

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



دانشگاه صنعتی شاهرود

دانشکده: فیزیک

گروه: فیزیک ذرات بنیادی

# جستجوی کوانتومی با کیوتریت‌ها

دانشجو:

الهام علی بخشی فرد

استاد راهنما:

دکتر حسین موحدیان

پایان نامه ارشد جهت اخذ درجه کارشناسی ارشد

بهمن ۱۳۸۹

دانشگاه صنعتی شاهرود

دانشکده: فیزیک

گروه: ذرات بنیادی

پایان نامه کارشناسی ارشد الهام علی بخشی فرد

تحت عنوان:

جستجوی کوانتومی با کیوتریت ها

در تاریخ ..... توسط کمیته تخصصی زیر جهت اخذ مدرک کارشناسی ارشد  
مورد ارزیابی و با درجه ..... مورد پذیرش قرار گرفت.

امضاء	اساتید مشاور	امضاء	اساتید راهنما
	نام و نام خانوادگی:		نام و نام خانوادگی:
	نام و نام خانوادگی:		نام و نام خانوادگی:

امضاء	نماینده تحصیلات تکمیلی	امضاء	اساتید داور
	نام و نام خانوادگی:		نام و نام خانوادگی:
			نام و نام خانوادگی:
			نام و نام خانوادگی:
			نام و نام خانوادگی:

## تقدیم به

خانواده‌ی عزیز و همسر مهربانم که در تمام مراحل زندگی مدیون حمایت‌هایشان هستم.

## تشکر و قدردانی

خداوند مهربان را شاکرم که توفیق طی این مرحله از آموختن را بر من عطا نمود. بر خود لازم می‌دانم کمال تشکر و قدردانی خود را از زحمات استاد بزرگوارم جناب آقای دکتر حسین موحدیان که راهنمایی این پایان‌نامه برعهده ایشان بود ابراز نمایم. همچنین از پدر و مادر مهربان، خانواده‌ی عزیز و همسر گرامی‌ام که دشواری‌های این مسیر با وجود ایشان هموار گردید تشکر می‌نمایم و از تمام اساتید ارجمند و دوستان گرامی که بنده را در انجام و تدوین این پایان‌نامه یاری نمودند سپاسگزارم.

# تعهد نامه

اینجانب الهام علی بخشی فرد دانشجوی دوره کارشناسی ارشد، رشته ذرات بنیادی، دانشکده فیزیک دانشگاه صنعتی شاهرود، نویسنده‌ی پایان نامه‌ی جستجوی کوانتومی با کیوتریت‌ها تحت راهنمایی دکتر حسین موحدیان متعهد می‌شوم:

- تحقیقات در این پایان نامه توسط اینجانب انجام شده است و از صحت و اصالت برخوردار است.
- در استفاده از نتایج پژوهش‌های محققان دیگر به مرجع مورد استفاده استناد شده است.
- مطالب مندرج در پایان نامه تاکنون توسط خود یا فرد دیگری برای دریافت هیچ نوع مدرک یا امتیازی در هیچ جا ارائه نشده است.
- کلیه حقوق معنوی این اثر متعلق به دانشگاه صنعتی شاهرود می‌باشد و مقالات مستخرج با نام «دانشگاه صنعتی شاهرود» و یا «Shahrood University of Technology» به چاپ خواهد رسید.
- حقوق معنوی تمام افرادی که در به‌دست آمدن نتایج اصلی پایان نامه تأثیرگذار بوده‌اند در مقالات مستخرج از پایان نامه رعایت می‌گردد.
- در کلیه مراحل انجام این پایان‌نامه، در مواردی که از موجود زنده (یا بافتهای آنها) استفاده شده است ضوابط و اصول اخلاقی رعایت شده است.
- در کلیه مراحل انجام این پایان نامه، در مواردی که به حوزه اطلاعات شخصی افراد دسترسی یافته یا استفاده شده است اصل رازداری، ضوابط و اصول اخلاق انسانی رعایت شده است.

## امضای دانشجو

تاریخ ۸۹/۱۱/۱۲

### مالکیت نتایج و حق نشر

- کلیه حقوق معنوی این اثر و محصولات آن (مقالات مستخرج، کتاب، برنامه‌های رایانه‌ای، نرم‌افزارها و تجهیزات ساخته شده است) متعلق به دانشگاه صنعتی شاهرود می‌باشد. این مطلب باید به نحو مقتضی در تولیدات علمی مربوطه ذکر شود.
- استفاده از اطلاعات و نتایج موجود در پایان نامه بدون ذکر مرجع مجاز نمی‌باشد.

## چکیده

کامپیوترها و ابزارهای محاسباتی همواره در کانون توجه متخصصین و دانشمندان بوده و تلاش برای پیشرفت و بهبود آنها ادامه دارد. با ظهور ایده‌ی استفاده از مکانیک کوانتومی در کامپیوترها، علم محاسبات کوانتومی متولد شد و دانشمندان را بر آن داشت تا از خواص منحصر بفرد آن در کامپیوترها استفاده کنند. ساخت کامپیوترهای کوانتومی پیشرفتی را به همراه دارد که قابل مقایسه با سیستم‌های کلاسیکی نیست.

الگوریتم جستجوی کوانتومی که اصول اولیه‌ی آن توسط گراور کشف شد می‌توانست یک گزینه‌ی مشخص را در یک فضای جستجوی نامنظم به اندازه‌ی  $N$  در  $O(\sqrt{N})$  مرحله بیابد که احتمال موفقیت آن حداقل ۵۰٪ بود. [28] احمد یونس توانست با تغییراتی در روش گراور، احتمال دستیابی با جواب را به حداقل ۸۷/۸۸٪ برساند. [29]

در این پایان‌نامه بر اساس استفاده از واحدهای حافظه‌ی کیوتریتی و تفکیک حالت‌های جواب به جواب زوج و جواب فرد، دو طرح برای الگوریتم گراور ارائه داده‌ایم که با استفاده از آن، در تکرارهای زوج دامنه‌ی جواب زوج افزایش یابد و در تکرارهای فرد، دامنه‌ی جواب فرد. در ادامه یک الگوی جدید برای حالت کلی ضرایب الگوریتم یونس پیشنهاد داده و نیز با ایجاد تغییراتی در الگوریتم یونس آن را برای جستجو با استفاده از کیوتریت‌ها با همان احتمال بالای الگوریتم مذکور عملی ساخته‌ایم.

**کلمات کلیدی:** مکانیک کوانتومی- کامپیوتر کوانتومی- اطلاعات کوانتومی و محاسبات کوانتومی- جستجوی

کوانتومی- الگوریتم گراور- الگوریتم احمد یونس- کیوتریت

# فهرست مطالب

ط	فهرست شکل‌ها	۱
ی	فهرست جدول‌ها	۱
ک	فهرست اختصارات	۱
۱	فصل اول: تاریخچه‌ای از محاسبات کوانتومی	۱
۲	۱-۱ مقدمه	۲
۱۵	فصل دوم: مفاهیم مقدماتی	۱۵
۱۶	۱-۲ اطلاعات کوانتومی و محاسبات کوانتومی	۱۶
۱۶	۲-۲ توازی کوانتومی	۱۶
۱۸	۳-۲ برهم‌نهی	۱۸
۲۰	۴-۲ درهم‌تنیدگی	۲۰
۲۱	۵-۲ حالت‌های خالص و حالت‌های آمیخته	۲۱
۲۲	۶-۲ بیت و پردازش اطلاعات کلاسیک	۲۲
۲۳	۷-۲ کیوبیت	۲۳
۲۴	۸-۲ کره‌ی بلاخ	۲۴
۲۶	۹-۲ کیوتریت	۲۶
۲۸	۱۰-۲ کره‌ی بلاخ	۲۸
۳۱	۱۱-۲ کیودیت	۳۱
۳۱	۱۲-۲ ویژگی‌های یک پایه‌ی ماتریسی کاربردی برای کیودیت‌ها:	۳۱
۳۲	۱۳-۲ بسط بردار بلاخ برای ماتریس چگالی	۳۲
۳۲	۱۴-۲ تعمیم پایه‌ی ماتریسی ژل - من	۳۲
۳۶	فصل سوم: الگوریتم‌های جستجوی کوانتومی	۳۶
۳۷	۱-۳ گیت کلاسیکی	۳۷
۳۷	۲-۳ گیت کوانتومی	۳۷
۳۹	۳-۳ الگوریتم کوانتومی	۳۹
۴۰	۴-۳ الگوریتم گراور	۴۰
۴۷	۵-۳ مراحل الگوریتم گراور	۴۷
۴۸	۶-۳ الگوریتم احمد یونس	۴۸
۴۹	۷-۳ مراحل الگوریتم احمد یونس	۴۹
۵۵	فصل چهارم: جستجوی کوانتومی با کیوتریت‌ها	۵۵
۵۶	۱-۴ گیت هادامارد کیوتریتی	۵۶



۵۷	..... ۲-۴ سری فوریه کلاسیکی
۵۷	..... ۳-۴ تبدیل فوریه کوانتومی با کیوبیت‌ها
۵۹	..... ۴-۴ تبدیل فوریه کوانتومی با کیوتریت‌ها
۶۱	..... ۵-۴ سازگاری تبدیل فوریه کیوتریتی و هادامارد کیوتریتی
۶۳	..... ۶-۴ $f$ - گیت کیوتریتی
۶۵	..... ۷-۴ الگوریتم گراور با کیوتریت‌ها
۶۶	..... ۸-۴ الگوی گیت‌های وابسته به تکرار
۷۰	..... ۹-۴ الگوی دوازده گیتی
۷۲	..... ۱۰-۴ بیانی دیگر از الگوریتم یونس
۷۵	..... ۱۱-۴ الگوریتم جستجوی کوانتومی یونس با کیوتریت‌ها:
۸۱	..... ۱۲-۴ بیانی دیگر از الگوریتم احمد یونس با کیوتریت‌ها:
۹۲	..... پیوست‌ها

## فهرست شکل‌ها

۲۶	شکل ۱-۲ نمایش هندسی کره‌ی بلاخ
۲۶	شکل ۲-۲ پولاریزه‌های راستگرد و چپگرد فوتون
۳۸	شکل ۱-۳ نمایش تاثیر عملگر هادامارد روی حالت $ 0\rangle$
۳۸	شکل ۲-۳ نمایش گیت هادامارد در مدار
۳۹	شکل ۳-۳ نمایش گیت CNOT در مدار
۳۹	شکل ۴-۳ نمایش $f$ گیت در مدار
۴۲	شکل ۵-۳ نمایش اثر عملگر $U_f$
۴۲	شکل ۶-۳ نمایش اثر عملگر $D$
۴۵	شکل ۷-۳ نمودار احتمال موفقیت الگوریتم گراور بر حسب تعداد داده‌ها
۴۵	شکل ۸-۳ نمودار احتمال موفقیت الگوریتم گراور بر حسب تعداد جواب‌ها
۴۸	شکل ۹-۳ نمودار الگوریتم گراور
۵۲	شکل ۱۰-۳ مقایسه‌ی احتمال موفقیت در تکرار اول الگوریتم یونس، گراور و حالت کلاسیکی
۵۳	شکل ۱۱-۳ مقایسه‌ی نمودارهای احتمال موفقیت الگوریتم یونس و گراور در تکرارهای دوم تا پنجم
۵۴	شکل ۱۲-۳ نمودار الگوریتم احمد یونس
۵۴	شکل ۱۳-۳ مقایسه‌ی نمودارهای موفقیت الگوریتم یونس و گراور
۷۰	شکل ۱-۴ نمودار الگوریتم پیشنهادی گیت وابسته به تکرار
۷۱	شکل ۲-۴ نمودار الگوریتم پیشنهادی ۱۲- $f$ گیتی
۸۰	شکل ۳-۴ نمودار الگوریتم پیشنهادی برای جواب زوج و فرد
۹۰	شکل ۴-۴ نمودارهای $P_s$ بر حسب $x = M/N$ برای الگوریتم یونس، کلی‌سازی پیشنهادی و الگوریتم کیوتریتی

## فهرست جدول‌ها

- جدول ۱-۴ فاز دامنه‌ی جواب‌های مربوط به هر تکرار ..... ۶۹
- جدول ۲-۴ مقادیر  $f$  برای تکرارهای اول تا ششم ..... ۷۱
- جدول ۳-۴ مقایسه‌ی ضرایب ۴ تکرار اول الگوریتم یونس با فرمول کلی و الگوی پیشنهادی ..... ۷۵

UTM	Universal Turing Machine
NMR	Nuclear Magnetic Resonance
Bit	Binary digit
Qubit	Quantum binary digit
Qutrit	Quantum ternary digit
SU(N)	Special Unitary (N)
GGB	Generalized Gell mann Basis
GGM	Generalized Gell mann Matrices
NAND	NOT AND
NOR	NOT OR
C-NOT	Controlled not
H-gate	Hadamard-gate
f-gate	Function- gate
D	Diffusion
QFT	Quantum Fourier Transform
I	Identity
Inv	Inversion



فصل اول: تاریخچه‌ای از محاسبات کوانتومی

## ۱-۱ مقدمه

در بخش اول سعی داریم به بررسی تحول در علم کامپیوتر و تاریخچه‌ی محاسبات کوانتومی بپردازیم.

کامپیوترهای امروزی در حقیقت نقطه‌ی اوج پیشرفت‌های فنی‌ای هستند که ایده‌های اولیه‌ی چارلز بابیج را تکامل بخشیدند. در ۱۸۳۶ چارلز بابیج<sup>۱</sup> ظهور اولین ماشین قابل برنامه‌ریزی، یک کامپیوتر مکانیکی که قابلیت انجام اعمال محاسباتی داشته باشد را پیشگویی نمود.

در سال ۱۹۳۶ آلن تورینگ<sup>۲</sup> که ملقب به پدر علوم کامپیوتر است، طی مقاله‌ای مدلی برای محاسبات ارائه داد. این مدل هم اکنون به‌عنوان ماشین تورینگ مشهور است. وی نشان داد که یک ماشین تورینگ جهانی وجود دارد که همه‌ی ماشین‌های تورینگ را می‌توان با آن شبیه‌سازی کرد و روشن ساخت که یک ماشین محاسبه‌گر چه توانایی‌هایی باید داشته باشد و همچنین به اهمیت برنامه‌نویسی تاکید کرد. تورینگ به‌طور کامل مفهوم آنچه که ما امروزه آن را کامپیوتر قابل برنامه‌ریزی می‌نامیم گسترش داد. او مدعی بود که ماشین تورینگ جهانی هر آنچه که توسط ماشین‌های الگوریتمی قابل اجرا باشند می‌تواند اجرا کند. یعنی اگر یک الگوریتم قابل اجرا روی هر بخشی از سخت افزار باشد، الگوریتمی برای ماشین تورینگ جهانی وجود دارد که دقیقاً همان وظیفه‌ی الگوریتم را اجرا می‌کند. این بیان، به افتخار آلن تورینگ و یکی دیگر از پیشگامان علم کامپیوتر، چرچ<sup>۳</sup>، اصل چرچ - تورینگ نامیده شد. با یک مثال، مفهوم ماشین تورینگ را روشن می‌سازیم. خود را به جای یک ریاضیدان یا منطق‌دان قرار می‌دهیم که سعی می‌کند مسئله‌ی مشخصی را بررسی کند. چنین شخصی دقیقاً چه می‌کند؟ وی داده‌هایی از روی کاغذ می‌خواند، مطابق با این داده‌های دریافتی، حالت‌های ذهنی‌اش تغییر می‌کند. سپس مطابق با این حالت‌های ذهنی و داده‌هایی که دریافت کرده است داده‌های جدیدی را روی کاغذ می‌نویسد یا داده‌های قدیمی را پاک می‌کند. این که چگونه داده‌های خوانده شده و حالت‌های ذهنی، منجر به داده‌های جدید می‌شوند همان الگوریتم است. می‌توانیم فرض کنیم تمام داده‌ها به‌صورت علائمی از یک

---

<sup>1</sup> Charles Babbage

<sup>2</sup> Alan Turing

<sup>3</sup> Alenzo Church

حروف الفبا در مربع‌های کوچکی نوشته می‌شوند که این مربع‌ها می‌توانند در یک نوار یک بعدی مرتب شوند. به این ترتیب ماشینی درست می‌شود که آن را ماشین تورینگ می‌خوانیم. واضح است که توانایی محاسباتی این ماشین تورینگ محدود است. حال سوال این است: آیا می‌توان مدل محاسبه‌ای تصور کرد که توانایی‌اش بیشتر از ماشین تورینگ باشد؟ پاسخ این سوال که منفی نیز هست چیزی است که به نام نظریه‌ی چرچ - تورینگ شناخته می‌شود که در ادامه به آن خواهیم پرداخت.

ماشین‌های تورینگی که تاکنون درباره‌ی آن‌ها صحبت کردیم همگی کارهای خاصی را انجام می‌دهند و برنامه‌ی آنها چنان نوشته شده است که یک محاسبه‌ی معین را انجام دهند یا یک زبان خاص را شناسایی کنند. اما می‌توان یک ماشین تورینگ جهان‌شمول ساخت که بتواند هر ماشین تورینگ دیگری را شبیه‌سازی کند. این ماشین که اختصاراً آن را با UTM<sup>1</sup> نشان می‌دهیم در واقع مدل نظری کامپیوترهای قابل برنامه‌ریزی امروزی است و ماشین تورینگ جهانی خوانده می‌شود. [1]

ممکن است این سوال پیش بیاید که معنی کارایی کامپیوترهای کوانتومی چیست؟ کارایی یعنی اجرای الگوریتم در زمان چند جمله‌ای. بطور کاملاً مشخص الگوریتم غیرکارآمد، الگوریتمی است که به زمان ابرچند جمله‌ای و یا به‌طور نمادین به زمان نمایی احتیاج دارد. آنچه در حدود سال ۱۹۷۰، یعنی زمان تولد محاسبات و اطلاعات کوانتومی، بدان توجه شد، این مساله بود که مدل محاسباتی ماشین تورینگ از هر مدل محاسباتی دیگری، توانایی بیشتری دارد. در واقع مساله‌ای که با یک مدل محاسباتی به‌طور کارآمد قابل حل است را می‌توان توسط مدل ماشین تورینگ نیز به‌طور کارآمد حل کرد. زیرا هر مدلی از محاسبات را می‌توان توسط ماشین تورینگ شبیه‌سازی کرد.

اولین کامپیوتر شامل اجزای الکترونیکی به نام  $Z_3$  توسط کونارد زوس<sup>۲</sup> آلمانی در سال ۱۹۴۱ اختراع شد. کامپیوترهای مدرن و پرسرعت امروزی، چیزی جز یک ماشین تورینگ نیستند و از نظر اصول کار تفاوت

---

<sup>1</sup> Universal Turing Machine

<sup>2</sup> Konard Zuse

بنیادینی با ابعاد خود که ۳۰ تن وزن داشتند و حدوداً از ۱۸۰۰۰ لامپ خلاء و بیش از ۹۰۰ کیلومتر سیم ساخته شده بودند، ندارند.

جان فون نیومن<sup>۱</sup> (۱۹۵۸ - ۱۹۰۳) یک مدل تئوری ساده ارائه داد که چگونه می‌توان اجزای لازم برای یک کامپیوتر را در کنار هم گذاشت تا توانایی‌های یک ماشین تورینگ جهانی را داشته باشد.

پیشرفت بخش سخت‌افزار کامپیوتر از سال ۱۹۴۷ با کشف ترانزیستور توسط جان باردین، والتر برایتن و ویلیام شاکلی<sup>۲</sup> جهش بزرگی یافت. پیشرفت تکنولوژی تنها باعث تفاوت‌هایی در اندازه و سرعت کامپیوترها شده است. گرچه امروزه کامپیوترها به صورت کم‌حجم درآمده‌اند و وظیفه‌ی خود را با سرعت بیشتری انجام می‌دهند، اما کاری که انجام می‌دهند تغییر نکرده است: محاسبه روی رشته‌ای از بیت‌ها. [1]

در سال ۱۹۴۸ شانون پدر علم اطلاعات در مقاله‌ی «نظریه‌ی ریاضی اطلاعات» نشان داد که با در نظر گرفتن حدود خاصی می‌توان داده‌ها را بدون از دست دادن اطلاعاتش فشرده سازی ساخت. در خارج از حیطه‌ی این شرایط خاص، از دست رفتن پاره‌ای از اطلاعات اجتناب ناپذیر است. [2] ۵۰ سال بعد، در سال ۱۹۹۵ شوماخر در مقاله‌ی «کد گذاری کوانتومی» یافته‌های خود را در حوزه‌ی کدگذاری ارائه داد. [3]

در سال ۱۹۶۱ قانون لاندائر با این مضمون بیان شد: "محو شدن اطلاعات ضرورتاً فرآیندی اتلافی است و آنتروپی محیط حداقل به مقدار  $k_b T \ln 2$  افزایش می‌یابد که  $k_b$  ثابت بولتزمن می‌باشد."

پیشرفت و رشد سخت افزار با سرعت ادامه یافت به طوری که یک قانون تجربی، مشهور به قانون مور، در سال ۱۹۶۵ توسط گوردون مور<sup>۳</sup> بدین مضمون ارائه شد:

"هر هجده ماه یک بار تعداد ترانزیستورهایی که در یک حجم معین به کار برده می‌شود دو برابر و در نتیجه توان کامپیوترها دو برابر می‌شود که این امر باعث افزایش سرعت پردازش و میزان حافظه‌ی کامپیوترها می‌گردد". [1] قانون مور به طور تقریبی تاکنون برقرار بوده است و به عقیده‌ی بسیاری اگر این روند ادامه یابد تا

---

<sup>1</sup> John von Newmann

<sup>2</sup> John Bardeen, Walter Brattain and Will Shockley

<sup>3</sup> Gordon Moore



سال ۲۰۲۰ می‌توان قطعات کوچکتری ساخت و به جایی رسید که هرگیت تنها تعداد کمی اتم داشته باشد. در واقع یکی از دلایل اصلی برای تلاش در کنترل سیستم‌های کوانتومی مجزا، در ابعاد بسیار کوچک همین مطلب است. اما در چنین ابعادی قوانین فیزیک کلاسیک قادر به توضیح رفتار ذرات نیستند و قوانین مکانیک کوانتومی حکم‌فرما می‌باشد. بنابراین اگر کامپیوترها و ابعاد مدارهای الکترونیکی همچنان کم‌حجم‌تر و کوچک‌تر شوند، تکنولوژی کوانتومی باید جایگزین تکنولوژی امروز شود، یا در کنار آن قرار گیرد و آن را تکمیل کند. امروزه با روش‌های پیشرفته‌ی لیتوگرافی می‌توان عملگرهای منطقی با ضخامت کسری از میکرون ساخت و در چیپ‌های سیلیکونی از آنها استفاده کرد.

یکی از نخستین کارها در زمینه‌ی استفاده از مکانیک کوانتومی، مقاله‌ی محقق بد اقبالی به نام استفان ویزنر<sup>۱</sup> است که اگرچه در سال‌های آغازین دهه‌ی ۷۰ نگاشته شد، اما تا سال ۱۹۸۳ چاپ نشد. در همین مقطع زمانی ایده‌ی به‌کارگیری یک دستگاه محاسباتی که از قوانین مکانیک کوانتومی تبعیت کند توسط چند فیزیک‌دان و متخصص کامپیوتر به‌طور مستقل پیگیری و پروراند شد که از میان آنان می‌توان به چارلز بنت از IBM<sup>۲</sup>، پل بنیف<sup>۳</sup> از آزمایشگاه ملی آرگون در ایلینویز آمریکا، دیوید دویچ<sup>۴</sup> از دانشگاه آکسفورد و سرانجام ریچارد فاینمن<sup>۵</sup> فیزیک‌دان معروف موسسه‌ی فناوری کالیفرنیا و برنده جایزه‌ی نوبل اشاره کرد. ریچارد فاینمن از نخستین کسانی بود که در سال ۱۹۸۱ پیشنهاد داد که سیستم‌های مکانیک کوانتومی بسیار قدرتمندتر از کامپیوترهای کلاسیکی‌اند. وی در مقاله‌ای که در مجله‌ی International Journal of Theoretical Physics در سال ۱۹۸۲ چاپ شد با مطرح کردن این سوال که چه نوعی از کامپیوترها قادر به شبیه‌سازی فیزیک‌اند، پاسخ می‌دهد که تنها کامپیوتر کوانتومی قادر است به‌طور کارا فیزیک کوانتوم را شبیه‌سازی کند. [4] و [1] فاینمن فیزیک کوانتومی را بیشتر از فیزیک کلاسیکی در مرکز توجه خود قرار داد، چرا که به گفته‌ی خودش: "طبیعت

---

<sup>1</sup> Stephen Wiesner

<sup>2</sup> Charles Bennet

<sup>3</sup> Paul Benioff

<sup>4</sup> David Deutsch

<sup>5</sup> Richard P.Feynman

کلاسیکی نیست و اگر خواهان شبیه‌سازی طبیعت هستیم بهتر است شبیه‌سازی خود را با مکانیک کوانتومی بسازیم." وی در سال ۱۹۸۲ با ارائه‌ی یک مدل انتزاعی کوشید نشان دهد که یک سیستم کوانتومی چگونه قادر به محاسبه خواهد بود. او مشاهده کرد که نمی‌توان دسته‌ی خاصی از محاسبات کوانتومی را توسط کامپیوترهای کلاسیکی به‌طور کارا و موثر شبیه‌سازی کرد و بیان داشت که شبیه‌سازی سیستم‌های کوانتومی با کامپیوترهای کلاسیکی کاری دشوار است. این مشاهده به این حدس منجر شد که اگر در محاسبات، از اثرات کوانتومی استفاده شود شاید بتوان در حالت کلی آنها را با کارایی بیشتری انجام داد، و همچنین توضیح داد که چگونه کامپیوتر کوانتومی، فیزیک‌دانان را قادر به شبیه‌سازی دنیای کوانتومی خواهد ساخت و اینکه یک کامپیوتر کوانتومی می‌تواند بسیار قدرتمندتر از یک ماشین تورینگ باشد. بنابراین او پیشنهاد کرد که برای رهایی از چنین مشکلاتی کامپیوترهایی ساخته شوند که اساس کارشان مکانیک کوانتومی باشد. بدین ترتیب جرقه‌ی طراحی کامپیوترهای کوانتومی زده شد. اما ساختن کامپیوترهای کوانتومی بسیار پردردسر به‌نظر می‌رسید و تا زمانی که کسی مطمئن نبود چگونه از اثرات کوانتومی برای افزایش سرعت محاسبات استفاده کند، پیشرفت در این حوزه به‌کندی انجام می‌شد. [1] و [4]

در همان محدوده‌ی زمانی بنیف<sup>۱</sup> در سال ۱۹۸۰ در مقاله‌ی «مدل‌های کوانتومی برای ماشین تورینگ که انرژی را هدر نمی‌دهند» نشان داد چگونه می‌توان از مکانیک کوانتومی برای پیاده‌سازی ماشین تورینگ استفاده کرد و ثابت کرد که سیستم‌های مکانیک کوانتومی قادرند ماشین تورینگ را شبیه‌سازی کنند. به بیان دیگر او استدلال کرد که محاسبات کوانتومی لااقل به قدرتمندی محاسبات کلاسیکی است. بنیف پیشنهاد داد که تحول یک هامیلتونی کوانتوم مکانیکی می‌تواند در پیاده‌سازی و درک هر ماشین تورینگی به‌کار رود و چنین روشی حداقل به اندازه‌ی مدل محاسباتی کلاسیکی قدرتمند است. حال این سوال ایجاد می‌شود: آیا محاسبات کوانتومی قوی‌تر از محاسبات کلاسیکی‌اند؟

---

<sup>1</sup> Benioff

دیوید دویچ<sup>۱</sup> این سوال و سوالات مشابه با آن را در مقاله‌ی «نظریه‌ی کوانتومی، اصل چرچ - تورینگ و کامپیوترهای کوانتومی جهانی» در سال ۱۹۸۵ مورد کاوش قرار داد. ابتدا او کامپیوترهای کوانتومی را برای ماشین تورینگ و ماشین تورینگ جهانی معرفی کرد، سپس ثابت کرد که یک کامپیوتر کوانتومی جهانی قادر به انجام محاسباتی است که ماشین تورینگ جهانی نمی‌تواند انجام دهد، از جمله: تولید اعداد تصادفی، انجام محاسبات موازی در یک حافظه و شبیه‌سازی کامل سیستم‌های فیزیکی با فضای حالت دارای بعد محدود. او از افرادی بود که سهم مهمی در گسترش محاسبات کوانتومی داشت. در واقع دویچ به دنبال این بود که بداند آیا توسط کامپیوترهای کوانتومی امکان حل کارآمد مسائلی که هیچ حل کارآمدی در ماشین تورینگ کلاسیک ندارند، وجود دارد. از این‌رو تلاش کرد تا تعریف جامعی از اجزای محاسباتی که برای محاسبه‌ی کارآمد هر سیستم فیزیکی لازم‌اند، ارائه دهد. [1] و [4] از آنجایی که قوانین فیزیک دست آخر کوانتومی‌اند، دویچ به این فرض رهنمون شد که اجزای محاسبات نیز بایستی بر پایه‌ی مکانیک کوانتومی عمل کنند. او عملاً این موضوع را در سال ۱۹۸۵ نشان داد. در این زمان بود که توان شگفت‌انگیز محاسبات کوانتومی معلوم شد. دویچ به دنبال تئوری فیزیکی‌ای بود که رهیافتی برای اصل چرچ- تورینگ ارائه دهد. این اصل را می‌توان به این صورت بیان داشت:

"هر تابعی که ذاتاً قابل محاسبه باشد توسط یک ماشین تورینگ هم قابل محاسبه است، به عبارت دیگر هر فرآیند الگوریتمی را می‌توان به‌طور کارا با ماشین تورینگ شبیه‌سازی کرد". در سال ۱۹۸۵ فرمول‌بندی جدید دویچ که نسخه‌ی قویتر اصل چرچ - تورینگ نامیده می‌شود بیان شد:

"هر سیستم فیزیکی قابل درک محدود می‌تواند توسط یک ماشین محاسبه‌ی جهانی که با روش‌های محدودی عمل می‌کند به صورت کامل شبیه‌سازی شود." [1]

این نظریه بیان می‌دارد که هیچ مدل محاسبه‌ی دیگری وجود ندارد که قدرتمندتر از ماشین تورینگ باشد، به عبارت دیگر هر نوع ماشین دیگر و هر نوع مدل محاسبه‌ی دیگری قابل شبیه‌سازی توسط ماشین

---

<sup>1</sup> David Deutsch

تورینگ است. این نظریه از یک سو تعیین کننده‌ی الگوریتم است، یعنی هر آن چیزی که توسط ماشین تورینگ قابل شبیه‌سازی باشد و از سوی دیگر، نشان دهنده‌ی محدودیت‌های قوانین و پدیده‌های فیزیکی برای محاسبه کردن و استدلال الگوریتمی است. در سال ۱۹۸۹ در مقاله‌ی «شبکه‌های محاسباتی کوانتومی» دویچ دومین مدل محاسبات کوانتومی را توصیف کرد، "مدارهای کوانتومی". او اثبات کرد که گیت‌های کوانتومی را می‌توان برای انجام محاسبات کوانتومی با هم ترکیب کرد. به‌طریق مشابهی که گیت‌های بولی قادر به ترکیب شدن برای انجام محاسبات کلاسیکی‌اند، گیت‌های کوانتومی را نیز می‌توان برای دست یافتن به محاسبات کوانتومی با هم ترکیب کرد. همچنین او نشان داد که مدارهای کوانتومی قادرند هرآنچه که کامپیوتر جهانی قادر است محاسبه کند، محاسبه نماید و بالعکس. در واقع او نشان داد که ایده‌ی فاینمن می‌تواند منجر به ساخت کامپیوتر کوانتومی همه‌منظوره‌ای شود که قادر به مدل کردن هر فرآیند فیزیکی است. از این زمان بود که جستجو برای یافتن کاربردهای چنین ماشینی آغاز شد. او نشان داد که ماشین تورینگ اصل چرچ - تورینگ را ارضا نمی‌کند، ولی یک تئوری کوانتومی برای محاسبه، این اصل را ارضا می‌کند. الگوریتم دویچ و تعمیم آن، الگوریتم دویچ - جوزا<sup>۱</sup>، نمونه‌هایی از به‌کارگیری توازی ذاتی کامپیوتر کوانتومی برای کسب نتایجی است که دستیابی به آن‌ها برای کامپیوترهای کلاسیک غیرممکن است. الگوریتم دویچ راهی را برای تعیین ثابت یا متوازن بودن یک تابع تک بیتی ارائه می‌داد که با استفاده از آن، تعداد تکرار لازم از دو به یک کاهش می‌یابد. با ارائه‌ی این الگوریتم، دویچ توان بالاتر کامپیوترهای کوانتومی نسبت به کامپیوترهای کلاسیک را به‌وضوح نشان داد. در طول یک دهه بعد، این ایده توسط بسیاری دنبال شد. هدف نهایی، شبیه‌سازی سیستم‌های کوانتومی بر روی کامپیوترهایی است که بر پایه‌ی اصول مکانیک کوانتومی کار می‌کنند. [1] و [4]

در سال ۱۹۸۳ ویزنر<sup>۲</sup> در مقاله‌ی «کد گذاری آمیخته» راهی برای ارسال پیام به‌طریقی که تنها یک تن

قادر به خواندن آن باشد و راهی برای طراحی پول به‌طریقی که قابل جعل نباشد ارائه داد.

---

<sup>1</sup> Deutsch – Jozsa

<sup>2</sup> Stephen Wiesner

رمزنگاری کوانتومی در سال ۱۹۸۴ در مقاله‌ی «رمزنگاری کوانتومی» توسط بنت و براسرد<sup>۱</sup> معرفی

شد. [5]

در سال ۱۹۹۱ جوزا توابعی که می‌توان با توازی کوانتومی محاسبه کرد و نمی‌توان محاسبه کرد را دسته‌بندی نمود.

در سال ۱۹۹۳ "اندرو یو"<sup>۲</sup> نشان داد که هر تابعی که توسط ماشین تورینگ کوانتومی در زمانی از مرتبه‌ی چندجمله‌ای قابل محاسبه باشد را می‌توان با مدار کوانتومی‌ای با اندازه‌ی چند جمله‌ای محاسبه کرد. [4]

همچنین در سال ۱۹۹۳ برنشتاین و وزیرانی<sup>۳</sup> مقاله‌ی «نظریه‌ی پیچیدگی‌های کوانتومی» را ارائه دادند که در آن ماشین تورینگ جهانی‌ای معرفی کردند که می‌توانست به‌طور کارا هر ماشین تورینگ کوانتومی را شبیه‌سازی کند. آنان برای اولین بار مسئله‌ای را ارائه کردند که با کامپیوترهای کوانتومی در زمانی از مرتبه‌ی چندجمله‌ای قابل حل است، درحالی‌که با حل کلاسیکی به زمانی از مرتبه‌ی کثیرالجمله‌ای نیاز دارد. [1]

در سال ۱۹۹۵ دانشمندان در دسته‌ای از مقالات، در جستجوی گروهی از گیت‌های کوانتومی که برای محاسبات کوانتومی کافی باشند برآمدند. یعنی گروهی از گیت‌ها که برای پیاده‌سازی هر مدار کوانتومی‌ای کافی باشند. در مقاله‌ی «گیت‌های بنیادی برای محاسبات کوانتومی» بارنکو<sup>۴</sup> نشان داد که هر مدار کوانتومی را می‌توان از گیت‌های کوانتومی عمل‌کننده روی یک کیوبیت و گیت‌های کنترل OR عمل‌کننده روی دو کیوبیت ساخت. «گیت‌های دو بیتی برای محاسبات کوانتومی، جهانی هستند» [6] و «دینامیک کوانتومی مشروط و گیت‌های منطقی»<sup>۵</sup> نمونه‌های دیگری از این مقالات هستند. [7]

---

<sup>1</sup> Charles H. Bennett and Gilles Brassard

<sup>2</sup> Andrew Chi-Chih Yao

<sup>3</sup> Ethan Bernstein and Umesh Vazirani

<sup>4</sup> Adriano Barenco et al

<sup>5</sup> Adriano Barenco, David Deutsch, and Artur Ekert

در سال ۱۹۹۲ دویچ و جوزا<sup>۱</sup> مشترکاً مقاله‌ی «راه‌حل‌های سریع با محاسبات کوانتومی» را تالیف کردند که در آن الگوریتمی را ارائه دادند که توسط آن نوع تابع، ثابت یا متوازن بودن آن، تعیین می‌شود. [8]

تابع را ثابت<sup>۲</sup> می‌نامیم اگر برای تمام ورودی‌ها مقدار ثابتی داشته باشد و متوازن<sup>۳</sup> می‌نامیم اگر برای نیمی از ورودی‌ها مقدار ۰ و برای نیمی دیگر مقدار ۱ را اختیار کند. الگوریتم دویچ - جوزا اولین الگوریتم کوانتومی است که از حالت مشابه کلاسیکی‌اش سریع‌تر عمل می‌کند. الگوریتم دویچ - جوزا در واقع تعمیمی از الگوریتم دویچ است و برای حالتی است که تابع ورودی  $n$  بیتی است. برای آن که تعداد توابع متوازن را بشماریم دقت می‌کنیم که تعداد ورودی‌های مختلف این تابع و در نتیجه خروجی‌های آن برابر است با  $2^n$ . تعداد توابع متوازن برابر است با تعداد طرقتی که می‌توان نیمی از  $2^n$  خروجی را برابر صفر و نیمی دیگر را برابر با یک گرفت و این تعداد برابر است با:  $2^{n-1} / (2^{n-1}!)^2$  و این عددی است که رابطه‌اش با  $n$  یک رابطه‌ی نمایی است. بنابراین تعداد کل توابع ممکن که می‌توانند ثابت یا متوازن باشند برابر است با  $2 + (2^{n-1} / (2^{n-1}!)^2)$ . اگر بخواهیم یک الگوریتم تعیینی (یعنی الگوریتمی که با قطعیت پاسخ را مشخص کند) برای این مسئله به کار ببریم باید به ترتیب زیر عمل کنیم. اعداد  $n$  بیتی  $x$  را یک به یک می‌دهیم و تابع را فرا می‌خوانیم تا  $f(x)$  را محاسبه کند. هر گاه به ازای دو مقدار مختلف  $x$  مقادیر متفاوتی برای  $f(x)$  به دست بیاوریم الگوریتم را متوقف کرده و حکم می‌کنیم که تابع متوازن است. اما اگر چنین نبود الگوریتم را ادامه می‌دهیم تا نیمی از اعداد به‌علاوه‌ی یک، یعنی  $2^{n-1} + 1$  عدد خوانده شود. اگر برای این تعداد ورودی نیز تابع مقدار یکسان داشته باشد، حتماً تابع ثابت است. با استفاده از مکانیک کوانتومی با یک بار فراخوانی تابع، نوع آن را مشخص می‌کنیم.

در مقاله‌ی «تحقق تجربی یک کامپیوتر کوانتومی» چوانگ<sup>۴</sup> با جزئیات، روشی را شرح داد که در آن از

رزونانس مغناطیسی هسته جرمی برای عملی ساختن مدل ساده‌ی الگوریتم دویچ جوزا استفاده کرد. [4]

<sup>1</sup> David Deutsch and Richard Jozsa

<sup>2</sup> Constant

<sup>3</sup> Balance

<sup>4</sup> Isaac L. Chuang et al

در سال بعد سیمون<sup>۱</sup> مسئله‌ای معرفی کرد که یک الگوریتم کوانتومی می‌تواند آن را از مرتبه‌ی نمایی سریع‌تر از هر الگوریتم کلاسیکی که تا آن زمان شناخته شده بود حل کند.

این الگوریتم الهام بخش پیتر شور<sup>۲</sup> بود و او توانست دو الگوریتم کوانتومی ارائه دهد. الگوریتمی با زمانی از مرتبه‌ی چند جمله‌ای برای پیدا کردن عوامل اول و الگوریتمی برای لگاریتم گسسته، مسائلی که عمیقاً اعتقاد بر این بود که به زمانی از مرتبه‌ی نمایی برای حل توسط کامپیوترهای کلاسیکی نیاز دارند. پیتر شور<sup>۳</sup> یک متخصص کامپیوتر در آزمایشگاه‌های بل *AT & T*<sup>۴</sup> در نیوجرسی آمریکا و دانشجوی قبلی دوره‌ی لیسانس در کلتک<sup>۵</sup> توانست ثابت کند، مساله‌ی تجزیه به عوامل اول یک عدد و مساله‌ی معروف به لگاریتم گسسته به‌طور کارآمد در کامپیوترهای کوانتومی قابل حل است و در سال ۱۹۹۴ یک الگوریتم کوانتومی برای تجزیه‌ی اعداد ارائه داد که می‌تواند این مسئله را در زمان چند جمله‌ای حل کند. مسئله‌ی یافتن عوامل اول صحیح به‌لحاظ کلاسیکی مسئله‌ای سخت است. برای یک  $N$  صحیح موثرترین الگوریتم کلاسیکی به نام *number field sieve*، به تکراری از مرتبه‌ی  $O(\exp[(\log N)^{1/3}(\log \log N)^{2/3}])$  نیاز دارد که به‌همان نسبت زمان حل مسئله افزایش می‌یابد. درحالی‌که با استفاده از الگوریتم شور، زمان و تکراری از مرتبه‌ی:

$$O(\log N)^2 (\log \log N) (\log \log \log N)$$

مورد نیاز است. در نتیجه الگوریتم شور الگوریتمی است که تعداد تکرار را از مرتبه‌ی نمایی به چندجمله‌ای کاهش می‌دهد. هر عددی مثل  $p$  به‌طور تقریبی با  $L = \log_2^p$  بیت مشخص می‌شود، بنابراین تعداد بیت‌های لازم برای محاسبه‌ی  $n = pq$  در حدود  $L = \log_2^q \log_2^p$  می‌باشد. زمان لازم برای پیدا کردن عوامل اول به صورت ابر چند جمله‌ای با  $L = \log_2^n$  ارتباط دارد. بنابراین وقتی  $n$  زیاد می‌شود، در بدترین حالت زمان لازم برای پیدا کردن تجزیه‌ی آن، سریع‌تر از هر توانی از

<sup>1</sup> Daniel R. Simon

<sup>2</sup> Peter W. Shor

<sup>3</sup> Peter shor

<sup>4</sup> AT & T's Bell labs

<sup>5</sup> Caltech

$L = \log_2^n$  افزایش می‌یابد. این زمان با استفاده از بهترین الگوریتم تجزیه‌ای که برای این کار می‌شناسیم، عبارت است از  $t \approx \exp\left[c(Lnn)^{\frac{1}{3}}(LnLnn)^{\frac{2}{3}}\right]$  که در آن  $c = (64/9)^{\frac{1}{3}} \approx 1.9$  می‌باشد.

جالب اینکه تجزیه‌ی یک عدد ۱۳۰ رقمی می‌تواند از مرتبه‌ی یک ماه توسط شبکه‌ای از صدها ایستگاه کاری انجام شود. علت این امر آن است که ما الگوریتم سریع برای ضرب داریم ولی برای تجزیه نداریم. طبق تعریف استاندارد آنچه باعث می‌شود بگوئیم یک الگوریتم سریع یا قابل استفاده است، دقیقاً مدت زمانی نیست که برای اجرای آن صرف می‌شود. در واقع اگر با بزرگ‌شدن اعداد، زمان اجرای الگوریتم خیلی سریع زیاد نشود می‌گوییم، الگوریتم سریع و قابل استفاده است. در علوم کامپیوتر یک تعریف دقیق برای الگوریتم‌های سریع و کند وجود دارد. اگر زمان اجرای الگوریتم سریع‌تر از یک تابع توانی از تعداد بیت‌های ورودی افزایش نیابد، می‌گوییم الگوریتم سریع است. به عبارت دیگر، اگر زمان اجرای بهترین الگوریتمی که برای یک مساله‌ی مشخص می‌شناسیم، از بالا یک حد توانی داشته باشد، اصطلاحاً گفته می‌شود که مساله از نوع  $p$  است ولی عمل تجزیه در دسته‌ی  $p$  نیست و برای کامپیوترهای کلاسیک با هر سرعتی یک مساله‌ی سخت محسوب می‌شود.

اگر کامپیوترهای مدرن امروزی را با ماشین بابیج در قرن نوزدهم مقایسه کنیم، متوجه پیشرفت چشم‌گیر تکنولوژی می‌شویم، ولی مساله‌ای مثل مساله‌ی تجزیه، هم برای ماشین بابیج و هم برای کامپیوترهای امروزی یک مساله‌ی سخت محسوب می‌شود، زیرا زمان اجرای آن به صورت نمایی با افزایش تعداد بیت‌های ورودی، افزایش می‌یابد و نمی‌تواند در زمان محدودی حل شود. پس پیشرفت‌های تکنولوژی تا به امروز تنها توانسته است سرعت انجام محاسبات را بالا برد، ولی نتوانسته وابستگی نمایی بین تعداد بیت‌های ورودی و زمان اجرای الگوریتم را تغییر دهد. به عبارتی نتوانسته مسائل سخت را به مساله‌ی نوع  $p$  تبدیل کند. برای چنین تغییری باید از الگوریتم‌های جدیدتری استفاده شود. الگوریتم‌های کوانتومی این توانایی را دارند که بعضی از مسائل سخت را به مسائل نوع



$p$  تبدیل کنند. در این الگوریتم‌ها از خاصیت برهم‌نهی کوانتومی استفاده می‌شود که اجازه می‌دهد  $n$  کیوبیت در یک لحظه تمام  $2^n$  حالت ممکن را داشته باشند. پس از اینکه شور دنیا را با ارائه‌ی الگوریتم‌اش متعجب ساخت، نظریه‌ی محاسبات کوانتومی جان تازه‌ای گرفت. ارزش این کار زمانی مشخص می‌شود که بدانیم، تقریباً همه به این باور رسیده‌اند که این دو مساله حل کارآمدی در کامپیوترهای کلاسیک ندارند. نتایج شور نشان‌دهنده‌ی برتری کامپیوترهای کوانتومی بر کامپیوترهای کلاسیک است. [1]

در سال ۱۹۹۳ بنت جامعه‌ی علمی را با نشان دادن اینکه پدیده‌ی فرابرد کوانتومی به‌لحاظ نظری ممکن است متحیر ساخت.

سیمون و شور ابداعات خود را در سال ۱۹۹۴ در مقاله‌ی «قدرت محاسبات کوانتومی و الگوریتم‌هایی برای محاسبات کوانتومی» ارائه دادند. [9]

پیتر شور در سال ۱۹۹۵ در مقاله‌ی «طرحی برای کاهش همدوسی در حافظه‌ی کامپیوتر کوانتومی» اثبات کرد که کدگذاری هر کیوبیت از اطلاعات به ۹ کیوبیت، از پاره‌ای از ناهمدوسی‌ها جلوگیری می‌کند. [10] به‌طور هم‌زمان با مقاله‌ی شور، استین مقاله‌ی «تصحیح خطای کدگذاری در نظریه‌ی کوانتومی» را بدون اطلاع از مقاله‌ی شور تالیف کرد که نتایج مشابهی را ارائه می‌داد. [11]

از دیگر الگوریتم‌های بسیار تاثیرگذار، الگوریتم کوانتومی گراور برای جستجو در یک لیست نامنظم از داده‌هاست که در دو مقاله‌ی «یک الگوریتم مکانیک کوانتومی سریع برای جستجو در پایگاه داده‌ها» [12] و «مکانیک کوانتومی در جستجوی یک سوزن در کومه‌ی علف کمک می‌کند» در سال ۱۹۹۶ معرفی شد [13]. در سال ۱۹۹۸ چوانگ، گرشن فیلد و کوبینگ تحقق تجربی الگوریتم گراور را در مقاله‌ی «تحقق تجربی جستجوی سریع کوانتومی» ارائه دادند. [14]

ایزاک چوانگ و گروه تحقیقاتی‌اش در مقاله‌ی «تحقق تجربی الگوریتم کوانتومی شور» الگوریتم شور را با استفاده از روش رزونانس مغناطیسی هسته در سال ۲۰۰۱ عملی ساخت. [4]

در سال ۲۰۰۳ شور در مقاله‌ی «چرا الگوریتم‌های کوانتومی‌ای بیشتر از آنچه تاکنون ابداع شده کشف نمی‌شود؟» چندین توضیح ممکن را برای پاسخ به سوالش ارائه داد.

در سال ۱۹۹۸ اولین کامپیوتر کوانتومی با دو کیوبیت بر اساس روش NMR ساخته شد.

در سال ۲۰۰۰ کامپیوتر کوانتومی ۷ کیوبیتی با استفاده از روش NMR ساخته شد.

در سال ۲۰۰۱، IBM توانست عدد ۱۵ را با استفاده از الگوریتم شور به عوامل اول‌اش، ۳ و ۵ تجزیه

کند.

از سال ۱۹۹۸ تا ۲۰۰۱ کامپیوترهای کوانتومی ۲-۳-۵ و ۷ کیوبیتی ساخته شدند.

طی سالهای ۲۰۰۵ و ۲۰۰۶ آزمایشاتی با فوتون، نقطه‌های کوانتومی و نانوتیوب‌ها به‌عنوان دام‌های

ذرات انجام شد.[4]

در سال ۲۰۰۷ موسسه D-Wave تولید کامپیوتر کوانتومی ۱۶ کیوبیتی را اعلام کرد. این کامپیوتر

کوانتومی قادر به حل معمای سودوکو<sup>۱</sup> می‌باشد.

---

<sup>1</sup> sudoku puzzle

۲

فصل دوم: مفاهیم مقدماتی

## ۱-۲ اطلاعات کوانتومی و محاسبات کوانتومی<sup>۱</sup>

مکانیک کوانتومی یک چارچوب ریاضی یا مجموعه‌ای از قوانین برای ساختن نظریه‌های فیزیکی است که صحیح‌ترین و کامل‌ترین توصیف از جهان واقعی را ارائه می‌دهد.

محاسبات کوانتومی و اطلاعات کوانتومی، مطالعه‌ی فرآیندهای پردازش اطلاعات است که با سیستم‌های مکانیک کوانتومی انجام می‌شود که حاصل الحاق فیزیک جدید نظری با علم کامپیوتر تئوری است. به بیان دیگر، محاسبات کوانتومی و اطلاعات کوانتومی، مجموعه راه‌کارها و روش‌های تغییر یک سیستم کوانتومی منفرد و همچنین کشف روش‌های جدیدی در انجام آزمایش و تفسیر جنبه‌های جالب آن آزمایش می‌باشد. اطلاعات آن چیزی است که در حالت یک سیستم فیزیکی کدگذاری شده است. محاسبات نیز آن چیزی است که می‌توان روی یک وسیله‌ی قابل درک فیزیکی حقیقی انجام داد. کامپیوتر کوانتومی ماشینی است که محاسبات را بر اساس قوانین مکانیک کوانتومی انجام می‌دهد. یک کامپیوتر کوانتومی ابزاری است که در آن داده‌ها می‌توانند در شبکه‌ای از سیستم‌های دو حالته‌ی مکانیک کوانتومی ("کیوبیت‌ها") ذخیره شوند. کامپیوتر کوانتومی از ویژگی‌های ذرات بنیادی که توسط مکانیک کوانتومی پیش‌بینی می‌شود بهره می‌برد. [1]

از جمله پدیده‌هایی که موجب تفاوت‌های بنیادین محاسبات کوانتومی و کلاسیکی گشته می‌توان به برهم‌نهی، توازی کوانتومی، درهم‌تنیدگی، تکثیر ناپذیری، تصحیح خطای کوانتومی، رمزنگاری کوانتومی و فرابرد کوانتومی اشاره نمود که به شرح چند مورد آن‌ها که مرتبط با بحث ما است می‌پردازیم. [1] و [15] و [16]

## ۲-۲ توازی کوانتومی<sup>۲</sup>

اولین تفاوت مهم کامپیوتر کوانتومی با کامپیوترهای کلاسیکی این است که یک حافظه‌ی کوانتومی می‌تواند در آن واحد در تمام حالت‌های بالقوه‌ی خود قرار گیرد. این خصلت ناشی از برهم‌نهی حالت‌های

<sup>1</sup> Quantum Information and Quantum Computation

<sup>2</sup> Quantum parallelism

کوانتومی است و اصطلاحاً توازی کوانتومی خوانده می‌شود. توازی کوانتومی به کامپیوترهای کوانتومی اجازه می‌دهد تا به‌طور هم‌زمان به محاسبه‌ی تابع  $f(x)$  به‌ازای مقادیر مختلف  $x$  بپردازند. در این قسمت توضیح خواهیم داد که توازی کوانتومی چگونه صورت می‌گیرد و چه محدودیت‌هایی دارد.

فرض کنید تبدیل یکانی  $U_f$  ای داریم که دو کیوبیت را به دو کیوبیت دیگر به شکل زیر تبدیل می‌کند:

$$U_f : |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$$

چه اتفاقی می‌افتد اگر  $U_f$  روی یک ورودی به‌کار رود که برهم‌نهی‌ای از حالت‌های مختلف است؟ جواب

ساده، اما درعین حال قدرتمند است. از آنجایی که  $U_f$  یک تبدیل خطی است، روی تمام بردارهای پایه‌ی موجود در ورودی برهم‌نهاده به صورت هم‌زمان عمل کرده و برهم‌نهی‌ای از نتایج تولید می‌کند. با استفاده از این روش، محاسبه‌ی  $f(x)$  برای  $N$  مقدار از  $x$  در یک‌بار به‌کارگیری  $U_f$  امکان پذیر است. این خاصیت، "توازی کوانتومی" نامیده می‌شود.

می‌توانیم حالت ورودی را به‌صورت برهم‌نهی  $|0\rangle$  و  $|1\rangle$  انتخاب کنیم. اگر کیوبیت دوم در ابتدا در حالت

$$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
 آماده شود، در نتیجه داریم:

$$U_f : |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightarrow |x\rangle \frac{1}{\sqrt{2}}(|f(x)\rangle - |1 \oplus f(x)\rangle) = |x\rangle (-1)^{f(x)} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad (1-2)$$

بنابراین تابع  $f$  را به صورت یک فاز وابسته به  $x$  جدا کرده‌ایم. حال فرض کنید کیوبیت اول را به شکل

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
 آماده کرده‌ایم. بنابراین خواهیم داشت:

$$U_f : \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightarrow \frac{1}{\sqrt{2}} [(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle] \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad (2-2)$$

در نهایت، می‌توانیم اندازه‌گیری انجام دهیم که کیوبیت اول را روی پایه‌ی زیر تصویر کند:

$$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$$

بدیهی است که، اگر تابع متوازن باشد همواره  $|+\rangle$ ، و اگر ثابت باشد  $|-\rangle$  را به دست خواهیم آورد (اگر  $f(0) = f(1)$  باشد،  $f(x)$  ثابت و اگر  $f(0) \neq f(1)$  باشد، متوازن است).

این خاصیت، وجه تمایز میان آنچه که یک کامپیوتر کلاسیکی و یک کامپیوتر کوانتومی می‌توانند انجام دهند، می‌باشد. کامپیوتر کلاسیکی باید دوبار  $f$  را به کار برد تا یک تابع متوازن را از یک تابع ثابت تمیز دهد، اما یک کامپیوتر کوانتومی این کار را در یک مرحله انجام می‌دهد. یک کامپیوتر کوانتومی می‌تواند روی برهم‌نهی از دو حالت  $|0\rangle$  و  $|1\rangle$  اثر کند و به موجب آن اطلاعاتی را درباره‌ی تابع استخراج کند، اطلاعاتی که به هر دوی  $f(0)$  و  $f(1)$  بستگی دارد. [1] و [15] و [24]

## ۳-۲ برهم‌نهی<sup>۱</sup>

کامپیوترهای کلاسیکی از بیت، یک سلول دو حالتی، به عنوان حافظه‌ی اطلاعاتی استفاده می‌کنند. از سوی دیگر حالت یک سیستم کوانتومی دو حالتی که به آن "بیت کوانتومی" یا به اختصار "کیوبیت" می‌گویند، نه تنها مانند یک بیت کلاسیکی می‌تواند مقدار 0 و 1 به خود بگیرد بلکه می‌تواند در حالتی قرار بگیرد که در حقیقت حاصل برهم‌نهی دو حالت منطقی 0 و 1 است. کیوبیت همان نقش بیت را در کامپیوترهای کوانتومی ایفا می‌کند. یک کامپیوتر کوانتومی از مزیت موجود در مکانیک کوانتومی یعنی "برهم‌نهی" استفاده می‌کند. این ویژگی سیستم‌های کوانتومی در قرار گرفتن در ترکیبی از همه‌ی دیگر حالات مجاز به‌طور هم‌زمان، برخلاف حالتی که فقط در یکی از حالت‌های مجاز در هر لحظه از زمان قرار گیرد، مشابه کلاسیکی ندارد. استفاده از این واقعیت که یک بیت کوانتومی می‌تواند هم‌زمان دو مقدار 0 و 1 به خود بگیرد منجر به کسب نتایج جالب توجهی

---

<sup>1</sup> Superposition

می‌شود. به‌عنوان مثال قابلیت اجرای عملیات منطقی بر روی برهم‌نهی کوانتوم مکانیکی اعداد. این موضوع به زبان ریاضی به صورت زیر نشان داده می‌شود:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (۴-۲)$$

حافظه‌ی کلاسیکی را در نظر بگیرید که از سه بیت تشکیل شده باشد. این حافظه در هر لحظه از زمان می‌تواند یکی از هشت حالت ممکن  $110, 101, 100, 011, 010, 001, 000$  یا  $111$  را داشته باشد. اما یک حافظه‌ی کوانتومی سه‌کیوبیتی می‌تواند هم‌زمان همه‌ی هشت حالت را داشته باشد.

$$|\psi\rangle = a_1|000\rangle + a_2|001\rangle + a_3|010\rangle + a_4|011\rangle + a_5|100\rangle + a_6|101\rangle + a_7|110\rangle + a_8|111\rangle$$

به‌این ترتیب اگر تعداد کیوبیت‌های حافظه‌ی کوانتومی را زیاد کنیم، ظرفیت ذخیره‌ی اطلاعات روی آن به‌صورت نمایی زیاد می‌شود، یعنی  $n$  کیوبیت،  $2^n$  عدد را می‌توانند هم‌زمان ذخیره کنند. وقتی حافظه‌ی کوانتومی به صورت برهم‌نهی تمام حالات ممکن درآمد، می‌توان به‌صورت هم‌زمان روی تمام آنها عملیات محاسباتی را انجام داد. پس از انجام محاسبات، تمام حالت‌ها تغییر می‌کنند، به‌عبارتی محاسبات به‌صورت موازی انجام گرفته است. این بدین معنی است که یک کامپیوتر کوانتومی می‌تواند تنها در یک مرحله‌ی محاسباتی عملیات مورد نظر را روی  $2^n$  عدد متفاوت که نتیجه‌ی برهم‌نهی  $n$  کیوبیت هستند انجام دهد. یک کامپیوتر کلاسیک برای انجام عمل مشابه باید  $2^n$  بار یک مرحله‌ی محاسباتی را برای ورودی‌های مختلف تکرار کند یا باید  $2^n$  پردازشگر مختلف به‌طور هم‌زمان و موازی عملیات محاسباتی را بر روی ورودی‌های متفاوت انجام دهند. پس اگر بتوانیم با الگوریتم‌های هوشمندانه از خاصیت برهم‌نهی حالت‌ها استفاده کنیم، کامپیوترهای کوانتومی از نظر سرعت و میزان حافظه‌ی لازم بر کامپیوترهای کلاسیک ارجحیت دارند. [17]

ممکن است اینگونه تصور شود که کامپیوترهای کلاسیک می‌توانند همان کار کامپیوترهای کوانتومی را با صرف زمان و حافظه‌ی بیشتر انجام دهند. اما نکته‌ی مهم این است که نسبت حافظه و زمان لازم برای کامپیوترهای کلاسیک به حافظه و زمان لازم برای کامپیوترهای کوانتومی برای انجام عمل مشابه، نمایی است.

[18] و [15]

## ۲-۴ درهم‌تنیدگی<sup>۱</sup>

از مواردی که محاسبات کوانتومی را به شدت از نوع کلاسیک آن متمایز می‌کند، "درهم‌تنیدگی" کوانتومی است که یکی دیگر از ویژگی‌های دنیای کوانتومی است. همبستگی حالت‌های کوانتومی درهم‌تنیده، هیچ مشابه کلاسیکی ندارد و می‌توان گفت درهم‌تنیدگی از بنیادی‌ترین مفاهیمی است که باعث جدایی فیزیک کوانتومی از فیزیک کلاسیک می‌شود. با استفاده از حالت‌های درهم‌تنیده می‌توانیم کارهای جدیدی را در پردازش اطلاعات انجام دهیم که در فیزیک کلاسیک ممکن نیست، همچنین می‌توانیم بسیاری از روش‌هایی را که با استفاده از فیزیک کلاسیک برای پردازش اطلاعات به کار می‌بریم، بهبود بخشیم. از جمله کاربردهای حالات درهم‌تنیده، فرابرد کوانتومی و کدگذاری چگال است. برای هر حالت خالص دو قسمتی<sup>۲</sup> می‌توان یک عدد صحیح مثبت به نام عدد اشمیت<sup>۳</sup> نسبت داد که تعداد ویژه مقادیر غیر صفر  $\rho_a$  یا  $\rho_b$  و در نتیجه، تعداد جملات در تجزیه‌ی اشمیت  $|\psi\rangle_{AB}$  می‌باشد. بر حسب این کمیت می‌توانیم بگوییم درهم‌تنیده بودن یک حالت خالص دو قسمتی به چه معنی است:  $|\psi\rangle_{AB}$  درهم‌تنیده یا غیر قابل تفکیک است اگر عدد اشمیت آن بزرگ‌تر از یک باشد، در غیر این صورت قابل تفکیک یا غیردرهم‌تنیده است. در نتیجه یک حالت خالص دو قسمتی تفکیک‌پذیر، ضرب مستقیمی از حالت‌های خالص در فضای  $H_A$  و  $H_B$  است. هر حالتی که نتوان آن را به صورت یک ضرب مستقیم بیان کرد، درهم‌تنیده است. [1] و [15] و [18] حالت‌های درهم‌تنیده به‌طور طبیعی به‌عنوان نتیجه‌ای از برهم‌کنش بین ذرات ایجاد می‌شوند، مانند حالتی که یک جفت ذره به‌طور هم‌زمان تحت پاره‌ای از ویژگی‌ها تولید می‌شوند، از جمله حالتی که اسپین یا قطبش<sup>۴</sup> پایسته بماند. [16] هرگاه اندازه‌گیری روی یکی از دو جفت درهم‌تنیده انجام شود حالت‌های هر دو ذره تعیین می‌شوند و درهم‌تنیدگی از بین می‌رود. [19] و [15]

---

<sup>1</sup> Entanglement

<sup>2</sup> Bipartite pure state

<sup>3</sup> Schmidt

<sup>4</sup> Polarization



## ۲-۵ حالت‌های خالص و حالت‌های آمیخته<sup>۱</sup>

تاکنون فرض کرده‌ایم حالت یک دستگاه کوانتومی با یک بردار  $|\psi\rangle$  مشخص می‌شود. بنابر اصول مکانیک کوانتومی این امر مستلزم آن است که اولاً ما از آخرین اندازه‌گیری‌ای که روی دستگاه کوانتومی انجام شده است و طی آن حالت دستگاه مشخص شده است، مطلع باشیم و ثانیاً در طی این زمان، دستگاه کوانتومی از محیط خود منزوی باقی مانده باشد. برای دستگاه‌های واقعی هیچ کدام از این دو فرض صحیح نیستند. در غیاب هرگونه اطلاعات که یک حالت را بر دیگر حالت‌ها ترجیح دهد، تنها می‌توانیم با اطمینان قید کنیم که توزیع اتم‌ها روی حالات مختلف کاملاً یکنواخت است. حال ببینیم در چنین حالت‌هایی، دستگاه کوانتومی را چگونه می‌بایست توصیف کرد. اصطلاح آنسامبل یا مجمع به اجتماعی از سیستم‌های فیزیکی اطلاق می‌شود که به صورت یکسان فراهم آمده‌اند. بنا به تعریف، یک آنسامبل خالص اجتماعی است از سیستم‌های فیزیکی، به گونه‌ای که همه‌ی اعضا، با کت یکسان  $|\psi\rangle$  مشخص می‌شوند. به عکس، در یک آنسامبل آمیخته، کسری از اعضا با جمعیت نسبی  $p_i$  با کت حالت  $|\psi_i\rangle$  مشخص می‌شوند و کسر دیگری با جمعیت نسبی  $p_j$  با  $|\psi_j\rangle$ . به بیان غیر دقیق، می‌توان آنسامبل آمیخته را به صورت آمیزه‌ای از آنسامبل‌های خالص تصور نمود. فرض کنید که خاصیتی مثل خاصیت  $M$  را می‌خواهیم اندازه‌گیری کنیم. برای یک دستگاه آمیخته که توزیع اتم‌ها روی حالات مختلف کاملاً یکنواخت است متوسط خاصیت  $M$  به شکل زیر محاسبه خواهد شد:

$$\langle M \rangle = \sum_i p_i \langle \psi_i | M | \psi_i \rangle = \sum_i p_i \text{tr}(M | \psi_i \rangle \langle \psi_i |) = \text{tr}(M \rho) \quad (5-2)$$

که در آن  $\rho$  عبارتست از:

$$\rho = \sum p_i | \psi_i \rangle \langle \psi_i | \quad (6-2)$$

و ماتریس چگالی یا عملگر چگالی<sup>۲</sup> دستگاه کوانتومی نامیده می‌شود و ضرایب  $p_i$  احتمال قرار گرفتن سیستم

<sup>1</sup> Pure states and mixed states

<sup>2</sup> Density matrix

در هر یک از حالات ممکن است. این ماتریس چگالی در بردارنده‌ی تمام اطلاعاتی است که ما می‌توانیم از دستگاه کوانتومی کسب کنیم. این ماتریس دارای خاصیت‌های زیر است:

$$(۷-۲)$$

$$\text{tr}(\rho) = 1$$

$$\rho^T = \rho$$

$$\rho \geq 0$$

و جمعیت‌های نسبی  $p_i$  مقیدند که در شرط بهنجارش  $\sum p_i = 1$  صدق کنند.

در تمام مواردی که دستگاه کوانتومی مورد نظر ما، جزئی از یک دستگاه بزرگ‌تر است حالت آن با یک

ماتریس چگالی مشخص می‌شود. [15] و [1]

## ۲-۶ بیت و پردازش اطلاعات کلاسیک

می‌دانیم که در کامپیوترهای کلاسیک، تمام اطلاعات به شکل رشته‌ای از متغیرهای 0 و 1 ذخیره می‌شوند. پردازش داده‌ها از هر نوع که باشد، چیزی نیست جز انجام اعمال منطقی روی این رشته‌ها یا یک سلسله توابع پشت سرهم که روی یک رشته‌ی ورودی با طول معین انجام می‌شود. هر متغیر دو حالتی که می‌تواند دو مقدار 0 یا 1 را اختیار کند یک بیت نامیده می‌شود. اگر یک بیت را با متغیر  $x$  نشان دهیم، یک رشته‌ی دو بیتی را با نماد  $x_1x_0$  و یک رشته‌ی  $n$  بیتی را با نماد  $x_{n-1}x_{n-2}\dots x_1x_0$  نمایش می‌دهیم. از اصطلاح حافظه‌ی کلاسیک برای مجموعه‌ای از بیت‌ها که می‌توانند داده‌های گسترده‌تری را در خود ذخیره کنند استفاده می‌شود. از دیدگاه فیزیکی، یک بیت، یک سیستم فیزیکی است که می‌تواند با بار یک خازن یا مغناطیسی شدن نقطه‌ای از دیسک سخت کامپیوتر تجسم یابد. به عبارت دیگر می‌تواند در دو حالت مختلف که به آن "حالت منطقی" می‌گویند، قرار بگیرد. این حالات منطقی می‌تواند بله، خیر یا درست، غلط و یا 0 و 1 باشند. برای مثال در کامپیوترهای دیجیتال ولتاژ بین صفحات خازن می‌تواند نشان دهنده‌ی یک بیت اطلاعات باشد،

همچنین یک بیت اطلاعات می‌تواند به وسیله‌ی دو نوع قطبش مختلف نور و یا دو تراز مختلف الکترونی یک اتم (اتم‌های دو حالته) مشخص شود. [1] و [15] و [23]

## ۲-۷ کیوبیت

بیت که مفهوم پایه‌ای و بنیادین کامپیوتر کلاسیک و واحد پایه‌ی اطلاعات است، در دنیای کوانتومی جای خود را به کیوبیت می‌دهد. بیت‌های کلاسیک به وسیله‌ی سیستم‌های فیزیکی‌ای تجسم می‌یابند که از قوانین فیزیک کلاسیک تبعیت می‌کنند، در مقابل بیت‌های کوانتومی تابع قوانین فیزیک کوانتومی هستند و نه قوانین آشنای فیزیک کلاسیک. به زبان ریاضی، کیوبیت، عبارت است از یک ذره‌ی دو ترازه که یک حالت به آن منتسب می‌شود. یک حافظه‌ی کوانتومی  $n$  کیوبیتی عبارت است از مجموعه‌ای متشکل از  $n$  کیوبیت. حالت یک ذره‌ی دو ترازه به وسیله‌ی یک بردار یکه در فضای برداری دو بعدی روی میدان اعداد مختلط بیان می‌گردد،  $|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$  که پایه‌های ثابت این فضا با  $\{|0\rangle, |1\rangle\}$  مشخص می‌شوند. این پایه‌های راست هنجار  $|0\rangle$  و  $|1\rangle$  ممکن است به ترتیب با حالت‌های قطبش فوتون  $|\uparrow\rangle$  و  $|\rightarrow\rangle$  و یا با قطبش‌های  $|\square\rangle$  و  $|\square\rangle$  متناظر باشند و یا حتی می‌توانند به حالت‌های اسپین-بالا و اسپین-پایین یک الکترون (ذرات با اسپین  $1/2$ ) مرتبط باشند (یا اتم‌های دو حالته). تمام اندازه‌گیری‌ها با توجه به پایه‌های استاندارد برای محاسبات کوانتومی، یعنی  $\{|0\rangle, |1\rangle\}$  انجام می‌شوند. حالت‌های پایه‌ی فضا را با  $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$  و  $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$  نمایش می‌دهیم. حالت سیستم کیوبیتی با  $|\psi\rangle = a|0\rangle + b|1\rangle$ ، که  $a$  و  $b$  اعداد مختلطی هستند و در رابطه‌ی  $|a|^2 + |b|^2 = 1$  صدق می‌کنند، نمایش داده می‌شود. درست مانند حالت قطبش فوتون، اگر چنین برهم‌نهشی را نسبت به پایه‌ی  $\{|0\rangle, |1\rangle\}$  اندازه بگیریم، احتمال اینکه مقدار  $|0\rangle$  اندازه‌گیری شود برابر  $|a|^2$  و احتمال اینکه مقدار  $|1\rangle$  اندازه‌گیری شود برابر  $|b|^2$  است. بنابراین محاسبات توسط برهمکنش‌های بیرونی (همان اندازه‌گیری) با سیستم‌های دو حالته‌ی مختلفی که

دستگاه ما را می‌سازد، انجام خواهد شد. اگر چه حتی یک بیت کوانتومی می‌تواند در بینهایت حالت برهم‌نهی مختلف قرار بگیرد، اما فقط می‌توان از هر تک بیت کوانتومی، یک بیت اطلاعات مفید کلاسیک استخراج کرد. دلیل این که نمی‌توان اطلاعات بیشتری از یک کیوبیت در مقایسه با یک بیت کلاسیکی به دست آورد، این است که اطلاعات تنها توسط اندازه‌گیری به دست می‌آیند و اندازه‌گیری حالت سیستم را تقلیل می‌دهد. زمانی که یک کیوبیت مورد اندازه‌گیری قرار می‌گیرد، این اندازه‌گیری حالت کیوبیت را به یکی از حالت‌های پایه تبدیل می‌کند. [1] و [15] و [26]

## ۲-۸ کره بلاخ<sup>۱</sup>

کلی‌ترین حالت یک ذره‌ی اسپین یک دوم و یا هر ذره‌ی دیگری که فضای هیلبرت آن دو بعدی است با یک ماتریس چگالی دو در دو داده می‌شود که این ماتریس را نیز با  $\rho$  نمایش می‌دهیم. از آنجائی که ماتریس یکه و ماتریس‌های پائولی، یک پایه برای فضای ماتریس‌های دو در دو تشکیل می‌دهند، می‌توان این ماتریس را به شکل زیر بسط داد:

$$\rho = \frac{1}{2}(r_0 I + r \cdot \sigma) = \frac{1}{2} \begin{pmatrix} r_0 + z & x - iy \\ x + iy & r_0 - z \end{pmatrix} \quad (۸-۲)$$

که در آن  $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$  ماتریس‌های پائولی هستند و ضریب  $1/2$  برای راحتی بیرون کشیده شده است. حال دقت می‌کنیم که :

الف-  $\rho$  هرمیتی است. بنابراین ضرایب  $\vec{r}$  و  $r_0$  حقیقی هستند.

ب-  $tr(\rho) = 1$  بنابراین  $r_0 = 1$ .

ج-  $\rho \geq 0$ . برای تامین این شرط می‌بایست ویژه مقدرهای  $\rho$  را حساب کنیم. یک محاسبه‌ی ساده نشان می‌دهد که ویژه مقدرهای  $\rho$  عبارتند از:

<sup>1</sup> Bloch sphere

$$\lambda_{1,2} = \frac{1}{2}(1 \pm r) \quad (9-2)$$

که در آن  $r$  اندازه‌ی بردار  $\vec{r}$  است.

بنابراین برای مثبت بودن  $\rho$  کافی است که طول بردار  $\vec{r}$  از یک کمتر باشد، یعنی:  $\vec{r} \leq 1$ . به این ترتیب، بین هر ماتریس چگالی و یک نقطه از یک کره به شعاع واحد، یک تناظر یک به یک برقرار می‌شود و مجموعه‌ی تمام بردارهای بلاخ در یک توپ سه بعدی واقعی محدود می‌شوند. این کره، کره‌ی بلاخ نام دارد. زیبایی توپ بلاخ با این حقیقت آشکار می‌شود که تقارنش تنها برای نمایش مناسب حالات کیوبیتی مفید نیست، بلکه تصویری شهودی از دینامیک سیستم به دست می‌دهد. هر عملگر یکانی را می‌توان به سادگی با نوعی چرخش این گوی متناظر ساخت، به عبارتی هر تبدیلی روی حالت کیوبیتی را می‌توان با چرخش مناسبی از کره‌ی بلاخ متناظر ساخت. در مکانیک کوانتومی، کره‌ی بلاخ، نمایش هندسی فضای حالت خالص یک سیستم مکانیک کوانتومی دو حالتی است که به افتخار فیلیکس بلاخ<sup>۱</sup> به این نام خوانده می‌شود. این کره را گاهی کره‌ی پوانکاره<sup>۲</sup> نیز می‌نامند. نقاط روی سطح کره‌ی بلاخ نقاطی هستند که در آنها  $r = 1$  و بنابراین، ویژه مقادیر  $\rho$  برابر با یک و صفر هستند، در نتیجه این نقاط متناظر با حالت‌های خالص هستند و برای مرکز کره داریم:

$$\lambda_1 = \lambda_2 = 1/2 \quad \text{که نشان دهنده‌ی حالت کاملاً آمیخته می‌باشد. [1] و [15] و [23]}$$

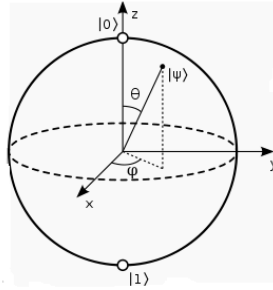
حالت نرمالیزه‌ی کلی برای یک کیوبیت عبارتست از:  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  و چون ضرایب  $\alpha$  و  $\beta$

می‌بایستی در رابطه‌ی  $|\alpha|^2 + |\beta|^2 = 1$  صدق کنند می‌توانیم آن‌ها را به صورت زیر انتخاب کنیم که زوایای  $\theta$  و  $\varphi$  را می‌توان به عنوان زوایای قطبی و سمتی یک نقطه‌ی دلخواه روی سطح کره‌ی بلاخ به کار برد.

$$\begin{aligned} \alpha &= \cos \frac{\theta}{2} \\ \beta &= e^{i\varphi} \sin \frac{\theta}{2} \\ 0 \leq \theta \leq \pi, 0 \leq \varphi \leq 2\pi \end{aligned} \quad (10-2)$$

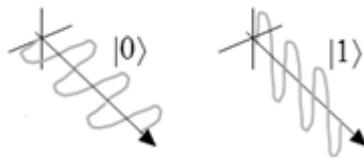
<sup>1</sup> Felix Bloch

<sup>2</sup> Poincare



شکل ۱-۲ نمایش هندسی کره ی بلاخ

برای نمایش فیزیکی کیوبیت‌ها می‌توان از قطبش‌های راستگرد و چپگرد فوتون یا ترازهای اتمی اتم‌ها استفاده کرد که روش اول در شکل زیر نشان داده شده است.



شکل ۲-۲ پولاریزه‌های راستگرد و چپگرد فوتون

## ۹-۲ کیوتریت

رشته‌ی تازه متولد شده‌ی اطلاعات کوانتومی که شامل شاخه‌هایی از تکنولوژی مربوط به آینده از جمله محاسبات کوانتومی، رمزنگاری کوانتومی و ارتباطات کوانتومی است، بر پایه‌ی مفاهیم درهم‌تنیدگی و استفاده از کیوبیت‌ها بنا نهاده شده است. از سال‌های اخیر سیستم‌های کوانتومی با ابعاد بزرگ‌تر کانون توجه مجامع علمی قرار گرفت. اولین سیستم کوانتومی بزرگ‌تر از کیوبیت، یا به عبارتی اولین کیودیت، کیوتریت<sup>۱</sup> است. [28] استفاده از کیوتریت‌ها چند مزیت دارد، فضای قابل دسترسی سیستم نسبت به کیوبیت‌ها افزایش می‌یابد و کارایی و امنیت بسیاری از قراردادهای اطلاعات کوانتومی، با استفاده از کیوتریت‌ها افزایش می‌یابد. همچنین انتظار می‌رود نقض گسترده‌تر غیرموضعیتهای آزمایش‌های بل در سیستم‌های درهم‌تنیده‌ی کیوتریتی رخ دهد. [29] و [30]

<sup>1</sup> Qutrit

یک کیوتریت در فضای مختلط سه بعدی  $H^3$  که با بردارهای پایه  $|0\rangle, |1\rangle, |2\rangle$  یا  $|1\rangle, |2\rangle, |3\rangle$  ساخته می‌شود، تعریف می‌گردد. حالت کلی یک کیوتریت عبارتست از:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle \quad (11-2)$$

که ضرایب در حالت کلی اعداد مختلطاند و شرط  $|\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1$  بر آن‌ها حاکم است. معمولاً پایه‌های فضای  $H^3$  با بردارهای زیر نمایش داده می‌شود:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, |2\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \quad (12-2)$$

نقش گروه تقارنی  $SU(2)$  و ماتریس‌های پائولی در کیوبیت‌ها، توسط گروه  $SU(3)$  و مولد جبر متناظر  $SU(3)$  ایفا می‌شود. یکی از مجموعه‌های هرمیتی مناسب مولد، ماتریس‌های ژل - من<sup>۱</sup>  $\lambda_r$  ها هستند.

$$\begin{aligned} \lambda_1 &= \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \lambda_2 = \begin{pmatrix} 0 & -i & 0 \\ i & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \lambda_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \\ \lambda_4 &= \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \lambda_5 = \begin{pmatrix} 0 & 0 & -i \\ 0 & 0 & 0 \\ i & 0 & 0 \end{pmatrix}, \lambda_6 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \\ \lambda_7 &= \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -i \\ 0 & i & 0 \end{pmatrix}, \lambda_8 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{pmatrix} \end{aligned} \quad (13-2)$$

که در شرط جابجایی زیر صدق می‌کنند:

$$[\hat{\lambda}_r, \hat{\lambda}_s] = 2if_{rst}\hat{\lambda}_t, r = (1, 2, \dots, 8) \quad (14-2)$$

که در آن قانون مجموع روی اندیس‌های تکراری<sup>۲</sup> به کار رفته است و ثابت‌های ساختار  $f_{rst}$  اعضای یک تانسور کاملاً پادمتقارن‌اند. همین‌طور رابطه‌ی پادجابجایی:

$$\{\hat{\lambda}_r, \hat{\lambda}_s\} = \frac{4}{3}\delta_{rs}\hat{1} + 2d_{rst}\hat{\lambda}_t \quad (15-2)$$

<sup>1</sup> Gell-Mann

<sup>2</sup> Summation over repeated indices

نیز برقرار است که ضرایب  $d_{rst}$ ، یک تانسور کاملاً متقارن می‌سازند.

بیان دیگری از روابط فوق، رابطه‌ی:

$$\hat{\lambda}_j \hat{\lambda}_k = \frac{2}{3} \delta_{jk} \hat{1} + \sum_l d_{jkl} \hat{\lambda}_l + i \sum_l f_{jkl} \hat{\lambda}_l \quad (۱۶-۲)$$

است که  $j, k = 1, 2, \dots, 8$ . ثوابت ساختار جبر لی گروه  $SU(3)$  پادمقارن عبارتند از:

$$f_{123} = 1, f_{458} = f_{678} = \frac{\sqrt{3}}{2}, \quad (۱۷-۲)$$

$$f_{147} = f_{246} = f_{257} = f_{345} = f_{516} = f_{637} = \frac{1}{2}$$

و ضرایب متقارن برابرند با: [31]

$$d_{118} = d_{228} = d_{338} = -d_{888} = \frac{1}{\sqrt{3}}$$

$$d_{448} = d_{558} = d_{668} = d_{778} = -\frac{1}{2\sqrt{3}} \quad (۱۸-۲)$$

$$d_{146} = d_{157} = -d_{247} = d_{256} = d_{344} = d_{355} = -d_{366} = -d_{377} = \frac{1}{2}$$

با هشت مولد ژل-من و یک ماتریس  $\lambda_0 = (\sqrt{2/3})I$  می‌توانیم یک پایه‌ی اپراتوری هرمیتی برای

فضای اپراتورهای خطی در فضای هیلبرت کیوتریتی بسازیم که شرط  $\text{tr}(\lambda_\alpha \lambda_\beta) = 2\delta_{\alpha\beta}$  برای آنها صادق است و اندیس‌های  $\beta, \alpha$  مقادیر ۰ تا ۸ را اختیار می‌کنند.

## ۲-۱۰ کره‌ی بلاخ

هر عملگر چگالی را می‌توان به صورت یکتای زیر بسط داد:

$$\rho = \frac{1}{3} c_\alpha \lambda_\alpha \quad (۱۹-۲)$$

که ضرایب بسط حقیقی توسط رابطه‌ی  $c_\alpha = 3/2 \text{tr}(\rho \lambda_\alpha)$  تعریف می‌شوند. شرط نرمالیزه بودن ایجاب می‌کند

که  $c_0 = 3/2$ ، در نتیجه عملگر چگالی به شکل زیر در می‌آید:



$$\rho = \frac{1}{3}(1 + c_j \lambda_j) = \frac{1}{3}(1 + c \cdot \lambda) \quad (20-2)$$

که  $c = c_j e_j$  را می‌توان به‌عنوان یک بردار در فضای برداری حقیقی  $\lambda$  بعدی و  $\lambda = \lambda_j e_j$  را به‌عنوان بردار عملگری<sup>۱</sup> در نظر گرفت. با استفاده از رابطه‌ی (۲-۱۶) داریم:

$$\rho^2 = \frac{1}{9} \left(1 + \frac{2}{3} c \cdot c\right) + \frac{1}{3} \lambda \cdot \left(\frac{2}{3} c + \frac{1}{3\sqrt{3}} c * c\right) \quad (21-2)$$

که باید  $c \cdot c = 3$  و  $c * c = \sqrt{3}c$  باشد و  $n$  یک بردار حقیقی هشت مولفه‌ای است که  $n = c/\sqrt{3}$  و ضرب "ستاره"<sup>۲</sup> به شکل  $c * d = e_j d_{jkl} c_k d_l$  تعریف می‌شود. از آنجائی‌که برای حالت‌های خالص داریم  $\rho^2 = \rho$ ، می‌توانیم ماتریس چگالی  $\rho$  را بر حسب ماتریس یکه و ماتریس‌های ژل-من به شکل زیر بسط دهیم:

$$\rho = |\psi\rangle\langle\psi| = \frac{1}{3}(1 + \sqrt{3}n \cdot \lambda) \quad (22-2)$$

این نوع توصیف، معادل توپ بلاخ برای یک کیوتریت است. حالت‌های خالص ارضا کننده‌ی شرط  $\rho^2 = \rho$ ، با شرط زیر تعیین می‌شوند:

$$n \cdot n = 1, \quad n * n = n \quad (23-2)$$

در نتیجه هر حالت خالص کیوتریتی با یک بردار واحد از کره‌ی واحد  $\lambda$  بعدی متناظر است. به‌علاوه این بردار باید در شرط  $n * n = n$  صدق کند. با اضافه شدن سه قید ناشی از این شرط، تعداد پارامترهای حقیقی که برای تعیین یک بردار یک‌ه‌ی  $\lambda$  بعدی دلخواه نیاز است از ۷ پارامتر به ۴ کاهش می‌یابد. دو شرط نرمالیزه بودن و انتخاب یک فاز کلی، به ما اجازه می‌دهد این ۴ پارامتر مستقل را به شکل زیر انتخاب کنیم:

$$|\psi\rangle = e^{i\chi_1} \sin\theta \cos\varphi |1\rangle + e^{i\chi_2} \sin\theta \sin\varphi |2\rangle + \cos\theta |3\rangle \quad (24-2)$$

که برای حالات خالص زوایای  $\chi_1, \chi_2, \theta, \varphi$  در محدوده‌ی زیر قرار می‌گیرند.

$$0 \leq \theta < \frac{\pi}{2}, \quad 0 \leq \varphi \leq \frac{\pi}{2}, \quad 0 \leq \chi_1, \chi_2 < 2\pi$$

<sup>1</sup> Operator vector

<sup>2</sup> Star

$\theta, \varphi$  بزرگی مولفه‌های  $|\psi\rangle$  را تعیین می‌کنند و  $\chi_1$  به عنوان فاز نسبی  $|1\rangle$  نسبت به  $|2\rangle$  و همین‌طور برای  $\chi_2$  تعبیر کرد. با استفاده از زوایای مذکور بردار یکه‌ی ۸ مولفه‌ای را می‌توان به شکل زیر نوشت:

[32] و [33]

$$n = \sqrt{3}(\sin^2 \theta \sin \varphi \cos \varphi \cos(\chi_2 - \chi_1)\mathbf{e}_1, \sin^2 \theta \sin \varphi \cos \varphi \sin(\chi_2 - \chi_1)\mathbf{e}_2, \quad (2-25)$$

$$\begin{aligned} & \frac{1}{2} \sin^2 \theta (\cos^2 \varphi - \sin^2 \varphi) \mathbf{e}_3, \sin \theta \cos \theta \cos \varphi \cos \chi_1 \mathbf{e}_4, \\ & -\sin \theta \cos \theta \cos \varphi \sin \chi_1 \mathbf{e}_5, \sin \theta \cos \theta \sin \varphi \cos \chi_2 \mathbf{e}_6, \\ & -\sin \theta \cos \theta \sin \varphi \sin \chi_2 \mathbf{e}_7, \frac{1}{2\sqrt{3}}(1 - 3\cos^2 \theta) \mathbf{e}_8 \end{aligned}$$

یکی از ویژگی‌های جالب هندسی پواینکاره‌ی کیوتریت‌ها این است که هرگاه دو بردار یکه‌ی  $n$  و  $n'$  داشته باشیم که هر دو نشان دهنده‌ی حالت خالص باشند، این بردارها در شرط:

$$0 \leq \arccos(n \cdot n') \leq \frac{2\pi}{3}$$

صدق می‌کنند. در نتیجه بردارهای دو به دو متعامد در فضای  $H^3$  شامل نقاط مخالف متقاطع (واقع در نقطه‌ی مقابل در امتداد قطر) در کره‌ی پواینکاره نیستند، بلکه نقاطی هستند که با زاویه‌ی منفرجه  $2\pi/3$  نسبت به هم قرار دارند. [34], [35], [36], [37], [38]

## ۲-۱۱ کیودیت<sup>۱</sup>

واحد  $d$  حالته‌ی اطلاعات، کیودیت خوانده می‌شود. همان‌طور که کیوبیت به‌عنوان سیستم منطقی دو حالته تعریف می‌شود، یک کیودیت به‌عنوان سیستم منطقی چند مقداره تعریف می‌شود. چنین سیستمی از کیودیت‌ها و گیت‌های چند مقداره، انعطاف بیشتری در ذخیره‌ی اطلاعات داشته و کاهش زمان برای انجام گیت منطقی متوالی را به‌همراه دارند، اما به قیمت افزایش پیچیدگی گیت‌ها و نیاز به کنترل بیشتر سیستم تمام

<sup>1</sup> Qudit

می‌شود. نمایش هندسی‌ای که برای نمایش کیوبیت‌ها به کار می‌رود، (کره‌ی بلاخ)، به سادگی قابل تعمیم برای نمایش هندسی کیودیت‌ها نمی‌باشد. نمایش فیزیکی کیودیت‌ها را می‌توان با اتمی  $d$  ترازه با اسپین  $n/2$  شبیه‌سازی کرد که  $n = d - 1$ . [39].

یک حالت کیودیتی با عملگر چگالی در فضای هیلبرت - اشمیت نمایش داده می‌شود که روی فضای  $d$  حالت عمل می‌کند و می‌توان این عملگر را به شکل ماتریس - ماتریس چگالی - در پایه‌های استاندارد نوشت. حالت کلی یک کیودیت به شکل زیر نمایش داده می‌شود که  $|0\rangle, |1\rangle, \dots, |d-1\rangle$  پایه‌های فضا را تشکیل می‌دهند و شرط یک بودن مجموع مجذور ضرایب نیز صادق است.

$$|\psi\rangle = a_0 |0\rangle + a_1 |1\rangle + a_2 |2\rangle + \dots + a_{d-1} |d-1\rangle \quad (26-2)$$

## ۲-۱۲ ویژگی‌های یک پایه‌ی ماتریسی کاربردی برای کیودیت‌ها:

(۱) پایه‌ها شامل ماتریس یکه و  $d^2 - 1$  ماتریس  $\{A_i\}$  که  $d \times d$  بعدی هستند می‌باشند که تریس یا رد آنها صفر است.

$$Tr A_i = 0 \quad (27-2)$$

(۲) ماتریس‌های پایه‌های  $\{A_i\}$  متعامدند، یعنی:

$$Tr A_i^t A_j = N \delta_{ij} \quad (28-2)$$

## ۲-۱۳ بسط بردار بلاخ برای ماتریس چگالی

از آنجائی که هر ماتریس  $d$  بعدی در فضای هیلبرت - اشمیت را می توان با پایه های ماتریسی  $\{A_i\}$  تجزیه کرد، ماتریس چگالی یک کیودیت را می توان تجزیه کرده و به بسط یا توزیع ماتریس چگالی آن دست یافت.

$$\rho = \frac{1}{d} I + \vec{b} \cdot \vec{\Gamma} \quad (2-29)$$

که  $\vec{b} \cdot \vec{\Gamma}$  ترکیبی خطی از تمام ماتریس های  $\{A_i\}$  است و بردار  $b$  متعلق به فضای  $\mathbb{R}^{d^2-1}$  که  $b_i = \langle \Gamma_i \rangle = Tr \rho \Gamma_i$  می باشد، بردار بلاخ نامیده می شود. ضریب  $(1/d)I$  مقدار ثابتی است که ناشی از شرط  $Tr \rho = 1$  می باشد. اگرچه یک ماتریس چگالی  $\rho$  را می توان به بردار بلاخ تجزیه کرد، اما هر برداری که به فرم  $(1/d)I + \vec{b} \cdot \vec{\Gamma}$  باشد نشان دهنده ی ماتریس چگالی نیست. حتی اگر شرط  $Tr \rho = 1$  و  $Tr \rho \leq 1$  را ارضا کند، ممکن است شرط  $\rho \geq 0$  برقرار نباشد. هر پایه ی ماتریس، یک بردار بلاخ درون ابر کره ی بلاخ می سازد، اما هر نقطه ای داخل این ابر توپ نشان دهنده ی یک حالت فیزیکی با  $\rho \geq 0$  نمی باشد. این نقاط استثنا، حفره نامیده می شوند. ویژگی های هندسی فضای بلاخ در ابعاد بزرگ تر پیچیده بوده و موضوع مورد علاقه ی دانشمندان است.

## ۲-۱۴ تعمیم پایه ی ماتریسی ژل - من

تعمیم یافته ی ماتریس های ژل - من<sup>۱</sup>، کلی سازی ماتریس های پائولی برای کیوبیت ها و ماتریس های ژل - من برای کیوتریت ها است. این ماتریس ها مولد استاندارد گروه  $SU(N)$  هستند که به صورت سه نوع ماتریس مختلف تعریف می شوند. برای ساده سازی از نمایش عملگری استفاده می کنیم. بدین ترتیب ماتریس چگالی به راحتی به صورت عملگری در پایه ی استاندارد نوشته می شود: [41] و [40] و [42]

$$(1) \quad \text{GGM} \quad \frac{d(d-1)}{2}$$

<sup>1</sup> GGM: Generalized Gell-Mann matrices

$$\Lambda_s^{jk} = |j\rangle\langle k| + |k\rangle\langle j|, \quad 1 \leq j < k \leq d \quad (30-2)$$

ماتریس پاد متقارن GGM  $\frac{d(d-1)}{2}$  (2)

$$\Lambda_a^{jk} = -i|j\rangle\langle k| + i|k\rangle\langle j|, \quad 1 \leq j < k \leq d \quad (31-2)$$

ماتریس قطری GGM  $(d-1)$  (3)

$$\Lambda^l = \sqrt{\frac{2}{l(l+1)}} \left( \sum_{j=1}^l |j\rangle\langle j| - l|l+1\rangle\langle l+1| \right), \quad 1 \leq l \leq d-1 \quad (32-2)$$

در کل  $d^2 - 1$  ماتریس داریم که با توجه به تعریفشان همگی هرمیتی با تریس صفر و متعامد می‌باشند و

یک پایه- پایه‌ی ماتریسی ژل من تعمیم یافته GGB- را تشکیل می‌دهند. مثلاً برای حالت کیوتریتی، این شکل

تعمیم یافته، به صورت ماتریس های ژل من در می‌آید:

سه ماتریس متقارن ژل - من:

$$\lambda_s^{12} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \lambda_s^{13} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \lambda_s^{23} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

سه ماتریس پادمتقارن ژل - من:

$$\lambda_a^{12} = \begin{pmatrix} 0 & -i & 0 \\ i & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \lambda_a^{13} = \begin{pmatrix} 0 & 0 & -i \\ 0 & 0 & 0 \\ i & 0 & 0 \end{pmatrix}, \lambda_a^{23} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -i \\ 0 & i & 0 \end{pmatrix}$$

دو ماتریس قطری ژل - من:

$$\lambda^1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \lambda^2 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{pmatrix}$$

به‌عنوان مثالی دیگر، برای  $d=4$ :

شش ماتریس متقارن GGM

$$\Lambda_s^{12} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \Lambda_s^{13} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \Lambda_s^{14} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

$$\Lambda_s^{23} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \Lambda_s^{24} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \Lambda_s^{34} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

شش ماتریس متقارن GGM

$$\Lambda_a^{12} = \begin{pmatrix} 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \Lambda_a^{13} = \begin{pmatrix} 0 & 0 & -i & 0 \\ 0 & 0 & 0 & 0 \\ i & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \Lambda_a^{14} = \begin{pmatrix} 0 & 0 & 0 & -i \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ i & 0 & 0 & 0 \end{pmatrix}$$

$$\Lambda_a^{23} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & -i & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \Lambda_a^{24} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \end{pmatrix}, \Lambda_a^{34} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \end{pmatrix}$$

سه ماتریس قطری GGM

$$\Lambda^1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \Lambda^2 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \Lambda^3 = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -3 \end{pmatrix}$$

با استفاده از GGB حالت کلی بسط بردار بلاخ برای یک ماتریس چگالی را می توان به صورت :

$$\rho = \frac{1}{d} \mathbf{I} + \vec{b} \cdot \vec{\Lambda} \quad (33-2)$$

نوشت که  $b$  بردار بلاخ است  $\vec{b} = (\{b_s^{jk}\}, \{b_a^{jk}\}, \{b^l\})$  و مولفه ها به صورت منظم مرتب می شوند، اندیس ها نیز در قید  $1 \leq j, k \leq d$  و  $1 \leq l \leq d-1$  قرار می گیرند. مولفه ها با روابط  $b_s^{jk} = \text{Tr} \Lambda_s^{jk} \rho$  و  $b_a^{jk} = \text{Tr} \Lambda_a^{jk} \rho$  و  $b^l = \text{Tr} \Lambda^l \rho$  تعیین می شوند. همه ی بردارهای بلاخ داخل ابرکره ای به شعاع

برای کیوتریت‌ها مولفه‌های بردار بلاخ متناظر با ماتریس‌های  
 ژل-من عبارتند از:

$$\vec{b} = (b_s^{12}, b_s^{12}, b_s^{23}, b_a^{12}, b_a^{13}, b_a^{23}, b^1, b^2) \quad (۳۴-۲)$$

در تمام ابعاد، حالات خالص روی سطح ابر کره و حالات آمیخته درون آن قرار می‌گیرند. [43] و [44] و

[45] و [46]

۳

فصل سوم: الگوریتم‌های جستجوی کوانتومی



### ۳-۱ گیت کلاسیکی

محاسبات کلاسیکی که روی اطلاعات ذخیره شده در بیت‌ها انجام می‌شود توسط واحدهای پردازشگری اجرا می‌گردد که گیت نام دارند. هدف اصلی یک گیت منطقی کلاسیکی، پردازش کردن اطلاعات در سطح بیت می‌باشد. گیت‌های کلاسیکی بر اساس تعداد بیت‌های ورودی به سه دسته‌ی گیت‌هایی با یک بیت ورودی: گیت NOT، گیت FANOUT (کپی)، گیت ERASE، گیت‌هایی با دو بیت ورودی: گیت AND، گیت OR، گیت XOR، گیت NAND و گیت NOR و گیتی با سه بیت ورودی که گیت TOFFOLI (تافلی) نام دارد، طبقه‌بندی می‌شوند. [47] هیچ‌کدام از این توابع مقدماتی که به آنها اشاره شد وارون‌پذیر نیستند. یک تابع وارون‌پذیر، به لحاظ نظری حتماً توانی مصرف می‌کند که نمی‌توان با هیچ پیشرفتی در فناوری از آن جلوگیری کرد. یک حد تئوریک از اتلاف انرژی وجود دارد که نمی‌توان از آن حذر کرد. این حد، نخستین بار همان‌طور که در فصل اول اشاره شد توسط رالف لاندائر در سال ۱۹۶۱ نشان داده شده است. مبنای استدلال او این است که در تابع وارون‌ناپذیر، مقداری از اطلاعات گم می‌شود، زیرا نمی‌توان از خروجی تابع به ورودی آن پی برد و هر نوع پاک کردن اطلاعات نیز با کاهش آنتروپی سیستم و افزایش آنتروپی محیط همراه است.

### ۳-۲ گیت کوانتومی

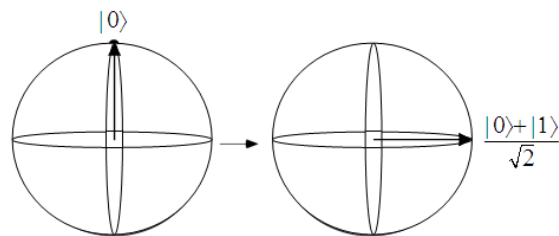
اگر اطلاعات را در کیوبیت‌ها یعنی حالت‌های کوانتومی ذخیره کنیم به‌ناچار پردازش اطلاعات می‌بایستی یا با عملگرهای یکانی که تحول را نشان می‌دهند و یا با اندازه‌گیری‌ها انجام گیرند. معمولاً اصطلاح گیت کوانتومی برای عملگر یکانی به‌کار برده می‌شود. گیت کوانتومی هرگاه روی یک کیوبیت اثر کند آن را گیت تک کیوبیتی و هرگاه روی  $n$  تا کیوبیت اثر کند گیت  $n$  کیوبیتی خوانده می‌شود. از آنجائی که عملگرهای کوانتومی را می‌توان به کمک ماتریس‌ها نشان داد، یک گیت کوانتومی متشکل از  $n$  کیوبیت ورودی و خروجی را می‌توان توسط ماتریس‌های  $2^n \times 2^n$  نمایش داد. [48] از گیت‌های کوانتومی با یک کیوبیت ورودی می‌توان به گیت NOT(X)، گیت Z و گیت Hadamard (هادامارد)، از گیت‌های کوانتومی با دو کیوبیت ورودی می‌توان به گیت

Controlled NOT (CNOT) و گیت function (f-gate) اشاره کرد. گیت‌هایی که در الگوریتم‌های پیشنهادی از آن‌ها استفاده خواهیم نمود را به اختصار شرح می‌دهیم.

**الف) گیت کوانتومی Hadamard (هادامارد):** عملکرد گیت هادامارد به صورت زیر است:

$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$



شکل ۱-۳ نمایش تاثیر عملگر هادامارد روی حالت  $|0\rangle$

و ماتریس متناظر با آن برابر است با:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

و به شکل زیر در مدارها نمایش داده می‌شود:

$$|x\rangle \text{ --- } \boxed{H} \text{ --- } (-1)^x |x\rangle + |1-x\rangle$$

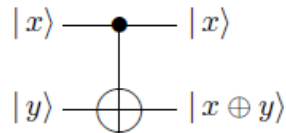
شکل ۲-۳ نمایش گیت هادامارد در مدار

**ب) گیت کوانتومی Controlled NOT (CNOT):** این گیت دو کیوبیت ورودی دارد که کیوبیت اول معروف

به کیوبیت کنترل و کیوبیت دوم معروف به کیوبیت هدف است. عملکرد این گیت به صورت زیر تعریف می‌شود:

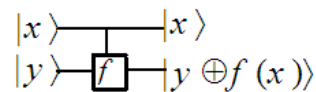
$$|a,b\rangle \rightarrow |a,b \oplus a\rangle$$

چنانچه کیوبیت کنترل در حالت  $|0\rangle$  باشد، هیچ تغییری در کیوبیت هدف به وجود نمی‌آید، ولی اگر کیوبیت کنترل در حالت  $|1\rangle$  باشد، آنگاه ماتریس  $X$  یا NOT برای کیوبیت هدف اعمال می‌شود.



شکل ۳-۳ نمایش گیت CNOT در مدار

ج) گیت کوانتومی **(f-gate)function**: این گیت،  $|x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$ ، حالت تعمیم یافته‌ی گیت C-NOT است و به شکل زیر در مدار نشان داده می‌شود:



شکل ۳-۴ نمایش گیت f در مدار

### ۳-۳ الگوریتم کوانتومی

برای انجام یک محاسبه‌ی مشخص، کامپیوترها طبق یک دستورالعمل کاملاً مشخص یک سری اعمال را انجام می‌دهند. به چنین دستورالعملی یک "الگوریتم" می‌گویند. الگوریتم کوانتومی در ساده‌ترین شکل آن به مجموعه‌ای از گیت‌های کوانتومی متوالی گفته می‌شود که روی یک حالت معین اولیه اثر می‌کنند و چنان تنظیم شده‌اند که حالت نهایی چنان باشد که پس از اندازه‌گیری‌های سنجیده‌ای روی آن، جواب یک مسئله‌ی معین را با احتمال بسیار خوب در بر داشته باشد. [49] از نخستین الگوریتم‌های کوانتومی می‌توان به الگوریتم دویچ<sup>۱</sup> - دویچ جوزا<sup>۲</sup> - سیمون<sup>۳</sup> - برنشتاین وزیرانی<sup>۴</sup> - شور<sup>۱</sup> - گراور<sup>۲</sup> و یونس اشاره نمود.

<sup>1</sup> Deutsch

<sup>2</sup> Deutsch-Jozsa

<sup>3</sup> Simon

<sup>4</sup> Bernstein-vazirani

### ۳-۴ الگوریتم گراور

مثالی از الگوریتم‌های کوانتومی که در سال ۱۹۹۶ توسط گراور<sup>۳</sup> ارائه شد، الگوریتم جستجوی گراور است که در زمان کوتاه‌تری نسبت به الگوریتم‌های کلاسیک عمل جستجو را انجام می‌دهد و در مقایسه با الگوریتم جستجوی کلاسیک به تکراری از مرتبه‌ی  $O(\sqrt{N})$  نیاز دارد. گراور نشان داد که مساله‌ی جستجو در یک فضای درهم ریخته را می‌توان با سرعت بیشتری در کامپیوترهای کوانتومی حل کرد و با این کار جنبه‌ی دیگری از توان بالای کامپیوترهای کوانتومی را نمایان ساخت. البته این افزایش سرعت از مرتبه‌ی افزایش سرعت در الگوریتم شور نبود، اما از این نقطه‌نظر که جستجو می‌تواند به عنوان یک زیر روال و زیر برنامه در بسیاری از برنامه‌ها و مسائل مهم به کار رود، با اهمیت است. او نشان داد که تعداد تکرار مورد نیاز که برای رسیدن به جواب با کمترین میزان تکرار و بیشترین احتمال که بهینه نیز باشد برابر است با  $\pi/4\sqrt{N}$ ، به شرطی که دقیقاً یک جواب در بین داده‌ها موجود باشد.

در مقاله‌ی الگوریتم جستجوی کوانتومی گراور برای یک حالت اولیه دلخواه<sup>۴</sup> و مقاله‌ی خانواده‌ی الگوریتم‌های جستجوی کوانتومی<sup>۵</sup>، الگوریتم گراور با نشان دادن این که برهم‌نهی یکنواخت اولیه را می‌توان با هر برهم‌نهی دلخواه و نیز تغییر فاز را با اوراکل و عملگر پراکندگی جایگزین کرد، کلی‌سازی شد.

صورت مجرد یک مسئله‌ی جستجو را می‌توان به شکل زیر بیان کرد: فرض کنید پایگاه داده‌هایی نامنظم با  $N$  داده داریم: مجموعه‌ی  $S := \{x_1, x_2, \dots, x_N\}$  شامل  $N$  شی. بدون از دست دادن کلیت مسئله فرض می‌کنیم  $N = 2^n$ . همچنین فرض می‌کنیم که داده‌های لیست، با اعداد صحیح  $\{0, 1, \dots, N-1\}$  اندیس‌گذاری شده‌اند. می‌دانیم که مقدار تابع  $f$  به ازای تنها یکی از اعضای این مجموعه برابر با یک و برای

---

<sup>1</sup> Shor

<sup>2</sup> Grover

<sup>3</sup> Lov K. Grover

<sup>4</sup> E. Biham and D. Dan kenigsberg ( Grover's quantum search algorithm for an arbitrary initial mixed state )

<sup>5</sup> G.L. Long

دیگر عناصر مجموعه برابر با صفر است، ولی نمی‌دانیم که کدام یک از آنهاست. هدف ما یافتن داده‌ی خاص  $w$  است. با استفاده از تابع کمکی که به طریق زیر تعریف می‌شود:

$$f(x) = \begin{cases} 0 & \text{if } x \neq w \\ 1 & \text{if } x = w \end{cases} \quad (1-3)$$

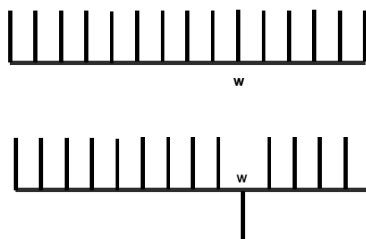
می‌توانیم  $w$  ای که در شرط  $f(w) = 1$  صدق کند را بیابیم. به روش کلاسیکی در غیاب هر نوع اطلاعات اضافی، تنها کاری که باید انجام دهیم این است که داده‌های مختلف را یک به یک به تابع بدهیم و خروجی‌اش را مشاهده کنیم. هرگاه خروجی تابع برابر با یک شد، نتیجه می‌گیریم که عنصر داده شده به تابع  $w$  است. در نتیجه در جستجوی کلاسیکی بطور متوسط به  $N/2$  فراخوانی تابع  $f$  برای پیدا کردن داده‌ی مورد نظر نیاز است، اما با کامپیوتر کوانتومی، تنها به فراخوانی‌ای از مرتبه‌ی  $\sqrt{N}$  برای رسیدن به هدف نیاز داریم. همان‌طور که می‌بینیم افزایش سرعت جستجوی ایجاد شده از مرتبه‌ی ۲ است که برای  $N$  های بزرگ، افزایش سرعت قابل ملاحظه‌ای است. اگرچه کلاس حل پذیری این مسئله با این ابداع تغییری نکرده است و همچنان این مسئله در کلاس حل پذیری چندجمله‌ای است اما به دلیل نقشی که یک الگوریتم جستجو در اغلب الگوریتم‌های دیگر بازی می‌کند، این پیشرفت اهمیت زیادی دارد. نخست از عملگر  $U_f$  استفاده خواهیم کرد:

$$U_f |x_i, y\rangle = |x_i, f(x_i) \oplus y\rangle \quad (2-3)$$

با استفاده از تعریف تابع  $f(x)$  می‌توان اثر عملگر  $U_f$  را به صورت  $U_f |x\rangle = (-1)^{f(x)} |x\rangle$  نوشت که نتیجه‌ی اعمال آن روی حالت‌های جواب و غیر جواب به شکل زیر است:

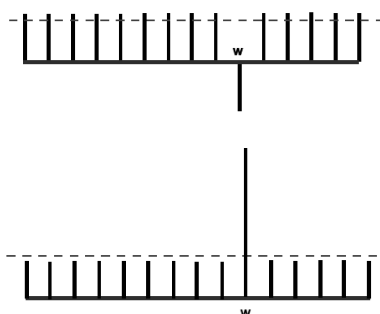
$$\begin{aligned} U_f |w\rangle &= -|w\rangle \\ U_f |x_i\rangle &= |x_i\rangle, \quad x_i \neq w \end{aligned} \quad (3-3)$$

بنابراین اثر این عملگر روی زیرفضای جواب‌ها به شکل یک انعکاس ظاهر می‌شود. نتیجه‌ی عمل این عملگر را می‌توان به شکل زیر نمایش داد:



شکل ۳-۵ نمایش اثر عملگر  $U_f$

در مرحله‌ی بعد، از عملگر  $D$  (عملگر معکوس نسبت به میانگین) استفاده خواهیم کرد که حالت فوق را روی متوسط دامنه‌های آن که در شکل زیر به صورت خط چین نشان داده شده انعکاس می‌دهد، نتیجه در شکل زیر نمایش داده شده است:



شکل ۳-۶ نمایش اثر عملگر  $D$

می‌توان نشان داد که این انعکاس حول متوسط نیز یک عملگر یکانی است. عملگر انعکاس حول میانگین یا همان عملگر پراکندگی را می‌توان به شکل زیر نمایش داد:

$$D = \begin{pmatrix} \frac{2}{\sqrt{N}} - 1 & \frac{2}{\sqrt{N}} & \dots & \frac{2}{\sqrt{N}} \\ \frac{2}{\sqrt{N}} & \frac{2}{\sqrt{N}} - 1 & \dots & \frac{2}{\sqrt{N}} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{\sqrt{N}} & \frac{2}{\sqrt{N}} & \dots & \frac{2}{\sqrt{N}} - 1 \end{pmatrix} \quad (4-3)$$

یا به شکل ساده‌تر:

$$D_{ij} = \begin{cases} \frac{2}{N} & \text{if } i \neq j \\ \frac{2}{N} - 1 & \text{if } i = j \end{cases} \quad (5-3)$$

این عملگر دو ویژگی دارد:

الف- یکانی است. این عملگر را می‌توان به سه عملگر یکانی تجزیه کرد: دو عملگر هادامارد و یک عملگر

تغییر فاز، در نتیجه می‌توان آن را به شکل زیر نوشت:

$$D = HRH \quad (6-3)$$

که نمایش ماتریسی عملگر تغییر فاز  $R$  عبارتست از:

$$R = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & -1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & -1 \end{pmatrix} \quad (7-3)$$

حال با استفاده از عملگر فوق نشان می‌دهیم که می‌توان عملگر معکوس نسبت به میانگین را به صورت

حاصلضرب سه ماتریس مذکور نوشت:

$$D = H^{\otimes n} \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & -1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & -1 \end{pmatrix} H^{\otimes n} = H^{\otimes n} \left[ \begin{pmatrix} 2 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix} - I \right] H^{\otimes n}$$

$$\begin{aligned}
&= H^{\otimes n} \begin{pmatrix} 2 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix} H^{\otimes n} - I = H^{\otimes n} \begin{pmatrix} \frac{2}{\sqrt{N}} & \frac{2}{\sqrt{N}} & \dots & \frac{2}{\sqrt{N}} \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix} - I \\
&= \begin{pmatrix} \frac{2}{\sqrt{N}} & \frac{2}{\sqrt{N}} & \dots & \frac{2}{\sqrt{N}} \\ \frac{2}{\sqrt{N}} & \frac{2}{\sqrt{N}} & \dots & \frac{2}{\sqrt{N}} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{\sqrt{N}} & \frac{2}{\sqrt{N}} & \dots & \frac{2}{\sqrt{N}} \end{pmatrix} - I = \begin{pmatrix} \frac{2}{\sqrt{N}} - 1 & \frac{2}{\sqrt{N}} & \dots & \frac{2}{\sqrt{N}} \\ \frac{2}{\sqrt{N}} & \frac{2}{\sqrt{N}} - 1 & \dots & \frac{2}{\sqrt{N}} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{\sqrt{N}} & \frac{2}{\sqrt{N}} & \dots & \frac{2}{\sqrt{N}} - 1 \end{pmatrix} \quad (8-3)
\end{aligned}$$

عملگر  $D$  که به صورت حاصلضرب سه عملگر یکانی است خود نیز یکانی می‌باشد.

ب- می‌توان آن را به عنوان عملگر معکوس نسبت به میانگین تعبیر کرد: اگر حالت قبل از اعمال عملگر

$D$  را به صورت  $|\psi\rangle = \sum_{i=0}^{N-1} a_i |i\rangle$  داشته باشیم، حالت سیستم بعد از اعمال آن برابر خواهد بود با

$|\psi'\rangle = \sum_{i=0}^{N-1} a'_i |i\rangle$  که  $a'_i = (2/N - 1)a_i + \sum_{i \neq j} (2/N)a_j$  می‌توانیم این ضرایب را به شکل

$a'_i + a_i = \sum_{j=0}^{N-1} (2/N)a_j$  و  $a'_i - a_i = \sum_{j=0}^{N-1} (2/N)a_j$  بازنویسی کنیم. اگر متوسط دامنه‌ها را

$A = \sum_{j=0}^{N-1} (1/N)a_j$  قرار دهیم در نتیجه  $a'_i + a_i = 2A$  اگر  $a_i = A + \Delta$  در نتیجه  $a'_i = A - \Delta$  پس نتیجه‌ی

اثر خالص عملگر  $D$  این است که به جای هر دامنه‌ی  $a_i$ ، انعکاس یافته‌ی آن حول متوسط همه‌ی دامنه‌های  $a_i$  جایگذاری می‌شود.

می‌توانیم نشان دهیم تبدیل  $U_f$  برابر است با عملگر یکانی  $I_w$  که برابر است با:

$$I_w = I - 2|w\rangle\langle w| \quad (9-3)$$

تبدیل یکانی معادل عملگر  $D$  را نیز با  $I_s$  نمایش می‌دهیم که برابر است با  $I_s = I - 2|s\rangle\langle s|$  که در آن :



$$|s\rangle := \frac{1}{\sqrt{N}} (|x_1\rangle + |x_2\rangle + \dots + |x_N\rangle) \quad (10-3)$$

$I_s$  را روی یک حالت دلخواه مثل  $x_j$  اثر می‌دهیم:

$$I_s |x_j\rangle = |x_j\rangle - 2 \frac{1}{\sqrt{N}} |s\rangle = |x_j\rangle - \frac{2}{\sqrt{N}} |s\rangle \quad (11-3)$$

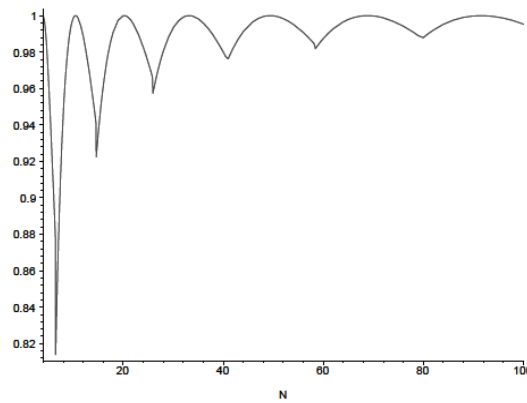
حال اگر عملگر  $I_s$  را روی  $|\psi\rangle = \sum_i a_i |x_i\rangle$  اثر دهیم نتیجه عبارت خواهد بود از:

$$I_s |\psi\rangle = \sum_i a_i (|x_i\rangle - \frac{2}{\sqrt{N}} |s\rangle) = \sum_i a_i (|x_i\rangle - 2\bar{a} |s\rangle) \quad (12-3)$$

که در آن  $\bar{a} := (1/\sqrt{N})(a_1 + a_2 + \dots + a_N)$  متوسط دامنه‌های حالت  $|\psi\rangle$  است. حالت فوق را می‌توان به شکل زیر نوشت که به روشنی نشان می‌دهد دامنه‌ی  $a_i$  حول مقدار متوسط دامنه‌ها یعنی  $\bar{a}$  انعکاس یافته است.

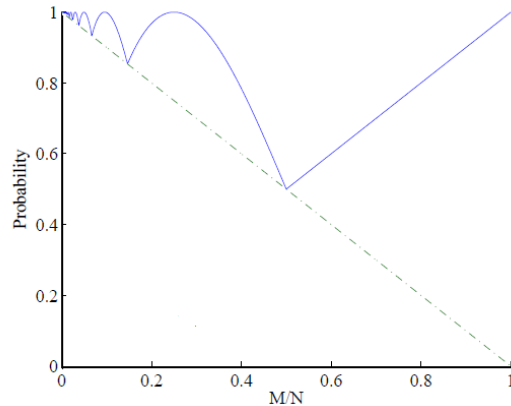
$$I_s |\psi\rangle = \sum_i (a_i - 2\bar{a}) |x_i\rangle \quad (13-3)$$

احتمال موفقیت الگوریتم گراور بر حسب تعداد داده‌ها به شکل زیر است:



شکل ۷-۳ نمودار احتمال موفقیت الگوریتم گراور بر حسب تعداد داده‌ها

نمودار زیر نیز احتمال موفقیت را بر حسب نسبت تعداد جواب‌ها به تعداد کل داده‌ها نشان می‌دهد.



شکل ۳-۸ نمودار احتمال موفقیت الگوریتم گراور بر حسب تعداد جوابها

از نمودار فوق می‌توان دریافت که کمترین احتمال یافتن جواب در الگوریتم گراور تقریباً ۵۰٪ است و زمانی اتفاق می‌افتد که  $M/N = 0.5$ ، یعنی زمانی که تعداد جوابها نصف تعداد داده‌ها می‌باشد. برای حالتی که  $M/N > 0.5$  الگوریتم مشابه حالت کلاسیکی عمل می‌کند. برای رفع مشکل حالتی که تعداد جوابها بیش از نیمی از تعداد کل داده‌ها می‌باشد راه‌حلی در کتاب Quantum Computation and Quantum Information<sup>۱</sup> ارائه شد که با دو برابر کردن فضای جستجو با اضافه کردن  $N$  داده‌ی غیر جواب، تعداد جوابها کمتر از نیمی از تعداد کل داده‌ها گشته و تعداد تکرار الگوریتم به جای  $\pi/4\sqrt{N/M}$  تبدیل به  $\pi/4\sqrt{2N/M}$  می‌شود که همچنان در مرتبه‌ی  $O(\sqrt{N/M})$  عمل می‌کند. [13] و [12]. اگرچه الگوریتم گراور برای زمانی که یک داده‌ی جواب در فضای جستجو داشته باشیم بهینه است اما اعتبار آن برای حالتی که تعداد جوابها بیش از یکی‌ست کاهش می‌یابد. یعنی رفتار الگوریتم در کل بازه، معتبر نیست. بهترین رفتار الگوریتم را زمانی که  $M/N < 0.145$  و نیز در همسایگی  $M/N = 0.25$  مشاهده می‌کنیم. [۵۰] و [51] و [52] و [56]

<sup>1</sup> M.Nielsen and I.Chuang

پس به طور کلی این الگوریتم با بهره‌گیری از توازی کوانتومی، با ایجاد یک برهم‌نهی یکنواخت که نشان دهنده‌ی همه‌ی داده‌های لیست است با اعمال اوراکلی که حالت جواب را با اثر عملگر تغییر فاز<sup>۱</sup>  $(e^{i\theta_1}, \theta_1 = \pi)$  روی آن تغییر می‌دهد و باقی حالت‌ها  $(e^{i\theta_2}, \theta_2 = 0)$  را بدون تغییر باقی می‌گذارد و نیز اعمال عملگر پراکنندگی<sup>۲</sup>، دامنه‌ی حالت جواب را افزایش می‌دهد. بعد از چند بار خواندن تابع و انعکاس حول متوسط، یعنی بعد از چند بار اعمال عملگر  $G := I_s I_w$  حالت سیستم به‌صورتی در خواهد آمد که در آن دامنه‌ی مربوط به جواب نسبت به بقیه‌ی دامنه‌ها افزایش قابل ملاحظه‌ای پیدا کرده است و نتیجه‌ی اندازه‌گیری چنین حالتی با احتمال زیاد،  $|w\rangle$  خواهد بود.

### ۳-۵ مراحل الگوریتم گراور

(۱)  $n+1$  حافظه‌ی کیوبیتی را در حالت زیر ایجاد می‌کنیم.

$$|\psi_0\rangle = |0^{\otimes n}\rangle \otimes |1\rangle \quad (۱۴-۳)$$

(۲) گیت هادامارد را روی همه‌ی کیوبیت‌ها اعمال می‌کنیم.

$$|\psi_1\rangle = H^{\otimes n+1} |\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \quad (۱۵-۳)$$

(۳) مراحل زیر را  $\sqrt{N}$  مرتبه تکرار می‌کنیم:

الف) تبدیل  $U_f$  یا  $I_s$  را اعمال می‌کنیم.

$$|\psi_2\rangle = U_f |\psi_1\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle \otimes \left( \frac{1}{\sqrt{2}} (|0 \oplus f(i)\rangle - |1 \oplus f(i)\rangle) \right) \quad (۱۶-۳)$$

حالت ایجاد شده را می‌توان به‌صورت زیر نوشت:

$$|\psi_2\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle \otimes \left( \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right) - \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle \otimes \left( \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right)$$

<sup>1</sup> Phase shift

<sup>2</sup> Diffusion operator

که مجموع اول نشان دهندهی حالت‌های غیر جواب و مجموع دوم نشان دهندهی حالت‌های جواب است.

(ب) تبدیل  $I_s$  (معکوس نسبت به میانگین) را اعمال می‌کنیم که حالت نهایی ناشی از

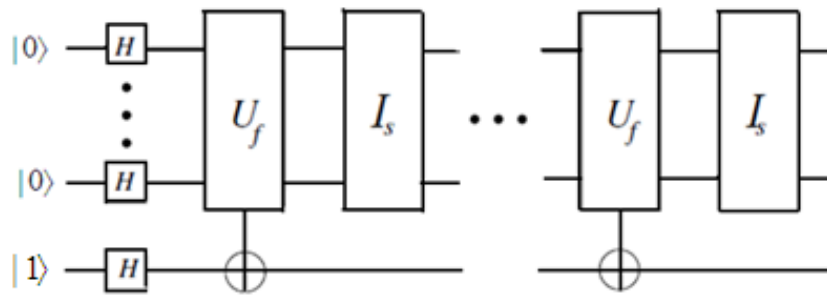
اعمال  $G = I_s I_w$  را می‌توان به شکل زیر نوشت:

$$|\psi_3\rangle = G |\psi_1\rangle = b_1 \sum_{i=0}^{N-1} |i\rangle + a_1 \sum_{i=0}^{N-1} |i\rangle \quad (17-3)$$

که:

$$\begin{cases} a_1 = \frac{N-2M}{N} a_0 + \frac{2(N-M)}{N} b_0 & , & b_1 = \frac{N-2M}{N} b_0 - \frac{2M}{N} a_0 \\ a_0 = \frac{1}{\sqrt{N}} & , & b_0 = \frac{1}{\sqrt{N}} \end{cases} \quad (18-3)$$

(۴)  $n$  کیوبیت اول را اندازه می‌گیریم. جواب با احتمال بالایی به دست می‌آید. [۵۰] و [51]



شکل ۳-۹ نمودار الگوریتم گراور

### ۳-۶ الگوریتم احمد یونس<sup>۱</sup>

در این الگوریتم به جای استفاده از عملگر  $I_s$  از عملگر دیگری مشابه با آن به نام عملگر انتشار جزئی  $P_{inv}$

یا  $Y$  که در فضای  $n+1$  کیوبیتی عمل می‌کند استفاده می‌شود که عمل انعکاس نسبت به میانگین را تنها در

<sup>1</sup> Ahmed Younes

یک زیر فضا از سیستم انجام می‌دهد و هم چنین از درهم‌تنیدگی بین  $n$  کیوبیت تشکیل دهنده‌ی گزینه‌ها با کیوبیت هدف بهره برده شده است.

ورودی این الگوریتم حالت  $|0\rangle \otimes |0^{\otimes n}\rangle$  است و کیوبیت هدف بر خلاف الگوریتم گراور در حالت  $|0\rangle$  است و مستقیماً با همین حالت به اپراتور  $U_f$  می‌رسد. عملی که این اپراتور انجام می‌دهد نیز با  $I_w$  در الگوریتم گراور متفاوت است. در الگوریتم یونس مانند الگوریتم گراور از  $U_f$  که به شکل زیر عمل می‌کند استفاده می‌شود:

$$U_f |i, y\rangle \rightarrow |i, y \oplus f(i)\rangle \quad (19-3)$$

که در آن  $f(i)$  تابعی است که برای حالت جواب مقدارش برابر یک و برای غیر جواب‌ها صفر است. [52] و [53]

### ۳-۷ مراحل الگوریتم احمد یونس

برای لیست داده‌های  $N = 2^n$  مراحل الگوریتم به قرار زیر است:

(۱) ایجاد حافظه‌ی اولیه - حالت اولیه  $n+1$  کیوبیتی که همه کیوبیت‌ها در حالت  $|0\rangle$  هستند را ایجاد می‌کنیم که کیوبیت اضافی (اوراکل) برای محاسبه‌ی  $U_f$  می‌باشد:

$$|W_0\rangle = |0^{\otimes n}\rangle \otimes |0\rangle \quad (20-3)$$

(۲) مقدار دهی اولیه به حافظه - اپراتور هادامارد را روی  $n$  حالت اولیه به‌طور موازی اعمال می‌کنیم که در نتیجه  $2^n$  حالت زیر ایجاد می‌شود و  $i$  عدد صحیحی است که نشان دهنده‌ی شماره‌ی داده در لیست می‌باشد:

$$|W_1\rangle = (H^{\otimes n} \otimes I) |W_0\rangle = \left( \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle \right) \otimes |0\rangle \quad (21-3)$$

(۳) مراحل زیر را  $\sqrt{N}$  مرتبه تکرار می‌کنیم:

الف) اعمال اوراکل - اپراتور  $U_f$  را برای نگاشت داده‌های لیست به  $|0\rangle$  یا  $|1\rangle$  به‌طور

همزمان اثر می‌دهیم و نتیجه را در یک کیوبیت دیگر ذخیره می‌کنیم:

$$U_f |W_1\rangle = |W_2\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (|i\rangle \otimes |0 \oplus f(i)\rangle) = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (|i\rangle \otimes |f(i)\rangle) \quad (22-3)$$

$$= \sum_{i=0}^{N-1} \alpha_i |i\rangle \otimes |0\rangle + \sum_{i=0}^{N-1} \beta_i |i\rangle \otimes |1\rangle$$

که :

$$\alpha_i = \begin{cases} 0 & \text{matches} \\ \frac{1}{\sqrt{N}} & \text{non matches} \end{cases}, \beta_i = \begin{cases} \frac{1}{\sqrt{N}} & \text{matches} \\ 0 & \text{non matches} \end{cases} \quad (23-3)$$

ب) اعمال عملگر انتشار جزئی - در این قسمت عملگر جدیدی به‌جای عملگر پراکندگی گراور و مشابه

با آن اعمال می‌شود. تفاوت آن با عملگر پراکندگی گراور این است که عمل معکوس نسبت به میانگین را تنها

روی زیر فضایی از سیستم انجام می‌دهد که شامل تمام حالت‌های غیرجواب و نیمی از جواب‌هاست، درحالی‌که

برای نیمه‌ی دیگر جواب‌ها تنها دامنه برای اثر عملگر انتشار جزئی در تکرار بعدی منفی می‌شود. این عملگر را

در نمایش قطری به شکل زیر نشان می‌دهیم:

$$Y = H^{\otimes n} \otimes I (2|0^{\otimes n+1}\rangle\langle 0^{\otimes n+1}| - I^{\otimes n+1}) H^{\otimes n} \otimes I \quad (24-3)$$

عملگر  $Y$  را اعمال می‌کنیم:

$$\begin{aligned}
|W_3\rangle &= Y |W_2\rangle \\
&= \sum_{i=0}^{N-1} \alpha_i [(H^{\otimes n} \otimes I)(2|0^{\otimes n+1}\rangle\langle 0^{\otimes n+1}| - I^{\otimes n+1})(H^{\otimes n} \otimes I)(|i\rangle \otimes |0\rangle) \\
&+ \sum_{i=0}^{N-1} \beta_i [(H^{\otimes n} \otimes I)(2|0^{\otimes n+1}\rangle\langle 0^{\otimes n+1}| - I^{\otimes n+1})(H^{\otimes n} \otimes I)(|i\rangle \otimes |1\rangle) \\
&= \sum_{i=0}^{N-1} \alpha_i [(H^{\otimes n} \otimes I)(2|0^{\otimes n+1}\rangle\langle 0^{\otimes n+1}|)(H^{\otimes n} \otimes I) - (H^{\otimes n} \otimes I)(I^{\otimes n+1})(H^{\otimes n} \otimes I)](|i\rangle \otimes |0\rangle) \\
&+ \sum_{i=0}^{N-1} \beta_i [(H^{\otimes n} \otimes I)(2|0^{\otimes n+1}\rangle\langle 0^{\otimes n+1}|)(H^{\otimes n} \otimes I) - (H^{\otimes n} \otimes I)(I^{\otimes n+1})(H^{\otimes n} \otimes I)](|i\rangle \otimes |1\rangle) \\
&= \sum_{i=0}^{N-1} \alpha_i [(H^{\otimes n} (2|0\rangle\langle 0|)H^{\otimes n})|i\rangle \otimes (I|0\rangle\langle 0|I)|0\rangle - (H^{\otimes n} I^{\otimes n} H^{\otimes n})|i\rangle \otimes (III)|0\rangle) \\
&+ \sum_{i=0}^{N-1} \beta_i [(H^{\otimes n} \otimes I)(2|0^{\otimes n+1}\rangle\langle 0^{\otimes n+1}|)(H^{\otimes n} \otimes I) - (H^{\otimes n} \otimes I)(I^{\otimes n+1})(H^{\otimes n} \otimes I)](|i\rangle \otimes |1\rangle) \\
&= \sum_{i=0}^{N-1} \alpha_i \{ [(H^{\otimes n} (2|0\rangle\langle 0|)H^{\otimes n})|i\rangle \otimes |0\rangle - (H^{\otimes n} I^{\otimes n} H^{\otimes n})|i\rangle \otimes |0\rangle) \} \\
&+ \sum_{i=0}^{N-1} \beta_i \{ 2(H^{\otimes n} (|0\rangle\langle 0|)H^{\otimes n})|i\rangle \otimes (I|0\rangle\langle 0|I)|1\rangle - (H^{\otimes n} I^{\otimes n} H^{\otimes n})|i\rangle \otimes (III)|1\rangle \} \\
&= \sum_{i=0}^{N-1} \alpha_i \{ [(H^{\otimes n} (2|0\rangle\langle 0| - I^{\otimes n})H^{\otimes n})|i\rangle \otimes |0\rangle - \sum_{i=0}^{N-1} \beta_i |i\rangle \otimes |1\rangle \} \\
&= \sum_{i=0}^{N-1} \alpha_i [(2 \frac{1}{\sqrt{N}} \sum_i |i\rangle \frac{1}{\sqrt{N}} \sum_j \langle j| - I^{\otimes n})|i\rangle] \otimes |0\rangle - \sum_{i=0}^{N-1} \beta_i |i\rangle \otimes |1\rangle \\
&= \sum_{i=0}^{N-1} \alpha_i [\frac{2}{N} \sum_i |i\rangle \sum_j \langle j| \otimes |0\rangle] - \sum_{i=0}^{N-1} \alpha_i |i\rangle \otimes |0\rangle - \sum_{i=0}^{N-1} \beta_i |i\rangle \otimes |1\rangle \\
&= 2 \sum_{i=0}^{N-1} \frac{\alpha_i}{N} \sum_{i=0}^{N-1} |i\rangle \otimes |0\rangle - \sum_{i=0}^{N-1} \alpha_i |i\rangle \otimes |0\rangle - \sum_{i=0}^{N-1} \beta_i |i\rangle \otimes |1\rangle \\
&= \sum_{i=0}^{N-1} (2\langle \alpha \rangle - \alpha_i) (|i\rangle \otimes |0\rangle) - \sum_{i=0}^{N-1} \beta_i (|i\rangle \otimes |1\rangle)
\end{aligned} \tag{۲۵-۳}$$

که  $\langle \alpha \rangle = (1/N) \sum_{i=0}^{N-1} \alpha_i$  میانگین دامنه‌های زیر فضای  $\sum_{i=0}^{N-1} \alpha_i (|i\rangle \otimes |0\rangle)$  است و  $|0\rangle = |0^{\otimes n}\rangle$ . اثر عملگر  $Y$ ، انعکاس نسبت به میانگین تنها روی زیر فضای  $\sum_{i=0}^{N-1} \alpha_i (|i\rangle \otimes |0\rangle)$  و منفی کردن دامنه‌های زیر فضای  $\sum_{i=0}^{N-1} \beta_i (|i\rangle \otimes |1\rangle)$  است. اگر  $M$  تعداد جواب‌ها،  $\sum_{i=0}^{N-1} \beta_i (|i\rangle \otimes |1\rangle)$  مجموع روی تمام حالت‌های جواب و  $\sum_{i=0}^{N-1} \alpha_i (|i\rangle \otimes |0\rangle)$  مجموع روی حالت‌های غیر جواب باشد، حالت  $|W_2\rangle$  را می‌توان به شکل زیر بازنویسی کرد:

$$|W_2\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (|i\rangle \otimes |0\rangle) + \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (|i\rangle \otimes |1\rangle) \tag{۲۶-۳}$$

مجموع اول شامل  $N$  جمله است، جمله‌هایی که جزو جواب هستند ضریب‌شان صفر است، مجموع دوم نیز شامل  $N$  جمله است، در این مجموع نیز جمله‌هایی که جزو جواب نیستند ضریب‌شان صفر است.

حالت  $|W_3\rangle$  را نیز بازنویسی می‌کنیم:

$$|W_3\rangle = a_1 \sum_{i=0}^{N-1} (|i\rangle \otimes |0\rangle) + b_1 \sum_{i=0}^{N-1} (|i\rangle \otimes |0\rangle) + c_1 \sum_{i=0}^{N-1} (|i\rangle \otimes |1\rangle) \quad (27-3)$$

که ضرایب عبارتند از:

$$a_1 = 2\langle\alpha_1\rangle - \frac{1}{\sqrt{N}} \quad ; \quad b_1 = 2\langle\alpha_1\rangle \quad ; \quad c_1 = \frac{-1}{\sqrt{N}} \quad ; \quad \langle\alpha_1\rangle = \left(\frac{N-M}{N\sqrt{N}}\right) \quad (28-3)$$

و شرط زیر ناشی از یک بودن مجموع احتمالات بین این ضرایب برقرار است:

$$(N-M)a_1^2 + Mb_1^2 + Mc_1^2 = 1 \quad (29-3)$$

(۴) روی  $n$  کیوبیت اول اندازه‌گیری انجام می‌دهیم. جواب مورد نظر با احتمال بالاتر از  $88/87\%$  به دست می‌آید.

احتمال موفقیت  $P_s$  در اولین تکرار برابر است با:

$$P_s = M(b_1^2 + c_1^2) = M \left( \left( \frac{2(N-M)}{N\sqrt{N}} \right)^2 + \left( \frac{-1}{\sqrt{N}} \right)^2 \right) = 5 \left( \frac{M}{N} \right) - 8 \left( \frac{M}{N} \right)^2 + 4 \left( \frac{M}{N} \right)^3 \quad (30-3)$$

و احتمال عدم موفقیت  $P_{ns}$  برابر است با:

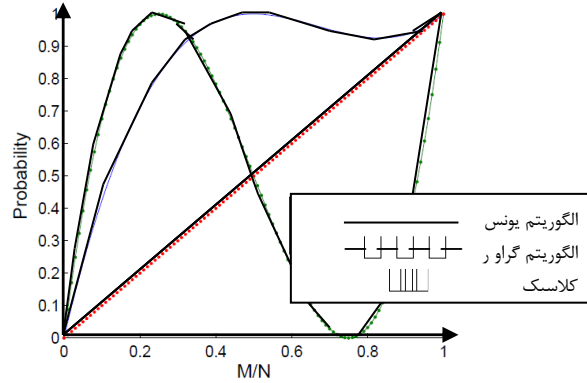
$$P_{ns} = (N-M)a_1^2 \quad (31-3)$$

به طوری که مجموع احتمال موفقیت و عدم موفقیت همواره برابر با یک شود.

$$P_s + P_{ns} = 1 \quad (32-3)$$

احتمال موفقیت در تکرار اول در الگوریتم یونس، گراور و حالت کلاسیکی در نمودار زیر مقایسه شده است.





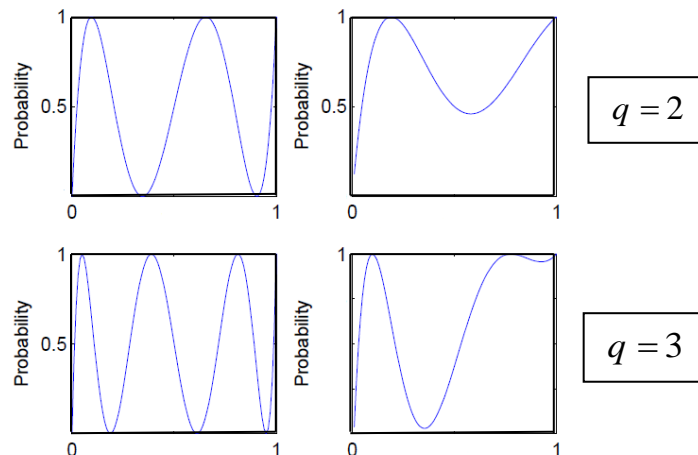
۱۰-۳ مقایسه احتمال موفقیت در تکرار اول الگوریتم یونس، گراور و حالت کلاسیکی

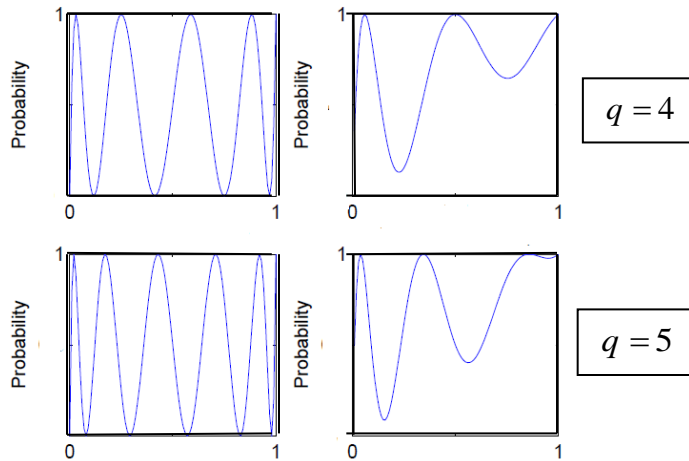
حالت کلی سیستم بعد از  $q \geq 2$  تکرار با رابطه‌ی بازگشتی زیر توصیف می‌شود:

$$|W_q\rangle = a_q \sum_{i=0}^{N-1} |i\rangle \otimes |0\rangle + b_q \sum_{i=0}^{N-1} |i\rangle \otimes |0\rangle + c_q \sum_{i=0}^{N-1} |i\rangle \otimes |1\rangle \quad (33-3)$$

$$\begin{cases} a_q = 2\langle\alpha_q\rangle - a_{q-1} ; & a_0 = \frac{1}{\sqrt{N}} ; & a_1 = \frac{1}{\sqrt{N}}(2(1 - \frac{M}{N}) - 1) \\ b_q = 2\langle\alpha_q\rangle - c_{q-1} ; & b_0 = \frac{1}{\sqrt{N}} ; & b_1 = 2\frac{1}{\sqrt{N}}(1 - \frac{M}{N}) \\ c_q = -b_{q-1} ; & c_0 = 0 ; & c_1 = -\frac{1}{\sqrt{N}} \\ \langle\alpha_q\rangle = (1 - \frac{M}{N})a_{q-1} + \frac{M}{N}c_{q-1} \end{cases} \quad (34-3)$$

برای تکرارهای دوم تا پنجم نمودارهای احتمال موفقیت بر حسب نسبت  $M/N$  به شکل زیر است:

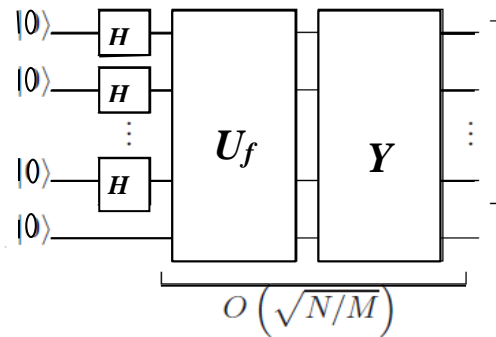




شکل ۳-۱۱ مقایسه‌ی نمودارهای احتمال موفقیت الگوریتم یونس (سمت راست) و گراور (سمت چپ) در تکرارهای دوم

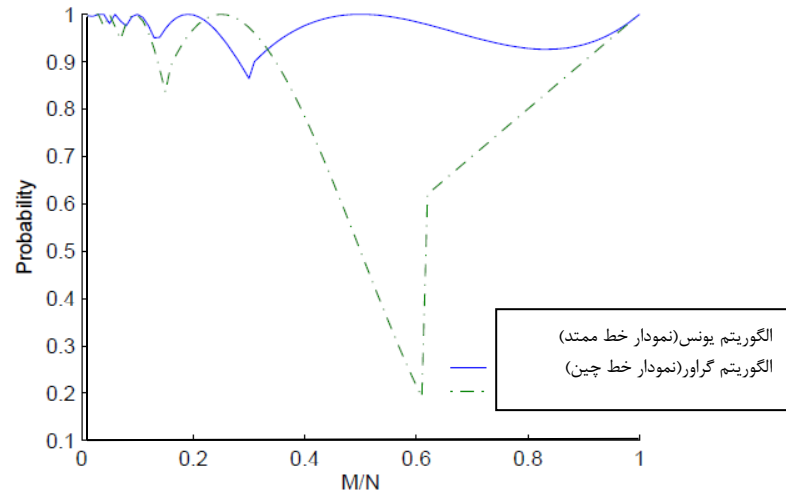
تا پنجم

این الگوریتم چند مزیت نسبت به الگوریتم گراور دارد: اول اینکه الگوریتم گراور تنها برای حالت تک جوابی با احتمال بالا به نتیجه دست می‌یابد و در حالت‌هایی که تعداد جواب‌ها بیش از نیمی از تعداد کل داده‌ها باشد احتمال موفقیت به شدت سقوط می‌کند که این مشکل در الگوریتم یونس وجود ندارد. همچنین احتمال دستیابی به جواب در الگوریتم احمد یونس بیش از الگوریتم گراور است. در نهایت با توجه به تعریف خاص عملگر انتشار جزئی، در هر تکرار نیمی از جواب‌ها به همراه غیر جواب‌ها نسبت به میانگین‌شان انعکاس می‌یابند و دامنه‌ی نیمی دیگر از جواب‌ها منفی می‌شود که همین استفاده‌ی هوشمندانه، نتیجه را با احتمال بالاتری به دست می‌دهد. [54] نمودار الگوریتم احمد یونس به شکل زیر می‌باشد.



شکل ۳-۱۲ نمودار الگوریتم احمد یونس

نمودار احتمال موفقیت الگوریتم یونس در مقایسه با الگوریتم گراور به شکل زیر است. [53]



شکل ۳-۱۳ مقایسه‌ی نمودارهای موفقیت الگوریتم یونس و گراور

# ۴

فصل چهارم: جستجوی کوانتومی با کیوتریت‌ها

## ۴-۱ گیت هادامارد کیوتربیتی

در فصل سوم در بحث گیت‌های کوانتومی به گیت هادامارد که نمایش ماتریسی آن به شکل:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

بود اشاره کردیم. با اعمال گیت هادامارد روی یک پایه‌ی فضا، می‌توانیم برهم‌نهدی از همه‌ی پایه‌ها را با دامنه‌ی یکسان به‌دست آوریم. به‌عنوان مثال اگر به ترتیب در فضای یک، دو، سه و چهار کیوبیتی از عملگر هادامارد استفاده کنیم خواهیم داشت:

$$H |0\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

$$H^{\otimes 2} |00\rangle = \frac{1}{\sqrt{4}} (|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

$$H^{\otimes 3} |000\rangle = \frac{1}{\sqrt{8}} (|000\rangle + |001\rangle + |011\rangle + |101\rangle + |110\rangle + |100\rangle + |010\rangle + |111\rangle) \quad (۱-۴)$$

$$H^{\otimes 4} |0000\rangle = \frac{1}{\sqrt{16}} (|0000\rangle + |0101\rangle + |1010\rangle + |0010\rangle + |0011\rangle + |0111\rangle + |0110\rangle + |1001\rangle + |0001\rangle + |0100\rangle + |1000\rangle + |1100\rangle + |1110\rangle + |1011\rangle + |1101\rangle + |1111\rangle)$$

همان‌طور که می‌بینیم همه‌ی پایه‌های این فضاها با دامنه‌ی یکسان ایجاد می‌شوند. در فضای کیوتربیتی ابتدا نیاز داریم هاداماردی متناظر با هادامارد کیوبیتی تعریف کنیم، به‌قسمی که با اعمال آن بر حالت  $|0^{\otimes n}\rangle$  کیوتربیتی، تمام پایه‌های فضا با دامنه‌ی یکسان ایجاد شود. بدین منظور عملگری معرفی کنیم که به‌صورت زیر تعریف می‌شود: [۵۷]

$$H = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & e^{i\frac{2\pi}{3}} & e^{i\frac{4\pi}{3}} \\ 1 & e^{i\frac{4\pi}{3}} & e^{i\frac{2\pi}{3}} \end{pmatrix} \quad (۲-۴)$$

با اعمال این گیت روی پایه‌ی  $|0^{\otimes n}\rangle$  همه‌ی پایه‌های فضای  $N = 3^n$  بعدی با دامنه‌ی یکسان ظاهر می‌شوند. تفاوتی که این هادامارد با هادامارد کیوبیتی دارد نحوه‌ی عمل بر روی دیگر پایه‌های فضا می‌باشد. اثر عملگر هادامارد کیوبیتی بر روی دیگر پایه‌های فضا نیز ایجاد برهم‌نهدی از کل پایه‌ها با دامنه‌ی یکسان با ضرایب فاز  $e^{\pm i\pi}$  است، اما با اعمال عملگر هادامارد کیوتربیتی روی پایه‌های  $|1\rangle, |2\rangle$  علاوه بر دامنه‌ی یکسان تمام

پایه‌ها،  $(1/\sqrt{N})$ ، برای برخی پایه‌ها جملات فاز متفاوت با حالت کیوبیتی ظاهر می‌شود. برای یک، دو، سه و چهار کیوبیت در حالت  $|0\rangle$  داریم:

$$H|0\rangle = \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle)$$

$$H^{\otimes 2}|00\rangle = \frac{1}{\sqrt{9}}(|00\rangle + |01\rangle + |10\rangle + \dots + |22\rangle) \quad (3-4)$$

$$H^{\otimes 3}|000\rangle = \frac{1}{\sqrt{27}}(|000\rangle + |001\rangle + |011\rangle + |101\rangle + |110\rangle + \dots + |222\rangle)$$

$$H^{\otimes 4}|0000\rangle = \frac{1}{\sqrt{81}}(|0000\rangle + |0101\rangle + |1010\rangle + |0010\rangle + \dots + |2222\rangle)$$

در الگوریتم‌هایی که در ادامه معرفی خواهند شد از این عملگر استفاده خواهیم کرد.

#### ۴-۲ سری فوریه کلاسیکی

تبدیل فوریه یک تبدیل انتگرالی است که هر تابع  $f(x)$  را به یک تابع دیگر  $F(x)$  منعکس می‌کند. در این صورت به  $F(x)$  تبدیل فوریه‌ی تابع  $f(x)$  می‌گویند. حالت خاص تبدیل فوریه، سری فوریه نام دارد و آن زمانی کاربرد دارد که تابع  $f(x)$  متناوب باشد. چنانچه تابع متناوب نباشد و یا به عبارتی تناوب آن برابر بی‌نهایت باشد از سری فوریه به راحتی عبارت زیر به دست می‌آید:

$$F(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} f(x) e^{-ikx} dx \quad (4-4)$$

تبدیل فوریه گسسته نیز، برداری از اعداد مختلط  $(x_0, x_1, \dots, x_{N-1})$  به طول  $N$  را به عنوان ورودی دریافت می‌کند و برداری با اعداد مختلط  $(y_0, y_1, \dots, y_{N-1})$  تولید می‌کند که به صورت زیر تعریف می‌شود: [1]

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{\frac{2\pi ijk}{N}} x_j \quad (5-4)$$

#### ۴-۳ تبدیل فوریه کوانتومی با کیوبیت‌ها

تبدیل فوریه‌ی  $n$  کیوبیتی کوانتومی با تبدیل یکانی  $U_{FT}$  تعریف می‌شود که روی پایه‌های محاسباتی متعامد به صورت زیر عمل می‌کند:

$$U_{Fr} |x\rangle_n = \frac{1}{2^{n/2}} \sum_{y=0}^{N-1} e^{\frac{2\pi i xy}{N}} |y\rangle_n \quad (6-4)$$

که  $N = 2^n$ . ضرب  $xy$  در اینجا ضرب معمولی است. تبدیل فوریه، نرمالیزه به یک بوده و دو تبدیل متعامدند مگر در حالت  $x = x'$ .

از آنجائی که کیوبیت، سیستم کوانتومی دو حالته است، یک رشته‌ی  $n$  کیوبیتی می‌تواند  $2^n$  داده را در خود ذخیره نماید. اگر  $n$  عددی صحیح باشد،  $N = 2^n$ . با معرفی نمادگذاری‌های زیر: تعداد کیوبیت‌ها:

پایه‌های محاسباتی برای یک کامپیوتر  $n$  کیوبیتی:  $|0\rangle, |1\rangle, |2\rangle, \dots, |2^{n-1}\rangle$

نمایش حالت  $|j\rangle$  در مبنای ۲:

$$|j\rangle = |j_1 j_2 j_3 \dots j_n\rangle \quad (7-4)$$

که  $j$  برابر است با:

$$j = j_1 2^{n-1} + j_2 2^{n-2} + j_3 2^{n-3} + \dots + j_n 2^0 = \sum_{i=1}^n j_i 2^{n-i} \quad (8-4)$$

نمایش عدد کسری در مبنای ۲<sup>۱</sup>:

$$0.j_1 j_{l+1} \dots j_m = \frac{j_1}{2} + \frac{j_{l+1}}{4} + \dots + \frac{j_m}{2^{m-l+1}} \quad (9-4)$$

با شروع از صورت اولیه‌ی تبدیل فوریه داریم:

$$\begin{aligned} |j\rangle &\xrightarrow{U_{Fr}} \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi i j k / 2^n} |k\rangle = \frac{1}{2^{n/2}} \sum_{k_1=0}^1 \dots \sum_{k_n=0}^1 e^{2\pi i j (\sum_{l=1}^n k_l 2^{-l})} |k_1 \dots k_n\rangle \\ &= \frac{1}{2^{n/2}} \sum_{k_1=0}^1 \dots \sum_{k_n=0}^1 \bigotimes_{l=1}^n e^{2\pi i j k_l 2^{-l}} |k_l\rangle \\ &= \frac{1}{2^{n/2}} \bigotimes_{l=1}^n \left[ \sum_{k_l=0}^1 e^{2\pi i j k_l 2^{-l}} |k_l\rangle \right] \end{aligned} \quad (10-4)$$

<sup>1</sup> Binary friction

$$\begin{aligned}
&= \frac{1}{2^{n/2}} \bigotimes_{l=1}^n [ |0\rangle + e^{2\pi i j 2^{-l}} |1\rangle ] \\
&= \frac{(|0\rangle + e^{2\pi i 0 \cdot j_n} |1\rangle)(|0\rangle + e^{2\pi i 0 \cdot j_{n-1} j_n} |1\rangle) \dots (|0\rangle + e^{2\pi i 0 \cdot j_1 j_2 \dots j_n} |1\rangle)}{2^{n/2}}
\end{aligned}$$

تعریف حاصل ضربی فوق بسیار مفید است. این تعریف به ما اجازه می‌دهد مدار کوانتومی مناسبی برای تبدیل فوریه بسازیم. [1]

#### ۴-۴ تبدیل فوریه‌ی کوانتومی با کیوتریت‌ها

برای کیوتریت‌ها صورت اولیه‌ی تبدیل، مشابه حالت کیوبیتی است، در نتیجه تبدیل فوریه روی یک حالت کیوتریتی برابر است با:

$$|j\rangle \xrightarrow{U_F} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i j k}{N}} |k\rangle \quad (11-4)$$

که  $N = 3^n$ . با معرفی نمادگذاری‌های زیر:

$n$  تعداد کیوتریت‌ها:

$|0\rangle, |1\rangle, |2\rangle, \dots, |3^{n-1}\rangle$  پایه‌های محاسباتی برای یک کامپیوتر  $n$  کیوتریتی:

نمایش حالت  $|j\rangle$  در مبنای ۳:

$$|j\rangle = |j_1 j_2 j_3 \dots j_n\rangle \quad (12-4)$$

که  $j$  برابر است با:

$$j = j_1 3^{n-1} + j_2 3^{n-2} + j_3 3^{n-3} + \dots + j_n 3^0 = \sum_{i=1}^n j_i 3^{n-i} \quad (13-4)$$

نمایش عدد کسری در مبنای ۳<sup>۱</sup>:

$$0.j_l j_{l+1} \dots j_m = \frac{j_l}{3} + \frac{j_{l+1}}{9} + \dots + \frac{j_m}{3^{m-l+1}} \quad (14-4)$$

با اعمال تغییرات ناشی از تبدیل حافظه‌ی کیوبیتی به کیوتریتی، رابطه‌ی (۱۱-۴) را به صورت زیر می‌نویسیم:

<sup>1</sup> Trinary fraction



$$|j\rangle \xrightarrow{U_F} \frac{1}{3^{\frac{n}{2}}} \sum_{k=0}^{3^n-1} e^{\frac{2\pi ijk}{3^n}} |k\rangle \quad (15-4)$$

با جایگذاری  $k = \sum_{i=1}^n k_i 3^{n-i}$  از رابطه ی

$$|j\rangle \xrightarrow{U_F} \frac{1}{3^{\frac{n}{2}}} \sum_{k=0}^{3^n-1} e^{\frac{2\pi ijk}{3^n}} |k\rangle = \frac{1}{3^{\frac{n}{2}}} \sum_{k=0}^{3^n-1} e^{\frac{2\pi ij}{3^n} (\sum_{l=1}^n k_l 3^{n-l})} |k\rangle \quad (16-4)$$

با تقسیم  $\sum$  ی از 0 تا  $N-1=3^n-1$  به  $N=3^n$  تا  $\sum$  ی از 0 تا 2 داریم:

$$\begin{aligned} |j\rangle &\rightarrow \frac{1}{3^{\frac{n}{2}}} \sum_{k=0}^{3^n-1} e^{\frac{2\pi ij}{3^n} (\sum_{l=1}^n k_l 3^{n-l})} |k\rangle = \frac{1}{3^{\frac{n}{2}}} \sum_{k_1=0}^2 \sum_{k_2=0}^2 \dots \sum_{k_n=0}^2 e^{\frac{2\pi ij}{3^n} (\sum_{l=1}^n k_l 3^{n-l})} |k_1 k_2 \dots k_n\rangle \\ &= \frac{1}{3^{\frac{n}{2}}} \sum_{k_1=0}^2 \sum_{k_2=0}^2 \dots \sum_{k_n=0}^2 \otimes_{l=1}^n e^{2\pi i j k_l 3^{-l}} |k_l\rangle = \frac{1}{3^{\frac{n}{2}}} \otimes_{l=1}^n \sum_{k_l=0}^2 e^{2\pi i j k_l 3^{-l}} |k_l\rangle \quad (17-4) \\ &= \frac{1}{3^{\frac{n}{2}}} \otimes_{l=1}^n [|0\rangle + e^{2\pi i j 3^{-l}} |1\rangle + e^{2\pi i j (2)3^{-l}} |2\rangle] = \frac{1}{3^{\frac{n}{2}}} \otimes_{l=1}^n [|0\rangle + e^{2\pi i j 3^{-l}} |1\rangle + e^{4\pi i j 3^{-l}} |2\rangle] \end{aligned}$$

صورت نهایی رابطه ی فوق را می توان به شکل زیر بازنویسی کرد:

$$\begin{aligned} |j\rangle \xrightarrow{U_F} \frac{1}{3^{\frac{n}{2}}} [ &(|0\rangle + e^{2\pi i 0 \cdot j_n} |1\rangle + e^{4\pi i 0 \cdot j_n} |2\rangle) \otimes (|0\rangle + e^{2\pi i 0 \cdot j_{n-1} j_n} |1\rangle + e^{4\pi i 0 \cdot j_{n-1} j_n} |2\rangle) \\ &\otimes \dots \otimes (|0\rangle + e^{2\pi i 0 \cdot j_1 j_2 \dots j_n} |1\rangle + e^{4\pi i 0 \cdot j_1 j_2 \dots j_n} |2\rangle)] \quad (18-4) \end{aligned}$$

برای مثال، بسط فوق را برای حالت های اول و دوم محاسبه می کنیم. با استفاده از رابطه ی

برای  $l=1$  داریم:  $j = \sum_{i=1}^n j_i 3^{n-i}$

$$\begin{aligned} |j\rangle \xrightarrow{U_F} \frac{1}{3^{\frac{n}{2}}} [ &(|0\rangle + e^{2\pi i 3^{-1} (\sum_{l=1}^n j_l 3^{n-l})} |1\rangle + e^{4\pi i 3^{-1} (\sum_{l=1}^n j_l 3^{n-l})} |2\rangle) \\ &= \frac{1}{3^{\frac{n}{2}}} [ &(|0\rangle + e^{2\pi i (j_1 3^{n-1-1} + j_2 3^{n-2-1} + \dots + j_n 3^{-1})} |1\rangle + e^{4\pi i (j_1 3^{n-1-1} + j_2 3^{n-2-1} + \dots + j_{n-1} 3^0 + j_n 3^{-1})} |2\rangle) \end{aligned} \quad (19-4)$$

با اندکی ساده سازی خواهیم داشت:

$$|j\rangle \xrightarrow{U_F} \frac{1}{3^{\frac{n}{2}}} [ |0\rangle + (e^{2\pi i j_1 3^{n-2}} e^{2\pi i j_2 3^{n-3}} e^{2\pi i j_3 3^{n-4}} \dots e^{2\pi i j_n 3^{-1}}) |1\rangle ] \quad (20-4)$$

$$+ (e^{4\pi i j_1 3^{n-2}} e^{4\pi i j_2 3^{n-3}} \dots e^{4\pi i j_{n-1} 3^0} e^{4\pi i j_n 3^{-1}}) |2\rangle ]$$

$$= \frac{1}{3^{\frac{n}{2}}} [ |0\rangle + \left( \prod_{i=1}^n e^{2\pi i j_i 3^{n-i-1}} \right) |1\rangle + \left( \prod_{i=1}^n e^{4\pi i j_i 3^{n-i-1}} \right) |2\rangle ]$$

با استفاده از رابطه‌ی (۴-۱۴) برای نمایش کسری عدد در مبنای ۳ می‌رسیم به :

$$|j\rangle \xrightarrow{U_F} \frac{1}{3^{\frac{n}{2}}} [ |0\rangle + e^{2\pi i 0 \cdot j_n} |1\rangle + e^{4\pi i 0 \cdot j_n} |2\rangle ] \quad (21-4)$$

با انجام محاسبات مشابه برای  $l = 2$  بدست می‌آوریم:

$$|j\rangle \xrightarrow{U_F} \frac{1}{3^{\frac{n}{2}}} [ |0\rangle + e^{2\pi i 0 \cdot j_{n-1} j_n} |1\rangle + e^{4\pi i 0 \cdot j_{n-1} j_n} |2\rangle ] \quad (22-4)$$

#### ۴-۵ سازگاری تبدیل فوریه‌ی کیوتریتی و هادامارد کیوتریتی

همان‌طور که تبدیل فوریه کیوبیتی و هادامارد کیوبیتی برای استفاده در الگوریتم گراور سازگار می‌باشند، با توجه به تعریف تبدیل هادامارد کیوتریتی، مشاهده می‌کنیم این سازگاری در تبدیل فوریه کوانتومی کیوتریتی و تبدیل هادامارد کیوتریتی نیز وجود دارد.

در تعریف هادامارد کیوبیتی، از آنجائی که  $e^{i\pi} = -1$  لذا می‌توان تبدیل هادامارد که به صورت:

$$H^{\otimes n} |x\rangle_n = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle_n \quad (23-4)$$

تعریف می‌شود را به شکل زیر بازنویسی کرد:

$$H^{\otimes n} |x\rangle_n = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} e^{\pi i x \cdot y} |y\rangle_n \quad (24-4)$$

با مقایسه‌ی تعریف تبدیل فوریه،  $U_{Ft} |x\rangle = (1/2^{n/2}) \sum_{y=0}^{2^n-1} e^{\frac{2\pi ixy}{N}} |y\rangle$  و تعریف عملگر هادامارد

$H^{\otimes n} |x\rangle_n = (1/2^{n/2}) \sum_{y=0}^{2^n-1} e^{\pi i x \cdot y} |y\rangle_n$  مشاهده می‌کنیم گذشته از ظاهر شدن توان‌های متفاوت ۲ در نمای

تعریف تبدیل فوریه، تنها تفاوت در تعاریف تبدیل هادامارد و فوریه کیوبیتی در تعریف ضرب  $xy$  می‌باشد. در تبدیل فوریه  $xy$  ضربی معمولی<sup>۱</sup> است درحالی که در تبدیل  $n$  تایی هادامارد،  $xy$  ضرب داخلی بیتی<sup>۲</sup> است که به‌صورت زیر تعریف می‌شود:

$$x \cdot y = x_0 y_0 \oplus x_1 y_1 \oplus \dots \quad (۲۵-۴)$$

که  $\oplus$  نمایشگر باقیمانده‌ی تقسیم بر ۲ می‌باشد که می‌تواند ۰ یا ۱ باشد. [26]

این سازگاری در تشکیل حالت اولیه در الگوریتم گراور مورد استفاده قرار می‌گیرد. بدین ترتیب که اوراکل کمکی در الگوریتم گراور را در حالت  $|1\rangle$  در نظر گرفته و با اعمال هادامارد بر روی آن، حالت  $(1/\sqrt{2})(|0\rangle - |1\rangle)$  ایجاد می‌شود. از طرفی همین بر هم نهی با اعمال تبدیل فوریه بر حالت  $|1\rangle$  به‌دست می‌آید، یعنی:

$$U_{Ft} |j\rangle \rightarrow \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n} |k\rangle \quad (۲۶-۴)$$

$$|j\rangle = 1, \quad n = 1 \quad \Rightarrow 2^n - 1 = 1 \quad (۲۷-۴)$$

$$\begin{aligned} \Rightarrow U_{Ft} |1\rangle &= \frac{1}{2^{1/2}} \sum_{k=0}^1 e^{\frac{2\pi i(1)k}{2}} |k\rangle = \frac{1}{\sqrt{2}} (e^{\frac{2\pi i(1)0}{2}} |0\rangle + e^{\frac{2\pi i(1)1}{2}} |1\rangle) \\ &= \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \end{aligned} \quad (۲۸-۴)$$

در نتیجه:

$$\begin{aligned} H |1\rangle &= \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \\ U_{Ft} |1\rangle &= \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \end{aligned} \quad (۲۹-۴)$$

<sup>1</sup> Ordinary multiplication

<sup>2</sup> Bitwise inner product

مشاهده می‌کنیم برهم‌نهدی که از اعمال هادامارد بر حالت  $|1\rangle$  ایجاد می‌شود از اعمال تبدیل فوریه بر آن نیز به دست می‌آید. حال برای حالت کیوتریتی داریم:

$$U_{Ft} |j\rangle = \frac{1}{3^{\frac{n}{2}}} \sum_{k=0}^{3^n-1} e^{\frac{2\pi ijk}{3^n}} |k\rangle$$

$$|j\rangle = 1, \quad n=1 \Rightarrow 3^n - 1 = 2$$

$$\Rightarrow U_{Ft} |1\rangle = \frac{1}{3^{\frac{1}{2}}} \sum_{k=0}^2 e^{\frac{2\pi i(1)k}{3^1}} |k\rangle = \frac{1}{\sqrt{3}} (e^{\frac{2\pi i(1)0}{3^1}} |0\rangle + e^{\frac{2\pi i(1)1}{3^1}} |1\rangle + e^{\frac{2\pi i(1)2}{3^1}} |2\rangle) \quad (30-4)$$

$$= \frac{1}{\sqrt{3}} (|0\rangle + e^{\frac{2\pi i}{3}} |1\rangle + e^{\frac{4\pi i}{3}} |2\rangle)$$

از طرفی:

$$H |1\rangle = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & e^{i\frac{2\pi}{3}} & e^{i\frac{4\pi}{3}} \\ 1 & e^{i\frac{4\pi}{3}} & e^{i\frac{2\pi}{3}} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ e^{i\frac{2\pi}{3}} \\ e^{i\frac{4\pi}{3}} \end{pmatrix} = \frac{1}{\sqrt{3}} (|0\rangle + e^{\frac{2\pi i}{3}} |1\rangle + e^{\frac{4\pi i}{3}} |2\rangle) \quad (31-4)$$

مجدداً مشاهده می‌کنیم برهم‌نهدی که از اعمال هادامارد بر حالت  $|1\rangle$  کیوتریتی ایجاد می‌شود از اعمال تبدیل فوریه کیوتریتی بر آن نیز به دست می‌آید.

#### ۶-۴ - گیت کیوتریتی

با استفاده از تعریف  $f$  گیت ( $U_f$ ) برای کیوبیت‌ها که به صورت زیر بود: [32]

$$|x\rangle |y\rangle \xrightarrow{U_f} |x\rangle |y \oplus f(x) \bmod 2^m\rangle \quad (32-4)$$

اگر کیوبیت هدف را در حالت  $|0\rangle$  در نظر بگیریم خواهیم داشت:

$$|y\rangle = |0\rangle$$

$$\Rightarrow |x\rangle |0\rangle \xrightarrow{U_f} |x\rangle |0 + f(x)\rangle = |x\rangle |f(x)\rangle \quad (33-4)$$

$$\Rightarrow \sum_x |x\rangle |0\rangle \xrightarrow{U_f} \sum_x |x\rangle |f(x)\rangle$$

حال اگر به جای کیوبیت هدف  $|y\rangle$  در رابطه‌ی (۴-۳۳) داشته باشیم (که حالت  $|u\rangle$  از اعمال تبدیل فوریه بر حالت  $|1\rangle$  به دست می‌آید):

$$\begin{aligned}
 |y\rangle \rightarrow |u\rangle &= \frac{1}{2^{m/2}} \sum_{y=0}^{2^m-1} e^{-2\pi i y / 2^m} |y\rangle \\
 \Rightarrow \sum_x |x\rangle |u\rangle &\xrightarrow{U_f} \sum_x (2^{-m/2} |x\rangle \sum_{y=0}^{2^m-1} e^{-2\pi i y / 2^m} |y + f(x)\rangle) \\
 &= \sum_x (2^{-m/2} e^{2\pi i f(x)/2^m} |x\rangle \sum_{y=0}^{2^m-1} e^{-2\pi i (y + f(x))/2^m} |y + f(x)\rangle)
 \end{aligned} \tag{۴-۳۴}$$

با اندیس‌گذاری مجدد جمع داخل پرانتز خواهیم داشت:

$$\begin{aligned}
 \Rightarrow \sum_x |x\rangle |u\rangle &\xrightarrow{U_f} \sum_x (2^{-m/2} e^{2\pi i f(x)/2^m} |x\rangle \sum_{y=0}^{2^m-1} e^{-2\pi i y / 2^m} |y\rangle) \\
 &= \sum_x e^{2\pi i f(x)/2^m} |x\rangle |u\rangle
 \end{aligned} \tag{۴-۳۵}$$

حال اگر در رابطه‌ی  $|u\rangle = \frac{1}{2^{m/2}} \sum_{y=0}^{2^m-1} e^{-2\pi i y / 2^m} |y\rangle$  مقدار  $m = 1$  باشد:

$$|u\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \tag{۴-۳۶}$$

$$\begin{aligned}
 \Rightarrow \sum_x |x\rangle |u\rangle &\xrightarrow{U_f} \sum_x e^{2\pi i / 2^m} |x\rangle |u\rangle \\
 \Rightarrow \sum_x |x\rangle \frac{1}{\sqrt{2}} [|0\rangle - |1\rangle] &\xrightarrow{U_f} \sum_x e^{2\pi i / 2^m} |x\rangle |u\rangle = \sum_x (-1)^{f(x)} |x\rangle \frac{1}{\sqrt{2}} [|0\rangle - |1\rangle]
 \end{aligned}$$

با استفاده از ضریب  $(-1)^{f(x)}$  و دو مقداری بودن  $f(x)$ ، همان‌طور که در فصل سوم اشاره شد، به حالت‌های جواب تغییر فاز  $\pi$  رادین اعمال می‌شود.

حال برای کیوتریت،  $-f$  گیتی معرفی می‌کنیم که مشابه با حالت کیوبیتی، ولی در مبنای ۳ عمل می‌کند. برای کیوتریت داریم:

$$|x\rangle |y\rangle \xrightarrow{U_f} |x\rangle |y \oplus f(x) \bmod 3^m\rangle \tag{۴-۳۷}$$

در اینجا  $\oplus$  باقیمانده‌ی تقسیم بر ۳ را نشان می‌دهد که می‌تواند ۰، ۱ و ۲ باشد.

اگر مشابه با حالت کیوبیتی الگوریتم گراور، کیوبیت هدف را در حالت  $|0\rangle$  در نظر بگیریم خواهیم داشت:

$$\begin{aligned}
|y\rangle &= |0\rangle \\
\Rightarrow |x\rangle |0\rangle &\xrightarrow{U_f} |x\rangle |f(x)\rangle \quad (38-4) \\
\Rightarrow \sum_x |x\rangle |0\rangle &\xrightarrow{U_f} \sum_x |x\rangle |f(x)\rangle
\end{aligned}$$

حال اگر به جای کیوبیت هدف  $y$  داشته باشیم:

$$|y\rangle \rightarrow |w\rangle = \frac{1}{3^{m/2}} \sum_{y=0}^{3^m-1} e^{\frac{2\pi i}{3^m} y} |y\rangle \quad (39-4)$$

$$\begin{aligned}
\Rightarrow \sum_x |x\rangle |w\rangle &\xrightarrow{U_f} \sum_x \frac{1}{3^{m/2}} |x\rangle \sum_{y=0}^{3^m-1} e^{\frac{-2\pi i}{3^m} y} |y+f(x)\rangle \\
&= \sum_x \frac{1}{3^{m/2}} e^{\frac{2\pi i}{3^m} f(x)} |x\rangle \sum_{y=0}^{3^m-1} e^{\frac{-2\pi i}{3^m} (y+f(x))} |y+f(x)\rangle \quad (40-4) \\
&= \sum_x e^{\frac{+2\pi i}{3^m} f(x)} |x\rangle |w\rangle
\end{aligned}$$

در نتیجه با ایجاد حالت مشابه با الگوریتم کیوبیتی گراور، با اعمال عملگر  $U_f$  بر حالت کیوتریتی، فاز  $e^{2\pi i f(x)/3^m}$  ظاهر می‌شود:

$$\Rightarrow \sum_x |x\rangle |w\rangle \xrightarrow{U_f} \sum_x e^{\frac{2\pi i f(x)}{3^m}} |x\rangle |w\rangle \quad (41-4)$$

اگر  $|w\rangle$  را به صورت  $|y\rangle = (1/3^{m/2}) \sum_{y=0}^{3^m-1} e^{\frac{2\pi i}{3^m} y}$  تعریف می‌کردیم عامل فاز  $\sum_x e^{\frac{2\pi i f(x)}{3^m}} |x\rangle |w\rangle$

ایجاد می‌گردید. هر دو تعریف به نتایج مشابهی منجر می‌شود. ما صورت دوم را به عنوان مبنا در نظر می‌گیریم. از محاسبات فوق در معرفی الگوریتم کیوتریتی گراور استفاده خواهیم نمود.

#### ۷-۴ الگوریتم گراور با کیوتریت‌ها

با توجه به تعریف  $-f$  گیت برای حافظه‌ی کیوبیتی، با اختیار کیوبیت هدف در حالت  $|0\rangle$  اثر  $-f$  گیت به صورت زیر در می‌آید:

$$|x\rangle |0\rangle \rightarrow |x\rangle |f(x)\rangle \quad (42-4)$$

که  $f$ ، می‌تواند مقادیر ۰ و ۱ را اختیار کند.

حال که می‌خواهیم از کیوتریت‌ها به‌عنوان واحد حافظه استفاده کنیم، اگر مشابه با حالت کیوبیتی، کیوتریت کنترل را در حالت  $|0\rangle$  قرار دهیم، اثر  $-f$  گیت مشابه با حالت کیوبیتی خواهد بود، با این تفاوت که مقادیر  $f$  از دو به سه مقدار تغییر می‌یابد، چرا که باقیمانده‌ی تقسیم بر ۳ می‌تواند ۰، ۱ یا ۲ باشد. همین سه مقداری بودن  $-f$  گیت، ما را به استفاده از این امکان در کاربرد کیوتریت هدایت می‌کند. برای پیاده‌سازی الگوریتم گراور با کیوتریت‌ها، دو طرح پیشنهاد می‌شود که هر دو به امکان تولید  $f$ -گیت‌های خاص بستگی دارد. این دو طرح به‌منظور استفاده از هر سه حالت کیوتریت پیشنهاد می‌شود و علاوه بر حالت خاصی که در اینجا جواب زوج و فرد است، برای هر حالت دیگری که در آن بتوان دو شرط برای جواب‌های مطلوب (زوج - فرد) یا سه شرط برای کل داده‌ها (غیر جواب-جواب زوج-جواب فرد) در نظر گرفت با معرفی  $-f$  گیت مناسب مربوط به آن شرط‌ها قابل استفاده می‌باشد.

ما در اینجا حالتی را در نظر گرفته‌ایم که حالت اولیه که بر هم نهی از همه‌ی حالت‌ها است، شامل حالت‌های غیرجواب-جواب زوج و جواب فرد باشد. هدف ما یافتن جواب (زوج یا فرد) است. ابتدا به شرح اولین طرح پیشنهادی می‌پردازیم:

#### ۴-۸ الگوی گیت‌های وابسته به تکرار

با توجه به عامل فاز ایجاد شده برای کیوتریت‌ها در الگوریتم کیوتریتی گراور:

$$\sum_x |x\rangle |w\rangle \rightarrow \sum_x e^{-\frac{2\pi i}{3} f(x)} |x\rangle |w\rangle \quad (43-4)$$

ابتدا نیاز به عملگری داریم که بتواند اثر فوق را داشته باشد.

در الگوریتم کیوبیتی گراور که حالت‌های جواب و غیر جواب داشتیم در مرحله‌ی اول، حالت‌های غیر جواب بدون تغییر باقی می‌مانند و حالت جواب،  $\pi$  رادیان تغییر فاز می‌یابد.

در اینجا که سه حالت غیرجواب-جواب زوج و جواب فرد داریم، بر اساس آن سه مقدار مختلف برای  $f$

در نظر می‌گیریم:

$$f(x) = \begin{cases} f(0) & \text{non-matches} \\ f(1) & \text{odd-matches} \\ f(2) & \text{even-matches} \end{cases} \quad (44-4)$$

اگر حالت های غیرجواب- جواب زوج و جواب فرد را به ترتیب با حالت های  $|\zeta\rangle$  و  $|\eta\rangle$  نمایش دهیم و نماد  $Q$  نمایشگر عملگر باشد، می خواهیم عملگری بسازیم که برای حالت های غیرجواب، فاز:

$$Q|\zeta\rangle = e^{-\frac{2\pi i}{3}f^{(0)}}|\zeta\rangle \quad (45-4)$$

برای حالت جواب فرد، فاز:

$$Q|\eta\rangle = e^{-\frac{2\pi i}{3}f^{(1)}}|\eta\rangle \quad (46-4)$$

و برای حالت جواب زوج، فاز:

$$Q|\xi\rangle = e^{-\frac{2\pi i}{3}f^{(2)}}|\xi\rangle \quad (47-4)$$

را ایجاد کند. عملگر یکانی ای که برای این منظور معرفی می کنیم عبارت است از:

$$Q = \{e^{-\frac{2\pi i}{3}f^{(0)}}(I - |w_{even}\rangle\langle w_{even}| - |w_{odd}\rangle\langle w_{odd}|) + e^{-\frac{2\pi i}{3}f^{(1)}}|w_{odd}\rangle\langle w_{odd}| + e^{-\frac{2\pi i}{3}f^{(2)}}|w_{even}\rangle\langle w_{even}|\} \quad (48-4)$$

حال اثر عملگر فوق را روی حالت اولیه که طبق فرض مان، شامل حالت های غیرجواب- جواب زوج و جواب فرد است را بررسی می کنیم:

$$|\psi_0\rangle = \frac{1}{\sqrt{N}}\{\sum_{i \neq w} |i\rangle + |w_{odd}\rangle + |w_{even}\rangle\} \quad (49-4)$$

اثر عملگر فوق روی سه زیرفضای غیرجواب- جواب زوج و جواب فرد را به طور جداگانه به ترتیب زیر محاسبه می کنیم. برای حالت های غیر جواب:

$$\begin{aligned} Q \frac{1}{\sqrt{N}} \sum_{i \neq w} |i\rangle &= \{e^{-\frac{2\pi i}{3}f^{(0)}}(I - |w_{even}\rangle\langle w_{even}| - |w_{odd}\rangle\langle w_{odd}|) \\ &+ e^{-\frac{2\pi i}{3}f^{(1)}}|w_{odd}\rangle\langle w_{odd}| + e^{-\frac{2\pi i}{3}f^{(2)}}|w_{even}\rangle\langle w_{even}|\} \frac{1}{\sqrt{N}} \sum_{i \neq w} |i\rangle \\ &= e^{-\frac{2\pi i}{3}f^{(0)}} I \frac{1}{\sqrt{N}} \sum_{i \neq w} |i\rangle - e^{-\frac{2\pi i}{3}f^{(0)}} |w_{even}\rangle\langle w_{even}| \frac{1}{\sqrt{N}} \sum_{i \neq w} |i\rangle - e^{-\frac{2\pi i}{3}f^{(0)}} |w_{odd}\rangle\langle w_{odd}| \frac{1}{\sqrt{N}} \sum_{i \neq w} |i\rangle \\ &+ e^{-\frac{2\pi i}{3}f^{(1)}} |w_{odd}\rangle\langle w_{odd}| \frac{1}{\sqrt{N}} \sum_{i \neq w} |i\rangle + e^{-\frac{2\pi i}{3}f^{(2)}} |w_{even}\rangle\langle w_{even}| \frac{1}{\sqrt{N}} \sum_{i \neq w} |i\rangle = e^{-\frac{2\pi i}{3}f^{(0)}} \frac{1}{\sqrt{N}} \sum_{i \neq w} |i\rangle \end{aligned} \quad (50-4)$$



برای حالت جواب زوج:

$$\begin{aligned}
 Q \frac{1}{\sqrt{N}} |w_{\text{even}}\rangle &= \{ e^{-\frac{2\pi i}{3} f(0)} (I - |w_{\text{even}}\rangle\langle w_{\text{even}}| - |w_{\text{odd}}\rangle\langle w_{\text{odd}}|) \\
 &+ e^{-\frac{2\pi i}{3} f(1)} |w_{\text{odd}}\rangle\langle w_{\text{odd}}| + e^{-\frac{2\pi i}{3} f(2)} |w_{\text{even}}\rangle\langle w_{\text{even}}| \} \frac{1}{\sqrt{N}} |w_{\text{even}}\rangle \quad (51-4) \\
 &= e^{-\frac{2\pi i}{3} f(0)} I \frac{1}{\sqrt{N}} |w_{\text{even}}\rangle - e^{-\frac{2\pi i}{3} f(0)} |w_{\text{even}}\rangle\langle w_{\text{even}}| \frac{1}{\sqrt{N}} |w_{\text{even}}\rangle \\
 &- e^{-\frac{2\pi i}{3} f(0)} |w_{\text{odd}}\rangle\langle w_{\text{odd}}| \frac{1}{\sqrt{N}} |w_{\text{even}}\rangle + e^{-\frac{2\pi i}{3} f(1)} |w_{\text{odd}}\rangle\langle w_{\text{odd}}| \frac{1}{\sqrt{N}} |w_{\text{even}}\rangle \\
 &+ e^{-\frac{2\pi i}{3} f(2)} |w_{\text{even}}\rangle\langle w_{\text{even}}| \frac{1}{\sqrt{N}} |w_{\text{even}}\rangle = e^{-\frac{2\pi i}{3} f(2)} \frac{1}{\sqrt{N}} |w_{\text{even}}\rangle
 \end{aligned}$$

و برای حالت جواب فرد داریم:

$$\begin{aligned}
 Q \frac{1}{\sqrt{N}} |w_{\text{odd}}\rangle &= \{ e^{-\frac{2\pi i}{3} f(0)} (I - |w_{\text{even}}\rangle\langle w_{\text{even}}| - |w_{\text{odd}}\rangle\langle w_{\text{odd}}|) \\
 &+ e^{-\frac{2\pi i}{3} f(1)} |w_{\text{odd}}\rangle\langle w_{\text{odd}}| + e^{-\frac{2\pi i}{3} f(2)} |w_{\text{even}}\rangle\langle w_{\text{even}}| \} \frac{1}{\sqrt{N}} |w_{\text{odd}}\rangle \\
 &= e^{-\frac{2\pi i}{3} f(0)} I \frac{1}{\sqrt{N}} |w_{\text{odd}}\rangle - e^{-\frac{2\pi i}{3} f(0)} |w_{\text{even}}\rangle\langle w_{\text{even}}| \frac{1}{\sqrt{N}} |w_{\text{odd}}\rangle \quad (52-4) \\
 &- e^{-\frac{2\pi i}{3} f(0)} |w_{\text{odd}}\rangle\langle w_{\text{odd}}| \frac{1}{\sqrt{N}} |w_{\text{odd}}\rangle + e^{-\frac{2\pi i}{3} f(1)} |w_{\text{odd}}\rangle\langle w_{\text{odd}}| \frac{1}{\sqrt{N}} |w_{\text{odd}}\rangle \\
 &+ e^{-\frac{2\pi i}{3} f(2)} |w_{\text{even}}\rangle\langle w_{\text{even}}| \frac{1}{\sqrt{N}} |w_{\text{odd}}\rangle = e^{-\frac{2\pi i}{3} f(1)} \frac{1}{\sqrt{N}} |w_{\text{odd}}\rangle
 \end{aligned}$$

عملگر  $Q$  یکانی است. (پیوست ۱)

$$QQ^t = I \quad (53-4)$$

حال می‌خواهیم  $f(0)$  و  $f(1)$  و  $f(2)$  را به‌گونه‌ای انتخاب کنیم که در تکرار زوج، دامنه‌ی جواب زوج و در تکرار فرد، دامنه‌ی جواب فرد منفی شود و در عین حال فاز حالت‌های غیر جواب تغییر نکند. اگر مقادیر  $f(0)$  و  $f(1)$  و  $f(2)$  را به‌ترتیب زیر انتخاب کنیم به هدف مطلوب خواهیم رسید:

$$f(x) = \begin{cases} f(0) = 0 & \text{non-matches} \\ f(1) = \begin{cases} \frac{3}{2k} & \text{odd-matches} \\ \frac{3}{k} & \text{even-matches} \end{cases} \\ f(2) = \begin{cases} \frac{3}{k} & \text{odd-matches} \\ \frac{3}{2k} & \text{even-matches} \end{cases} \end{cases} \quad (54-4)$$

اگر  $k$  شماره‌ی تکرار باشد و  $k \bmod 2 = \chi$ ، در نتیجه  $(k+1) \bmod 2 = \chi \oplus 1$ ، می‌توان  $f$  های مورد نظر را در رابطه‌ی زیر خلاصه نمود:

$$f(x) = \begin{cases} f(0) = 0 & \text{non-matches} \\ f(1) = \chi \frac{3}{2k} + (\chi \oplus 1) \frac{3}{k} \\ f(2) = (\chi \oplus 1) \frac{3}{2k} + \chi \frac{3}{k} \end{cases} \quad \text{odd \& even matches} \quad (55-4)$$

در این صورت فاز جواب‌های زوج و فرد، یک در میان منفی می‌شوند.

جدول ۱-۴ فاز دامنه‌ی جواب‌های مربوط به هر تکرار

شماره‌ی تکرار	۱	۲	۳	۴	۵	...
فاز دامنه‌ی جواب زوج	$(\frac{2\pi i}{3})f(2)$	$2(\frac{2\pi i}{3})f(2)$	$3(\frac{2\pi i}{3})f(2)$	$4(\frac{2\pi i}{3})f(2)$	$5(\frac{2\pi i}{3})f(2)$	...
فاز دامنه‌ی جواب فرد	$(\frac{2\pi i}{3})f(1)$	$2(\frac{2\pi i}{3})f(1)$	$3(\frac{2\pi i}{3})f(1)$	$4(\frac{2\pi i}{3})f(1)$	$5(\frac{2\pi i}{3})f(1)$	...

به‌عنوان مثال می‌خواهیم در تکرار اول، دوم و سوم، فازها به‌گونه‌ی زیر باشند:

در تکرار اول:

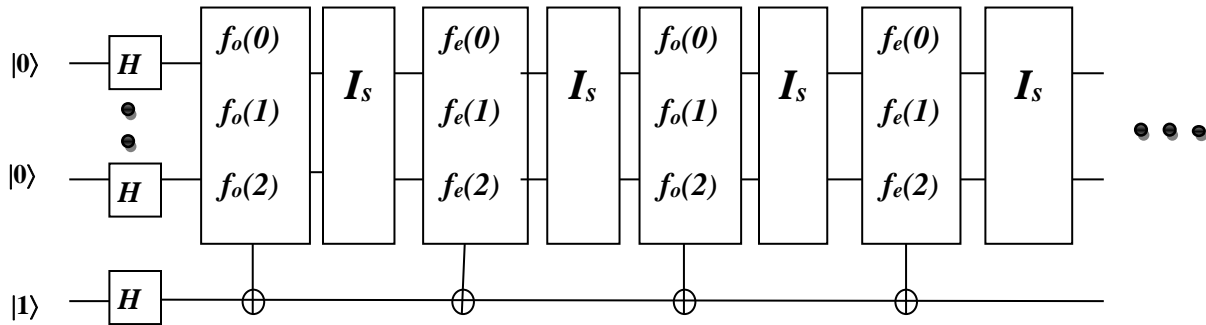
$$k = 1: \begin{cases} e^{\frac{2\pi i}{3} f(1)} = e^{i\pi} \Rightarrow \frac{2\pi i}{3} f(1) = i\pi \Rightarrow f(1) = \frac{3}{2} = \frac{3}{2(k)} \\ e^{\frac{2\pi i}{3} f(2)} = e^{2i\pi} \Rightarrow \frac{2\pi i}{3} f(2) = 2i\pi \Rightarrow f(2) = \frac{3}{1} = \frac{3}{k} \end{cases} \quad (56-4)$$

در تکرار دوم و سوم:

$$k = 2: \begin{cases} e^{\frac{2\pi i}{3} f(1)} = e^{2i\pi} \Rightarrow 2\frac{2\pi i}{3} f(1) = 2i\pi \Rightarrow f(1) = \frac{3}{2} = \frac{3}{k} \\ e^{\frac{2\pi i}{3} f(2)} = e^{i\pi} \Rightarrow 2\frac{2\pi i}{3} f(2) = i\pi \Rightarrow f(2) = \frac{3}{4} = \frac{3}{2(k)} \end{cases} \quad (57-4)$$

$$k = 3: \begin{cases} e^{\frac{2\pi i}{3} f(1)} = e^{i\pi} \Rightarrow 3\frac{2\pi i}{3} f(1) = i\pi \Rightarrow f(1) = \frac{3}{6} = \frac{3}{2(k)} \\ e^{\frac{2\pi i}{3} f(2)} = e^{2i\pi} \Rightarrow 3\frac{2\pi i}{3} f(2) = 2i\pi \Rightarrow f(2) = \frac{3}{3} = \frac{3}{k} \end{cases} \quad (58-4)$$

و به همین ترتیب برای تکرارهای بالاتر. استفاده از الگوریتم مذکور منوط به امکان ساخت گیت‌های متغیر (وابسته به تعداد تکرار) است. نمودار این الگوریتم به شکل زیر خواهد بود:



شکل ۴-۱ نمودار الگوریتم پیشنهادی گیت وابسته به تکرار

پیشنهاد دوم برای الگوریتم گراور:

#### ۹-۴ الگوی دوازده گیتی

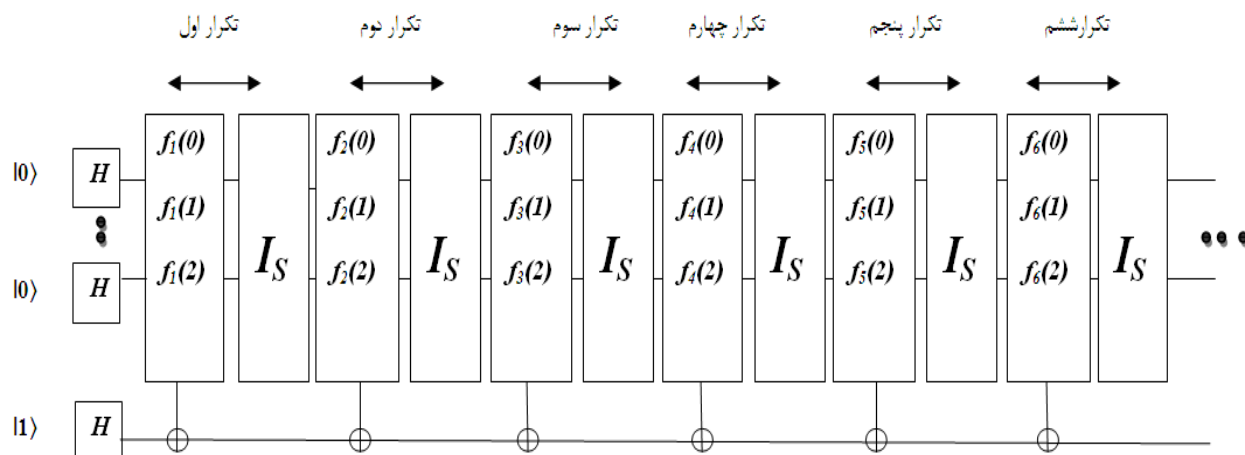
در دومین الگوی پیشنهادی، هم‌چنان علاقه‌مندیم در تکرار زوج، دامنه‌ی جواب زوج و در تکرار فرد، دامنه‌ی جواب فرد منفی شود و در عین حال فاز حالت‌های غیر جواب تغییر نکند. با انتخاب ۶ گیت خاص، به

هدف فوق می‌رسیم. بعد از ۶ تکرار، فازها، با خارج کردن عامل صحیح  $e^{2\pi i}$  و مضارب صحیح آن، تکرار می‌شوند.  $f$  - گیت‌ها به طریق زیر انتخاب می‌شوند:

جدول ۲-۴ مقادیر  $f$  برای تکرارهای اول تا ششم

تکرار اول	$f(1) = 3/2$
	$f(2) = 3$
تکرار دوم	$f(1) = 3/2$
	$f(2) = 3/4$
تکرار سوم	$f(1) = 1/2$
	$f(2) = 1$
تکرار چهارم	$f(1) = 3$
	$f(2) = 3/2$
تکرار پنجم	$f(1) = 3/4$
	$f(2) = 3/2$
تکرار ششم	$f(1) = 1$
	$f(2) = 1/2$

با اندکی دقت متوجه می‌شویم از تکرار سوم تا ششم، مقدار عددی فازها تغییر نمی‌کند، فقط بین  $f(1)$  و  $f(2)$  جابه‌جا می‌شوند. در این طرح نمودار اصلی الگوریتم شامل هر شش تعریف  $f(1)$  و  $f(2)$  می‌باشد و بعد از اعمال هر جفت از  $f$  ها عملگر  $P_{inv}$  اعمال می‌شود. نمودار الگوریتم به شکل زیر خواهد بود.



شکل ۲-۴ نمودار الگوریتم پیشنهادی ۱۲-  $f$  گیتی

#### ۴-۱۰ بیانی دیگر از الگوریتم یونس

الگوریتم احمد یونس در فصل گذشته بررسی شد. حال می‌خواهیم الگوریتم مذکور را با بیانی جدید ارائه داده و برای حالت کلی ضرایب آن، الگوی جدیدی معرفی نماییم. در بیان جدید، حالت اولیه‌ی سیستم مشابه با قبل است:

$$|\varphi_0\rangle = |0^{\otimes n}\rangle |0\rangle \quad (۴-۵۹)$$

با اعمال عملگر هادامارد روی  $n$  کیوبیت اولیه و عملگر یکانی روی کیوبیت کمکی، حالت ایجاد شده برابر خواهد بود با:

$$|\varphi_1\rangle = H^{\otimes n} \otimes I |0^{\otimes n}\rangle |0\rangle = \frac{1}{\sqrt{N}} \sum_i^{N-1} |i\rangle |0\rangle \quad (۴-۶۰)$$

با اعمال عملگر  $U_f$  روی حالت فوق داریم:

$$U_f \frac{1}{\sqrt{N}} \sum_i |i\rangle |0\rangle = \frac{1}{\sqrt{N}} \sum_i |i\rangle |0+f(i)\rangle = \frac{1}{\sqrt{N}} \sum_i (\alpha_i |i\rangle |0\rangle + \beta_i |i\rangle |1\rangle) \quad (۴-۶۱)$$

حالت سیستم با اعمال  $P_{inv}$ :

$$P_{inv} = H^{\otimes n} \otimes I (2|0^{\otimes n+1}\rangle\langle 0^{\otimes n+1}| - I^{\otimes n+1}) H^{\otimes n} \otimes I \quad (۴-۶۲)$$

که می‌توان به صورت زیر نیز نوشت:

$$P_{inv} = 2|\varphi_1\rangle\langle 0| \langle 0| \langle \varphi_1| - I^{\otimes n+1} \quad (۴-۶۳)$$

به دو دسته‌ی جواب‌ها  $\sum \beta_i |i\rangle |1\rangle$  و غیر جواب‌ها  $\sum \alpha_i |i\rangle |0\rangle$  تقسیم می‌شود، که در آن:

$$f(i) = \begin{cases} 1 & \text{if } i \text{ match} \\ 0 & \text{if } i \text{ not match} \end{cases} \quad , \quad \alpha_i = \begin{cases} 0 & \text{if } i \text{ match} \\ 1 & \text{if } i \text{ does not match} \end{cases} \quad , \quad \beta_i = 1 - \alpha_i \quad (۴-۶۴)$$

حالت‌های کلی اعمال عملگر  $U_f$  روی زیر فضاهای ممکن سیستم برابر است با:

$$U_f \sum_i^{N-1} \alpha_i |i\rangle |0\rangle = \sum_i^{N-1} \alpha_i |i\rangle |0\rangle \quad (۴-۶۵)$$

$$U_f \sum_i^{N-1} \beta_i |i\rangle |0\rangle = \sum_i^{N-1} \beta_i |i\rangle |1\rangle$$

$$U_f \sum_i^{N-1} \beta_i |i\rangle |1\rangle = \sum_i^{N-1} \beta_i |i\rangle |0\rangle$$

حالت‌های کلی اعمال عملگر  $P_{inv}$  روی زیر فضاهای ممکن سیستم نیز برابر است با:

$$\begin{aligned}
P_{inv} \sum_i^{N-1} \alpha_i |i\rangle |0\rangle &= 2 \sum_i^{N-1} \alpha_i \left( \sum_j^{N-1} \frac{1}{\sqrt{N}} |j\rangle |0\rangle \right) \left( \sum_k^{N-1} \frac{1}{\sqrt{N}} \langle 0 | \langle k | |i\rangle |0\rangle \right) - \sum_i^{N-1} \alpha_i |i\rangle |0\rangle \\
&= 2 \sum_j^{N-1} \left( \sum_i^{N-1} \frac{\alpha_i}{N} \sum_k^{N-1} \delta_{ki} \right) |j\rangle |0\rangle - \sum_i^{N-1} \alpha_i |i\rangle |0\rangle \\
&= 2 \sum_j^{N-1} \left( \sum_i^{N-1} \frac{\alpha_i}{N} \right) |j\rangle |0\rangle - \sum_i^{N-1} \alpha_i |i\rangle |0\rangle \\
&= 2 \sum_i^{N-1} \bar{\alpha} |i\rangle |0\rangle - \sum_i^{N-1} \alpha_i |i\rangle |0\rangle \\
&= 2 \sum_i^{N-1} \alpha_i \bar{\alpha} |i\rangle |0\rangle + 2 \sum_i^{N-1} \beta_i \bar{\alpha} |i\rangle |0\rangle - \sum_i^{N-1} \alpha_i |i\rangle |0\rangle \\
&= (2\bar{\alpha} - 1) \sum_i^{N-1} \alpha_i |i\rangle |0\rangle + 2\bar{\alpha} \sum_i^{N-1} \beta_i |i\rangle |0\rangle
\end{aligned} \tag{۶۶-۴}$$

که در محاسبه‌ی عبارت فوق از رابطه‌ی  $\sum_i^{N-1} |i\rangle |0\rangle = \sum_i (\alpha_i |i\rangle |0\rangle + \beta_i |i\rangle |0\rangle)$  بهره برده‌ایم.

به طریقی مشابه برای حالت‌های دیگر داریم:

$$P_{inv} \sum_i^{N-1} \beta_i |i\rangle |0\rangle = 2\bar{\beta} \sum_i^{N-1} \alpha_i |i\rangle |0\rangle + (2\bar{\beta} - 1) \sum_i^{N-1} \beta_i |i\rangle |0\rangle \tag{۶۷-۴}$$

$$P_{inv} \sum_i^{N-1} \beta_i |i\rangle |1\rangle = - \sum_i^{N-1} \beta_i |i\rangle |1\rangle$$

که  $\bar{\alpha}, \bar{\beta}$  به صورت زیر تعریف می‌شوند:

$$\bar{\alpha} = \frac{N-M}{N}, \bar{\beta} = \frac{M}{N} \tag{۶۸-۴}$$

با داشتن روابط فوق برای تکرار اول داریم:

$$\begin{aligned}
|\xi_1\rangle &= U_f |\varphi_1\rangle = \frac{1}{\sqrt{N}} \sum_i^{N-1} (\alpha_i |i\rangle |0\rangle + \beta_i |i\rangle |1\rangle) \\
|\psi_1\rangle &= P_{inv} |\xi_1\rangle = \frac{A_1}{\sqrt{N}} \sum_i^{N-1} \alpha_i |i\rangle |0\rangle + \frac{B_1^0}{\sqrt{N}} \sum_i^{N-1} \beta_i |i\rangle |0\rangle + \frac{B_1^1}{\sqrt{N}} \sum_i^{N-1} \beta_i |i\rangle |1\rangle
\end{aligned} \tag{۶۹-۴}$$

$$\begin{cases} A_1 = 2\bar{\alpha} - 1 \\ B_1^0 = 2\bar{\alpha} \\ B_1^1 = -1 \end{cases}$$

که اندیس بالای ضرایب، مربوط به کیوبیت کمکی است که حالت سیستم با آن درهم‌تنیده شده است. برای

تکرار دوم داریم:

$$\begin{aligned}
|\xi_2\rangle &= U_f |\psi_1\rangle = \frac{A_1}{\sqrt{N}} \sum_i^{N-1} \alpha_i |i\rangle |0\rangle + \frac{B_1^0}{\sqrt{N}} \sum_i^{N-1} \beta_i |i\rangle |1\rangle + \frac{B_1^1}{\sqrt{N}} \sum_i^{N-1} \beta_i |i\rangle |0\rangle \\
|\psi_2\rangle &= P_{inv} |\xi_2\rangle = \frac{A_2}{\sqrt{N}} \sum_i^{N-1} \alpha_i |i\rangle |0\rangle + \frac{B_2^0}{\sqrt{N}} \sum_i^{N-1} \beta_i |i\rangle |0\rangle + \frac{B_2^1}{\sqrt{N}} \sum_i^{N-1} \beta_i |i\rangle |1\rangle
\end{aligned} \tag{۷۰-۴}$$

$$\begin{cases}
A_2 = A_1(2\bar{\alpha} - 1) + 2B_1^1\bar{\beta} \\
B_2^0 = 2A_1\bar{\alpha} + B_1^1(2\bar{\beta} - 1) \\
B_2^1 = -B_1^0
\end{cases}$$

و به همین ترتیب برای تکرارهای بالاتر. برای حالت کلی سیستم و ضرایب در یک تکرار دلخواه، الگوی زیر را پیشنهاد می‌کنیم:

$$\begin{aligned}
|\psi_k\rangle &= \frac{A_{k+1}}{\sqrt{N}} \sum_i^{N-1} \alpha_i |i\rangle |0\rangle + \frac{B_{k+1}^0}{\sqrt{N}} \sum_i^{N-1} \beta_i |i\rangle |0\rangle + \frac{B_{k+1}^1}{\sqrt{N}} \sum_i^{N-1} \beta_i |i\rangle |1\rangle \\
\begin{cases}
A_{k+1} = A_k(2\bar{\alpha} - 1) + 2B_k^1\bar{\beta} \\
B_{k+1}^0 = 2A_k\bar{\alpha} + B_k^1(2\bar{\beta} - 1) \\
B_{k+1}^1 = -B_k^0
\end{cases}
\end{aligned} \tag{۷۱-۴}$$

که  $k > 1$  می‌باشد و برای حالت  $k = 1$  داریم:

$$\begin{cases}
A_1 = 2\bar{\alpha} - 1 \\
B_1^0 = 2\bar{\alpha} \\
B_1^1 = -1
\end{cases} \tag{۷۲-۴}$$

فرمول کلی ضرایب در [54] برای حالت کلی  $|W_q\rangle = a_q \sum_i^{N-1} |i\rangle |0\rangle + b_q \sum_i^{N-1} |i\rangle |0\rangle + c_q \sum_i^{N-1} |i\rangle |1\rangle$  به شکل زیر معرفی شده است: (در فصل سوم به شکل دیگری از آن اشاره شد).

$$\begin{cases}
a_q = 2\langle \alpha_q \rangle - a_{q-1} \quad , \quad a_0 = s \quad , \quad a_1 = s(2y - 1) \\
b_q = 2\langle \alpha_q \rangle - c_{q-1} \quad , \quad b_0 = s \quad , \quad b_1 = 2sy \\
c_q = -b_{q-1} \quad , \quad c_0 = 0 \quad , \quad c_1 = -s
\end{cases} \tag{۷۳-۴}$$

که ضرایب  $\alpha_q, s, y$  به صورت زیر تعریف می‌شوند:

$$\begin{aligned}
\alpha_q &= (ya_{q-1} + (1-y)c_{q-1}) \\
s &= \frac{1}{\sqrt{N}} \\
y &= 1 - \frac{M}{N}
\end{aligned} \tag{۷۴-۴}$$

با مقایسه‌ی ضرایب تولید شده توسط این الگو و ضرایبی که از الگوی پیشنهادی ما به دست می‌آیند، مشاهده

می‌کنیم هر دو به نتایج یکسانی منجر می‌شوند. در نتیجه قانون ضرایب کلی پیشنهاد شده می‌تواند به‌عنوان یک کلی سازی جدید برای ضرایب الگوریتم کیوبیتی یونس در نظر گرفته شود. به‌عنوان مثال ضرایب چند تکرار اول را از دو الگو محاسبه می‌کنیم:

جدول ۳-۴ مقایسه‌ی ضرایب ۴ تکرار اول الگوریتم یونس با استفاده از فرمول کلی یونس و الگوی پیشنهادی

شماره‌ی تکرار	$\frac{A_{k+1}}{\sqrt{N}}$	$\frac{B_{k+1}^0}{\sqrt{N}}$	$\frac{B_{k+1}^1}{\sqrt{N}}$
تکرار اول	$\frac{1}{\sqrt{N}} - \frac{2M}{N\sqrt{N}}$	$\frac{2}{\sqrt{N}} - \frac{2M}{N\sqrt{N}}$	$-\frac{1}{\sqrt{N}}$
تکرار دوم	$\frac{4M^2}{N^2\sqrt{N}} - \frac{6M}{N\sqrt{N}} + \frac{1}{\sqrt{N}}$	$\frac{4M^2}{N^2\sqrt{N}} - \frac{8M}{N\sqrt{N}} + \frac{3}{\sqrt{N}}$	$-\frac{2}{\sqrt{N}} + \frac{2M}{N\sqrt{N}}$
تکرار سوم	$\frac{-8M^3}{N^3\sqrt{N}} + \frac{20M^2}{N^2\sqrt{N}} - \frac{12M}{N\sqrt{N}} + \frac{1}{\sqrt{N}}$	$\frac{-8M^3}{N^3\sqrt{N}} + \frac{24M^2}{N^2\sqrt{N}} - \frac{20M}{N\sqrt{N}} + \frac{4}{\sqrt{N}}$	$\frac{-4M^2}{N^2\sqrt{N}} + \frac{8M}{N\sqrt{N}} - \frac{3}{\sqrt{N}}$
تکرار چهارم	$\frac{16M^4}{N^4\sqrt{N}} - \frac{56M^3}{N^3\sqrt{N}} + \frac{60M^2}{N^2\sqrt{N}} - \frac{20M}{N\sqrt{N}} + \frac{1}{\sqrt{N}}$	$\frac{16M^4}{N^4\sqrt{N}} - \frac{64M^3}{N^3\sqrt{N}} + \frac{84M^2}{N^2\sqrt{N}} - \frac{40M}{N\sqrt{N}} + \frac{5}{\sqrt{N}}$	$\frac{8M^3}{N^3\sqrt{N}} - \frac{24M^2}{N^2\sqrt{N}} + \frac{20M}{N\sqrt{N}} - \frac{4}{\sqrt{N}}$

شماره‌ی تکرار	$a_q$	$b_q$	$c_q$
تکرار اول	$\frac{1}{\sqrt{N}} - \frac{2M}{N\sqrt{N}}$	$\frac{2}{\sqrt{N}} - \frac{2M}{N\sqrt{N}}$	$-\frac{1}{\sqrt{N}}$
تکرار دوم	$\frac{4M^2}{N^2\sqrt{N}} - \frac{6M}{N\sqrt{N}} + \frac{1}{\sqrt{N}}$	$\frac{4M^2}{N^2\sqrt{N}} - \frac{8M}{N\sqrt{N}} + \frac{3}{\sqrt{N}}$	$-\frac{2}{\sqrt{N}} + \frac{2M}{N\sqrt{N}}$
تکرار سوم	$\frac{-8M^3}{N^3\sqrt{N}} + \frac{20M^2}{N^2\sqrt{N}} - \frac{12M}{N\sqrt{N}} + \frac{1}{\sqrt{N}}$	$\frac{-8M^3}{N^3\sqrt{N}} + \frac{24M^2}{N^2\sqrt{N}} - \frac{20M}{N\sqrt{N}} + \frac{4}{\sqrt{N}}$	$\frac{-4M^2}{N^2\sqrt{N}} + \frac{8M}{N\sqrt{N}} - \frac{3}{\sqrt{N}}$
تکرار چهارم	$\frac{16M^4}{N^4\sqrt{N}} - \frac{56M^3}{N^3\sqrt{N}} + \frac{60M^2}{N^2\sqrt{N}} - \frac{20M}{N\sqrt{N}} + \frac{1}{\sqrt{N}}$	$\frac{16M^4}{N^4\sqrt{N}} - \frac{64M^3}{N^3\sqrt{N}} + \frac{84M^2}{N^2\sqrt{N}} - \frac{40M}{N\sqrt{N}} + \frac{5}{\sqrt{N}}$	$\frac{8M^3}{N^3\sqrt{N}} - \frac{24M^2}{N^2\sqrt{N}} + \frac{20M}{N\sqrt{N}} - \frac{4}{\sqrt{N}}$

#### ۴-۱۱ الگوریتم جستجوی کوانتومی یونس با کیوبریت‌ها:

حال برآنیم تا با بهره بردن از سه حالتی بودن حافظه‌ی کیوبریتی، برای الگوریتم یونس، طرحی را برای استفاده از کیوبریت‌ها به‌عنوان واحدهای حافظه پیاده کنیم. با فرض اینکه دو دسته جواب زوج و فرد داریم به شرح طرح پیشنهادی می‌پردازیم:

$|\psi_0\rangle$  حالت اولیه در الگوریتم یونس برابر است با:

$$|\psi_0\rangle = |0^{\otimes n}\rangle \otimes |0\rangle \quad (۷۵-۴)$$

که متشکل از  $n$  کیوبریت کنترل و یک کیوبریت هدف است.



با اعمال هادامارد کیوتزیتی، برهم‌نهی از همه‌ی حالت‌ها با دامنه‌ی یکسان ایجاد می‌شود که هادامارد  $n$  بعدی روی  $n$  کیوتزیت کنترل اعمال می‌شود و عملگر یکانی روی کیوتزیت هدف:

$$(H^{\otimes n} \otimes I) |\psi_0\rangle = |\psi_1\rangle = \left[ \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle \right] \otimes |0\rangle \quad (76-4)$$

مرحله‌ی بعدی اعمال گیت  $U_f$  است. تابع  $f(x)$  با استفاده از تعریف  $f$ -گیت کیوتزیتی به صورت زیر تعریف می‌شود:

$$f(x) = \begin{cases} 0 & \text{non-matches} \\ 1 & \text{odd-matches} \\ 2 & \text{even-matches} \end{cases} \quad (77-4)$$

که مقدار 0 برای حالت غیر جواب، مقدار 1 برای جواب فرد و مقدار 2 برای جواب زوج است. بدین ترتیب اثر عملگر  $U_f$  ایجاد درهم‌تنیدگی حالت‌های غیر جواب با حالت  $|0\rangle$ ، حالت‌های جواب فرد با حالت  $|1\rangle$  و حالت‌های جواب زوج با  $|2\rangle$  می‌باشد. فرض کرده‌ایم  $|\psi_1\rangle$  برهم‌نهی از همه‌ی حالت‌ها، شامل حالت‌های غیر جواب، جواب زوج و جواب فرد است. با اعمال  $U_f$  کیوتزیتی که به شکل  $|x\rangle |y\rangle \xrightarrow{U_f} |x\rangle |y \oplus f(x) \bmod 3^m\rangle$  تعریف شد داریم:

$$\begin{aligned} |\psi_2\rangle &= U_f |\psi_1\rangle = U_f \left[ \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle \right] \otimes |0\rangle \\ &= U_f \left[ \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle \otimes |0\rangle + 0 \times \sum_{i=0}^{N-1} |i\rangle \otimes |1\rangle + 0 \times \sum_{i=0}^{N-1} |i\rangle \otimes |2\rangle \right] \\ &= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} U_f |i\rangle |0\rangle + 0 \times \sum_{i=0}^{N-1} U_f |i\rangle |1\rangle + 0 \times \sum_{i=0}^{N-1} U_f |i\rangle |2\rangle \\ &= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle \otimes |f(i)\rangle + 0 \times \sum_{i=0}^{N-1} |i\rangle \otimes |1+f(i)\rangle + 0 \times \sum_{i=0}^{N-1} |i\rangle \otimes |2+f(i)\rangle \end{aligned} \quad (78-4)$$

هر کدام از  $\sum$  ها را به سه دسته‌ی: حالت‌های غیر جواب- جواب زوج و جواب فرد تقسیم می‌کنیم، در نتیجه:

$$|\psi_2\rangle = \frac{1}{\sqrt{N}} (\sum^{n-m} |i\rangle|0\rangle + \sum^{o-m} |i\rangle|1\rangle + \sum^{e-m} |i\rangle|2\rangle) \quad (79-4)$$

$$+ 0 \otimes (\sum^{n-m} |i\rangle|1\rangle + \sum^{o-m} |i\rangle|2\rangle + \sum^{e-m} |i\rangle|0\rangle)$$

$$+ 0 \otimes (\sum^{n-m} |i\rangle|2\rangle + \sum^{o-m} |i\rangle|0\rangle + \sum^{e-m} |i\rangle|1\rangle)$$

که علائم  $\sum^{n-m}$  و  $\sum^{o-m}$  و  $\sum^{e-m}$  به ترتیب نشان دهنده‌ی حالت‌های غیرجواب non-matches، جواب‌های فرد

odd-matches و جواب‌های زوج even-matches است. حالت  $|\psi_2\rangle$  را به شکل زیر بازنویسی می‌کنیم:

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{\sqrt{N}} \sum^{n-m} |i\rangle|0\rangle + 0 \otimes \sum^{o-m} |i\rangle|0\rangle + 0 \otimes \sum^{e-m} |i\rangle|0\rangle \\ &+ \frac{1}{\sqrt{N}} \sum^{o-m} |i\rangle|1\rangle + 0 \otimes \sum^{n-m} |i\rangle|1\rangle + 0 \otimes \sum^{e-m} |i\rangle|1\rangle \\ &+ \frac{1}{\sqrt{N}} \sum^{e-m} |i\rangle|2\rangle + 0 \otimes \sum^{o-m} |i\rangle|2\rangle + 0 \otimes \sum^{n-m} |i\rangle|2\rangle \\ &= \sum \alpha_i |i\rangle|0\rangle + \sum \beta_i |i\rangle|1\rangle + \sum \gamma_i |i\rangle|2\rangle \end{aligned} \quad (80-4)$$

که ضرایب به صورت زیر تعریف می‌شوند:

$$\alpha_i = \begin{cases} \frac{1}{\sqrt{N}} & \text{non-matches} \\ 0 & \text{odd-matches} \\ 0 & \text{even-matches} \end{cases} \quad \beta_i = \begin{cases} 0 & \text{non-matches} \\ \frac{1}{\sqrt{N}} & \text{odd-matches} \\ 0 & \text{even-matches} \end{cases} \quad \gamma_i = \begin{cases} 0 & \text{non-matches} \\ 0 & \text{odd-matches} \\ \frac{1}{\sqrt{N}} & \text{even-matches} \end{cases} \quad (81-4)$$

حال  $P_{inv}$  را اعمال می‌کنیم،  $P_{inv}$  به شکل زیر است:

$$P_{inv} = (H^{\otimes n} \otimes I)(2|0^{\otimes n+1}\rangle\langle 0^{\otimes n+1}| - I^{\otimes n+1})(H^{\otimes n} \otimes I) \quad (82-4)$$

در نتیجه:

$$P_{inv} |\psi_2\rangle = P_{inv} \sum \alpha_i |i\rangle|0\rangle + P_{inv} \sum \beta_i |i\rangle|1\rangle + P_{inv} \sum \gamma_i |i\rangle|2\rangle$$

توجه داریم که  $P_{inv}$  یکانی است:

$$\begin{aligned}
P_{inv} &= (H^{\otimes n} \otimes I)(2|0^{\otimes n+1}\rangle\langle 0^{\otimes n+1}| - I^{\otimes n+1})(H^{\otimes n} \otimes I) \\
P_{inv}^\dagger &= (H^{\otimes n} \otimes I)^\dagger(2|0^{\otimes n+1}\rangle\langle 0^{\otimes n+1}| - I^{\otimes n+1})^\dagger(H^{\otimes n} \otimes I)^\dagger \\
&= (H^{\otimes n} \otimes I)(2|0^{\otimes n+1}\rangle\langle 0^{\otimes n+1}| - I^{\otimes n+1})(H^{\otimes n} \otimes I) \\
\Rightarrow P_{inv}P_{inv}^\dagger &= (H^{\otimes n} \otimes I)(2|0^{\otimes n+1}\rangle\langle 0^{\otimes n+1}| - I^{\otimes n+1})(H^{\otimes n} \otimes I)(H^{\otimes n} \otimes I)(2|0^{\otimes n+1}\rangle\langle 0^{\otimes n+1}| - I^{\otimes n+1})(H^{\otimes n} \otimes I) \\
&= (H^{\otimes n} \otimes I)(2|0^{\otimes n+1}\rangle\langle 0^{\otimes n+1}| - I^{\otimes n+1})(2|0^{\otimes n+1}\rangle\langle 0^{\otimes n+1}| - I^{\otimes n+1})(H^{\otimes n} \otimes I) \\
&= (H^{\otimes n} \otimes I)(4|0^{\otimes n+1}\rangle\langle 0^{\otimes n+1}| - 2|0^{\otimes n+1}\rangle\langle 0^{\otimes n+1}| - 2|0^{\otimes n+1}\rangle\langle 0^{\otimes n+1}| + I^{\otimes n+1})(H^{\otimes n} \otimes I) \\
&= (H^{\otimes n} \otimes I)I^{\otimes n+1}(H^{\otimes n} \otimes I) = I^{\otimes n+1}
\end{aligned}$$

نتیجه‌ی اعمال  $P_{inv}$  روی حالت های غیر جواب- جواب زوج و جواب فرد را به ترتیب محاسبه می‌کنیم:

$$\begin{aligned}
P_{inv} \sum_{i=0}^{N-1} \alpha_i |i\rangle \otimes |0\rangle &= \sum_{i=0}^{N-1} \alpha_i [(H^{\otimes n} (2|0^{\otimes n+1}\rangle\langle 0^{\otimes n+1}|)H^{\otimes n})|i\rangle \otimes |0\rangle \langle 0|0\rangle \\
&\quad - (H^{\otimes n} I^{\otimes n} H^{\otimes n})|i\rangle \otimes (I \otimes I \otimes I)|0\rangle] \\
&= \sum_{i=0}^{N-1} (2\langle \alpha \rangle - \alpha_i) |i\rangle \otimes |0\rangle
\end{aligned} \tag{۸۳-۴}$$

که در آن  $\langle \alpha \rangle = \sum_{i=0}^{N-1} \alpha_i / N$  میانگین دامنه‌ها است.

$$\begin{aligned}
P_{inv} \sum_{i=0}^{N-1} \beta_i |i\rangle \otimes |1\rangle &= \sum_{i=0}^{N-1} \beta_i [(H^{\otimes n} (2|0^{\otimes n+1}\rangle\langle 0^{\otimes n+1}|)H^{\otimes n})|i\rangle \otimes |0\rangle \langle 0|1\rangle \\
&\quad - (H^{\otimes n} I^{\otimes n} H^{\otimes n})|i\rangle \otimes (I \otimes I \otimes I)|1\rangle] \\
&= -\sum_{i=0}^{N-1} \beta_i |i\rangle \otimes |1\rangle
\end{aligned} \tag{۸۴-۴}$$

جملات اول و دوم مشابه با الگوریتم یونس است. تغییر ایجاد شده، ظاهر شدن جمله‌ی سوم است که به

ترتیب زیر محاسبه می‌شود:

$$\begin{aligned}
P_{inv} \sum_{i=0}^{N-1} \gamma_i |i\rangle \otimes |2\rangle &= \sum_{i=0}^{N-1} \gamma_i [(H^{\otimes n} (2|0^{\otimes n+1}\rangle\langle 0^{\otimes n+1}|)H^{\otimes n})|i\rangle \otimes |0\rangle \langle 0|2\rangle \\
&\quad - (H^{\otimes n} I^{\otimes n} H^{\otimes n})|i\rangle \otimes (I \otimes I \otimes I)|2\rangle] \\
&= -\sum_{i=0}^{N-1} \gamma_i |i\rangle \otimes |2\rangle
\end{aligned} \tag{۸۵-۴}$$

در نتیجه:

$$|\psi_3\rangle = \sum_{i=0}^{N-1} (2\langle \alpha \rangle - \alpha_i) |i\rangle \otimes |0\rangle - \sum_{i=0}^{N-1} \beta_i |i\rangle \otimes |1\rangle - \sum_{i=0}^{N-1} \gamma_i |i\rangle \otimes |2\rangle \tag{۸۶-۴}$$

با تقسیم  $\sum$  ی اول به سه دسته‌ی غیر جواب- جواب زوج و جواب فرد داریم:

$$|\psi_3\rangle = \sum^{n-m} (2\langle\alpha\rangle - \alpha_i) |i\rangle \otimes |0\rangle + \sum^{e-m} (2\langle\alpha\rangle - 0) |i\rangle \otimes |0\rangle \quad (87-4)$$

$$+ \sum^{o-m} (2\langle\alpha\rangle - 0) |i\rangle \otimes |0\rangle - \sum^{o-m} \frac{1}{\sqrt{N}} |i\rangle \otimes |1\rangle - \sum^{e-m} \frac{1}{\sqrt{N}} |i\rangle \otimes |2\rangle$$

در الگوریتم یونس با اعمال  $P_{inv}$  دامنه‌های زیر فضای  $|i\rangle \otimes |0\rangle$  چه جواب چه غیر جواب نسبت به میانگین‌شان انعکاس می‌یابند و جای زیر فضاهای شامل جواب در هر تکرار جابجا می‌شود.

حال در تکرار دوم برای اینکه جای زیر فضاهای جواب در این حالت کیوتریتی نیز جابجا شود  $U_f$  را دو

بار اعمال می‌کنیم. بدین ترتیب که:

اعمال اولین  $U_f$ :

$$\begin{aligned} n-m : & \quad \sum \alpha |i\rangle \otimes |0\rangle \rightarrow \sum \alpha |i\rangle \otimes |0\rangle \\ o-m : & \quad \sum \beta |i\rangle \otimes |0\rangle \rightarrow \sum \beta |i\rangle \otimes |1\rangle \\ o-m : & \quad \sum \beta |i\rangle \otimes |1\rangle \rightarrow \sum \beta |i\rangle \otimes |2\rangle \\ e-m : & \quad \sum \gamma |i\rangle \otimes |2\rangle \rightarrow \sum \gamma |i\rangle \otimes |1\rangle \\ e-m : & \quad \sum \gamma |i\rangle \otimes |0\rangle \rightarrow \sum \gamma |i\rangle \otimes |2\rangle \end{aligned} \quad (88-4)$$

حالت ایجاد شده ناشی از اعمال اولین  $U_f$  عبارتست از:

$$\begin{aligned} |\psi_4\rangle = & \sum^{n-m} (2\langle\alpha\rangle - \alpha_i) |i\rangle \otimes |0\rangle + \sum^{odd-m} (2\langle\alpha\rangle - 0) |i\rangle \otimes |1\rangle \\ & + \sum^{even-m} (2\langle\alpha\rangle - 0) |i\rangle \otimes |2\rangle - \sum^{odd-m} \frac{1}{\sqrt{N}} |i\rangle \otimes |2\rangle - \sum^{even-m} \frac{1}{\sqrt{N}} |i\rangle \otimes |1\rangle \end{aligned} \quad (89-4)$$

با اعمال دومین  $U_f$  داریم:

$$\begin{aligned} n-m : & \quad \sum \alpha |i\rangle \otimes |0\rangle \rightarrow \sum \alpha |i\rangle \otimes |0\rangle \\ e-m : & \quad \sum \gamma |i\rangle \otimes |2\rangle \rightarrow \sum \gamma |i\rangle \otimes |1\rangle \\ o-m : & \quad \sum \beta |i\rangle \otimes |1\rangle \rightarrow \sum \beta |i\rangle \otimes |2\rangle \\ o-m : & \quad \sum \beta |i\rangle \otimes |2\rangle \rightarrow \sum \beta |i\rangle \otimes |0\rangle \\ e-m : & \quad \sum \gamma |i\rangle \otimes |1\rangle \rightarrow \sum \gamma |i\rangle \otimes |0\rangle \end{aligned} \quad (90-4)$$

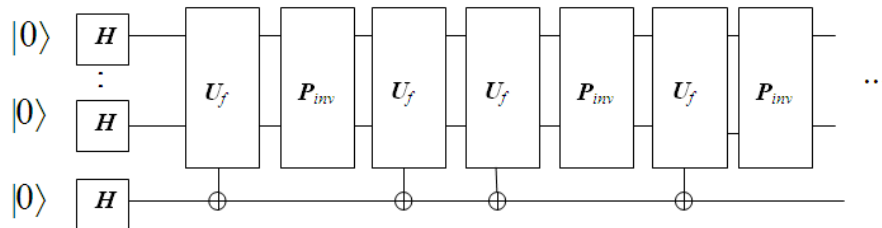
حالت ایجاد شده ناشی از اعمال دومین  $U_f$  عبارتست از:

$$|\psi_5\rangle = \sum^{n-m} (2\langle\alpha\rangle - \alpha_i) |i\rangle \otimes |0\rangle + \sum^{odd-m} (2\langle\alpha\rangle - 0) |i\rangle \otimes |2\rangle \quad (91-4)$$

$$+ \sum^{even-m} (2\langle\alpha\rangle - 0) |i\rangle \otimes |1\rangle - \sum^{odd-m} \frac{1}{\sqrt{N}} |i\rangle \otimes |0\rangle - \sum^{even-m} \frac{1}{\sqrt{N}} |i\rangle \otimes |0\rangle$$

همان طور که با مقایسه‌ی روابط (۴-۸۷) و (۴-۹۱) می‌بینیم جواب‌ها با دامنه‌ی  $2\alpha$  در زیر فضای  $|i\rangle \otimes |0\rangle$  و با دامنه‌ی  $-1/\sqrt{N}$  در زیر فضای  $|i\rangle \otimes |2\rangle$  و  $|i\rangle \otimes |1\rangle$  ظاهر شدند که با دو بار اعمال  $f$  گیت، جواب‌ها با دامنه‌ی  $2\alpha$  در زیر فضای  $|i\rangle \otimes |1\rangle, |i\rangle \otimes |2\rangle$  و جواب‌ها با دامنه‌ی  $-1/\sqrt{N}$  در زیر فضای  $|i\rangle \otimes |0\rangle$  ظاهر شدند. لذا مشاهده می‌کنیم همان تغییراتی که روی دامنه‌های جواب و غیر جواب در الگوریتم کیوبیتی احمد یونس انجام می‌شود، در اینجا برای دامنه‌های زوج و فرد جواب و غیر جواب کیوتیریتی پیشنهادی رخ می‌دهد. یعنی جای زیر فضاهای شامل حالت‌های جواب در هر تکرار جابجا می‌شوند تا عملگر  $P_{inv}$  روی یک دسته از آنها اثر کند و دسته‌ی دیگر تغییر فاز  $\pi$  رادیان دهند. تغییر ایجاد شده، افزایش زیر فضاها، استفاده از کیوتیریت و سه حالتی بودن آن و دو بار استفاده از گیت  $f$  کیوتیریتی در تکرارهای زوج است.

نمودار تکرارهای زوج و فرد به صورت زیر تغییر می‌کند:



شکل ۴-۳ نمودار الگوریتم پیشنهادی برای جواب زوج و فرد

برای مقایسه با حالت کیوبیتی یونس توجه داریم که مثلاً در تکرار اول دامنه‌ها به صورت زیر تغییر

می‌کنند، بعد از اعمال  $U_f$  و  $P_{inv}$ :

$$|\psi_3\rangle = \sum^{n-m} (2\langle\alpha\rangle - \alpha_i) |i\rangle \otimes |0\rangle + \sum^{e-m} (2\langle\alpha\rangle - 0) |i\rangle \otimes |0\rangle + \sum^{o-m} (2\langle\alpha\rangle - 0) |i\rangle \otimes |0\rangle - \sum^{o-m} \frac{1}{\sqrt{N}} |i\rangle \otimes |1\rangle - \sum^{e-m} \frac{1}{\sqrt{N}} |i\rangle \otimes |2\rangle \quad (۴-۹۲)$$

رابطه‌ی فوق را به شکل زیر بازنویسی می‌کنیم:

$$|\psi_3\rangle = a_1 \sum^{n-m} |i\rangle \otimes |0\rangle + b_1 \sum^{e-m} |i\rangle \otimes |0\rangle + c_1 \sum^{o-m} |i\rangle \otimes |0\rangle + d_1 \sum^{o-m} |i\rangle \otimes |1\rangle + e_1 \sum^{e-m} |i\rangle \otimes |2\rangle \quad (۴-۹۳)$$

که ضرایب برابرند با:

$$\begin{cases} a_1 = 2\langle\alpha\rangle - \alpha_i \\ b_1 = 2\langle\alpha\rangle \\ c_1 = 2\langle\alpha\rangle \\ d_1 = -\frac{1}{\sqrt{N}} \\ e_1 = -\frac{1}{\sqrt{N}} \end{cases} \quad (94-4)$$

که در الگوریتم کیوبیتی یونس به قرار زیر بود:

$$|\psi_3\rangle = a_1 \sum^{n-m} |i\rangle \otimes |0\rangle + b_1 \sum^m |i\rangle \otimes |0\rangle + c_1 \sum^m \frac{1}{\sqrt{N}} |i\rangle \otimes |1\rangle \quad (95-4)$$

$$\begin{cases} a_1 = (2\langle\alpha\rangle - \frac{1}{\sqrt{N}}) \\ b_1 = 2\langle\alpha\rangle \\ c_1 = -\frac{1}{\sqrt{N}} \end{cases}$$

#### ۴-۱۲ بیانی دیگر از الگوریتم احمد یونس با کیوتزیت‌ها:

در بیان جدید حالت کیوتزیتی پیشنهادی الگوریتم یونس، حالت اولیه چون گذشته برابر است با:

$$|\phi_0\rangle = |0^{\otimes n}\rangle \otimes |0\rangle \quad (96-4)$$

روی  $n$  کیوبیت اول عملگر هادامارد و روی اوراکل  $|0\rangle$ ، عملگر یکانی اعمال می‌شود:

$$|\phi_1\rangle = (H^{\otimes n} \otimes I) |\phi_0\rangle = \left[ \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle \right] \otimes |0\rangle \quad (97-4)$$

گیت  $U_f$  را اعمال می‌کنیم:

$$U_f \sum_i |i\rangle \otimes |0\rangle = \sum_i |i\rangle \otimes |0+f(i)\rangle = \sum_i (\alpha_i |i\rangle \otimes |0\rangle + \beta_i |i\rangle \otimes |1\rangle + \gamma_i |i\rangle \otimes |2\rangle) \quad (98-4)$$

که  $f(i)$  یا همان  $f(x)$  با توجه به کیوتزیت بودن واحدهای حافظه همان طور که قبلاً نیز اشاره شد، سه حالتی

می‌باشد:

$$f(x) = \begin{cases} 0 & \text{non-matches} \\ 1 & \text{odd-matches} \\ 2 & \text{even-matches} \end{cases} \quad (99-4)$$

و ضرایب در رابطه‌ی (۹۸-۴) عبارتند از:

$$\beta_i = \begin{cases} 0 & \text{non-matches} \\ 1 & \text{odd-matches} \\ 0 & \text{even-matches} \end{cases} \quad \gamma_i = \begin{cases} 0 & \text{non-matches} \\ 0 & \text{odd-matches} \\ 1 & \text{even-matches} \end{cases} \quad \alpha_i = \begin{cases} 1 & \text{non-matches} \\ 0 & \text{odd-matches} \\ 0 & \text{even-matches} \end{cases} \quad (100-4)$$

بدین ترتیب حالت کلی  $|\phi_1\rangle$  را به سه قسمت، غیر جواب‌ها، جواب‌های زوج و جواب‌های فرد تقسیم

کردیم. اثر  $U_f$  را در حالت‌های مختلف بررسی می‌کنیم:

$$\begin{aligned} n-m : & \quad U_f \sum \alpha |i\rangle \otimes |0\rangle \rightarrow \sum \alpha |i\rangle \otimes |0\rangle \\ o-m : & \quad U_f \sum \beta |i\rangle \otimes |0\rangle \rightarrow \sum \beta |i\rangle \otimes |1\rangle \\ o-m : & \quad U_f \sum \beta |i\rangle \otimes |1\rangle \rightarrow \sum \beta |i\rangle \otimes |2\rangle \\ o-m : & \quad U_f \sum \beta |i\rangle \otimes |2\rangle \rightarrow \sum \beta |i\rangle \otimes |0\rangle \\ e-m : & \quad U_f \sum \gamma |i\rangle \otimes |0\rangle \rightarrow \sum \gamma |i\rangle \otimes |2\rangle \\ e-m : & \quad U_f \sum \gamma |i\rangle \otimes |1\rangle \rightarrow \sum \gamma |i\rangle \otimes |0\rangle \\ e-m : & \quad U_f \sum \gamma |i\rangle \otimes |2\rangle \rightarrow \sum \gamma |i\rangle \otimes |1\rangle \end{aligned} \quad (101-4)$$

همان‌طور که مشاهده می‌کنیم اثر اعمال  $U_f$ ، ایجاد درهم‌تنیدگی حالت‌های غیرجواب با حالت  $|0\rangle$ ،

درهم‌تنیدگی حالت‌های جواب فرد با حالت  $|1\rangle$  و حالت‌های جواب زوج با حالت  $|2\rangle$  می‌باشد.

$P_{inv}$  را به شکل زیر می‌نویسیم:

$$P_{inv} = (H^{\otimes n} \otimes I)(2|0^{\otimes n+1}\rangle\langle 0^{\otimes n+1}| - I^{\otimes n+1})(H^{\otimes n} \otimes I) = (2|\phi_1\rangle\langle 0| \langle \phi_1| - I^{\otimes n+1}) \quad (102-4)$$

تاثیر اعمال  $P_{inv}$  را روی زیر فضای  $\sum \alpha_i |i\rangle \otimes |0\rangle$  محاسبه می‌کنیم:

$$\begin{aligned} P_{inv} \sum \alpha_i |i\rangle \otimes |0\rangle &= 2 \sum \alpha_i \left( \sum \frac{1}{\sqrt{N}} |j\rangle \otimes |0\rangle \right) \left( \sum \frac{1}{\sqrt{N}} \langle 0| \otimes \langle k| \right) |i\rangle \otimes |0\rangle - \sum \alpha_i |i\rangle \otimes |0\rangle \\ &= 2 \sum_j \left( \sum \frac{\alpha_i}{N} \delta_{ki} \right) |j\rangle \otimes |0\rangle - \sum \alpha_i |i\rangle \otimes |0\rangle = 2 \sum \bar{\alpha} |i\rangle \otimes |0\rangle - \sum \alpha_i |i\rangle \otimes |0\rangle \end{aligned}$$

$$\begin{aligned}
&= 2\sum \bar{\alpha}(\alpha_i |i\rangle \otimes |0\rangle + \beta_i |i\rangle \otimes |0\rangle + \gamma_i |i\rangle \otimes |0\rangle) - \sum \alpha_i |i\rangle \otimes |0\rangle \\
&= (2\bar{\alpha} - 1)\sum \alpha_i |i\rangle \otimes |0\rangle + 2\bar{\alpha}\sum \beta_i |i\rangle \otimes |0\rangle + 2\bar{\alpha}\sum \gamma_i |i\rangle \otimes |0\rangle
\end{aligned} \tag{۱۰۳-۴}$$

که  $\bar{\alpha} = (N - O - E)/N$  میانگین دامنه‌های حالت‌های غیرجواب است.  $O$  تعداد جواب‌های فرد،  $E$  تعداد جواب‌های زوج و  $M$  تعداد کل جواب‌هاست، به‌قسمی که  $M = O + E$  و  $N$  تعداد کل داده‌ها می‌باشد.

در محاسبه‌ی فوق از این رابطه استفاده کردیم:

$$\sum |i\rangle \otimes |0\rangle = \sum \alpha_i |i\rangle \otimes |0\rangle + \sum \beta_i |i\rangle \otimes |0\rangle + \sum \gamma_i |i\rangle \otimes |0\rangle \tag{۱۰۴-۴}$$

به همین ترتیب:

$$\begin{aligned}
P_{inv} \sum \beta_i |i\rangle \otimes |0\rangle &= 2\bar{\beta}\sum \alpha_i |i\rangle \otimes |0\rangle + (2\bar{\beta} - 1)\sum \beta_i |i\rangle \otimes |0\rangle + 2\bar{\beta}\sum \gamma_i |i\rangle \otimes |0\rangle \\
P_{inv} \sum \gamma_i |i\rangle \otimes |0\rangle &= 2\bar{\gamma}\sum \alpha_i |i\rangle \otimes |0\rangle + 2\bar{\gamma}\sum \beta_i |i\rangle \otimes |0\rangle + (2\bar{\gamma} - 1)\sum \gamma_i |i\rangle \otimes |0\rangle \\
P_{inv} \sum \beta_i |i\rangle \otimes |1\rangle &= -\sum \beta_i |i\rangle \otimes |1\rangle \\
P_{inv} \sum \gamma_i |i\rangle \otimes |1\rangle &= -\sum \gamma_i |i\rangle \otimes |1\rangle \\
P_{inv} \sum \beta_i |i\rangle \otimes |2\rangle &= -\sum \beta_i |i\rangle \otimes |2\rangle \\
P_{inv} \sum \gamma_i |i\rangle \otimes |2\rangle &= -\sum \gamma_i |i\rangle \otimes |2\rangle
\end{aligned} \tag{۱۰۵-۴}$$

که  $\bar{\beta} = O/N$  و  $\bar{\gamma} = E/N$  به ترتیب میانگین دامنه‌های حالت‌های جواب فرد و زوج است. (لازم به ذکر است

که در الگوی پیشنهادی الگوریتم کیوبیتی یونس مقادیر  $\bar{\beta}_{qubit}, \bar{\alpha}$  به صورت  $\bar{\alpha} = (N - M)/N$  که در الگوی پیشنهادی کیوتریتی یونس، مقادیر  $\bar{\gamma}, \bar{\beta}_{qubit}, \bar{\alpha}$  به صورت  $\bar{\alpha} = (N - O - E)/N$  و  $\bar{\beta}_{qubit} = M/N$  تعریف می‌شوند. در حالی که برابری ضرایب کیوتریتی پیشنهادی با ضرایب کیوبیتی را نشان می‌دهیم، از رابطه‌ی  $M = O + E$  استفاده کرده و  $\bar{\beta}_{qubit} + \bar{\gamma}$  را به صورت  $O/N + E/N = M/N$  می‌نویسیم که برابر با  $\bar{\beta}_{qubit}$  است.)

حال تکرار اول الگوریتم با استفاده از روابط فوق:

$$\begin{aligned}
|\xi_1\rangle &= U_f |\phi_1\rangle = \frac{1}{\sqrt{N}} (\sum \alpha_i |i\rangle \otimes |0\rangle + \sum \beta_i |i\rangle \otimes |1\rangle + \sum \gamma_i |i\rangle \otimes |2\rangle) \\
&= \text{non-matches} + \text{odd-matches} + \text{even-matches}
\end{aligned} \tag{۱۰۶-۴}$$



$$|\psi_1\rangle = P_{inv} |\xi_1\rangle = \frac{(2\bar{\alpha}-1)}{\sqrt{N}} \sum \alpha_i |i\rangle \otimes |0\rangle + \frac{2\bar{\alpha}}{\sqrt{N}} \sum \beta_i |i\rangle \otimes |0\rangle + \frac{2\bar{\alpha}}{\sqrt{N}} \sum \gamma_i |i\rangle \otimes |0\rangle - \frac{1}{\sqrt{N}} \sum \beta_i |i\rangle \otimes |1\rangle - \frac{1}{\sqrt{N}} \sum \gamma_i |i\rangle \otimes |2\rangle \quad (107-4)$$

$$|\psi_1\rangle = \frac{A_1}{\sqrt{N}} \sum \alpha_i |i\rangle \otimes |0\rangle + \frac{B_1^0}{\sqrt{N}} \sum \beta_i |i\rangle \otimes |0\rangle + \frac{C_1^0}{\sqrt{N}} \sum \gamma_i |i\rangle \otimes |0\rangle + \frac{B_1^1}{\sqrt{N}} \sum \beta_i |i\rangle \otimes |1\rangle + \frac{C_1^2}{\sqrt{N}} \sum \gamma_i |i\rangle \otimes |2\rangle$$

که ضرایب عبارتند از:

$$\begin{cases} A_1 = 2\bar{\alpha} - 1 \\ B_1^0 = 2\bar{\alpha} \\ C_1^0 = 2\bar{\alpha} \\ B_1^1 = -1 \\ C_1^2 = -1 \end{cases} \quad (108-4)$$

و چون گذشته اندیس بالای ضرایب  $B$  و  $C$  را به عنوان اندیسی معرفی می‌کنیم که مربوط به اوراکلی باشد که حالتها با آن درهم‌تنیده شده‌اند و اندیس پایین، مربوط به شماره‌ی تکرار است. به عنوان مثال،  $C_1^0$  مربوط به تکرار اول و حالت  $\sum \gamma_i |i\rangle \otimes |0\rangle$  است که با  $|0\rangle$  درهم‌تنیده شده است. توجه داریم که کت حالت  $|\psi_1\rangle$  نرمالیزه می‌باشد (پیوست ۲):

$$(N - O - E) \left(\frac{2\bar{\alpha}-1}{\sqrt{N}}\right)^2 + O \left(\frac{2\bar{\alpha}}{\sqrt{N}}\right)^2 + E \left(\frac{2\bar{\alpha}}{\sqrt{N}}\right)^2 + O \left(\frac{-1}{\sqrt{N}}\right)^2 + E \left(\frac{-1}{\sqrt{N}}\right)^2 = 1 \quad (109-4)$$

در تکرار دوم اعمال اولین  $U_f$ :

$$|\xi_2\rangle = U_f |\psi_1\rangle = \frac{A_1}{\sqrt{N}} \sum \alpha_i |i\rangle \otimes |0\rangle + \frac{B_1^0}{\sqrt{N}} \sum \beta_i |i\rangle \otimes |1\rangle + \frac{B_1^1}{\sqrt{N}} \sum \beta_i |i\rangle \otimes |2\rangle + \frac{C_1^0}{\sqrt{N}} \sum \gamma_i |i\rangle \otimes |2\rangle + \frac{C_1^1}{\sqrt{N}} \sum \gamma_i |i\rangle \otimes |1\rangle \quad (110-4)$$

اعمال دومین  $U_f$ :

$$|\xi_2'\rangle = U_f |\xi_2\rangle = \frac{A_1}{\sqrt{N}} \sum \alpha_i |i\rangle \otimes |0\rangle + \frac{B_1^0}{\sqrt{N}} \sum \beta_i |i\rangle \otimes |2\rangle + \frac{B_1^1}{\sqrt{N}} \sum \beta_i |i\rangle \otimes |0\rangle \\ + \frac{C_1^0}{\sqrt{N}} \sum \gamma_i |i\rangle \otimes |1\rangle + \frac{C_1^1}{\sqrt{N}} \sum \gamma_i |i\rangle \otimes |0\rangle \quad (111-4)$$

اعمال  $P_{inv}$ :

$$|\psi_2\rangle = P_{inv} |\xi_2'\rangle = \left\{ \frac{A_1}{\sqrt{N}} (2\bar{\alpha} - 1) + \frac{2B_1^1}{\sqrt{N}} \bar{\beta} + \frac{2C_1^1}{\sqrt{N}} \bar{\gamma} \right\} \sum \alpha_i |i\rangle \otimes |0\rangle \\ + \left\{ \frac{2A_1}{\sqrt{N}} \bar{\alpha} + \frac{B_1^1}{\sqrt{N}} (2\bar{\beta} - 1) + \frac{2C_1^1}{\sqrt{N}} \bar{\gamma} \right\} \sum \beta_i |i\rangle \otimes |0\rangle + \left\{ \frac{2A_1}{\sqrt{N}} \bar{\alpha} + \frac{2B_1^1}{\sqrt{N}} \bar{\beta} \right. \\ \left. + \frac{C_1^1}{\sqrt{N}} (2\bar{\gamma} - 1) \right\} \sum \gamma_i |i\rangle \otimes |0\rangle - \frac{B_1^0}{\sqrt{N}} \sum \beta_i |i\rangle \otimes |2\rangle - \frac{C_1^0}{\sqrt{N}} \sum \gamma_i |i\rangle \otimes |1\rangle \quad (112-4)$$

$$|\psi_2\rangle = \frac{A_2}{\sqrt{N}} \sum \alpha_i |i\rangle \otimes |0\rangle + \frac{B_2^0}{\sqrt{N}} \sum \beta_i |i\rangle \otimes |0\rangle + \frac{C_2^0}{\sqrt{N}} \sum \gamma_i |i\rangle \otimes |0\rangle + \frac{B_2^2}{\sqrt{N}} \sum \beta_i |i\rangle \otimes |2\rangle \\ + \frac{C_2^1}{\sqrt{N}} \sum \gamma_i |i\rangle \otimes |1\rangle$$

که ضرایب عبارتند از:

$$\begin{cases} A_2 = A_1(2\bar{\alpha} - 1) + 2B_1^1\bar{\beta} + 2C_1^1\bar{\gamma} \\ B_2^0 = 2A_1\bar{\alpha} + B_1^1(2\bar{\beta} - 1) + 2C_1^1\bar{\gamma} \\ C_2^0 = 2A_1\bar{\alpha} + 2B_1^1\bar{\beta} + C_1^1(2\bar{\gamma} - 1) \\ B_2^2 = -B_1^0 \\ C_2^1 = -C_1^0 \end{cases} \quad (113-4)$$

حالت سیستم در تکرار سوم عبارت است از:

$$|\psi_3\rangle = \frac{A_3}{\sqrt{N}} \sum \alpha_i |i\rangle \otimes |0\rangle + \frac{B_3^0}{\sqrt{N}} \sum \beta_i |i\rangle \otimes |0\rangle + \frac{C_3^0}{\sqrt{N}} \sum \gamma_i |i\rangle \otimes |0\rangle + \frac{B_3^1}{\sqrt{N}} \sum \beta_i |i\rangle \otimes |1\rangle \\ + \frac{C_3^2}{\sqrt{N}} \sum \gamma_i |i\rangle \otimes |2\rangle \quad (114-4)$$

که ضرایب برابرند با:

$$\begin{cases} A_3 = A_2(2\bar{\alpha}-1) + 2B_2^2\bar{\beta} + 2C_2^1\bar{\gamma} \\ B_3^0 = 2A_2\bar{\alpha} + B_2^2(2\bar{\beta}-1) + 2C_2^1\bar{\gamma} \\ C_3^0 = 2A_2\bar{\alpha} + 2B_2^2\bar{\beta} + C_2^1(2\bar{\gamma}-1) \\ B_3^1 = -B_2^0 \\ C_3^2 = -C_2^0 \end{cases} \quad (115-4)$$

برای حالت کلی سیستم داریم:

$$\begin{aligned} |\psi_{k+1}\rangle &= \frac{A_{k+1}}{\sqrt{N}} \sum \alpha_i |i\rangle \otimes |0\rangle + \frac{B_{k+1}^0}{\sqrt{N}} \sum \beta_i |i\rangle \otimes |0\rangle + \frac{C_{k+1}^0}{\sqrt{N}} \sum \gamma_i |i\rangle \otimes |0\rangle \\ &+ \begin{cases} \frac{B_{k+1}^1}{\sqrt{N}} \sum \beta_i |i\rangle \otimes |1\rangle + \frac{C_{k+1}^2}{\sqrt{N}} \sum \gamma_i |i\rangle \otimes |2\rangle & \text{odd iteration} \\ \frac{B_{k+1}^2}{\sqrt{N}} \sum \beta_i |i\rangle \otimes |2\rangle + \frac{C_{k+1}^1}{\sqrt{N}} \sum \gamma_i |i\rangle \otimes |1\rangle & \text{even iteration} \end{cases} \end{aligned} \quad (116-4)$$

که به صورت زیر برای تکرار فرد ( $k+1 = \text{odd}$ ) و تکرار زوج ( $k+1 = \text{even}$ ) تفکیک می شوند:

$$\begin{aligned} |\psi_{k+1}^{odd}\rangle &= \frac{A_{k+1}}{\sqrt{N}} \sum \alpha_i |i\rangle \otimes |0\rangle + \frac{B_{k+1}^0}{\sqrt{N}} \sum \beta_i |i\rangle \otimes |0\rangle + \frac{C_{k+1}^0}{\sqrt{N}} \sum \gamma_i |i\rangle \otimes |0\rangle \\ &+ \frac{B_{k+1}^1}{\sqrt{N}} \sum \beta_i |i\rangle \otimes |1\rangle + \frac{C_{k+1}^2}{\sqrt{N}} \sum \gamma_i |i\rangle \otimes |2\rangle \end{aligned} \quad (117-4)$$

$$\begin{aligned} |\psi_{k+1}^{even}\rangle &= \frac{A_{k+1}}{\sqrt{N}} \sum \alpha_i |i\rangle \otimes |0\rangle + \frac{B_{k+1}^0}{\sqrt{N}} \sum \beta_i |i\rangle \otimes |0\rangle + \frac{C_{k+1}^0}{\sqrt{N}} \sum \gamma_i |i\rangle \otimes |0\rangle \\ &+ \frac{B_{k+1}^2}{\sqrt{N}} \sum \beta_i |i\rangle \otimes |2\rangle + \frac{C_{k+1}^1}{\sqrt{N}} \sum \gamma_i |i\rangle \otimes |1\rangle \end{aligned} \quad (118-4)$$

در نتیجه در تکرار زوج،  $k$  فرد است و در تکرار فرد، مقدار  $k$  زوج می باشد. از آنجائی که فرمول کلی، برای حالت  $k+1$  در نظر گرفته شده، اگر زوج یا فرد بودن تکرار ( $k+1$ ) به عنوان مبنا در نظر گرفته شود و با استفاده از نمادگذاری که قبلاً نیز استفاده کرده بودیم ( $(k+1) \bmod 2 = \chi \oplus 1, k \bmod 2 = \chi$ )، هر دو رابطه ی فوق را می توان در یک رابطه به شکل زیر خلاصه نمود:

$$\begin{aligned} |\psi_{k+1}\rangle &= \frac{A_{k+1}}{\sqrt{N}} \sum \alpha_i |i\rangle \otimes |0\rangle + \frac{B_{k+1}^0}{\sqrt{N}} \sum \beta_i |i\rangle \otimes |0\rangle + \frac{C_{k+1}^0}{\sqrt{N}} \sum \gamma_i |i\rangle \otimes |0\rangle \\ &+ (\chi+1) \frac{B_{k+1}^1}{\sqrt{N}} \sum \beta_i |i\rangle \otimes |1\rangle + (\chi+1) \frac{C_{k+1}^2}{\sqrt{N}} \sum \gamma_i |i\rangle \otimes |2\rangle \\ &+ \chi \frac{B_{k+1}^2}{\sqrt{N}} \sum \beta_i |i\rangle \otimes |2\rangle + \chi \frac{C_{k+1}^1}{\sqrt{N}} \sum \gamma_i |i\rangle \otimes |1\rangle \end{aligned} \quad (119-4)$$

همان‌طور که مشاهده می‌کنیم در تکرار فرد، ضرایب  $B_{k+1}^1$  مربوط به حالاتی هستند که با حالت  $|1\rangle$  در هم تنیده شده‌اند و ضرایب  $C_{k+1}^2$  مربوط به حالاتی که با حالت  $|2\rangle$  در هم تنیده شده‌اند، و در تکرار زوج ضرایب  $B_{k+1}^2$  و  $C_{k+1}^1$  مربوط به حالاتی‌اند که به ترتیب با حالت‌های  $|2\rangle$  و  $|1\rangle$  درهم‌تنیده شده‌اند. با شرایط اولیه‌ی:

$$A_1 = 2\alpha - 1, B_1^0 = 2\alpha, C_1^0 = 2\alpha, B_1^1 = -1, C_1^2 = -1 \quad (120-4)$$

برای ضرایب در حالت کلی داریم:

$$\left\{ \begin{array}{ll} A_{k+1} = A_k (2\bar{\alpha} - 1) + \begin{cases} 2B_k^2 \bar{\beta} + 2C_k^1 \bar{\gamma} & \text{odd-iteration} \\ 2B_k^1 \bar{\beta} + 2C_k^2 \bar{\gamma} & \text{even-iteration} \end{cases} \\ B_{k+1}^0 = 2A_k \bar{\alpha} + \begin{cases} B_k^2 (2\bar{\beta} - 1) + 2C_k^1 \bar{\gamma} & \text{odd-iteration} \\ B_k^1 (2\bar{\beta} - 1) + 2C_k^2 \bar{\gamma} & \text{even-iteration} \end{cases} \\ C_{k+1}^0 = 2A_k \bar{\alpha} + \begin{cases} 2B_k^2 \bar{\beta} + C_k^1 (2\bar{\gamma} - 1) & \text{odd-iteration} \\ 2B_k^1 \bar{\beta} + C_k^2 (2\bar{\gamma} - 1) & \text{even-iteration} \end{cases} \\ \begin{cases} B_{k+1}^1 = -B_k^0 \\ B_{k+1}^2 = -B_k^0 \end{cases} & \begin{array}{l} \text{odd-iteration} \\ \text{even-iteration} \end{array} \\ \begin{cases} C_{k+1}^2 = -C_k^0 \\ C_{k+1}^1 = -C_k^0 \end{cases} & \begin{array}{l} \text{odd-iteration} \\ \text{even-iteration} \end{array} \end{array} \right. \quad (121-4)$$

که در رابطه‌ی زیر خلاصه می‌شود:

$$\left\{ \begin{array}{l} A_{k+1} = A_k (2\bar{\alpha} - 1) + (\chi + 1)2B_k^2 \bar{\beta} + (\chi + 1)2C_k^1 \bar{\gamma} + \chi 2B_k^1 \bar{\beta} + \chi 2C_k^2 \bar{\gamma} \\ B_{k+1}^0 = 2A_k \bar{\alpha} + (\chi + 1)B_k^2 (2\bar{\beta} - 1) + (\chi + 1)2C_k^1 \bar{\gamma} + \chi B_k^1 (2\bar{\beta} - 1) + \chi 2C_k^2 \bar{\gamma} \\ C_{k+1}^0 = 2A_k \bar{\alpha} + (\chi + 1)2B_k^2 \bar{\beta} + (\chi + 1)C_k^1 (2\bar{\gamma} - 1) + \chi 2B_k^1 \bar{\beta} + \chi C_k^2 (2\bar{\gamma} - 1) \\ B_{k+1}^{1,2} = -B_k^0 \\ C_{k+1}^{1,2} = -C_k^0 \end{array} \right. \quad (122-4)$$

با این روش می‌توانیم در تکرار فرد، دامنه‌ی جواب فرد و در تکرار زوج، دامنه‌ی جواب زوج را افزایش دهیم، به طریقی که جواب، (زوج یا فرد) با همان احتمال بالا به دست آید.

از آنجائی که  $M$  تعداد کل حالت‌های جواب،  $O$  تعداد جواب‌های فرد و  $E$  تعداد جواب‌های زوج است به‌قسمی که  $M = O + E$ ، برای تشکیل رابطه‌ی  $P_s$  (احتمال موفقیت) برای رابطه‌ی (4)-(7) داریم:

$$P_s^{k+1} = M \left( \frac{B_{k+1}^0}{\sqrt{N}} \right)^2 + M \left( \frac{B_{k+1}^1}{\sqrt{N}} \right)^2 \quad (123-4)$$

که ضرایب عبارتند از:

$$\begin{aligned} B_{k+1}^0 &= 2A_k \bar{\alpha} + B_k^1 (2\bar{\beta} - 1) \\ B_{k+1}^1 &= -B_k^0 \end{aligned} \quad (۱۲۴-۴)$$

برای رابطه‌ی (۴-۱۱۷) و ضرایب آن داریم:

$$\begin{aligned} P_s^{k+1} &= O\left(\frac{B_{k+1}^0}{\sqrt{N}}\right)^2 + E\left(\frac{C_{k+1}^0}{\sqrt{N}}\right)^2 + O\left(\frac{B_{k+1}^1}{\sqrt{N}}\right)^2 + E\left(\frac{C_{k+1}^2}{\sqrt{N}}\right)^2 \\ \begin{cases} A_{k+1} &= A_k (2\bar{\alpha} - 1) + 2B_k^2 \bar{\beta} + 2C_k^1 \bar{\gamma} \\ B_{k+1}^0 &= 2A_k \bar{\alpha} + B_k^2 (2\bar{\beta} - 1) + 2C_k^1 \bar{\gamma} \\ C_{k+1}^0 &= 2A_k \bar{\alpha} + 2B_k^2 \bar{\beta} + C_k^1 (2\bar{\gamma} - 1) \\ B_{k+1}^1 &= -B_k^0 \\ C_{k+1}^2 &= -C_k^0 \end{cases} \end{aligned} \quad (۱۲۵-۴)$$

همین‌طور برای رابطه‌ی (۴-۱۱۸) و ضرایب آن داریم:

$$\begin{aligned} P_s^{k+1} &= O\left(\frac{B_{k+1}^0}{\sqrt{N}}\right)^2 + E\left(\frac{C_{k+1}^0}{\sqrt{N}}\right)^2 + O\left(\frac{B_{k+1}^2}{\sqrt{N}}\right)^2 + E\left(\frac{C_{k+1}^1}{\sqrt{N}}\right)^2 \\ \begin{cases} A_{k+1} &= A_k (2\bar{\alpha} - 1) + 2B_k^1 \bar{\beta} + 2C_k^2 \bar{\gamma} \\ B_{k+1}^0 &= 2A_k \bar{\alpha} + B_k^1 (2\bar{\beta} - 1) + 2C_k^2 \bar{\gamma} \\ C_{k+1}^0 &= 2A_k \bar{\alpha} + 2B_k^1 \bar{\beta} + C_k^2 (2\bar{\gamma} - 1) \\ B_{k+1}^2 &= -B_k^0 \\ C_{k+1}^1 &= -C_k^0 \end{cases} \end{aligned} \quad (۱۲۶-۴)$$

با اندکی دقت در نحوه‌ی تغییر ضرایب  $B_{k+1}^0$  و  $C_{k+1}^0$ ، مشاهده می‌کنیم مقدارشان در هر تکرار همواره برابر می‌باشد، چرا که در تکرار فرد به صورت:

$$\begin{aligned} B_{k+1}^0 &= 2A_k \bar{\alpha} + 2\bar{\beta} B_k^2 + 2C_k^1 \bar{\gamma} - B_k^2 \\ C_{k+1}^0 &= 2A_k \bar{\alpha} + 2\bar{\beta} B_k^2 + 2C_k^1 \bar{\gamma} - C_k^1 \end{aligned} \quad (۱۲۷-۴)$$

بوده و ضرایب  $B_k^2$  و  $C_k^1$  از تکرار اول برابرند و در تکرارهای بعدی نیز به شکل یکسان تغییر می‌یابند، در نتیجه ضرایب  $B_{k+1}^0$  و  $C_{k+1}^0$  در تکرار فرد با هم برابرند، و در تکرار زوج به صورت:

$$\begin{aligned} B_{k+1}^0 &= 2A_k \bar{\alpha} + 2\bar{\beta} B_k^1 + 2C_k^2 \bar{\gamma} - B_k^1 \\ C_{k+1}^0 &= 2A_k \bar{\alpha} + 2B_k^1 \bar{\beta} + 2\bar{\gamma} C_k^2 - C_k^2 \end{aligned} \quad (۱۲۸-۴)$$

می‌باشد و ضرایب  $B_k^1$  و  $C_k^2$  نیز از تکرار اول برابر بوده و در تکرارهای بعدی نیز به شکل یکسان تغییر می‌یابند، در نتیجه ضرایب  $B_{k+1}^0$  و  $C_{k+1}^0$  در تکرار زوج نیز با هم برابرند. پس روابط (۴-۱۲۵) و (۴-۱۲۶) را می‌توان به شکل زیر بازنویسی نمود:

$$P_s^{Odd} = O \left( \frac{B_{k+1}^0}{\sqrt{N}} \right)^2 + E \left( \frac{B_{k+1}^0}{\sqrt{N}} \right)^2 + O \left( \frac{B_{k+1}^1}{\sqrt{N}} \right)^2 + E \left( \frac{B_{k+1}^1}{\sqrt{N}} \right)^2 \quad (129-4)$$

$$= (O + E) \left( \frac{B_{k+1}^0}{\sqrt{N}} \right)^2 + (O + E) \left( \frac{B_{k+1}^1}{\sqrt{N}} \right)^2 = M \left( \frac{B_{k+1}^0}{\sqrt{N}} \right)^2 + M \left( \frac{B_{k+1}^1}{\sqrt{N}} \right)^2$$

$$P_s^{Even} = O \left( \frac{B_{k+1}^0}{\sqrt{N}} \right)^2 + E \left( \frac{B_{k+1}^0}{\sqrt{N}} \right)^2 + O \left( \frac{B_{k+1}^2}{\sqrt{N}} \right)^2 + E \left( \frac{B_{k+1}^2}{\sqrt{N}} \right)^2$$

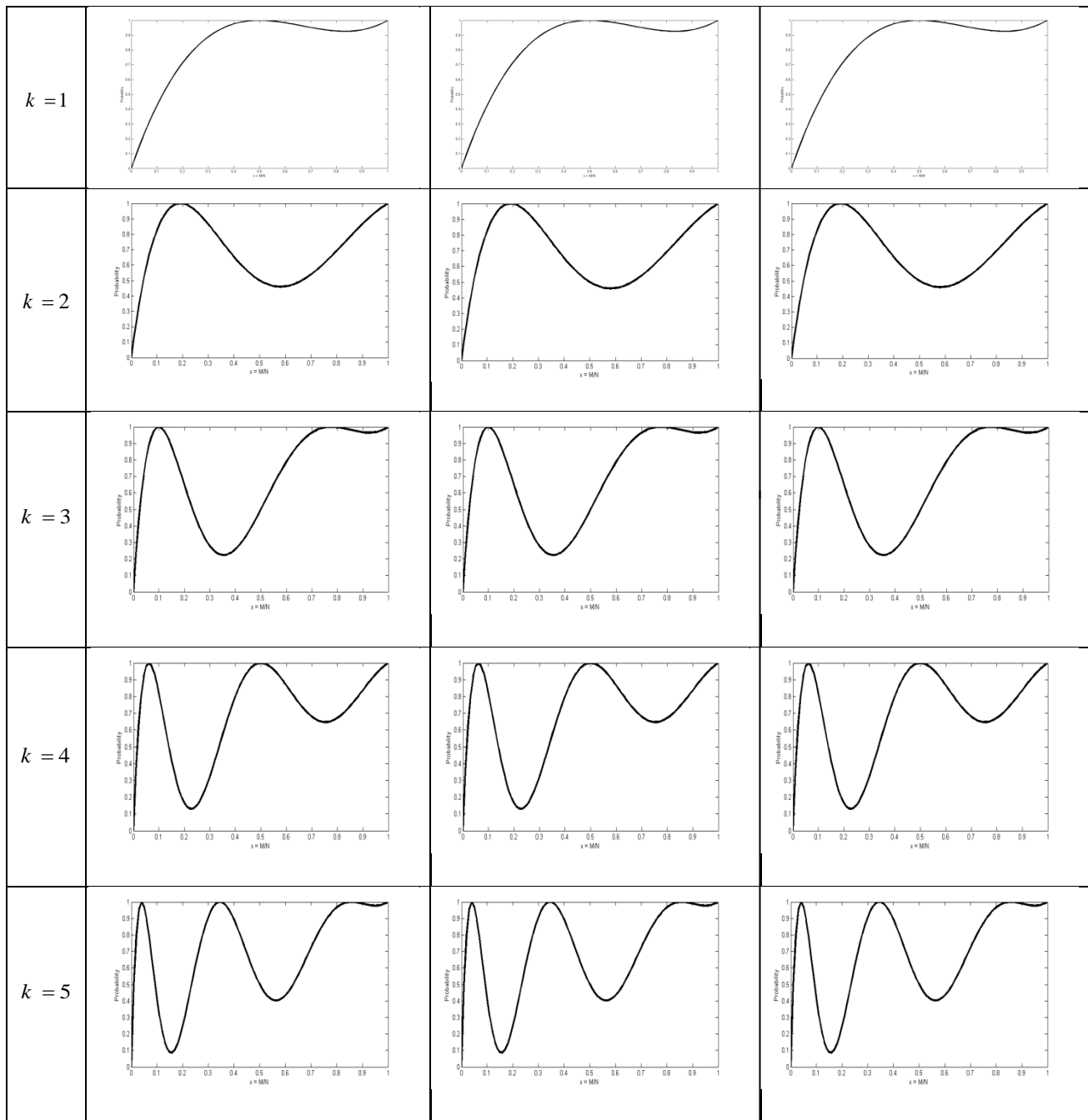
$$= (O + E) \left( \frac{B_{k+1}^0}{\sqrt{N}} \right)^2 + (O + E) \left( \frac{B_{k+1}^2}{\sqrt{N}} \right)^2 = M \left( \frac{B_{k+1}^0}{\sqrt{N}} \right)^2 + M \left( \frac{B_{k+1}^2}{\sqrt{N}} \right)^2$$

$$\begin{aligned} B_{k+1}^2 = B_{k+1}^1 = -B_k^0 \\ \Rightarrow = M \left( \frac{B_{k+1}^0}{\sqrt{N}} \right)^2 + M \left( \frac{B_{k+1}^1}{\sqrt{N}} \right)^2 \end{aligned} \quad (130-4)$$

که مشابه رابطه‌ی  $P_s$  برای الگوریتم کیوبیتی یونس است. در نهایت با بهره‌گیری از تساوی ضرایب، حالت کلی ضرایب الگوریتم کیوتزیتی پیشنهادی برابرست با:

$$\left\{ \begin{aligned} A_{k+1} &= A_k (2\bar{\alpha} - 1) + 2(\chi + 1)B_k^2 (\bar{\beta}_{qutrit} + \bar{\gamma}) + 2\chi B_k^1 (\bar{\beta}_{qutrit} + \bar{\gamma}) \\ &= A_k (2\bar{\alpha} - 1) + 2(\chi + 1)B_k^2 \bar{\beta}_{qubit} + 2\chi B_k^1 \bar{\beta}_{qubit} \\ B_{k+1}^0 &= 2A_k \bar{\alpha} + (\chi + 1)B_k^2 (2\bar{\beta}_{qutrit} - 1 + 2\bar{\gamma}) + \chi B_k^1 (2\bar{\beta}_{qutrit} - 1 + 2\bar{\gamma}) \\ &= 2A_k \bar{\alpha} + (\chi + 1)B_k^2 (2\bar{\beta}_{qubit} - 1) + \chi B_k^1 (2\bar{\beta}_{qubit} - 1) \\ C_{k+1}^0 &= 2A_k \bar{\alpha} + (\chi + 1)B_k^2 (2\bar{\beta}_{qutrit} + 2\bar{\gamma} - 1) + \chi B_k^1 (2\bar{\beta}_{qutrit} + 2\bar{\gamma} - 1) \\ &= 2A_k \bar{\alpha} + (\chi + 1)B_k^2 (2\bar{\beta}_{qubit} - 1) + \chi B_k^1 (2\bar{\beta}_{qubit} - 1) \\ B_{k+1}^{1,2} &= -B_k^0 \\ C_{k+1}^{1,2} &= -C_k^0 \end{aligned} \right. \quad (131-4)$$

توجه داریم که با تبدیل ضرایب کیوتزیتی به ضرایب کیوبیتی، تعریف  $\beta$  که در حالت کیوتزیتی برابر بود با  $\beta_{qutrit} = O/M$  به  $\beta_{qubit} = M/N$  تغییر می‌یابد. همان‌طور که می‌بینیم ضرایب الگوی پیشنهادی برای الگوریتم کیوتزیتی یونس از فرمول کلی الگوریتم کیوبیتی یونس تبعیت می‌کند، در نتیجه، تبدیل ضرایب الگوریتم جدید به ضرایب الگوریتم یونس، احتمال بالای دستیابی به جواب را مانند الگوریتم یونس متضمن می‌شود. به‌عنوان مثال نمودارهای  $P_s$  چند تکرار اول دو الگوریتم را با هم مقایسه می‌کنیم:



جدول ۴-۴ نمودارهای  $P_s$  بر حسب  $x = M/N$  برای الگوریتم یونس (ستون چپ)، کلی سازی پیشنهادی یونس (ستون وسط) و الگوریتم کیوتییتی پیشنهادی (ستون راست)

که معادلات  $P_s$  برای نمودارهای فوق به ترتیب برابر است با:

$$P_s^1 = 4x^3 - 8x^2 + 5x$$

$$P_s^2 = 16x^5 - 64x^4 + 92x^3 - 56x^2 + 13x$$

$$P_s^3 = 64x^7 - 384x^6 + 912x^5 - 1088x^4 + 680x^3 - 208x^2 + 25x$$

$$P_s^4 = 256x^9 - 2048x^8 + 6848x^7 - 12416x^6 + 13232x^5 - 8384x^4 + 3032x^3 - 560x^2 + 41x$$

$$P_s^5 = 1024x^{11} - 10240x^{10} + 44288x^9 - 108544x^8 + 165888x^7 - 163840x^6 + 104752x^5 - 42176x^4 + 10028x^3 - 1240x^2 + 61x$$

با ایده‌ی استفاده از واحدهای حافظه‌ی کیوتریتی، و معرفی  $f$  گیت کیوتریتی، با توجه به سه مقداری بودن این گیت، علاوه بر افزایش فضای قابل دسترسی سیستم، امکان استفاده از این مزیت حافظه‌ی کیوتریتی و تحدید جستجوی کلی جواب‌ها، به جستجوی جواب‌های خاص، زوج و فرد ایجاد می‌شود. در صورتی که مایل به یافتن جواب خواص، زوج یا فرد باشیم با افزایش تعداد تکرار، جواب مورد نظر را نیز می‌توان با احتمال بالا به دست آورد. با ایجاد تغییرات ناشی از تبدیل حافظه‌ی کیوبیتی به کیوتریتی و ایجاد تغییرات مورد نیاز برای تغییر زیر فضاها در مرحله‌ی اعمال  $U_f$  (اعمال دو گیت  $U_f$  در تکرارهای زوج) توانستیم الگوریتمی مشابه الگوریتم یونس با همان احتمال بالای دستیابی به جواب طرح کنیم.



۱- اثبات یکانی بودن عملگر  $Q$  معرفی شده در رابطه‌ی (۴-۴۸):

$$QQ^t = I$$

$$\begin{aligned} \Rightarrow & \left\{ e^{-\frac{2\pi i}{3}f(0)} (I - |w_{\text{even}}\rangle\langle w_{\text{even}}| - |w_{\text{odd}}\rangle\langle w_{\text{odd}}|) + e^{-\frac{2\pi i}{3}f(2)} |w_{\text{even}}\rangle\langle w_{\text{even}}| \right. \\ & + e^{-\frac{2\pi i}{3}f(1)} |w_{\text{odd}}\rangle\langle w_{\text{odd}}| \left. \right\} \otimes \left\{ e^{-\frac{2\pi i}{3}f(0)} (I - |w_{\text{even}}\rangle\langle w_{\text{even}}| - |w_{\text{odd}}\rangle\langle w_{\text{odd}}|) \right. \\ & + e^{-\frac{2\pi i}{3}f(2)} |w_{\text{even}}\rangle\langle w_{\text{even}}| + e^{-\frac{2\pi i}{3}f(1)} |w_{\text{odd}}\rangle\langle w_{\text{odd}}| \left. \right\}^t = I \end{aligned}$$

$$\begin{aligned} \Rightarrow & \left\{ e^{-\frac{2\pi i}{3}f(0)} (I - |w_{\text{even}}\rangle\langle w_{\text{even}}| - |w_{\text{odd}}\rangle\langle w_{\text{odd}}|) + e^{-\frac{2\pi i}{3}f(2)} |w_{\text{even}}\rangle\langle w_{\text{even}}| \right. \\ & + e^{-\frac{2\pi i}{3}f(1)} |w_{\text{odd}}\rangle\langle w_{\text{odd}}| \left. \right\} \otimes \left\{ e^{-\frac{2\pi i}{3}f(0)} (I - |w_{\text{even}}\rangle\langle w_{\text{even}}| - |w_{\text{odd}}\rangle\langle w_{\text{odd}}|) \right. \\ & + e^{-\frac{2\pi i}{3}f(2)} |w_{\text{even}}\rangle\langle w_{\text{even}}| + e^{-\frac{2\pi i}{3}f(1)} |w_{\text{odd}}\rangle\langle w_{\text{odd}}| \left. \right\} = I \end{aligned}$$

$$\begin{aligned} \Rightarrow & \left\{ e^{-\frac{2\pi i}{3}f(0)} I - e^{-\frac{2\pi i}{3}f(0)} |w_{\text{even}}\rangle\langle w_{\text{even}}| - e^{-\frac{2\pi i}{3}f(0)} |w_{\text{odd}}\rangle\langle w_{\text{odd}}| \right. \\ & + e^{-\frac{2\pi i}{3}f(2)} |w_{\text{even}}\rangle\langle w_{\text{even}}| + e^{-\frac{2\pi i}{3}f(1)} |w_{\text{odd}}\rangle\langle w_{\text{odd}}| \left. \right\} \otimes \left\{ e^{-\frac{2\pi i}{3}f(0)} I \right. \\ & - e^{-\frac{2\pi i}{3}f(0)} |w_{\text{even}}\rangle\langle w_{\text{even}}| - e^{-\frac{2\pi i}{3}f(0)} |w_{\text{odd}}\rangle\langle w_{\text{odd}}| + e^{-\frac{2\pi i}{3}f(2)} |w_{\text{even}}\rangle\langle w_{\text{even}}| \\ & + e^{-\frac{2\pi i}{3}f(1)} |w_{\text{odd}}\rangle\langle w_{\text{odd}}| \left. \right\} = I \end{aligned}$$

$$\begin{aligned} \Rightarrow & \left\{ e^{-\frac{2\pi i}{3}f(0)} I - e^{-\frac{2\pi i}{3}f(0)} |w_{\text{even}}\rangle\langle w_{\text{even}}| - e^{-\frac{2\pi i}{3}f(0)} |w_{\text{odd}}\rangle\langle w_{\text{odd}}| \right. \\ & + e^{-\frac{2\pi i}{3}f(2)} |w_{\text{even}}\rangle\langle w_{\text{even}}| + e^{-\frac{2\pi i}{3}f(1)} |w_{\text{odd}}\rangle\langle w_{\text{odd}}| \left. \right\} \otimes \left\{ e^{-\frac{2\pi i}{3}f(0)} I \right. \\ & - e^{-\frac{2\pi i}{3}f(0)} |w_{\text{even}}\rangle\langle w_{\text{even}}| - e^{-\frac{2\pi i}{3}f(0)} |w_{\text{odd}}\rangle\langle w_{\text{odd}}| + e^{-\frac{2\pi i}{3}f(2)} |w_{\text{even}}\rangle\langle w_{\text{even}}| \\ & + e^{-\frac{2\pi i}{3}f(1)} |w_{\text{odd}}\rangle\langle w_{\text{odd}}| \left. \right\} = I \end{aligned}$$

$$\begin{aligned} \Rightarrow & I - |w_{\text{even}}\rangle\langle w_{\text{even}}| - |w_{\text{odd}}\rangle\langle w_{\text{odd}}| + e^{-\frac{2\pi i}{3}(f(0)-f(1))} |w_{\text{odd}}\rangle\langle w_{\text{odd}}| \\ & + e^{-\frac{2\pi i}{3}(f(0)-f(2))} |w_{\text{even}}\rangle\langle w_{\text{even}}| - |w_{\text{even}}\rangle\langle w_{\text{even}}| + |w_{\text{even}}\rangle\langle w_{\text{even}}| \\ & - e^{-\frac{2\pi i}{3}(f(0)-f(1))} |w_{\text{odd}}\rangle\langle w_{\text{odd}}| - |w_{\text{odd}}\rangle\langle w_{\text{odd}}| + |w_{\text{odd}}\rangle\langle w_{\text{odd}}| \end{aligned}$$

$$\begin{aligned}
& -e^{-\frac{2\pi i}{3}(f(0)-f(2))} |w_{even}\rangle \langle w_{even}| + e^{-\frac{2\pi i}{3}(f(1)-f(0))} |w_{odd}\rangle \langle w_{odd}| \\
& -e^{-\frac{2\pi i}{3}(f(1)-f(0))} |w_{odd}\rangle \langle w_{odd}| + |w_{even}\rangle \langle w_{even}| + e^{-\frac{2\pi i}{3}(f(2)-f(0))} |w_{even}\rangle \langle w_{even}| \\
& -e^{-\frac{2\pi i}{3}(f(2)-f(0))} |w_{even}\rangle \langle w_{even}| + |w_{odd}\rangle \langle w_{odd}| = I
\end{aligned}$$

## ۲- اثبات نرمالیزه بودن کت حالت $|\psi_1\rangle$ معرفی شده در رابطه‌ی (۴-۱۰۹):

اگر  $N$  تعداد کل داده‌ها،  $(N - O - E)$  تعداد حالت‌های غیر جواب،  $E$  تعداد حالت‌های جواب زوج ( $Even$ ) و  $O$  تعداد حالت‌های جواب فرد ( $Odd$ ) باشد با اعمال شرط یک بودن مجموع احتمالات برای کت حالت  $|\psi_1\rangle$  داریم:

$$\begin{aligned}
& (N - O - E) \left(\frac{2\bar{\alpha} - 1}{\sqrt{N}}\right)^2 + O \left(\frac{2\bar{\alpha}}{\sqrt{N}}\right)^2 + E \left(\frac{2\bar{\alpha}}{\sqrt{N}}\right)^2 + O \left(\frac{-1}{\sqrt{N}}\right)^2 + E \left(\frac{-1}{\sqrt{N}}\right)^2 = 1 \\
\Rightarrow & \frac{(N - O - E)}{N} (2\bar{\alpha} - 1)^2 + \frac{O}{N} (2\bar{\alpha})^2 + \frac{E}{N} (2\bar{\alpha})^2 + \frac{O}{N} + \frac{E}{N} = 1 \\
\Rightarrow & \left(1 - \frac{O + E}{N}\right) (4\bar{\alpha}^2 + 1 - 4\bar{\alpha}) + 4\bar{\alpha}^2 \frac{O}{N} + 4\bar{\alpha}^2 \frac{E}{N} + \frac{O}{N} + \frac{E}{N} = 1 \\
\Rightarrow & 4\bar{\alpha}^2 + 1 - 4\bar{\alpha} - \frac{O + E}{N} (4\bar{\alpha}^2 + 1 - 4\bar{\alpha}) + 4\bar{\alpha}^2 \frac{O}{N} + 4\bar{\alpha}^2 \frac{E}{N} + \frac{O}{N} + \frac{E}{N} = 1 \\
\Rightarrow & 4\bar{\alpha}^2 + 1 - 4\bar{\alpha} - \frac{O}{N} (4\bar{\alpha}^2 + 1 - 4\bar{\alpha}) - \frac{E}{N} (4\bar{\alpha}^2 + 1 - 4\bar{\alpha}) + 4\bar{\alpha}^2 \frac{O}{N} + 4\bar{\alpha}^2 \frac{E}{N} + \frac{O}{N} + \frac{E}{N} = 1 \\
\Rightarrow & 4\bar{\alpha}^2 + 1 - 4\bar{\alpha} - 4\bar{\alpha}^2 \frac{O}{N} - \frac{O}{N} + 4\bar{\alpha} \frac{O}{N} - 4\bar{\alpha}^2 \frac{E}{N} - \frac{E}{N} + 4\bar{\alpha} \frac{E}{N} + 4\bar{\alpha}^2 \frac{O}{N} + 4\bar{\alpha}^2 \frac{E}{N} + \frac{O}{N} + \frac{E}{N} = 1 \\
\Rightarrow & 4\bar{\alpha}^2 + 1 - 4\bar{\alpha} + 4\bar{\alpha} \frac{E}{N} + 4\bar{\alpha} \frac{O}{N} = 1 \\
\Rightarrow & 4 \left(\frac{N - (O + E)}{N}\right)^2 + 1 - 4 \left(\frac{N - (O + E)}{N}\right) + 4 \left(\frac{N - (O + E)}{N}\right) \frac{E}{N} + 4 \left(\frac{N - (O + E)}{N}\right) \frac{O}{N} = 1 \\
\Rightarrow & 4 \left(1 - \frac{O + E}{N}\right)^2 + 1 - 4 \left(1 - \frac{O + E}{N}\right) + 4 \left(1 - \frac{O + E}{N}\right) \frac{E}{N} + 4 \left(1 - \frac{O + E}{N}\right) \frac{O}{N} = 1 \\
\Rightarrow & 4 \left(1 + \left(\frac{O + E}{N}\right)^2 - 2 \frac{O + E}{N}\right) + 1 - 4 + 4 \frac{E}{N} + 4 \frac{O}{N} + (4 - 4 \frac{O}{N} - 4 \frac{E}{N}) \frac{O}{N} + (4 - 4 \frac{O}{N} - 4 \frac{E}{N}) \frac{E}{N} = 1 \\
\Rightarrow & 4 \left(1 + \frac{O^2 + E^2 + 2OE}{N^2} - \frac{2E}{N} - \frac{2O}{N}\right) + 1 - 4 + 4 \frac{O}{N} + 4 \frac{E}{N} + 4 \frac{O}{N} - 4 \frac{O^2}{N^2} - 4 \frac{OE}{N^2} + 4 \frac{E}{N} - 4 \frac{OE}{N^2} - 4 \frac{E^2}{N^2} = 1 \\
\Rightarrow & 4 + 4 \frac{O^2}{N^2} + 4 \frac{E^2}{N^2} + 8 \frac{OE}{N^2} - 8 \frac{O}{N} - 8 \frac{E}{N} + 1 - 4 + 4 \frac{O}{N} + 4 \frac{E}{N} + 4 \frac{O}{N} - 4 \frac{O^2}{N^2} - 4 \frac{OE}{N^2} + 4 \frac{E}{N} - 4 \frac{OE}{N^2} - 4 \frac{E^2}{N^2} = 1
\end{aligned}$$

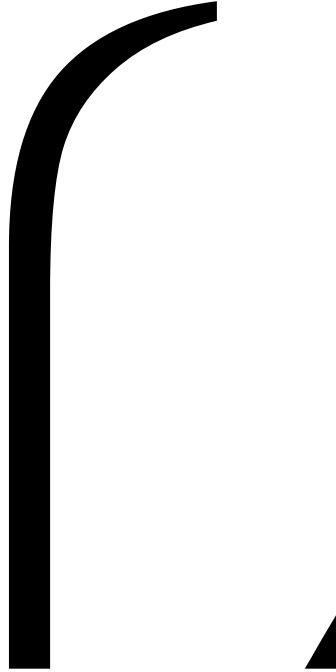
۳- ضرایب الگوریتم یونس، الگوی پیشنهادی برای الگوریتم یونس و الگوریتم

کیوتریتی:

ضرایب الگوریتم یونس:



ضرایب الگوی پیشنهادی یونس:



ضرایب الگوریتم کیوتریتی پیشنهادی:

$$\begin{cases} A_1 = 2\bar{\alpha} - 1 = 1 - 2x \\ B_1^0 = 2\bar{\alpha} = 2 - 2x \\ C_1^0 = 2\bar{\alpha} = 2 - 2x \\ B_1^1 = -1 \\ C_1^2 = -1 \end{cases}$$

$$\begin{cases} A_2 = 4\bar{\alpha}^2 - 4\bar{\alpha} - 2\bar{\beta} - 2\bar{\gamma} + 1 = 4x^2 - 6x + 1 \\ B_2^0 = 4\bar{\alpha}^2 - 2\bar{\alpha} - 2\bar{\beta} - 2\bar{\gamma} + 1 = 4x^2 - 8x + 3 \\ C_2^0 = 4\bar{\alpha}^2 - 2\bar{\alpha} - 2\bar{\beta} - 2\bar{\gamma} + 1 = 4x^2 - 8x + 3 \\ B_2^2 = -2\bar{\alpha} = 2x - 2 \\ C_2^1 = -2\bar{\alpha} = 2x - 2 \end{cases}$$

$$\begin{cases}
A_3 = 8\bar{\alpha}^3 - 12\bar{\alpha}^2 + 6\bar{\alpha} + 2\bar{\beta} + 2\bar{\gamma} - 8\bar{\alpha}\bar{\beta} - 8\bar{\alpha}\bar{\gamma} - 1 = -8x^3 + 20x^2 - 12x + 1 \\
B_3^0 = 8\bar{\alpha}^3 - 8\bar{\alpha}^2 + 4\bar{\alpha} - 8\bar{\alpha}\bar{\beta} - 8\bar{\alpha}\bar{\gamma} = -8x^3 + 24x^2 - 20x + 4 \\
C_3^0 = 8\bar{\alpha}^3 - 8\bar{\alpha}^2 + 4\bar{\alpha} - 8\bar{\alpha}\bar{\beta} - 8\bar{\alpha}\bar{\gamma} = -8x^3 + 24x^2 - 20x + 4 \\
B_3^1 = -4\bar{\alpha}^2 + 2\bar{\alpha} + 2\bar{\beta} + 2\bar{\gamma} - 1 = -4x^2 + 8x - 3 \\
C_3^2 = -4\bar{\alpha}^2 + 2\bar{\alpha} + 2\bar{\beta} + 2\bar{\gamma} - 1 = -4x^2 + 8x - 3 \\
A_4 = 16\bar{\alpha}^4 - 32\bar{\alpha}^3 + 24\bar{\alpha}^2 - 4\bar{\gamma} - 4\bar{\beta} - 8\bar{\alpha} + 16\bar{\alpha}\bar{\beta} + 16\bar{\alpha}\bar{\gamma} + 4\bar{\beta}^2 + 4\bar{\gamma}^2 + 8\bar{\beta}\bar{\gamma} - 24\bar{\alpha}^2\bar{\beta} + 24\bar{\alpha}^2\bar{\gamma} + 1 \\
= 16x^4 - 56x^3 + 60x^2 - 20x + 1 \\
B_4^0 = 16\bar{\alpha}^4 - 24\bar{\alpha}^3 + 16\bar{\alpha}^2 - 4\bar{\gamma} - 4\bar{\beta} - 4\bar{\alpha} + 8\bar{\alpha}\bar{\beta} + 8\bar{\alpha}\bar{\gamma} + 4\bar{\beta}^2 + 4\bar{\gamma}^2 + 8\bar{\beta}\bar{\gamma} - 24\bar{\alpha}^2\bar{\beta} + 24\bar{\alpha}^2\bar{\gamma} + 1 \\
= 16x^4 - 64x^3 + 84x^2 - 40x + 5 \\
C_4^0 = 16\bar{\alpha}^4 - 24\bar{\alpha}^3 + 16\bar{\alpha}^2 - 4\bar{\gamma} - 4\bar{\beta} - 4\bar{\alpha} + 8\bar{\alpha}\bar{\beta} + 8\bar{\alpha}\bar{\gamma} + 4\bar{\beta}^2 + 4\bar{\gamma}^2 + 8\bar{\beta}\bar{\gamma} - 24\bar{\alpha}^2\bar{\beta} + 24\bar{\alpha}^2\bar{\gamma} + 1 \\
= 16x^4 - 64x^3 + 84x^2 - 40x + 5 \\
B_4^2 = -8\bar{\alpha}^3 + 8\bar{\alpha}^2 - 4\bar{\alpha} + 8\bar{\alpha}\bar{\beta} + 8\bar{\alpha}\bar{\gamma} = 8x^3 - 24x^2 + 20x - 4 \\
C_4^1 = -8\bar{\alpha}^3 + 8\bar{\alpha}^2 - 4\bar{\alpha} + 8\bar{\alpha}\bar{\beta} + 8\bar{\alpha}\bar{\gamma} = 8x^3 - 24x^2 + 20x - 4 \\
A_5 = 32\bar{\alpha}^5 - 64\bar{\alpha}^3\bar{\gamma} - 64\bar{\alpha}^3\bar{\beta} + 24\bar{\alpha}\bar{\gamma}^2 + 24\bar{\alpha}\bar{\beta}^2 - 4\bar{\gamma}^2 - 8\bar{\beta}\bar{\gamma} - 4\bar{\beta}^2 + 72\bar{\alpha}^2\bar{\gamma} + 72\bar{\alpha}^2\bar{\beta} - 32\bar{\alpha}\bar{\gamma} - 32\bar{\alpha}\bar{\beta} \\
- 80\bar{\alpha}^4 + 80\bar{\alpha}^3 - 40\bar{\alpha}^2 + 48\bar{\alpha}\bar{\beta}\bar{\gamma} + 4\bar{\gamma} + 4\bar{\beta} + 10\bar{\alpha} - 1 = -32x^5 + 144x^4 - 224x^3 + 140x^2 - 30x + 1 \\
B_5^0 = 32\bar{\alpha}^5 - 64\bar{\alpha}^3\bar{\gamma} - 64\bar{\alpha}^3\bar{\beta} + 24\bar{\alpha}\bar{\gamma}^2 + 24\bar{\alpha}\bar{\beta}^2 + 48\bar{\alpha}^2\bar{\gamma} + 48\bar{\alpha}^2\bar{\beta} - 24\bar{\alpha}\bar{\gamma} - 24\bar{\alpha}\bar{\beta} - 64\bar{\alpha}^4 + 56\bar{\alpha}^3 \\
- 24\bar{\alpha}^2 + 48\bar{\alpha}\bar{\beta}\bar{\gamma} + 6\bar{\alpha} = -32x^5 + 160x^4 - 288x^3 + 224x^2 - 70x + 6 \\
C_5^0 = 32\bar{\alpha}^5 - 64\bar{\alpha}^3\bar{\gamma} - 64\bar{\alpha}^3\bar{\beta} + 24\bar{\alpha}\bar{\gamma}^2 + 24\bar{\alpha}\bar{\beta}^2 + 48\bar{\alpha}^2\bar{\gamma} + 48\bar{\alpha}^2\bar{\beta} - 24\bar{\alpha}\bar{\gamma} - 24\bar{\alpha}\bar{\beta} - 64\bar{\alpha}^4 + 56\bar{\alpha}^3 \\
- 24\bar{\alpha}^2 + 48\bar{\alpha}\bar{\beta}\bar{\gamma} + 6\bar{\alpha} = -32x^5 + 160x^4 - 288x^3 + 224x^2 - 70x + 6 \\
B_5^2 = -16\bar{\alpha}^4 + 24\bar{\alpha}^3 - 16\bar{\alpha}^2 + 4\bar{\gamma} + 4\bar{\beta} + 4\bar{\alpha} - 8\bar{\alpha}\bar{\beta} - 8\bar{\alpha}\bar{\gamma} - 4\bar{\beta}^2 - 4\bar{\gamma}^2 - 8\bar{\beta}\bar{\gamma} + 24\bar{\alpha}^2\bar{\beta} + 24\bar{\alpha}^2\bar{\gamma} - 1 \\
= -16x^4 + 64x^3 - 84x^2 + 40x - 5 \\
C_5^1 = -16\bar{\alpha}^4 + 24\bar{\alpha}^3 - 16\bar{\alpha}^2 + 4\bar{\gamma} + 4\bar{\beta} + 4\bar{\alpha} - 8\bar{\alpha}\bar{\beta} - 8\bar{\alpha}\bar{\gamma} - 4\bar{\beta}^2 - 4\bar{\gamma}^2 - 8\bar{\beta}\bar{\gamma} + 24\bar{\alpha}^2\bar{\beta} + 24\bar{\alpha}^2\bar{\gamma} - 1 \\
= -16x^4 + 64x^3 - 84x^2 + 40x - 5
\end{cases}$$

#### ۴- تجزیه‌ی اشمیت

فرض کنید که دستگاه مرکب  $A + B$  در یک حالت خالص  $|\psi\rangle_{AB}$  قرار دارد. در این صورت همواره می‌توان این حالت را به شکل زیربازنویسی کرد:

$$|\psi\rangle_{AB} = \sum_i \lambda_i |i, \hat{i}\rangle$$

که در آن  $\lambda_i$ ها اعداد مثبت و  $\{|i\rangle\}, \{|\hat{i}\rangle\}$  به ترتیب مجموعه بردارهای متعامد یکه در فضای هیلبرت دستگاه‌های  $A$  و  $B$  هستند. این تجزیه را تجزیه‌ی اشمیت می‌خوانند.

- [1] Michael A.Nielsen and Isaac L.Chuang, “**Quantum computation and quantum information**”, Cambridge, United Kingdom (2000)
- [2] Claude E. Shannon, “**A mathematical theory of communication**”, [ma.huji.ac.il/~matang02/shannon.pdf](http://ma.huji.ac.il/~matang02/shannon.pdf), 1948
- [3] Benjamin Schumacher, “**Quantum coding**”, Physical Review A 51:44, 2738-2747, American Physical Society, 4/1995
- [4] Jill Cirasella, “**Historical bibliography of quantum computing**”, Brooklyn College Library, 2008
- [5] Charles H. Bennett and Gilles Brassard, “**Quantum cryptography**”, 22 Jul 1998, [www.cs.mcgill.ca/~crepeau/CRYPTO/Biblio-QC.html](http://www.cs.mcgill.ca/~crepeau/CRYPTO/Biblio-QC.html)
- [6] David DiVincenzo, “**Two-bit gates are universal for quantum computation**”, [link.aps.org/doi/10.1103/PhysRevA.51.1015](http://link.aps.org/doi/10.1103/PhysRevA.51.1015)
- [7] Adriano Barenco, David Deutsch, and Artur Ekert , “**Conditional quantum dynamics and logic gates**” , quant-ph/9503017
- [8] David Deutsch and Richard Jozsa, “**Rapid solution of problems by quantum computation**”, [adsabs.harvard.edu/abs/1992RSPSA.439..553D](http://adsabs.harvard.edu/abs/1992RSPSA.439..553D), 1992
- [9] Shor and Simon, “**On the power of quantum computation and algorithms for quantum computation: Discrete logarithms and factoring**”, 1994
- [10] Shor, “**Scheme for reducing decoherence in quantum computer memory**”, Phys. Rev.A 52,R2493(1995)
- [11] Andrew M. Steane, “**Error correcting codes in quantum theory**”, Received 4 October 1995
- [12] Lov.K.Grover, “**A framework for fast quantum mechanical algorithms**”, lanl e-print quant-ph/ 9607024
- [13] Lov.K.Grover, “**A fast quantum mechanical algorithm for database search**”, quant-ph/9605043
- [14] Isaac L. Chuang, Neil Gershenfeld, and Mark Kubinec, “**Experimental implementation of fast quantum searching**”, Physical Review Letters, 1998
- [15] Johan Preskill, “**Lecture Notes for Physics 229: Quantum information and computation**”, California Institute of Technology, September, 1998
- [16] Michel Le Bellac, “**An introduction to quantum information and quantum computation**”, translated by Patricia de forcrand-millard, Cambridge, (2006)
- [17] Ashok Chatterjee, “**Introduction to quantum computation**”, Theory Group, Saha Institute of Nuclear Physics, Kolkata, India, e-print”quant-ph/0312111
- [18] Mark Oskin, “**Quantum computing-Lecture Notes**”, Department of Computer Science and Engineering University of Washington
- [19] Phillip Kaye, Raymond Laflamme and Michele Mosca, “**An Introduction to quantum computing**”, Oxford
- [20] A.Yu.Kitaev, A.H.Shen, M.N.Vyalyi, “**Classical and quantum computation**”, <http://books.google.com/books?id=TrMposZZ0MQC&lpg=PR7&ots=QGS25uO1tH&dq=classical%20and%20quantum%20computation&lr&pg=PP1#v=onepage&q&f=false>
- [21] Hoi-Kwong Lo, Sandu Popescu, Tim Spiller, “**Introduction to quantum computation and information**” Singapore, New Jersey, London, Hong Kong

- [22] David McMahon, **“Quantum computing explained”**, John Wiley & Sons, USA
- [23] Mladen Pavcic, **“Quantum computation and quantum communication”**, University of Zagreb, Zagreb, Croatia
- [24] Mikiyo Nakahara and Tetsuo Ohmi, **“Quantum computing, from linear algebra to physical realizations”**, Kinki University, Higashi-Osaka, Japan
- [25] Dirk Bouwmeester, Artur Ekert, Anton Zeilinger, **“The physics of quantum Information, quantum cryptography, quantum teleportation, and quantum computation”**
- [26] Artur Ekert, Patrick Hayden and Hitoshi Inamori, **“Basic concepts in quantum computation”**, Center for Quantum Computation, University of Oxford, United Kingdom
- [27] N.David Mermin, **“Quantum computer science”**, Cambridge
- [28] Andrei B.Klimov, Luis L.Sanchez-Soto, Hubert de Guise, Gunnar Bjork, **“Quantum phases of a qutrit”**, November 2, 2009
- [29] Acin A, Durt T, Gisin N and Latorre J I 2002 *Phys. Rev. A* **65** 052325
- [30] Collins D, Gisin N, Linden N, Massar S and Popescu S 2002 *Phys. Rev. Lett.* **88** 040404
- [31] A.T.Bolukbasi, T.Dereli, **“On the SU (3) parametrization of qutrits”**, [iopscience.iop.org/1742-6596/36/1/006](http://iopscience.iop.org/1742-6596/36/1/006)
- [32] B. P. Lanyon, T. J. Weinhold, N. K. Langford, J. L. O'Brien, K. J. Resch, A. Gilchrist, and A. G. White, **“Manipulating biphotonic qutrits”**, *Phys. Rev. Lett.* **100**, 060504 (2008)
- [33] Pawel Kurzynski, **“Multi-bloch vector representation of the qutrit”**, 16 Dec 2009
- [34] Emmanuel Briand, Jean Luque and Yves Thibon, **“The moduli space of three qutrit states”**, [quant-ph/0306122](http://quant-ph/0306122)
- [35] Michel Planat, Anne-Celin Baboin and Metod Saniga, **“Multi-line geometry of qubit-qutrit and higher-order pauli operator”**, [www.springerlink.com/index/x108x1nth8066r81.pdf](http://www.springerlink.com/index/x108x1nth8066r81.pdf)
- [36] Carlton M.Caves and Gerard J.Milburn, **“Qutrit entanglement”**, October 2, 2009
- [37] Istok P Mendes, **“The classification of three-parameter density matrices for a qutrit”**, August 2006
- [38] Caves C M and Milburn G J 2000 *Opt. Commun.* **179** 439
- [39] Rahul Bijurkar, **“Representation of qudits on a riemann sphere”**, (Submitted on 28 Apr 2006 (v1), last revised 20 Mar 2007)
- [40] Gen Kimura, **“The bloch vector for N-level systems”**, February 13, 2003
- [41] Reinhold A.Bertlmann and Philipp Krammer, **“Bloch vectors for qudits”**, 12 Jun 2007
- [42] P.Rungta, W.J.Munro, K.Nemoto, P.Deuar, G.J.Milburn, and C.M.Caves, **“Qudit entanglement”**, 2000 February 1
- [43] Bechmann-Pasquinucci H and Peres A 2000 *Phys. Rev. Lett.* **85** 3313
- [44] Brukner C, Zukowski M and Zeilinger A 2002 *Phys. Rev. Lett.* **89** 197901
- [45] Michel Planat and Metod Saniga, **“On the pauli graphs of N-qudits”**, arxiv: [quant-ph/0701211v3](http://quant-ph/0701211v3), 11Jun, 2007
- [46] Melikidze, V. V. Dobrovitski, H. A. De Raedt, M. I. Katsnelson, and B. N. Harmon, **“Parity effects in spin decoherence”**, *Phys. Rev. B* **70**, 014435 (2004)
- [47] Goong Chen, David A.Church, Berthold-Georg Englert, Carsten Hankel, Bernd Rohwedder, Marlan O.Scully, M.Suhail Zubairy, **“Quantum computing devices”**
- [48] Colin P.Williams, Scott H.Clearwater, **“Explorations in quantum computing”**

[49] وحید کریمپور، مقاله‌ی سوم، ماتریس چگالی و حالت‌های آمیخته، ص ۱۳ الی ۱۶

[۵۰] مجیدی، ع، ۱۳۸۸، پایان نامه ارشد، **“جستجوی کوانتومی”**، دانشکده فیزیک، دانشگاه صنعتی شاهرود

- [51]Eva Borbely, “**Grover search alorithm**”, Technological University Budapest, Hungary
- [52] L.Grover, **Quantum mechanics helps in searching for a needle in a haystack**”, 3C-404A Bell Labs, 600 Mountain Avenue, Murray Hill NJ 07974, lkgrover@bell-labs.com
- [53]Ahmed Younes, “**Strength and weakness in grover’s quantum search algorithm**”, Department of Mathematics and Computer Science, November 27, 2008
- [54] Ahmed Younes, John Rowe, Julian Miller, “**Quantum search with more reliable behaviour using partial diffusion**”,in:Proc.of the 7<sup>th</sup> int.conf of quantum communication.measurement and computing,pp 171-174 , February 1, 2008
- [55]A.Younes, J.Rowe, J.Miller, “**Enhanced quantum searching via entanglement and partial diffusion**”, December 31, 2007
- [56]A.Younes, Strength and Weakness in Grover’s Quantum Search Algorithm, arxiv:quant-ph/0811.448

[ ۵۷ ] خراط زاده، ا، ۱۳۸۸، پایان نامه ارشد، “**نظریه‌ی تصمیم و احتمال‌های کوانتومی**”، دانشکده فیزیک، دانشگاه صنعتی شاهرود