rangle\langle a_j| \langle b_\ell|b_k\rangle$.

Definimos a *distância de traço* entre dois operadores de densidade ρ e σ como

[1] Referimos o leitor a [Nielsen and Chuang 2011] para mais detalhes sobre Computação Quântica.

$\|\rho-\sigma\|_{\mathrm{tr}} \coloneqq \frac{1}{2}\sum_i|\lambda_i|$, sendo $\{\lambda_i\}$ os autovalores de $\rho-\sigma$. Se ρ e σ são matrizes diagonais, $\|\rho-\sigma\|_{\mathrm{tr}}$ é igual à distância estatística entre as distribuições que ρ e σ representam.

Distância de Traço para Um Qubit ((α,β)-*1QSD*), para $0 \leq \alpha < \beta \leq 1$ é o problema de promessa em que, dados dois circuitos quânticos Q_1 e Q_2, com $m > 1$ qubits de entrada e 1 qubit de saída cada, os quais devolvem respectivamente os estados mistos ρ e σ ao receberem $|0\rangle^{\otimes m}$, decidir entre $\|\rho-\sigma\|_{\mathrm{tr}} \leq \alpha$ e $\|\rho-\sigma\|_{\mathrm{tr}} \geq \beta$, prometido que vale um dos casos. É bem conhecido que este problema pode ser resolvido em tempo $O(\mathsf{poly}(m))$ quântico sempre que α e β não estão próximos demais.

Proposição 1. *Para* $0 \leq \alpha < \beta \leq 1$ *com* $1/(\beta-\alpha)^2 = \mathsf{poly}(m)$*, o problema* (α,β)-*1QSD está em* BQP. [2]

3. Um algoritmo quântico para BSDU

Recordemos, da definição do problema SDU, que recebemos um circuito booleano clássico C de tamanho polinomial em n que codifica uma distribuição de probabilidade X sobre todas as strings com n bits. Conforme trabalhos sobre classes quânticas de conhecimento zero [Watrous 2002, Kobayashi 2003], é possível, a partir de C, obter em tempo polinomial clássico um circuito quântico Q com n qubits de saída e $m > n$ de entrada tal que, recebendo $|0\rangle^{\otimes m}$, devolve o estado misto cuja matriz de densidade ρ é a matriz diagonal das probabilidades das 2^n strings. Deste modo, supomos, para nosso problema BSDU, que a entrada não é o circuito clássico C, mas o circuito quântico Q.

Mostramos que, quando os primeiros $2^n/2$ da diagonal de ρ não são maiores ou iguais aos outros $2^n/2$ elementos, pode-se resolver BSDU em tempo polinomial quântico ao se considerar apenas o primeiro qubit. Note-se que para SDU em geral esta estratégia não funciona, pois podemos ter o caso de ρ representar uma distribuição suficientemente distante da uniforme, i.e. $\|\rho - \mathbb{1}/2^n\|_{\mathrm{tr}} > 1 - 1/n$, e ainda assim a cada qubit individualmente corresponder a matriz de densidade maximalmente mista.

Teorema 2. *BSDU está em* BQP.

Prova. Supomos sem perda de generalidade que $n > 3$, pois, caso contrário, poderíamos decidir entre $\Delta(X,U_n) < 1/n$ e $\Delta(X,U_n) > 1-1/n$ em tempo $O(1)$ clássico. Seja ρ a matriz de densidade devolvida pelo circuito quântico Q, conforme discutimos. Sejam $\alpha = 1/n$, $\beta = 1-1/n$, $N = 2^n$, e σ a matriz de densidade reduzida do primeiro qubit obtida ao se fazer o *traço parcial* dos demais qubits de ρ. Vamos mostrar que: (i) se $\|\rho - \mathbb{1}/N\|_{\mathrm{tr}} < \alpha$, então $\|\sigma - \mathbb{1}/2\|_{\mathrm{tr}} < \alpha$; (ii) se $\|\rho - \mathbb{1}/N\|_{\mathrm{tr}} > \beta$, então $\|\sigma - \mathbb{1}/2\|_{\mathrm{tr}} > \beta/2$.

Observe que $\sigma = (\sum_{i=1}^{N/2}\rho_{ii})\,|0\rangle\langle 0| + (\sum_{i=N/2+1}^{N}\rho_{ii})\,|1\rangle\langle 1|$. Considerando a definição do problema BSDU e que ρ e σ são matrizes diagonais, fazendo $\delta_k \coloneqq \rho_{kk} - 1/N$ para todo k, temos $\delta_i \geq \delta_j$ para todo $i \leq N/2$ e todo $j > N/2$ e:

$$\|\rho - \mathbb{1}/N\|_{\mathrm{tr}} = \frac{1}{2}(|\delta_1| + \cdots + |\delta_N|)\,;$$
$$\|\sigma - \mathbb{1}/2\|_{\mathrm{tr}} = \frac{1}{2}(|\delta_1 + \delta_2 + \cdots + \delta_{N/2}| + |\delta_{N/2+1} + \cdots + \delta_N|)\,.$$

[2] Para uma discussão mais detalhada sobre a qual este resultado pode ser inferido, ver e.g. [Montanaro and de Wolf 2016, p. 44, Sec. 4.2, dois primeiros parágrafos].

(i) Por desigualdade triangular, $\|\sigma - \mathbb{1}/2\|_{\mathrm{tr}} < \alpha$ segue imediatamente da promessa $\|\rho - \mathbb{1}/N\|_{\mathrm{tr}} < \alpha$.

(ii) Como o traço de ρ é igual a 1 e todos os elementos de ρ são reais não-negativos, temos $\sum_{\delta_i>0} \delta_i = \sum_{\delta_i<0} |\delta_i| > \beta$, e $-1/N \leq \delta_i \leq 1 - 1/N$ para todo i. Observe que, de $\sum_{\delta_i<0} |\delta_i| > \beta$, segue que $x := |\{\delta_i : \delta_i > 0\}| > 0$ e $|\{\delta_i : \delta_i < 0\}| = N - x > N/2$. Portanto, como $\delta_i \geq \delta_j$ para todo $i \leq N/2$ e todo $j > N/2$, a soma $|\delta_1 + \delta_2 + \cdots + \delta_{N/2}| + |\delta_{N/2+1} + ... + \delta_N|$ é minimizada quando todos os $N - x$ valores em $\{|\delta_i| : \delta_i < 0\}$ são iguais a

$$\frac{\sum_{\delta_i<0} |\delta_i|}{N - x} > \frac{\beta}{N - x}.$$

Assim,

$$\begin{aligned}
\|\sigma - \mathbb{1}/2\|_{\mathrm{tr}} &= \frac{1}{2}(|\delta_1 + \delta_2 + \cdots + \delta_{N/2}| + |\delta_{N/2+1} + ... + \delta_N|) \\
&> \frac{1}{2}\left(\beta - \left(\frac{N}{2} - x\right)\frac{\beta}{N - x} + \frac{N}{2}\left(\frac{\beta}{N - x}\right)\right) \\
&\geq \frac{\beta}{2}\left(\frac{N}{N - x}\right) \geq \frac{\beta}{2}\left(\frac{N}{N - 1}\right) > \frac{\beta}{2}
\end{aligned}$$

Como consequência, o problema BSDU reduz-se a $(1/n, 1/2 - 1/(2n))$-1QSD; com isto, o algoritmo polinomial quântico para BSDU segue da Proposição 1. □

Referências

Goldreich, O., Sahai, A., and Vadhan, S. (1999). Can statistical zero knowledge be made non-interactive? or On the relationship of SZK and NISZK. In *Annual International Cryptology Conference*, pages 467–484.

Kobayashi, H. (2003). Non-interactive quantum perfect and statistical zero-knowledge. In *International Symposium on Algorithms and Computation*, pages 178–188.

Montanaro, A. and de Wolf, R. (2016). A survey of quantum property testing. *Theory Comput.*, (7):1–81.

Nielsen, M. A. and Chuang, I. L. (2011). *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 10th edition.

Watrous, J. (2002). Limits on the power of quantum statistical zero-knowledge. In *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings.*, pages 459–468. IEEE.