Önbilgi Sahibi Olunan Kümelerde Kuantum Arama

Umut Çalıkyılmaz
Danışman: Sadi Turgut

Orta Doğu Teknik Üniversitesi
umut.calikyilmaz@metu.edu.tr

Tübitak Kuantum Hesaplama ve Teknolojileri Çalıştayı
31 Mart 2022

Sunum İçeriği

Kuantum Hesaplama

Figure: Richard Feynman

- Kuantum hesaplama fikrini ilk olarak Richard Feynman, 1982 yılında ortaya attı.[a]
- Fikrin çıkış noktası karmaşık kuantum sistemleri klasik bilgisayarlara göre daha verimli şekilde simüle edebilecek bir hesaplama yöntemi bulmaktı.
- Klasik hesaplamada, n elektron spininden oluşan bir sistemi simüle etmek için 2^n adet değişken gerekiyor.
- Kuantum hesaplamayla aynı sistem n değişken kullanılarak simüle edilebiliyor.

[a] R. P. Feynman, Simulating physics with computers, International Journal of Theoretical Physics 21, 467 (1982).

Kuantum Hesaplama

- Zaman içinde kuantum hesaplamanın bazı klasik problemleri klasik hesaplamadan daha kısa sürede çözmek için de kullanılabileceği kanıtlandı.
- Peter Shor, 1994 yılında asal çarpan bulma ve ayrık logaritm için kullanılabilecek kuantum algoritmalar geliştirdi. [a]
- Lov K. Grover, 1996 yılında arama problemini klasik algoritmalardan daha kısa sürede çözebilen kuantum arama algoritmasını geliştirdi. [b]

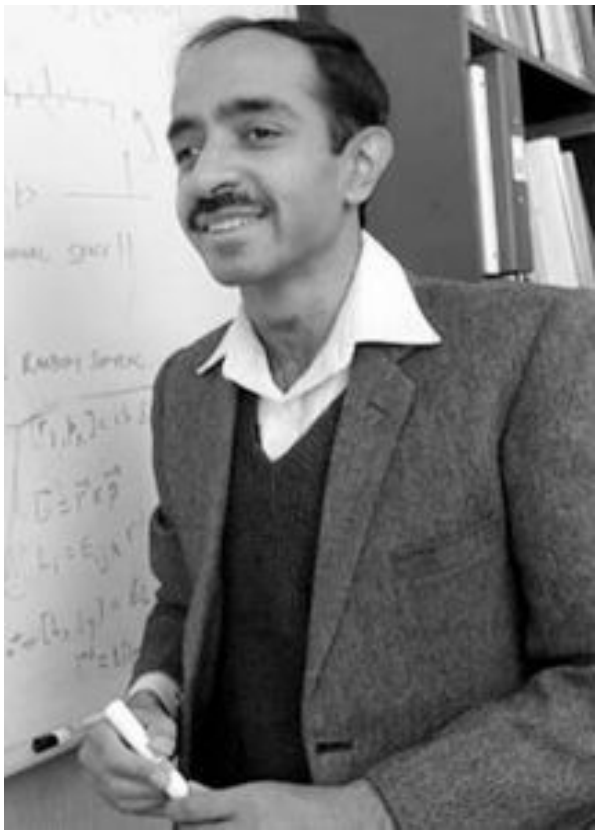


Figure: Lov K. Grover

[a] P. W. Shor, Polynomial-time algorithms for quantum computation: Discrete logarithms and factoring, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE, 1994).

[b] L. K. Grover, A fast quantum mechanical algorithm for database search, in

Arama Problemi

- Arama problemi, verilen bir küme içerisinden belli bir koşulu sağlayan bir elemanın yerini tespit etme problemidir.
- Verilen koşulu sağlayan elemanlara çözüm adı verilir.
- Arama kümesi içindeki bir eleman çözümse, bu elemanın indeksi olan i, $f(i) = 1$ sonucunu verir. Bu eleman bir çözüm değilse $f(i) = 0$ olur.
- En genel haliyle arama problemi, verilen bir kümede bulunan N adet eleman içinde M adet çözümden birinin bulunması olarak tanımlanabilir.
- Klasik hesaplamayla bu problemin çözülmesi ortalama N/M, en kötü durumda ise $N - M$ deneme gerektirir.
- Grover Algoritması bu problemi $O(\sqrt{N/M})$ denemede çözebilir. [1]

[1] L. K. Grover, Quantum mechanics helps in searching for a needle in a haystack, Physical Review Letters 79, 325 (1997).

Grover Algoritması

- Grover algoritması, bir kümedeki elemanları teker teker denemek yerine *n* qubitle temsil edilen bir kuantum uzayda rotasyon yaparak arama problemini çözer.
- Algoritmanın başlangıcında arama kümesinde bulunan tüm indekslerin süperpozisyonu durumundaki bir kuantum durumu oluşturulur.

$$|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle \tag{1}$$

- Sonrasında bu kuantum durumuna üst üste ”kahin” ve ”yansıtma” operatörleri uygulanarak rotasyon yapılır.

Grover Algoritması

- Kahin operatörü bir indeksin çözümlerden birine ait olup olmadığına bakar.
- Eğer indeks çözümlerden birine aitse kuantum durumuna bir faz uygular.

$$O\left|\psi_0\right\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (-1)^{f(i)} \left|i\right\rangle \tag{2}$$

- Yansıtma operatörü başlangıç durumuna ($\left|\psi_0\right\rangle$) göre bir yansıtma yapar.

$$R = 2\left|\psi_0\right\rangle\left\langle\psi_0\right| - I \tag{3}$$

- Bu iki operatörün ard arda uygulanmasına Grover yinelemesi (ya da Grover operatörü) adı verilir.

$$G = RO \tag{4}$$

Grover Algoritması

- Grover operatörünün nasıl çalıştığı görsel olarak anlatılabilir.
- Arama probleminin tüm çözümlerini içeren kümeye S adını verelim.
- Kuantum halleri $|s\rangle$ ve $|ns\rangle$ sırasıyla tüm çözüm indekslerinin ve çözüm olmayan tüm elemanların indekslerin süperpozisyonundan oluşur.

$$|s\rangle = \frac{1}{\sqrt{M}} \sum_{i \in S} |i\rangle \tag{5}$$

$$|ns\rangle = \frac{1}{\sqrt{N-M}} \sum_{i \notin S} |i\rangle \tag{6}$$

Grover Algoritması

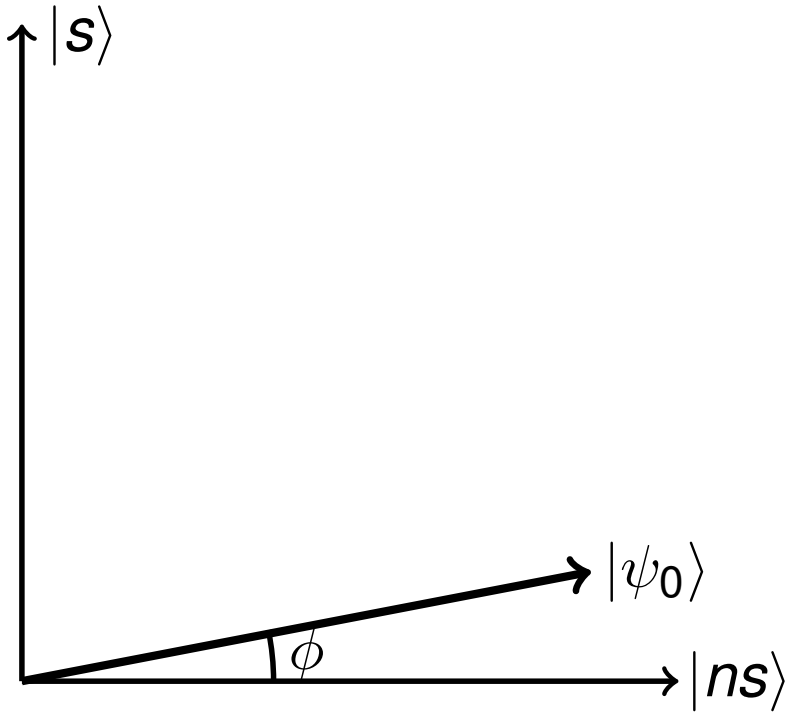


Figure: İlk Grover yinelemesi

- Grover yinelemesi kahin ve yansıtma operatörlerinin sırayla uygulanmasından oluşur ($G = RO$).
- Kahin operatörü $|ns\rangle$ durumuna göre bir yansıtma operatörü görevi görür.
- Sonrasında yansıtma operatörü $|\psi_0\rangle$ durumuna göre bir yansıtma yapar.
- Bu iki operatörün arka arkaya uygulanması sonucu 2ϕ miktarında bir rotasyon yapılmış olur.

Grover Algoritması

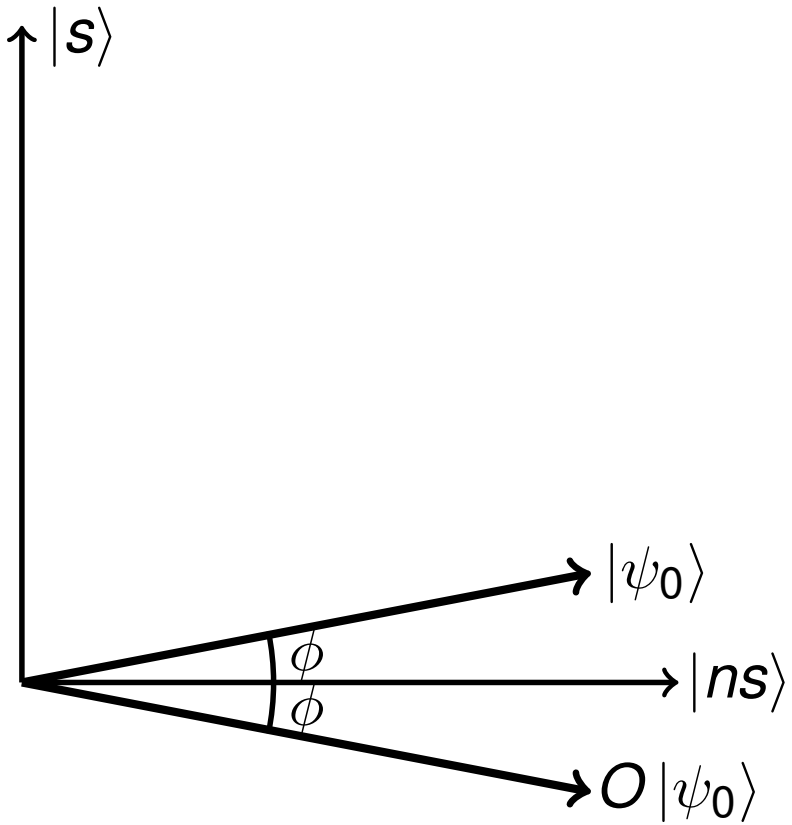


Figure: İlk Grover yinelemesi

- Grover yinelemesi kahin ve yansıtma operatörlerinin sırayla uygulanmasından oluşur ($G = RO$).
- Kahin operatörü $|ns\rangle$ durumuna göre bir yansıtma operatörü görevi görür.
- Sonrasında yansıtma operatörü $|\psi_0\rangle$ durumuna göre bir yansıtma yapar.
- Bu iki operatörün arka arkaya uygulanması sonucu 2ϕ miktarında bir rotasyon yapılmış olur.

Grover Algoritması

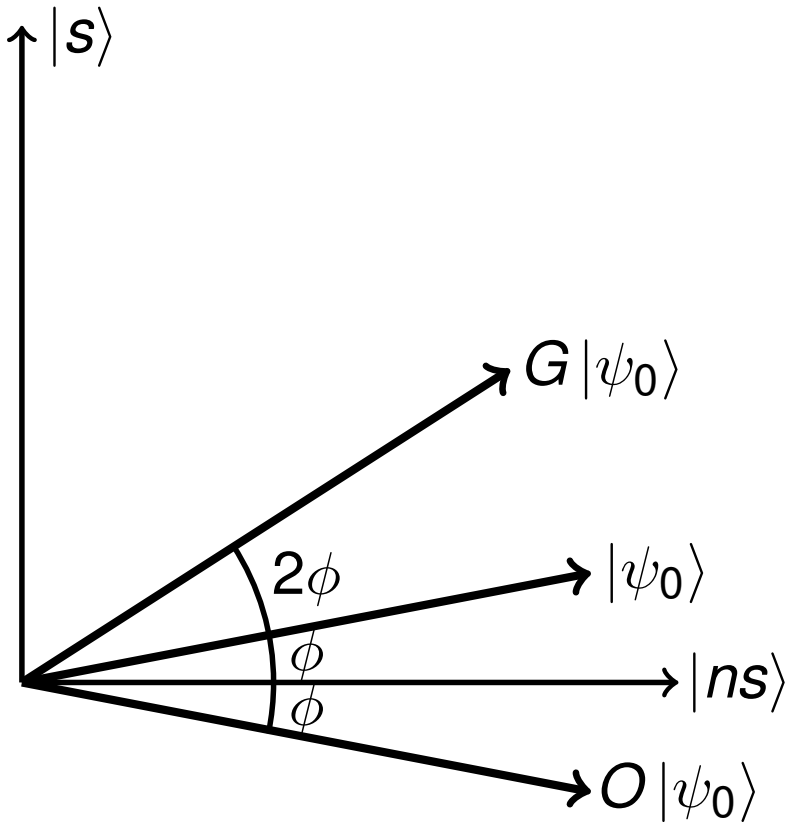


Figure: İlk Grover yinelemesi

- Grover yinelemesi kahin ve yansıtma operatörlerinin sırayla uygulanmasından oluşur ($G = RO$).
- Kahin operatörü $|ns\rangle$ durumuna göre bir yansıtma operatörü görevi görür.
- Sonrasında yansıtma operatörü $|\psi_0\rangle$ durumuna göre bir yansıtma yapar.
- Bu iki operatörün arka arkaya uygulanması sonucu 2ϕ miktarında bir rotasyon yapılmış olur.

Grover Algoritması

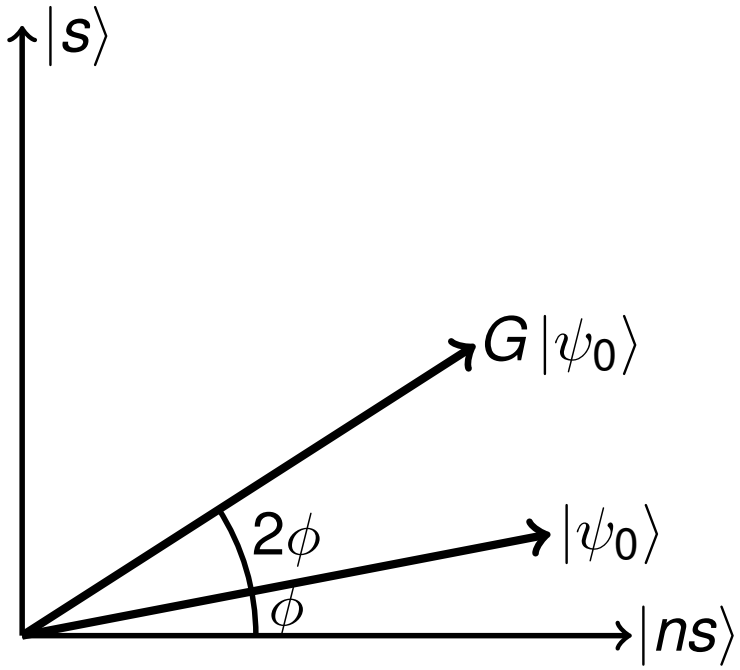


Figure: İkinci Grover yinelemesi

- Grover operatörü $G|\psi_0\rangle$ durumu üzerinde tekrar uygulandığında da benzer bir etki yapar.
- Önce kahin operatörü $G|\psi_0\rangle$ durumunu $|ns\rangle$ durumuna göre yansıtır.
- Sonrasında yansıtma operatörü $OG|\psi_0\rangle$ durumunu $|\psi_0\rangle$ durumuna göre yansıtır.
- Sonuç olarak Grover yinelemesi tekrar uygulandığında, bir kez daha 2ϕ miktarında rotasyon yapılmış olur.

Grover Algoritması

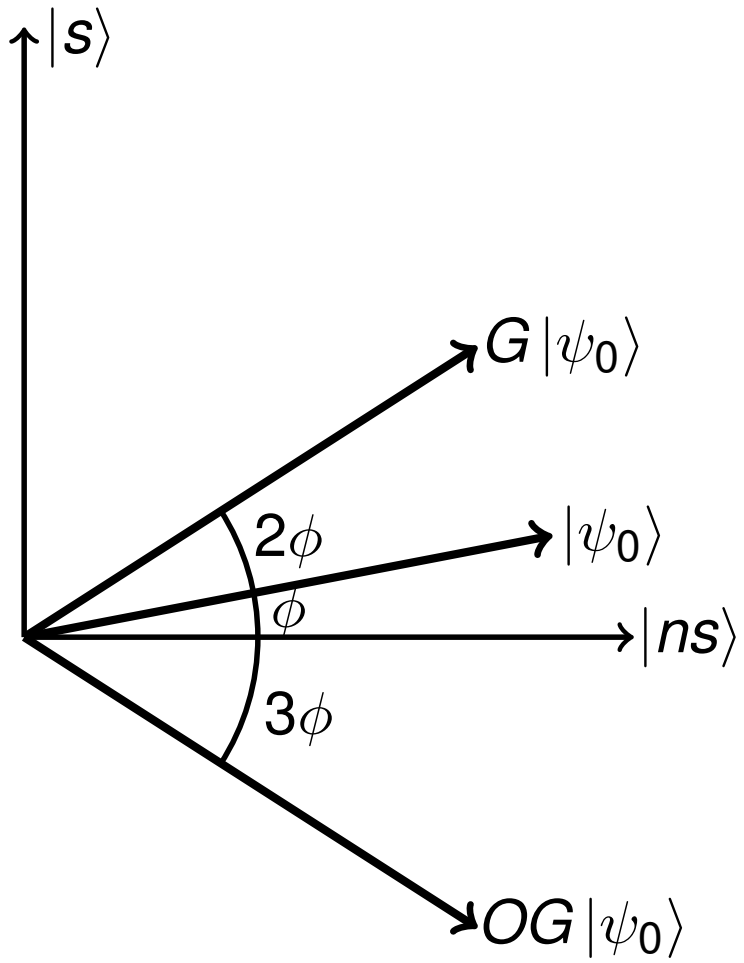


Figure: İkinci Grover yinelemesi

- Grover operatörü $G|\psi_0\rangle$ durumu üzerinde tekrar uygulandığında da benzer bir etki yapar.
- Önce kahin operatörü $G|\psi_0\rangle$ durumunu $|ns\rangle$ durumuna göre yansıtır.
- Sonrasında yansıtma operatörü $OG|\psi_0\rangle$ durumunu $|\psi_0\rangle$ durumuna göre yansıtır.
- Sonuç olarak Grover yinelemesi tekrar uygulandığında, bir kez daha 2ϕ miktarında rotasyon yapılmış olur.

Grover Algoritması

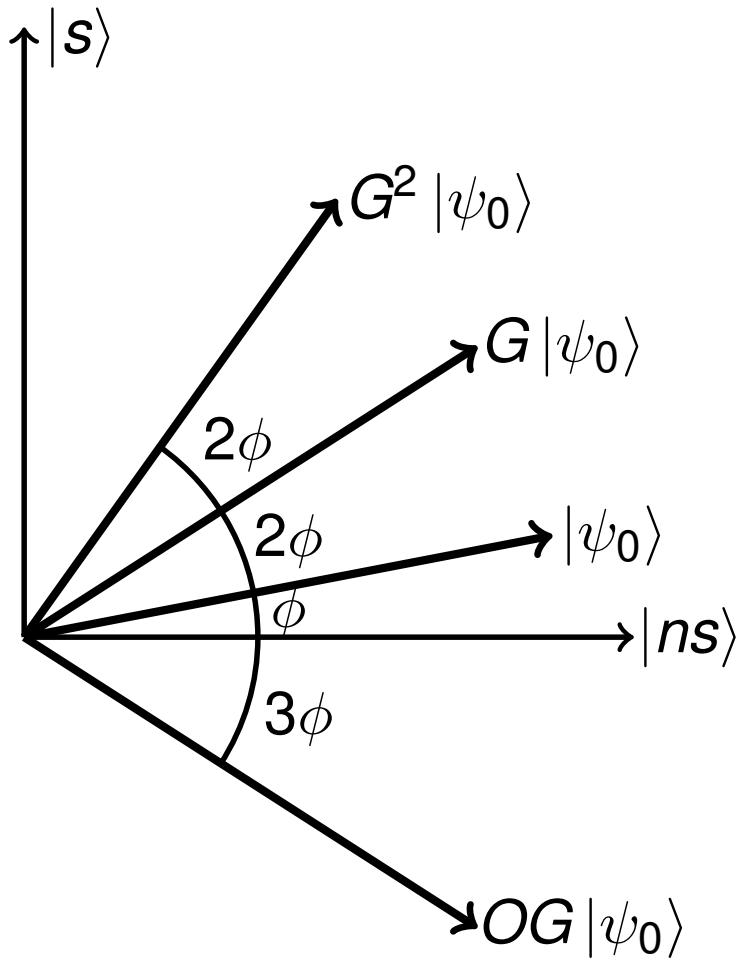


Figure: İlkinci Grover yinelemesi

- Grover operatörü $G|\psi_0\rangle$ durumu üzerinde tekrar uygulandığında da benzer bir etki yapar.
- Önce kahin operatörü $G|\psi_0\rangle$ durumunu $|ns\rangle$ durumuna göre yansıtır.
- Sonrasında yansıtma operatörü $OG|\psi_0\rangle$ durumunu $|\psi_0\rangle$ durumuna göre yansıtır.
- Sonuç olarak Grover yinelemesi tekrar uygulandığında, bir kez daha 2ϕ miktarında rotasyon yapılmış olur.

Grover Algoritması

- Grover yinelemesinin bu tanımı kullanılarak m defa Grover operatörü uygulandıktan sonra elde edilen kuantum durumu aşağıdaki gibi gösterilebilir.

$$G^m |\psi_0\rangle = \sin[(2m+1)\phi] |s\rangle + \cos[(2m+1)\phi] |ns\rangle \tag{7}$$

- Aranacak kümenin eleman sayısının çok büyük olduğu kabul edilebilir. ($N \gg 1$). Bu kabulle, tek çözüm olan durumda ($M = 1$) aşağıdaki yakınlaştırmalar kullanılabilir.

$$\sin\phi = \frac{1}{\sqrt{N}} \approx \phi \tag{8}$$

$$G^m |\psi_0\rangle \approx \sin\left(\frac{2m}{\sqrt{N}}\right) |s\rangle + \cos\left(\frac{2m}{\sqrt{N}}\right) |ns\rangle \tag{9}$$

Grover Algoritması

- Bu yakınlaştırmalarla, m adet Grover yinelemesi sonrasında oluşan kuantum durumunda yapılan bir ölçümde çözümün bulunma olasılığı şu şekilde olur:

$$P(m) = \sin^2\left(\frac{2m}{\sqrt{N}}\right) \tag{10}$$

- Bu durumda, $\pi/4\sqrt{N}$ adet Grover yinelemesi sonucunda çözümün bulunma olasılığı 1 olur.

Grover Algoritması

İyileştirmeler

- 1997 yılında yayınlanan bir makalede $0.785\sqrt{N}$ yerine daha az sayıda yineleme kullanılarak yapılan ard arda aramaların beklenen toplam yineleme sayısını düşürdüğü kanıtlandı.[2]

$$E = m + \cos^2\left(\frac{2m}{\sqrt{N}}\right) m + \cos^4\left(\frac{2m}{\sqrt{N}}\right) m + \ldots \tag{11}$$

$$E = m \sum_{j \geq 1} \left[\cos^2\left(\frac{2m}{\sqrt{N}}\right)\right]^{j-1} \tag{12}$$

- Bu eşitlik optimize edildiğinde, her arama için optimum yineleme sayısı $0.583\sqrt{N}$ olarak bulundu. Bu durumda beklenen toplam yineleme sayısının $0.690\sqrt{N}$ olduğu gösterildi.

[2] M. Boyer, G. Brassard, P. Høyer, and A. Tapp, Tight bounds on quantum searching, Fortschritte der Physik 46, 493 (1998).

Önbilgi Sahibi Olunan Kümeler

- Şimdiye kadar anlatılan tüm arama problemlerinde tüm elemanların çözüm olma olasılığının eşit olduğu varsayıldı.
- Önbilgi sahibi olunan kümelerde elemanların çözüm olma olasılığının önceden bilinen bir dağılım fonksiyonuna uyduğu var sayılır.
- İndeksi i olan bir elemanın problemin çözümlerinden biri olmasının olasılığı p_i olarak verilmiştir.
- Tek çözüm olan durumda, bu ayrık olasılıklar aşağıdaki koşulu sağlar.

$$\sum_{i=0}^{N-1} p_i = 1 \tag{13}$$

Jenerik Arama Metodu

Prosedür

- Orijinal Grover Algoritması'nda aranan küme içindeki tüm elemanların çözüm olma olasılığının eşit olduğu varsayılır ve başlangıç durumu olarak $|\psi_0\rangle$ kullanılır.
- Önbilgi sahibi olunan kümelerde arama yapıldığında, farklı kuantum durumları kullanılarak beklenen toplam yineleme sayısı azaltılabilir.

$$|\psi\rangle = \sum_{i=0}^{N-1} c_i |i\rangle \tag{14}$$

- Jenerik arama metodunda, çözüm bulunana kadar, farklı başlangıç durumları ve farklı yineleme sayılarıyla ard arda kuantum aramalar uygulanır.

Jenerik Arama Metodu

Değişkenler ve Sabitler

Jenerik Arama Methodu'nu tanımlamak ve beklenen toplam yineleme sayısını ifade edeblimek için kullanılan parametreler şöyledir:

- p_i: Bilinen olasılık dağılımında, çözümün indeksinin i olma olasılığı
- $|\psi_j\rangle$: Arama j için kullanılan başlangıç durumu
- $c_i^{(j)}$: Arama j için kullanılan başlangıç durumunda i indeksinin katsayısı
- ϕ_i: Çözüm indeksinin i olduğu durumda başlangıç durumuyla $|ns\rangle$ arasındaki açı
- m_j: Arama j sırasında uygulanan Grover yinelemesi sayısı
- $\theta_i^{(j)}$: Çözüm indeksinin i olduğu durumda, arama j bittikten sonraki kuantum durumu ile $|ns\rangle$ arasındaki açı

- Grover Algoritması için kullanılan tanımlar ve kabuller kullanılarak bu parametreler arasında aşağıdaki ilişkiler kurulabilir.

$$\left|\psi_j\right\rangle = \sum_{i=0}^{N-1} c_i^{(j)} \left|i\right\rangle \tag{15}$$

$$c_i^{(j)} = \arcsin \phi_i^{(j)} \approx \phi_i^{(j)} \tag{16}$$

$$\theta_i^{(j)} \approx 2 m_j c_i^{(j)} \tag{17}$$

- Gösterim kolaylığı için, beklenen değer ifadesinde m_j ve θ_i^j değişkenleri kullanıldı. Bu değişkenlerin optimum değerleri bulunduktan sonra $\left|\psi_j\right\rangle$ kolayca bulunabilir.

- Çözüm indeksinin *i* olduğu durumda, beklenen toplam yineleme sayısı, olasılıksal kuantum aramaya benzer şekilde bulunabilir.

$$E_i = m_1 + \cos^2\theta_i^{(1)} m_2 + \cos^2\theta_i^{(1)} \cos^2\theta_i^{(2)} m_3 + \ldots \tag{18}$$

$$E_i = \sum_{j\geq 1} m_j \prod_{k=1}^{j-1} \cos^2\theta_i^{(k)} \tag{19}$$

- Yukarıda verilen tanım ve olasılık değerleri kullanılarak, beklenen toplam yineleme sayısı şöyle gösterilir:

$$E = \sum_{i=0}^{N-1} p_i \sum_{j\geq 1} m_j \prod_{k=1}^{j-1} \cos^2\theta_i^{(k)} \tag{20}$$

- Beklenen yineleme sayısı için verilen ifade sonsuz sayıda değişken içerdiği için, analitik veya nümerik yöntemlerle parametreleri optimize etmek mümkün değildir.
- Beklenen değerin minimumuna yakınsamak için verilen metota çok benzeyen ancak sonlu sayıda kuantum arama içeren bir metot kullanılabilir.
- Bu metot, en fazla s adet arama içeren ve son adımı sonucu kesin olarak bulabilecek şekilde dizayn edilmiştir ($m_s = \pi/4\sqrt{N}$).

$$E = \sum_{i=0}^{N-1} p_i \sum_{j=1}^{s} m_j \prod_{k=1}^{j-1} \cos^2 \theta_i^{(k)} \tag{21}$$

- Metodun değiştirilmiş halinde beklenen yineleme sayısı sonlu sayıda parametre içerdiği için, bu parametrelerin optimum değerleri Lagrange çarpanları yöntemiyle bulunabilir.
- Bu yöntemi uygulamak için $\left|\psi_j\right\rangle$ durumunun normalizasyon eşitliği kullanılarak aşağıdaki kısıt ifadesi türetilmiştir.

$$\sum_{i=0}^{N-1}\left[\theta_i^{(j)}\right]^2 = 4m_j^2 \tag{22}$$

- Bu eşitlik ve E için verilen eşitlik kullanılarak aşağıdaki Lagrange fonksiyonu yazılmıştır.

$$\mathcal{L} = \sum_{i=0}^{N-1} p_i \sum_{j=1}^{s} m_j \prod_{k=1}^{j-1} \cos^2\theta_i^{(k)} - \sum_{j=1}^{s-1}\lambda_j\left(\sum_{i=0}^{N-1}\left[\theta_i^{(j)}\right]^2 - 4m_j^2\right) \tag{23}$$

- Beklenen yineleme sayısının minimum olduğu nokta, bu fonksiyonun varyasyonunun sıfıra eşit olduğu noktadır.
- Bu nokta, $\mathcal{L}$ fonksiyonunun m_j, $\theta_i^{(j)}$ ve λ_j parametrelerine göre alınan kısmi türevleri sıfıra eşitlenerek bulunabilir.

$$\sum_{i=0}^{N-1} p_i \prod_{k=1}^{j-1} \cos^2 \theta_i^{(j)*} = 8\lambda_j^* m_j^* \tag{24}$$

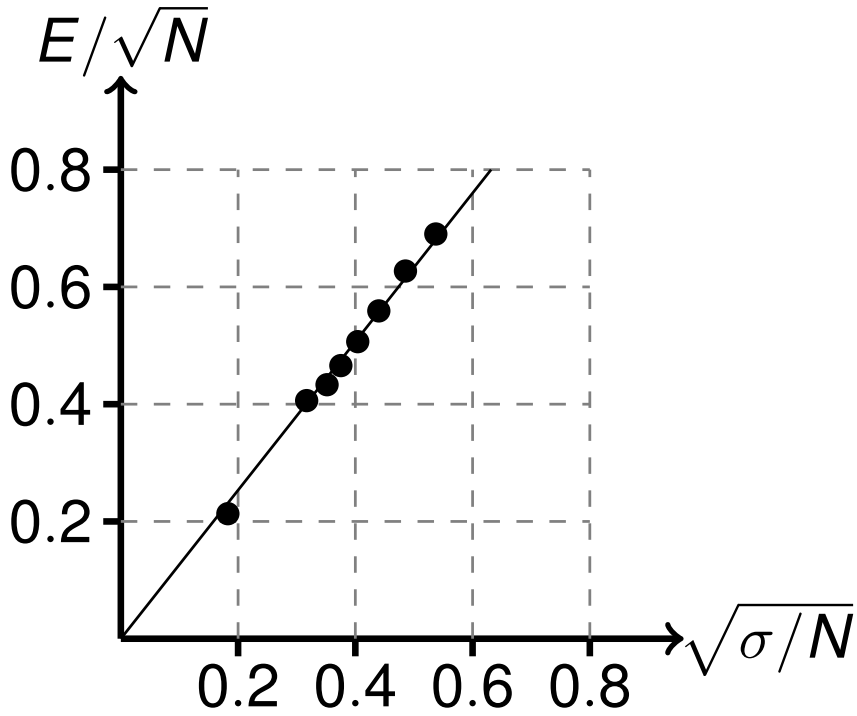
$$\sum_{i=0}^{N-1} \left[\theta_i^{(j)*}\right]^2 = 4m_j^{*2} \tag{25}$$

$$p_i \cos\theta_i^{(l)*} \sin\theta_i^{(l)*} \sum_{j=l+1}^{n} m_j^* \prod_{\substack{k<j \\ k\neq l}} \cos^2 \theta_i^{(k)*} = \lambda_l^* \theta_i^{(l)*} \tag{26}$$

Nümerik Analiz Sonuçları

8 farklı olasılık dağılımı için yapılan nümerik analizin sonucunda, E'nin minimum değeri için bulunan tahminlemeler aşağıda verilmiştir.[3] [4]

$p(x)$	σ	E
1	$0.287N$	$0.690\sqrt{N}$
$2x$	$0.236N$	$0.627\sqrt{N}$
$3x^2$	$0.194N$	$0.559\sqrt{N}$
$4x^3$	$0.163N$	$0.507\sqrt{N}$
$5x^4$	$0.141N$	$0.466\sqrt{N}$
$6x^5$	$0.124N$	$0.433\sqrt{N}$
exp	$0.033N$	$0.213\sqrt{N}$
hnorm	$0.100N$	$0.406\sqrt{N}$



[3] Orijinal grover algoritması çözüm için $0.785\sqrt{N}$ yineleme gerektirir.

[4] Olasılıksal kuantum aramada beklenen yineleme sayısı $0.690\sqrt{N}$'dir.

Nümerik Analiz Sonuçları

- Yukarıda verilen grafikte, beklenen yineleme sayısı ve verilen olasılık dağılımının standart sapmasının kökü arasında lineer bir ilişki olduğu görülmektedir.
- Bu lineer ilişki aşağıda verilmiştir.

$$E = 1.267\sqrt{\sigma} \tag{27}$$

- Bu ilişki kullanılarak verilen bir olasılık dağılımı için jenerik arama metodunun beklenen yineleme sayısı yaklaşık olarak bulunabilir.
- Bu analizde kullanılan tüm olasılık dağılımları monotondur. Monoton olmayan olasılık dağılımları için beklenen değer bulunurken önce dağılımın sıralanmış halinin standart dağılımı bulunup, sonrasında yukarıdaki eşitlik kullanılmalıdır.

Sonuçlar

- Jenerik arama metodu sayesinde olasılık dağılımı bilinen kümelerde daha az işlem gücüyle ve daha kısa sürede kuantum arama yapılabilir.
- Bulunan lineer ilişki sayesinde verilen bir olasılık dağılımı için kaç adet Grover yinelemesi uygulanarak sonucun bulunabileceği kolayca hesaplanabilir.
- Şifre çözmek için kullanılan kaba kuvvet algoritmalarında daha olası olan şifreler bilindiği için, bir olasılık dağılımı oluşturulup jenerik arama metodu kullanılabilir.
- Merkezi limit teoremi sayesinde, bazı büyük boyutlu problemlerde muhtemel çözümlerin normal dağılıma uyduğu kabul edilerek jenerik arama metodu kullanılabilir.

Referanslar

1) R. P. Feynman, Simulating physics with computers, International Journal of Theoretical Physics 21, 467 (1982).

2) R. P. Feynman, Quantum mechanical computers, Optics News 11, 11 (1985).

3) P. W. Shor, Polynomial-time algorithms for quantum computation: Discrete logarithms and factoring, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE, 1994).

4) L. K. Grover, A fast quantum mechanical algorithm for database search, in *Proceedings of the 28th Annual ACM Symposium on Theory of Computing* (ACM, 1996).

5) L. K. Grover, Quantum mechanics helps in searching for a needle in a haystack, Physical Review Letters 79, 325 (1997).

6) M. Boyer, G. Brassard, P. Høyer, and A. Tapp, Tight bounds on quantum searching, Fortschritte der Physik 46, 493 (1998).

7) M. A. Nielsen and I. L. Chuang, Quantum computation and quantum information (10th aniversary edition) (Cambridge University Press, 2010) Chap. Quantum Search Algorithm, pp. 248–276.

8) U. Çalıkyılmaz, *Quantum Search in Sets with Prior Knowledge*, Master's thesis, Middle East Technical University (2021).