الگوریتم های بکار رفته در محاسبات کوانتومی و دستاوردهای آن

سمینار درس الکترونیک کوانتومی

زیر نظر استاد محمد نژاد

دانشگاه علم و صنعت ایران

فهرست

- مقدمه
- الگوریتم های کوانتومی
- انواع الگوریتم های کوانتومی
- معرفی چندین الگوریتم پایه
- الگوریتم های تکاملی
- الگوریتم ژنتیک کوانتومی
- خلاصه
- منابع

مقدمه

- هدف محاسبات کوانتومی یافتن روش هایی برای طراحی مجدد ادوات شناخته شده ی محاسبات (مانند گیت ها و ترانزیستورها) به گونه ای است که بتوانند تحت اثرات کوانتومی ، که در محدوده ی ابعاد نانومتری و کوچکتر بروز می کنند کار کنند.
- ورود به دنیای محاسبات کوانتومی نیازمند دو پیش زمینه مهم است، نخست باید اصول اساسی و برخی تعابیر مهم مکانیک کوانتومی را به طور دقیق بررسی کرد سپس مفهوم اطلاعات در فیزیک نیز، چه به صورت کلاسیک و چه در معنای جدیدکوانتومی آن باید درک شود .
- موارد مهم در محاسبات کوانتومی: درهم تافتگی entanglement، کیوبیت ها، واهمدوسیDecoherence ⟵ دشمن محاسبات کوانتومی

الگوریتم های کوانتومی

- هرگاه ما الگوریتم های کلاسیکی خودمان رابر روی یک کامپیوتر کوانتومی مورداستفاده قراردهیم، به سادگی محاسبات را به طریقه مشابه با یک کامپیوتر کلاسیک انجام و اجرا خواهدکرد.

- به منظور نشان دادن برتری آن و بهره برداری از پدیده توازی کوانتومی ما نیاز داریم تا الگوریتم ها ی کوانتومی را پایه گذاری کنیم.

جعبه سیاه و توابع یک بیتی

- **جعبه سیاه Oracle**
  - هدف تعیین کامل تابع نیست، بلکه یک خاصیت مشخص از تابع هم یافته شود کافی است.
    - تابع ثابت: خروجی همواره ثابت (f1,f4)
    - تابع متوازن: خروجی به ازای نیمی از ورودی ها ۰ و نیمی دیگر ۱ (f2,f3)
- **انواع توابع تک بیتی**

f_1	
۰	0
۰	1

f_2	
۰	0
۱	1

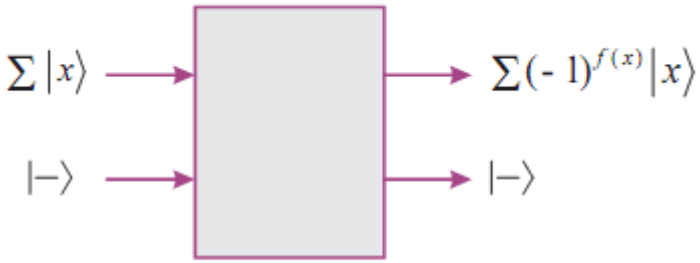
f_3	
۱	0
۰	1

f_4	
۱	0
۱	1

- می خواهیم ببینیم با چند بار فراخوانی، تابع f تعیین می گردد؟
  - با دو بار فراخوانی
  - یک بار با ورودی ۰ و یک بار با ورودی ۱

توازی کوانتومی

- استفاده از توازی کوانتومی در الگوریتم های کوانتومی



- اگر تابع f ثابت باشد

$$\overline{f(0)} = \overline{f(1)} = \overline{f} \text{ و } f(0) = f(1) = f$$

- اگر تابع f متوازن باشد

$$\overline{f(0)} = f(1) = \overline{f} \text{ و } f(0) = \overline{f(1)} = f$$

انواع الگوریتم های کوانتومی

- الگوریتم کوانتومی برای مسئله دویچ
- الگوریتم کوانتومی برای مسئله دویچ-جوزا
- الگوریتم کوانتومی برای مسئله برنشتاین-وزیرانی
- الگوریتم کوانتومی برای مسئله سیمن

الگوریتم کوانتومی برای مسئله دویچ

- بردار حالت در مراحل مختلف: $|\Psi_0\rangle = |s\rangle \otimes |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{2}(|00\rangle + |10\rangle - |01\rangle - |11\rangle)$
- اگر f تابع ثابت باشد

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|f\rangle - |\overline{f}\rangle)$$

$$|\Psi_3\rangle = |0\rangle \otimes \frac{1}{\sqrt{2}}(|f\rangle - |\overline{f}\rangle)$$

- اگر f تابع متوازن باشد

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes \frac{1}{\sqrt{2}}(|f\rangle - |\overline{f}\rangle)$$

$$|\Psi_3\rangle = |1\rangle \frac{1}{\sqrt{2}}(|f\rangle - |\overline{f}\rangle)$$

- با یک فراخوانی مسئله حل می شود:
  - خروجی برای توابع ثابت ۰ و برای توابع متوازن ۱

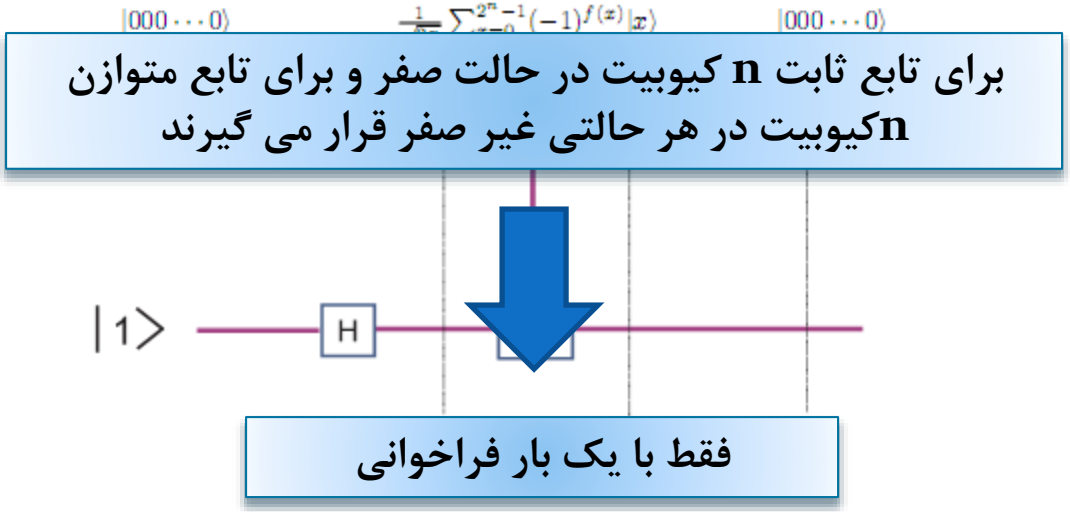
دانشگاه علم و صنعت ایران
تاسیس ۱۳۰۸

الگوریتم کوانتومی برای مسئله دویچ-جوزا

- مسئله دویچ جویزا تعمیمی از مسئله دویچ است
- از ما خواسته ثابت یا متوازن بودن مسئله را تعیین کنیم:
  - تعداد توابع ثابت ۲ تا
  - تعداد توابع متوازن $\frac{2^n!}{(2^{n-1}!)^2}$
- در الگوریتم کلاسیک باید به تعداد $2^{n-1}+1$ بار تابع f فراخوانی شود.
- در الگوریتم کوانتومی تنها با دو بار فراخوانی نوع تابع تعیین می گردد.

الگوریتم کوانتومی برای مسئله دویچ–جوزا

- مدار بکار رفته در الگوریتم کوانتومی برای مسئله دویچ–جوزا



- بردار حالت در مراحل مختلف

$$|\Psi_0\rangle = |s\rangle \otimes |-\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x,0\rangle - |x,1\rangle$$

اگر f تابع ثابت

اگر f تابع متوازن

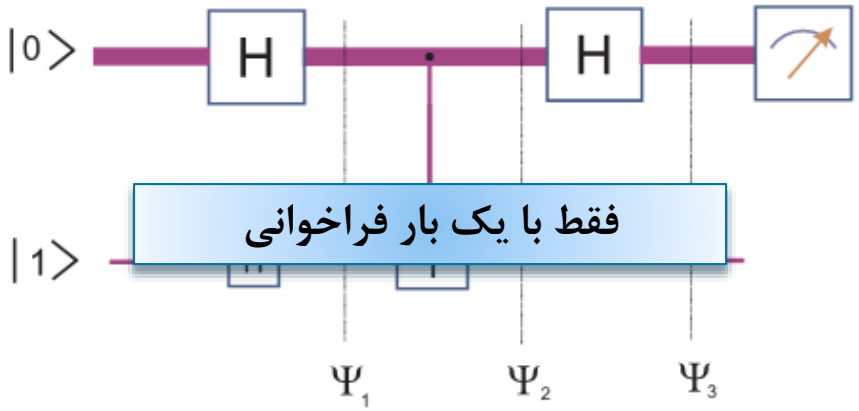
الگوریتم کوانتومی برای مسئله برنشتاین-وزیرانی

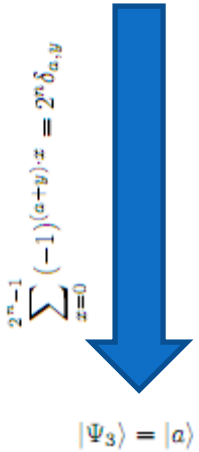
- مسئله: تابع f به صورت زیر و a یک عدد n بیتی است. با چند بار فراخوانی a تعیین می گردد؟

$$f(x) := a.x \qquad a.x = \sum_{k=0}^{n-1} a_k x_k \mod 2.$$

$$|\Psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{a.x} |x\rangle..$$

$$|\Psi_3\rangle = \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{x.(a+y)} |x\rangle.$$

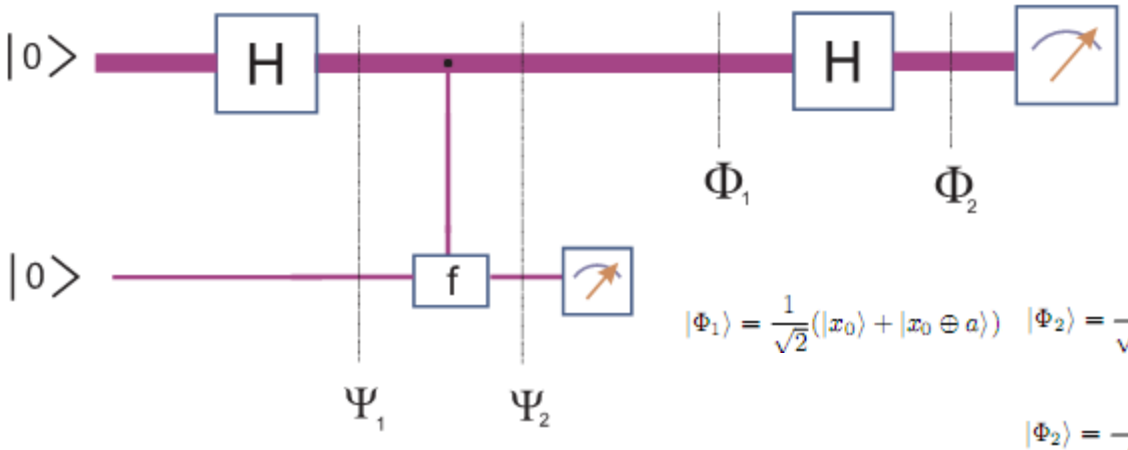




الگوریتم کوانتومی برای مسئله سیمن

- مسئله: تابع f به صورت زیر می باشد، با چند بار فراخوانی a تعیین می گردد؟

$$f(x) = f(x \oplus a)$$



$$|\Phi_1\rangle = \frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus a\rangle) \qquad |\Phi_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{y=0}^{2^n-1} [(-1)^{x_0 \cdot a}] |y\rangle.$$

$$|\Phi_2\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{a \cdot y=0} [(-1)^{x_0 \cdot y}] |y\rangle.$$

$$|\Psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x, 0\rangle \qquad |\Psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x, f(x)\rangle$$

. :

فقط با n بار فراخوانی

دانشگاه علم و صنعت ایران
تاسیس ۱۳۰۸

مهمترین الگوریتم های کوانتومی

- الگوریتم های ارائه شده، هیچ کدام کلاس حل مسئله را تغییر نداده است. یعنی نتوانسته مسئله را از کلاس نمایی به کلاس چند جمله ای ببرد.

- الگوریتم های مهم تغییر دهنده کلاس حل مسئله:
  - **الگوریتم شور Shor's Algorithm**
    - هدف این الگوریتم شکستن یا تجزیه یک عدد بزرگ به عامل های اول آن است
  - **الگوریتم گراور Graver's Algorithm**
    - این الگوریتم می تواند عملیات مرتب کردن داده ها راازمیان پایگاه های اطلاعاتی بزرگ ونامرتب انجام دهد.

الگوریتم های تکاملی

- در راستای بهبود عملکرد الگوریتم، رویکردهای جدیدی به الگوریتم اضافه شده است که در یک نگاه کلی می توان آنها در قالب بهبود شناسایی و بهره برداری به عنوان دو رویکرد بسیار مهم در الگوریتم‌های تکاملی تقسیم بندی کرد.

- ساختار الگوریتم تکاملی کوانتوم و عملگرهای استفاده شده در آن از یک طرف و رویه های اضافه شده به آن به گونه ای است که توازن بسیار خوبی را بین این دو رویکرد فراهم می آورد

الگوریتم تکاملی کوانتوم بهبود یافته(IQEA)

- الگوریتم کوانتوم را با استفاده از رویکردهای زیر بهبود داده می شود:

I. استفاده از رویکرد اندازه گیری چندگانه در تبدیل حالت کوانتومی به باینری.

II. استفاده از گیت چرخشی کوانتومی دیگری علاوه بر عملگر معمول که برای بروز رسانی مقادیر کیوبیتها در هر نسل بکار برده می شود.

III. استفاده از رویکرد کاهش حدود متغیرها بر اساس بهترین جوابهای بدست آمده در هر نسل.

IV. ورود افراد با مقادیر کوانتومی جدید، طبق شرایط مساله

- الگوریتم های تکاملی اصولاً روش های بهینه سازی و جستجوی تصادفی بر اساس اصول تکامل بیولوژیکی طبیعت هستند

الگوریتم تکاملی کوانتوم بهبود یافته(IQEA)

- در مقایسه با روش های بهینه سازی سنتی، الگوریتم های تکاملی نیرومندتر و در عمل جامع نگرترند
- در هر مرحله از الگوریتم های تکاملی، مجموعه جدیدی از جوابهای بروز رسانی شده وارد محدوده مشخصی از فضای جواب می شوند و بعد از اندازه گیری ها و محاسبات تابع برازندگی توسط عملگرهای متعدد،اعضای جدید برای نسل بعد را فراهم می کنند
- این روند به گونه ای طراحی می شود که افراد جمعیت در نسل جدید از مقادیر نسل جاری بدتر نباشند و حتی الامکان بهتر بوده و باعث هدایت اعضای جمعیت به سمت ناحیه جواب بهینه شوند
- ساختار الگوریتم تکاملی کوانتوم و عملگرهای استفاده شده در آن از یک طرف و رویه های اضافه شده به آن به گونه ای است که توازن بسیار خوبی را بین این دو رویکرد فراهم می آورد

الگوریتم های ژنتیک کوانتوم QGA

- الگوریتم ژنتیک کوانتوم بر پایه دیدگاه محاسبات و کامپیوترهای کوانتومی شکل گرفته اند.
- این الگوریتم ها در مقایسه با روش های دیگر بهینه سازی مانند روش های محاسباتی و روش های مبتنی بر گرادیان، مقاوم تر هستند.
- بسیاری روش های دیگر، از مشکل گیر کردن در قله های محلی رنج می برند، حال آنکه الگوریتمهای تکاملی تا حدی با این مشکل کنار آمده اند.
- در اینجا می کوشیم با کمک الگوریتم Simulated Annealingبه عنوان یک جستجوی محلی، کارایی QGAرا بهبود بخشیم. (SA-QGA)

الگوریتم های ژنتیک کوانتوم

- از نمایش پاسخ ها در قالبی احتمالی استفاده می کنند

$$\begin{bmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \beta_1 & \beta_2 & \cdots & \beta_n \end{bmatrix}$$

- نمونه کوانتوم- کروموزوم

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & \frac{1}{2} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} & \frac{\sqrt{3}}{2} \end{bmatrix}$$

- حالت این کوانتوم- کروموزوم

$$\frac{1}{4}|000\rangle + \frac{\sqrt{3}}{4}|001\rangle - \frac{1}{4}|010\rangle - \frac{\sqrt{3}}{4}|011\rangle + \frac{1}{4}|100\rangle + \frac{\sqrt{3}}{4}|101\rangle - \frac{1}{4}|100\rangle - \frac{\sqrt{3}}{4}|111\rangle$$

- احتمال رویداد حالات
- |000>، |001>، |010>، |011>، |100>، |101>، |110>، |111>
- ۱/۱۶ ۳/۱۶ ۱/۱۶ ۳/۱۶ ۱/۱۶ ۳/۱۶ ۱/۱۶ ۳/۱۶

دانشگاه علم و صنعت ایران
تاسیس ۱۳۰۸

روال یک الگوریتم ژنتیک کوانتومی

```
Procedure QGA
begin
    t ← 0
 i.     initialize Q(t)
 ii.    make P(t) by observing Q(t)
 iii.   evaluate P(t)
 iv.    store the best solutions among P(t) into b
 v.     while (not termination-condition) do
        begin
          t ← t+1
 vi.      make P(t) by observing the states of Q(t-1)
 vii.     evaluate P(t)
 viii.    update Q(t) using Q-gate
 ix.      store the best solutions among P(t) into b
        end
end
```

iii. کروموزوم های دودویی بدست آمده از مرحله دوم توسط تابع

iv. بهترین جواب یافته

v. تا ارضای شرط خاتمه، الگوریتم اجرا شود

vi. جواب های دودویی P(t) با مشاهده حالت‌های Q(t-1) ایجاد می شوند

vii. P(t) را ارزیابی

viii. به روزرسانی کوانتوم بیت ها

ix. بهترین جواب یافته شده را در b ذخیره می کنیم.

به کارگیری الگوریتم Simulated Annealing در الگوریتم های ژنتیک کوانتومی

```
Procedure SA-QGA
begin
    t ← 0
 x.     initialize Q(t)
 xi.    make P(t) by observing Q(t)
 xii.   evaluate P(t)
 xiii.  store the best solutions among P(t) into b
 xiv.   while (not termination-condition) do
        begin
           t ← t+1
 xv.       make P(t) by observing the states
 xvi.      Perform local search SA on P(t)
 xvii.     evaluate P(t)
 xviii.    update Q(t) using Q-gate
 xix.      store the best solution b among B(t)
       end
    end
```

xvi یک جستجویی محلی Simulated Annealing روی P(t) انجام می گیرد

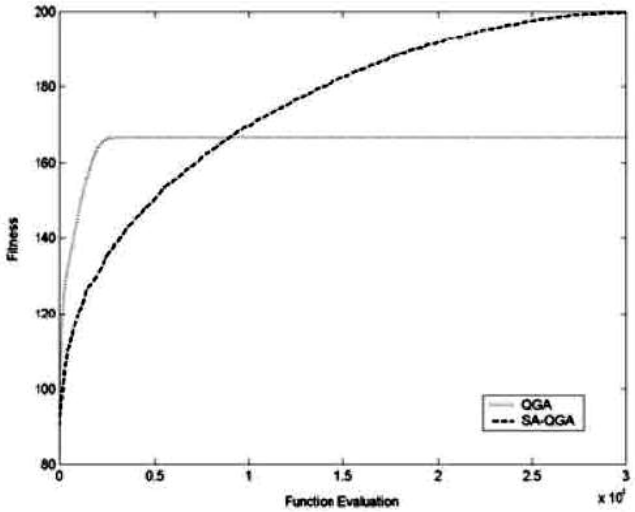
دانشگاه علم و صنعت ایران
تاسیس ۱۳۰۸

Simulated Annealing

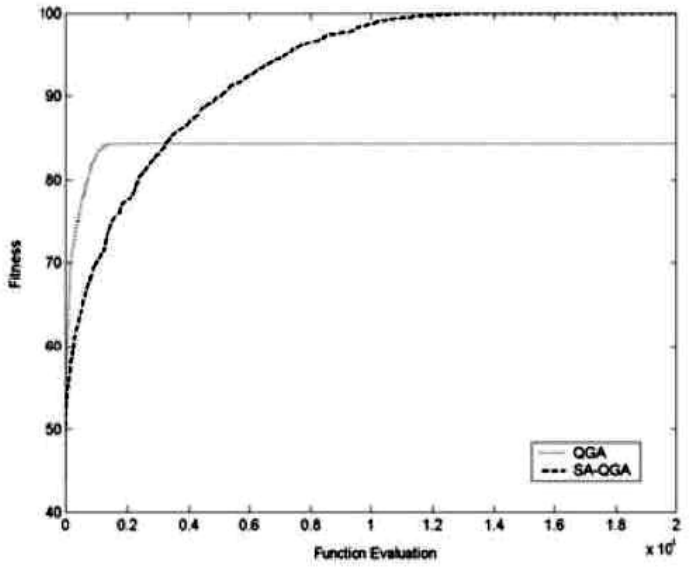
Procedure Local search SA
begin
T=T_0
t ← 0

while not (termination condition) do
begin
E_1 =evaluation ($P(t)$)
perform a small change on $P(t)$ and store the result in $P'(t)$
E_2 =evaluation ($P'(t)$)
$\Delta E = E_2 - E_1$
if $\Delta E > 0$ then
$P(t) = P'(t)$
else
$p = e^{-\frac{\Delta E}{T}}$
if $p < U(1,0)$ then $P(t) = P'(t)$
end
T=T*0.9
end
end

نتایج



مقایسه روش پیشنهادی SA-QGA با QGA در مساله Trap برای=۲۰ NTtap.
نمودار بر حسب تعداد ارزیابی تابع رسم شده است.



مقایسه کارایی الگوریتم QGA با الگوریتم SA-QGA
در مساله Trap برای=۴۰ NTtap،
نمودار بر حسب تعداد ارزیابی تابع رسم شده است

خلاصه

- الگوریتم های کوانتومی و انواع آن
  - الگوریتم کوانتومی برای مسئله دویچ
  - الگوریتم کوانتومی برای مسئله دویچ–جوزا
  - الگوریتم کوانتومی برای مسئله برنشتاین–وزیرانی
  - الگوریتم کوانتومی برای مسئله سیمن
  - الگوریتم شور
  - الگوریتم گراور
- الگوریتم های تکاملی
- الگوریتم ژنتیک کوانتومی
  - روشی مبتنی بر جستجوی محلی Simulated Annealingرا برای بهبود کارایی الگوریتم های QGAارایه کردیم. نتایج آزمایشی نشان می دهند در حالیکه QGA ابزار قدرتمندی برای بهینه سازی می باشد، به کارگیری روش های جستجوی محلی مانند Simulated Annealing موجب افزایش کارایی این الگوریتم می شود. در اینجا تلفیق قابلیت های جستجوی محلی در Simulated Annealing با جستجوی عمومی در الگوریتم های ژنتیک کوانتوم موجب بالا رفتن کارایی می شود

Reference

- 1) Magnus Gausdal Find, “Algorithms For Quantum Computers”, University of Southern Denmark, Odense, 2015.
- 2) Kenneth Mark Bryden, Daniel A. Ashlock, Steven Corns, and Stephen J. Willson. "Graph-Based Evolutionary Algorithms". IEEE Trans. Evol. Comput. Vol. 10, No. 5 pp. 550-567, October 2006
- 3) M. A. Sharbafi, M. Shakibas, Caro. Lucas, A. Mohammadi Nejad. "An Innoative Fuzzy Decision Making Based Genetic Algorithm". ". IEEE Trans. Comput and Tech. Vol. 13pp. 180-183 May 2006
- 4) Gunther R. Raidl, Gabriele Koller, Bryant A. Julstrom. "Biased Mutation Operators for Subgraph-Selection Problems". IEEE Trans. Evol. Comput. Vol. 10, No. 2 pp. 145-156, April 2006
- 5) http://math.nist.gov/quantum/zoo/
- 6) Michele Mosca, “Quantum Computer Algorithms: basics”, Canada Research Chair in Quantum Computation, June 2003
- 7) Emma Strubell, “An Introduction to Quantum Algorithms”, Spring 2011

Thank
you