XXXI Congresso de Iniciação Científica Unicamp 2023

Emaranhamento em códigos de acesso aleatório

Palavras-chave: emaranhamento, códigos de acesso aleatório, não-classicalidade

Autores:

Denis Freudenheim Moraes, IFGW - UNICAMP
Prof. Dr. Rafael Luiz da Silva Rabelo (orientador), IFGW - UNICAMP
Lucas da Silva Pollyceno (coautor), IFGW - UNICAMP

---

1 Introdução

O objetivo deste trabalho é o estudo de uma importante classe de tarefas de comunicação, os códigos de acesso aleatório [1]. Mais especificamente, buscamos explorar como recursos quânticos podem ser utilizados para melhorar a performance nessa tarefa. Nesse contexto, diversos cenários distintos foram examinados. Por exemplo, comparamos o caso em que a comunicação entre as partes é de natureza clássica com o cenário onde informação quântica pode ser transmitida. O caso de maior interesse, porém, se dá quando a comunicação entre as partes é clássica mas essas compartilham estados maximamente emaranhados. Esse projeto também tem por objetivo inserir os códigos de acesso aleatório em um contexto mais geral, o chamado cenário prepara e mede, onde uma das partes codifica uma quantidade de informação clássica em uma mensagem (clássica ou quântica), e a envia à outra, que devolve uma saída com base na informação transmitida. Assim, procuramos investigar como comportamentos obtidos em cenários prepara e mede podem ser usados como recurso em códigos de acesso aleatório.

2 Códigos de acesso aleatório

Como introduzido na seção anterior, códigos de acesso aleatórios (RACs - do inglês *random access codes*) são protocolos de comunicação entre duas partes, tipicamente apelidadas de Alice e Bob. A figura 1 mostra uma representação esquemática do cenário onde essa tarefa é realizada.

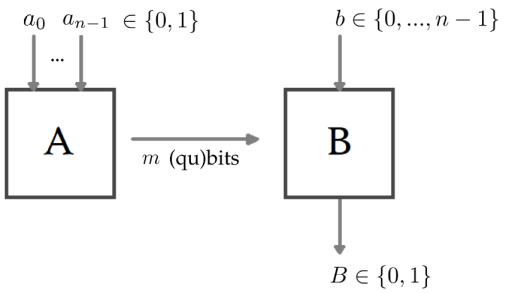

Figura 1: Representação esquemática de um cenário RAC

Como vemos na figura, o protocolo começa com Alice recebendo n bits de entrada $(a_0, a_1, ..., a_{n-1})$. Em seguida, Alice codifica sua entrada em m bits (no caso de comunicação clássica) ou em m qubits (no caso quântico), e os envia a Bob. Para que a tarefa não se torne trivial, ou seja, para que Alice não possa enviar a Bob toda a informação que recebe, fixamos $m < n$. Bob, por sua vez, recebe uma entrada $b \in \{0, ..., n-1\}$, que indicará qual dos bits iniciais de Alice ele deverá adivinhar. Finalmente, baseando-se na mensagem recebida e em sua entrada b, Bob obtém seu palpite $B \in \{0, 1\}$. Com isso, o objetivo das partes é que, ao final do procedimento, Bob obtenha uma saída B tal que $B = a_b$, isso é, que Bob obtenha como saída o b-ésimo bit de Alice.

Para caracterizar completamente um cenário RAC, como o da figura 1, precisamos de apenas três valores: n, m e p, onde n é o número de bits de entrada de Alice, m o número de bits (ou qubits) que Alice enviará a Bob, e p é tal que, dada qualquer entrada b de Bob, ele consiga adivinhar o b-ésimo bit de Alice com probabilidade maior ou igual a p. De maneira mais formal, definimos $p = \min_b\{p(B = a_b|b)\}$. Assim, como notação, caracterizamos um código de acesso aleatório com a tupla (n, m, p) ou com o símbolo $n \overset{p}{\mapsto} m$. Dizemos que uma codificação existe se existe um código (n, m) com $p > 0.5$. Outra figura de mérito comumente utilizada é a probabilidade média de sucesso, dada pela equação (1):

$$P_m = \frac{1}{n\ 2^n} \sum_{a_0,...,a_{n-1},b} p(B = a_b|a_0, ..., a_{n-1}, b). \tag{1}$$

A equação (1) assume que a distribuição das entradas de Alice e Bob são uniformes. Temos ainda que $p = P_m$ sempre que a probabilidade de sucesso for independente da entrada de Bob, o que não é verdade em todas as situações.

3 Vantagem quântica

Para ilustrar como recursos quânticos podem ser utilizados para obter vantagens nesse tipo de tarefa, começamos pelo caso mais simples, $2 \mapsto 1$, onde Alice recebe dois bits de entrada e envia apenas um bit para Bob. Classicamente, a melhor estratégia que podemos adotar é Alice sempre enviar a Bob seu primeiro bit, a_0, e Bob escolher como sua saída o bit que receber, ou seja, $B = a_0$ [2]. Dessa forma, sempre que $b = 0$, Bob irá acertar. Por outro lado, se $b = 1$, Bob acertará em média apenas metade das vezes (assumindo que as entradas de Alice obedecem uma distribuição uniforme), o que resulta em uma probabilidade média de sucesso $P_m = 0.75$. Porém, se Alice pode enviar um qubit a Bob, conseguimos uma probabilidade média de sucesso mais alta. Dados os bits de entrada a_0 e a_1, Alice prepara o qubit que será enviado a Bob seguindo a equação (2) [3]:

$$|\psi_{a_0a_1}\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle + \frac{1}{\sqrt{2}}((-1)^{a_0} + i(-1)^{a_1})|1\rangle\right]. \tag{2}$$

Ao receber o estado $|\psi_{a_0a_1}\rangle$, Bob realiza uma medição na base $M_0 = \{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$ se $b = 0$, e na base $M_1 = \{\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\}$ se $b = 1$. Utilizando a regra de Born, da teoria quântica, e a equação (1), é simples mostrar que esse protocolo resulta em uma probabilidade média $P_m = \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right) \approx 0.85$. Com isso, trocando apenas a natureza da mensagem enviada, obtemos uma probabilidade média de sucesso mais alta.

Como mostrado em [1], no cenário quântico mais geral, $n \overset{p}{\mapsto} m$, são necessários $m \geq (1 - H(p))n$ qubits para obter uma probabilidade mínima de sucesso $p > 0.5$, onde $H(p)$ é a entropia de Shannon binária. No caso clássico, por outro lado, necessitamos que $m \geq (1 - H(p))n + O(\log n)$ bits sejam

enviados de Alice para Bob para obtermos $p > 0.5$. Logo, apesar de sempre podermos utilizar menos qubits que bits para obter a mesma probabilidade mínima de sucesso $p > 0.5$, essa vantagem quântica cresce apenas de forma logarítmica, conforme aumentamos o número de bits de entrada de Alice.

Diversos outros resultados foram estudados e reproduzidos a respeito de RACs quânticas e recursos não-clássicos. Por exemplo, em [4], os autores mostram que as medições de Bob devem ser incompatíveis (no sentido de que não podem ser realizadas simultaneamente) para que comunicação quântica em RACs apresente vantagem sobre comunicação clássica. Também pode-se verificar, através de técnicas de otimização convexa e programação semidefinida, que mesmo se o canal quântico utilizado para comunicação for ruidoso, ainda existem estados e medições que resultam probabilidades de sucesso maiores ou iguais ao caso clássico não ruidoso [5]. Os resultados numéricos presentes em [5] para os canais quânticos ruidosos do tipo *dit flip* e *phase flip* foram reproduzidos utilizando a linguagem *Julia* e o otimizador *Mosek* [6]. Outro resultado interessante, apresentado em [7], é a possibilidade de utilizar outros recursos não-clássicos e não-locais, como generalizações de caixas PR [8], para obter códigos de acesso aleatório com probabilidade de sucesso $p = 1$.

4 Assistência de Emaranhamento

O cenário de maior interesse para essa pesquisa é o caso em que a comunicação entre Alice e Bob é clássica, mas estados maximamente emaranhados são compartilhados entre as duas partes (toda a discussão presente nessa seção foi baseada no artigo [9]). Nesse cenário, Alice, baseando-se em seus bits de entrada, realiza uma medição local em sua parte do estado emaranhado compartilhado, e constrói a mensagem clássica que será enviada a Bob com base no resultado de sua medição. Bob, por sua vez, também escolhe, com base em sua entrada, uma medição a ser realizada em sua parte do estado compartilhado. Finalmente, a partir do resultado de sua medição e da mensagem recebida, Bob produz seu palpite.

Novamente, começamos analisando o caso $2 \mapsto 1$, onde Alice recebe dois bits e envia um bit para Bob. Dessa vez, porém, Alice e Bob compartilham um estado singleto $|\psi\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)$. A estratégia ótima para essa tarefa está ilustrada na figura 2, e descrita a seguir.

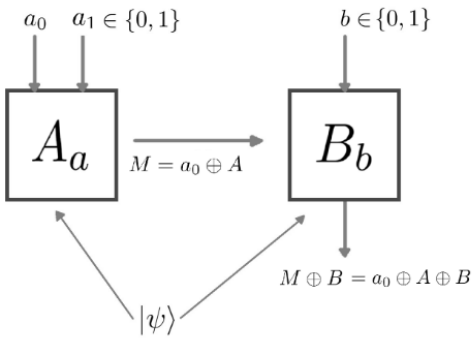

Figura 2: Representação da estratégia ótima para o RAC $2 \mapsto 1$ assistido por emaranhamento.

As medições utilizadas por Alice e Bob, que dependem de suas entradas, são dadas, respectivamente, pelas equações (3) e (4), onde o símbolo $\oplus$ representa adição módulo 2. Os estados das bases nas quais as medições serão realizadas estão expressos em termos de vetores de Bloch. O resultado da medição de Alice é $A = 0$ se o estado colapsar para os vetores com sinal (+) de A_a, caso contrário temos

$A = 1$. Para as medições de Bob fazemos o oposto, $B = 0$ se o estado colapsa para o os vetores com sinal negativo, e $B = 1$ caso contrário.

$$A_a = \left\{ \pm \frac{1}{\sqrt{2}} (1, (-1)^a, 0) \right\}, \quad \text{onde} \quad a = a_0 \oplus a_1. \tag{3}$$

$$B_0 = \{\pm(1, 0, 0)\} \quad \text{e} \quad B_1 = \{\pm(0, 1, 0)\}. \tag{4}$$

Assim, Alice envia a Bob a mensagem $M = a_0 \oplus A$, onde A é o resultado da medição na base A_a. Em seguida, após realizar sua medição, Bob terá como palpite o bit $M \oplus B$, onde B é o resultado da medição de Bob, realizada na base B_b. É importante observar que a tarefa será bem sucedida, ou seja, teremos $B = a_b$, sempre que $A \oplus B = a \cdot b = (a_0 \oplus a_1)b$. Utilizando essa estratégia, obtemos uma probabilidade mínima de sucesso $p = \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right) \approx 0.85$, a mesma que no caso $2 \mapsto 1$ com comunicação quântica.

Um protocolo análogo pode ser feito para o cenário $3 \mapsto 1$ assistido por emaranhamento, que resulta em $p = \frac{1}{2}\left(1 + \frac{1}{\sqrt{3}}\right) \approx 0.79$. Como mostrado em [9], as tarefas $2 \mapsto 1$ e $3 \mapsto 1$ podem ser usadas como primitivas para a construção de estratégias gerais $n \mapsto 1$, através de um processo de concatenação. Para $n > 3$, códigos de acesso aleatório com comunicação clássica e assistência de emaranhamento possuem maior probabilidade de sucesso que RACs quânticas, mesmo permitindo, no caso quântico, que as partes compartilhem uma variável aleatória clássica, como feito em [2].

5 O cenário prepara e mede

Finalmente, com o objetivo de explorar novas estratégias para aumentar a probabilidade de sucesso, buscamos inserir essa tarefa em um cenário mais geral, conhecido como cenário prepara e mede (PAM - do inglês *prepare and measure*). Nesse cenário, ilustrado na figura 3, Alice recebe uma entrada $x \in \{0, ..., n_x - 1\}$ e envia para Bob uma mensagem (que pode ser tanto clássica quanto quântica) de dimensão d. Bob, por sua vez, produz uma saída $z \in \{0, ..., n_z\}$ baseando-se em sua entrada $y \in \{0, ..., n_y\}$.

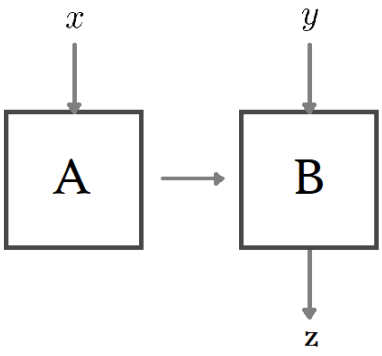

Figura 3: Ilustração geral de um cenário prepara e mede.

A maneira mais geral de caracterizar esse tipo de sistema é através de probabilidades condicionais do tipo $p(z|x, y)$. O conjunto $\{p(z|x, y)\}_{z,x,y}$, que nos dá as probabilidades condicionais para todos x, y, z possíveis é chamado comportamento do cenário. Em [10], os autores discutem como estados emaranhados compartilhados por Alice e Bob podem gerar novos comportamentos nesse tipo de cenário. Assim,

o objetivo nesse etapa do projeto é investigar a possibilidade de utilizar comportamentos encontrados em [10], para cenários PAM, como recurso em códigos de acesso aleatório. Mais formalmente, tendo em vista as figuras 1 e 3, procuramos funções F, H e Q tais que, tomando $x = F(a_0, ..., a_{n-1})$, $y = H(b)$ e $B = Q(z, b)$, possamos encontrar probabilidades de sucesso que superem o caso clássico.

6 Conclusão e perspectivas

Apesar de, até o momento, essa pesquisa não ter originado nenhum resultado novo, foi feita uma ampla revisão da bibliografia a respeito de códigos de acesso aleatório e da utilização de recursos quânticos para melhorar o desempenho nessa tarefa. Diversos resultados teóricos e numéricos recentes foram estudados e reproduzidos. No entanto, acreditamos que a parte final do projeto, onde buscamos explorar a utilização de comportamentos encontrados em cenários prepara e mede como recursos em códigos de acesso aleatório, ainda pode render resultados interessantes.

Referências

[1] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, "Dense quantum coding and quantum finite automata," *J. ACM*, vol. 49, no. 4, p. 496–511, 2002.

[2] A. Ambainis, D. Leung, L. Mancinska, and M. Ozols, "Quantum random access codes with shared randomness," *arXiv : 0810.2937*, 2009.

[3] C. H. de Souza Vieira, *Explorando o papel do emaranhamento em conjuntos de comportamentos de cenários de prepara-e-mede*. PhD thesis, Universidade Estadual de Campinas (UNICAMP), 2023.

[4] C. Carmeli, T. Heinosaari, and A. Toigo, "Quantum random access codes and incompatibility of measurements," *Europhysics Letters*, vol. 130, no. 5, p. 50001, 2020.

[5] R. A. da Silva and B. Marques, "Semidefinite-programming-based optimization of quantum random access codes over noisy channels," *Physical Review A*, vol. 107, no. 4, p. 042433, 2023.

[6] "Mosek aps." `https://www.mosek.com/`. Accessed: 2023-07-28.

[7] A. Chaturvedi, M. Pawlowski, and K. Horodecki, "Random access codes and nonlocal resources," *Physical Review A*, vol. 96, no. 2, p. 022125, 2017.

[8] S. Popescu and D. Rohrlich, "Quantum nonlocality as an axiom," *Foundations of Physics*, vol. 24, pp. 379–385, 1994.

[9] M. Pawłowski and M. Żukowski, "Entanglement-assisted random access codes," *Phys. Rev. A*, vol. 81, p. 042326, Apr 2010.

[10] C. Vieira, C. de Gois, L. Pollyceno, and R. Rabelo, "Interplays between classical and quantum entanglement-assisted communication scenarios," *arXiv: 2205.05171*, 2022.