دانشکده علوم ریاضی

پایان‌نامه کارشناسی ارشد کد و رمز

بررسی روش‌هایی برای ساخت کدهای LDPC کوانتومی با استفاده از کدهای کلاسیک

نگارنده: مائده نجفی

استاد راهنما

دکتر میثم علیشاهی

استاد مشاور

دکتر فرزانه امیرزاده دانا

آذر ۱۴۰۰

این پایان نامه را تقدیم می‌کنم به پدر، مادر و همسر عزیزم که حضورشان همیشه گرمابخش روح من بوده است.

سپاس‌گزاری...

اکنون که به یاری پروردگار و یاری و راهنمایی اساتید بزرگ موفق به پایان این رساله شده‌ام وظیفه خود دانسته که نهایت سپاسگزاری را از تمامی عزیزانی که در این راه به من کمک کرده‌اند به عمل آورم:

در آغاز از استاد بزرگ جناب آقای دکترمیثم علیشاهی که راهنمایی این پایان‌نامه را به عهده داشته‌اند کمال تشکر را دارم.

از خانم دکتر فرزانه امیرزاده دانا که استاد مشاور این پایان‌نامه بوده‌اند نیز قدردانی می‌نمایم.

از داوران گرامی که زحمت داوری و تصحیح این پایان‌نامه رابه‌عهده داشتند کمال سپاس را دارم.

مائده نجفی
آذر ۱۴۰۰

تعهد نامه

اینجانب **مائده نجفی** دانشجوی کارشناسی ارشد رشته **ریاضی کاربردی علوم ریاضی** دانشگاه شاهرود، نویسنده پایان‌نامه با عنوان **بررسی روش‌هایی برای ساخت کدهای** LDPC **کوانتومی با استفاده از کدهای کلاسیک** ، تحت راهنمایی **میثم علیشاهی** متعهد می‌شوم:

- تحقیقات در این پایان‌نامه توسط اینجانب انجام شده است و از صحت و اصالت برخوردار است.
- در استفاده از نتایج پژوهش‌های دیگر پژوهش‌گران، به مرجع مورد استفاده استناد شده است.
- مطالب این پایان‌نامه، تا کنون توسط خود، یا فرد دیگری برای دریافت هیچ نوع مدرک یا امتیازی در هیچ‌جا ارایه نشده است.
- حقوق معنوی این اثر، به دانشگاه صنعتی شاهرود تعلق دارد، و مقالات مستخرج با نام ‘‘ دانشگاه صنعتی شاهرود’’ یا “ Shahrood University of Technology ” به چاپ خواهد رسید.
- حقوق معنوی تمام افرادی که در به‌دست آوردن نتایج اصلی پایان‌نامه تاثیرگذار بوده‌اند، در مقالات مستخرج از پایان‌نامه رعایت می‌گردد.
- در تمام مراحل انجام این پایان‌نامه، در مواردی که از موجود زنده (یا بافت‌های آنها) استفاده شده است، ضوابط و اصول اخلاقی رعایت شده است.
- در تمام مراحل انجام این پایان‌نامه، در مواردی که به حوزه اطلاعات شخصی افراد دسترسی یافته (یا استفاده شده است)، اصل رازداری و اصول اخلاق انسانی رعایت شده است.

مائده نجفی
آذر ۱۴۰۰

مالکیت نتایج و حق نشر

- تمام حقوق معنوی این اثر و محصولات آن (مقالات مستخرج، کتاب، برنامه‌های رایانه‌ای، نرم‌افزارها و تجهیزات ساخته شده) 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 این پایان‌نامه بدون ذکر منبع مجاز نمی‌باشد.

چکیده

در این پایان‌نامه کلاسی از کدهای بررسی توازن تنک (LDPC) کوانتومی را بررسی می‌کنیم که کدهای پایدارساز شبه دوری (QCS) از کدهای بررسی توازن تنک شبه دوری QC-LDPC نامیده می‌شوند. کدهای QCS پیشنهادی شامل خانواده‌ای از کدهای پایدارساز غیر_کالدر بنک شوراستین (CSS) می‌باشند.

کدهای QC-LDPC با توجه به ضرب داخلی سیمپلکتیک (SIP) خودمتعامد می‌باشند و از زیر ماتریس‌های مربعی لاتین غیر متعامد با پراکندگی آرایه ساخته شده‌اند. مربع‌های لاتین با استفاده از مجموعه‌های (غیر) باقیمانده مربعی از پیمانه‌های اول p ساخته می‌شوند به طوری‌که $p = ۴n \pm ۱$. برای $p = ۴n - ۱$، دو ساختار مانند کدهای QCS نوع I-A و نوع I-B به ترتیب براساس انطباق ماتریس و الحاق ماتریس ارائه می‌شود. برای $p = ۴n + ۱$، کدهای QCS نوع_II براساس جایگشت ماتریس پایه ارائه می‌شود. نشان می‌دهیم که ماتریس بررسی توازن برای کدهای QCS نوع_I-B و نوع_II با در نظر گرفتن SIP برای همه مرتبه‌های ماتریس جایگشت دوری، خودمتعامد هستند. این منجر به مجموعه‌هایی از کدهای QCS می‌شود که با یک ماتریس پایه مشخص می‌شوند. نشان می‌دهیم که کمینه فاصله از کدهای QCS نوع_II از پایین کراندار به کمینه فاصله از کدهای QC-LDPC هستند. نتایج شبیه‌سازی نشان می‌دهد که کدهای QCS پیشنهادی نسبت به برخی از کدهای موجود با طبقه خطای زیر $۱۰^{-۷}$ بهتر از کانال‌های دپولاریز کوانتومی عمل می‌کنند.

کلمات کلیدی: کدهای بررسی توازن تنک، کدهای پایدارساز شبه دوری (QCS)، مجموعه‌های (غیر) باقی‌مانده مربعی، مربع‌های لاتین، ماتریس جایگشت دوری (CPM).

فهرست مطالب

فهرست تصاویر

فهرست جداول

پیشگفتار

ظهور نظریه کدگذاری در سال ۱۹۴۸ توسط کلود شانون صورت گرفت. کدگذاری گرایشی از ریاضیات است که متکی به ایده‌های ریاضیات محض می‌باشد و به ویژه، بیانگر زیبایی جبر است. نظریه کدگذاری، با استفاده از الگوهایی که از مفاهیم اصلی جبر ساخته می‌شوند، به تشخیص اصل داده‌های دریافتی می‌پردازد. کدهایی مفید هستند که قادر به تصحیح خطاها و تشخیص اصل داده‌های دریافتی باشند و به چنین کدهایی، کدهای تصحیح کننده خطا می‌گوییم [۵۲].

در ابتدا، بسیاری از محققان معتقد بودند که کدهای تصحیح خطای کوانتومی وجود ندارند و روند تصحیح خطای کوانتوم غیرقابل اجرا است. اواسط دهه ۹۰، با کشف کد ۹ـ کیوبیت توسط شور[۱] [۵۰] و کد ۷ـ کیوبیت توسط استین[۲] [۵۱] وجود کدهای کوانتومی ثابت شد. کارهای [۱۵، ۱۶، ۱۷] نشان دادند که می‌توان یک دسته از کدهای کوانتومی، یعنی کدهای کالدربنک‌ـ شورـ استین[۳] (CSS) را از یک جفت کد خطی به دست آورد. از آن زمان، انواع مختلفی از کدهای تصحیح خطای کوانتوم از جمله فرمالیزم کدهای پایدارساز ارائه شده است [۲۵]. فرمالیزم پایدارساز مفهوم اندازه‌گیری بررسی توازن را به نظریه اطلاعات کوانتومی می‌بخشد. به ویژه، نتیجه اندازه‌گیری بررسی توزان، بدون انطباق کوانتوم، مشابه بردار سندروم در نظریه اطلاعات کلاسیک است که می‌تواند به عنوان ورودی کدگذار استفاده شود. برای مثال، کدهای توربو کوانتوم [۹]، و کدهای بررسی توزان خلوت کوانتومی [۴۰]، زیرکلاس‌های معروف از کدهای پایدارساز هستند که می‌تواند با استفاده از روش تکراری براساس بردار سندروم کدگشایی شود.

کدهای LDPC کوانتومی ساخته شده از کدهای LDPC کلاسیک [۴۱]، در زمینه باینری یا میدان چهارتایی توجه محققان را در چند سال گذشته جلب کرده اند. به طور مستقیم اگر دو کد باینری کلاسیک دارای ماتریس‌های بررسی توازن از یک طول باشند، بنابراین محدودیت متعامد یک کد CSS به دو ماتریس متعامد تحت فضای ضرب داخلی اقلیدسی نیاز دارد، در حالی که محدودیت متعامد بودن کد کوانتومی غیرـ CSS به ماتریس متعامد تحت فضای

[1] Shor
[2] Steane
[3] Calderbank-Shor-Steane code

ضرب داخلی سیمپلکتیک [1] (SIP) نیاز دارد.

کامارا و همکاران[2] ساخت کدهای LDPC کوانتومی غیرـCSS از کدهای LDPC چهارگانه خودمتعامد را با استفاده از نظریه گروه‌ها پیشنهاد کردند [۱۴]. مشخص شد که گراف تنر[3] از کدهای چهارگانه خودـ متعامد باید دارای دورهایی به طول چهار باشد. این امر به دلیل نیاز مشترک بین هر جفت سطرهای ماتریس بررسی توازن اجتناب‌ناپذیر است. بنابراین تان[4] و لی[5] اولین کسانی بودند که کدهای LDPC کوانتومی غیرـCSS را با استناد به کدهای باینری کلاسیک با ماتریس دوری طراحی کردند.

بسیاری از کارها به ساختن کدهای LDPC شبه دوری[6] (QC) با استفاده از ماتریس جایگشت دوری[7] (CPM) برای طراحی کوانتوم تمرکز کرده‌اند [۳۰، ۳۱، ۵۳، ۵۸]. ماتریس پایه از کد QC-LDPC یک ماتریس صحیح است که درایه‌ها مقادیر تغییر از CPMs می‌باشد. بنابراین مشکل اصلی ساخت کدهای کوانتومی از کدهای QC-LDPC، طراحی مجموعه مقادیر تغییر از CPMs است. برای تعیین این مقادیر تغییر، روش‌های مختلفی بررسی شده اند. به عنوان مثال، ساختارهای جبری کدهای LDPC کوانتومی از مربع‌های لاتین و از هندسه‌های محدود [۷، ۱۹]. همچنین، تغییرات دوری را می‌توان با حل‌کردن معادلات خطی یا با جست‌وجوی عددی صحیح که شرایط خاصی را برآورد می‌کنند، به دست آورد [۵۳].

در این پایان‌نامه، طراحی انعطاف‌پذیر کدهای LDPC کوانتومی غیرـ CSS براساس رویکردهای جبری بررسی می‌شود. به ویژه، چندین ساختار سیستماتیک از کدهای LDPC کوانتومی غیرـ CSS براساس کدهای منظم QC-LDPC پیشنهاد می‌شود.

[1] symplectic inner product (SIP) space
[2] Camara et al.
[3] Tanner graph
[4] Tan
[5] Li
[6] quasi-cyclic
[7] circulant permutation matrix

فصل ۱

تعاریف و مفاهیم مقدماتی

۱.۱ مقدمه

نظریه کدگذاری که بر اساس مفاهیم جبر ـ مبنا نهاده شده است شامل سه حوزه اصلی کدگذاری کانال، کانال مخابراتی و کدگشایی کانال است. کدگذاری کانال شامل روش‌های کدگذاری دنباله خروجی از منبع اطلاعات با استفاده از مفهوم افزونگی[1] است. این افزونگی به گیرنده امکان شناسایی و تشخیص خطا در دنباله دریافتی از یک کانال آغشته به نویز را می‌دهد. یک کانال مخابراتی یک محیط فیزیکی برای تبادل اطلاعات بین فرستنده و گیرنده از طریق حمل سیگنال است. کدگشایی کانال فرایند تشخیص و بازیابی کدواژه ارسالی از روی دنباله دریافتی است. برای توضیحات بیشتر می‌توان به منابع [۱۳، ۴۷، ۴۹، ۵۲، ۵۴] مراجعه کرد.

[1] Redundancy

۲.۱ مفاهیم جبری پیش‌نیاز

در این بخش برخی از مفاهیم جبری پیش‌نیاز، شامل قضایا و تعاریف مربوطه ارائه می‌شود. مفاهیم این بخش از مرجع [۱۲] برگرفته شده اند.

تعریف ۱.۲.۱. یک فضای برداری $(V,+,\cdot)$ روی میدان F عبارت است از یک مجموعه ناتهی از بردارها با این شرایط که:

- $(V,+)$ یک گروه آبلی باشد.
- برای هر $a \in F$ و $u,v \in V$ داریم $a\cdot(u+v)=a\cdot u+a\cdot v$.
- برای هر $a \in F$ و $v \in V$، $av \in V$. هر عضو فضای برداری V را بردار می‌نامیم.

فرض کنیم V یک فضای برداری روی میدان F_q باشد و $\emptyset \neq S \subseteq V$. در این صورت گوییم S یک مجموعه **مستقل خطی** می‌باشد هرگاه داشته باشیم:

$$\lambda_1 v_1+\lambda_2 v_2+\ldots+\lambda_n v_n=0 \rightarrow \lambda_1=\lambda_2=\ldots=\lambda_n=0.$$

در غیر این صورت بردارهای v_1، v_2، ...، v_n را **وابسته خطی** گوییم.

فرض کنیم V یک فضای برداری روی میدان F_q باشد. در این صورت مجموعه $S=\{v_1,v_2,\ldots,v_n\}\subseteq V$ را یک **مولد** برای فضای برداری V می‌نامیم هرگاه داشته باشیم:

$$\langle S\rangle=\{\lambda_1 v_1+\lambda_2 v_2+\ldots+\lambda_n v_n \mid \lambda_i \in F_q,\ \ v_i \in S,\ \ 1\leq i\leq q\}.$$

اگر $S=\emptyset$ آنگاه $\langle S\rangle=\{0\}$.

فرض کنید V یک فضای برداری روی میدان F_q باشد. در این صورت

$$S=\{v_0,v_1,\ldots,v_n\}\subseteq V$$

یک **پایه**[1] برای V نامیم، هرگاه

الف) S مستقل خطی باشد.

ب) S مولد باشد.

[1] base

نکته ۱.۲.۱. یک فضای برداری روی میدان F_q می‌تواند چندین پایه مختلف داشته باشد ولی تمام پایه‌های آن باید هم عدد (هم کاردینال) باشند. این عدد را **بعد فضای برداری**[۱] می‌گوییم و با نماد $\dim_{f_q}(V)$ نمایش داده می‌شود.

یک پایه برای فضای برداری V مجموعه‌ای مستقل خطی از بردارهای V است که فضای برداری V را پدید آورد. تعداد اعضای پایه یک فضای برداری را بعد آن فضا می‌گویند.

تعریف ۲.۲.۱. در یک فضای برداری V روی میدان $\mathbb{C}$، عمل دوتایی $\langle , \rangle : V \times V \longrightarrow \mathbb{C}$ را یک ضرب داخلی[۲] می‌نامیم، هرگاه در شرایط زیر صدق کند:

۱) $\langle x, y + \alpha z \rangle = \langle x, y \rangle + \alpha \langle x, z \rangle \quad \forall\, x, y, z, \in V, \ \ \forall\, \alpha \in F$

۲) $\langle x, y \rangle = \langle y, x \rangle$

۳) $\forall\, x \in V \quad \langle x, x \rangle \in \mathbb{R}, \quad \langle x, x \rangle \geq ۰$

۴) $\langle x, x \rangle = ۰ \leftrightarrow x = ۰.$

فضایی را که به ضرب داخلی مجهز شده باشد، یک **فضای ضرب داخلی** [۳] می‌گوییم.

تعریف ۳.۲.۱. برای هر دو ماتریس A و B ازمرتبه $m \times n$ **ضرب داخلی اثر** به به صورت زیر تعریف می شود:

$$\langle A, B \rangle = \sum_{ij} a_{ij} b_{ij}.$$

نمادگذاری ۱.۲.۱. فضای برداری V، N بعدی با پایه $\{e_۱, e_۲, \ldots, e_N\}$ را در نظر می‌گیریم. هر بردار $v \in V$، بسطی از بردارهای پایه به شکل زیر است:

$$v = \sum_{i=۱}^{N} v_i e_i.$$

ضرب داخلی این بردار با خودش، به صورت زیر نوشته می‌شود:

$$\langle v, v \rangle = \sum_{i=۱}^{N} v_i^* v_i.$$

[1] dimention of the vector space
[2] Inner product
[3] Inner product space

می‌توان به ازای هر چنین برداری، یک بردار سطری با نماد $|v\rangle$ و یک بردار ستونی با نماد $\langle v|$ به شکل زیر تعریف کرد:

$$|v\rangle = \begin{pmatrix} v_۱ \\ v_۲ \\ \vdots \\ v_N \end{pmatrix}, \quad \langle v| = \begin{pmatrix} v_۱^* & v_۲^* & \dots & v_N^* \end{pmatrix}$$

بردار $|v\rangle$ را یک بردار Ket و بردار $\langle v|$ را یک بردار Bra می‌نامیم. حاصلضرب این دو بردار، بدین شکل است:

$$\langle v|\rangle = \sum_{i=۱}^{N} v_i^* v_i = \langle v, v\rangle.$$

طرف راست یک ضرب داخلی است، اما طرف چپ، ضرب دو ماتریس است.

تعریف ۴.۲.۱. یک ماتریس جایگشت دوری از بعد $N \in \mathcal{N}$ و اندازه دور $۰ \leq k \leq N-۱$ به ماتریس مربعی $N \times N$ گفته می‌شود که سطر اول آن از k تا انتقال به راست سطر اول ماتریس همانی I_N به دست آمده باشد و مابقی سطرهای آن از یک انتقال به راست سطر ماقبل خود به دست آمده باشد. این ماتریس را با I^K نشان می‌دهیم. واضح است که $I^۰$ برابر با ماتریس همانی است.

۳.۱ مجموعه‌های باقی‌مانده و غیرباقی‌مانده مربعی

فرض کنیم $Z_p^* = \{۱, ۲, \dots, p-۱\}$ گروه ضربی از مرتبه $p-۱$ باشد به طوری‌که p عدد اول فرد است. $Q^{\mathcal{R}}$ و $Q^{\mathcal{NR}}$ به ترتیب بیانگر مجموعه باقی‌مانده مربعی و مجموعه غیرباقی‌مانده مربعی می‌باشند. α را به عنوان عضو اولیه در $GF(p)$ در نظر بگیرید. در این صورت لم زیر را خواهیم داشت.

لم ۱.۳.۱. [۵۹] برای هر عدد صحیح مثبت n و $p = ۴n \pm ۱$، به طوری‌که p یک عدد اول فرد است، خواهیم داشت

$$Q^{\mathcal{R}} = \{\alpha^{۲i} \mid ۰ \leq i < (p-۱)/۲\}$$

$$Q^{\mathcal{NR}} = \{\alpha^{۲i+۱} \mid ۰ \leq i < (p-۱)/۲\}$$

با $|Q^{\mathcal{R}}| = |Q^{\mathcal{NR}}| = (p-۱)/۲$.

از لم ۱.۳.۱ برای عدد اول p داریم:

$$Q^{\mathcal{R}} \cup Q^{\mathcal{NR}} = Z_p^*$$

و در Z_p^* دقیقا نصفی در $Q^{\mathcal{R}}$ و نصف در $Q^{\mathcal{NR}}$ می‌باشند. به علاوه برای

$$۰ \leq i, i' < (p-۱)/۲$$

و $i \neq i'$، $\alpha^{۲i} \cdot \alpha^{۲i'} \in Q^{\mathcal{R}}$ و $\alpha^{۲i+۱} \cdot \alpha^{۲i'} \in Q^{\mathcal{NR}}$. شرط زیر را به عنوان یک نتیجه مستقیم از لم ۱.۳.۱، خواهیم داشت.

لم ۲.۳.۱. [۵۹] برای $۰ \leq i < (p-۱)/۲$ خواهیم داشت:

$$\alpha^{۲i} Q^{\mathcal{R}} = \alpha^{۲i+۱} Q^{\mathcal{NR}} = Q^{\mathcal{R}},$$

$$\alpha^{۲i+۱} Q^{R} = \alpha^{۲i} Q^{\mathcal{NR}} = Q^{\mathcal{NR}}.$$

۴.۱ مربع لاتین

مربع‌های لاتین یکی از مفاهیم بنیادی و اساسی در ریاضیات گسسته است. سابقه طرح این موضوع به زمانی برمی‌گردد که اویلر مفهوم مربع لاتین را در سال ۱۷۸۲ بنا نهاد و از آن تاریخ به بعد همواره یکی از موضوعات تحقیق و پژوهش علوم ریاضی بوده و با بسیاری از مفاهیم و حوزه‌های دیگر پیوند خورده است. از جمله می‌توان ارتباط آن با نظریه گراف، جبر، طرح‌های بلوکی، آرایه‌های متعامد و آمار و احتمال را نام برد [۵۹].

تعریف ۱.۴.۱. فرض کنید $L = \{l_۰, l_۱, \ldots, l_{q-۱}\}$ یک مجموعه با q عضو باشد. ماتریس مربعی $q \times q$، $\mathscr{S}$ یک مربع لاتین[1] از مرتبه q است اگر هر سطر و ستون $\mathscr{S}$ شامل هر عضو L دقیقا یک

[1] Latin square

بار باشد.مربع لاتین خاصیت جابه‌جایی دارد هرگاه به‌ازای هر جفت (i,j) برای هر $\circ \leq i,j < q$ داشته باشیم $\mathscr{S}_{(i,j)} = \mathscr{S}_{(j,i)}$.

تعریف ۲.۴.۱. دو مربع لاتین از مرتبه q، $\mathscr{S} = [s_{(i,j)}]$ ، $\mathscr{U} = [u_{(i,j)}]$ متعامد هستند اگر و تنها اگر زوج مرتب‌های $(s_{(i,j)}, u_{(i,j)})$ برای هر $\circ \leq i,j < q$ متمایز باشند. در غیراین صورت غیرمتعامد می‌باشند.

مثال ۱.۴.۱. در زیر دو مربع لاتین از مرتبه ۳ و ۴ مشاهده می‌شود.

$$A' = \begin{array}{|c|c|c|}\hline ۲ & ۱ & \circ \\ \hline \circ & ۲ & ۱ \\ \hline ۱ & \circ & ۲ \\ \hline \end{array} \qquad A = \begin{array}{|c|c|c|}\hline ۱ & ۲ & \circ \\ \hline \circ & ۱ & ۲ \\ \hline ۲ & \circ & ۱ \\ \hline \end{array} \qquad B = \begin{array}{|c|c|c|c|}\hline \circ & ۱ & ۲ & ۳ \\ \hline ۱ & \circ & ۳ & ۲ \\ \hline ۲ & ۳ & ۱ & \circ \\ \hline ۳ & ۲ & \circ & ۱ \\ \hline \end{array}$$

اگر ستون‌های یک مربع لاتین $\mathscr{S}$ از مرتبه n را از بالا به پایین و سطرهای آن را از چپ به راست به ترتیب به اعداد مجموعه $\{\circ, ۱, \ldots, n-۱\}$ شماره‌گذاری کنیم در این صورت می‌توان آن را به صورت مجموعه‌ای از سه‌تایی‌های مرتب به صورت زیر نمایش داد:

$$\mathscr{S} = \Big\{(i,j;k) | \text{اگر } (i,j) \text{ـامین درایه ماتریس‌برابر } k \text{ باشد}\Big\}$$

اگر (i,j)ـامین درایه ماتریس برابر k باشد، خواهیم نوشت $k \in (i,j)_{\mathscr{S}}$ یا $(i,j)_{\mathscr{S}} = k$. همچنین زیرمجموعه‌ای از ۳تایی مرتب مانند $\mathscr{S}$ با $n^۲$ عضو از $L \times L$ یک مربع لاتین از مرتبه n هست هرگاه:

اگر $(i,j;k) \in \mathscr{S}$ و $(i,j;k') \in \mathscr{S}$ آنگاه $k = k'$؛

اگر $(i,j;k) \in \mathscr{S}$ و $(i,j';k) \in \mathscr{S}$ آنگاه $j = j'$؛

اگر $(i,j;k) \in \mathscr{S}$ و $(i',j;k) \in \mathscr{S}$ آنگاه $i = i'$ است.

تعریف ۳.۴.۱. قطر پراکنده[1] $\mathcal{T} \subset \{(i,j) \mid \circ \leq i,j < q\}$ از مربع لاتین از مرتبه q یک مجموعه از q جایگاه متمایز از ماتریس است به طوری‌که هر سطر و ستون تنها شامل یک عضو از این مجموعه باشد.

[1] transversal

تعریف ۴.۴.۱. فرض کنید $\mathcal{T}$ یک قطر پراکنده از $\mathscr{S}$ باشد. $\pi_{\mathcal{T}}$ به عنوان یک ماتریس جایگشت دودویی از مرتبه $q \times q$ تعریف می‌شود به طوری‌که برای هر $\circ \leq i,j < q$، اگر $(i,j) \in \mathcal{T}$، آنگاه درایه (i,j)ـام دارای مقدار یک باشد و اگر $(i,j) \notin \mathcal{T}$، آنگاه دارای مقدار صفر باشد.

۵.۱ مقدمه‌ای بر فیزیک

هر نوع اندازه‌گیری، در واقع یک فرآیند است که طی آن یک دستگاه ماکروسکوپی ذرات را بر حسب یک خاصیت معین، از یک دیگر جدا می‌کنند. تفسیر نتایج آن، متکی بر یک نظریه است که بدون آن نظریه، نمی‌توان به نتایج آن اندازه‌گیری، معنا و مفهومی نسبت داد.

در دنیای ماکروسکوپی، برخی خواص، هر مقداری را می‌توانند اتخاذ کنند،مانند جرم، اندازه و تکانه و نظایر آن. برخی دیگر از خواص، تنها مقادیر گسسته‌ای را به خود می‌گیرند. مانند تعداد ذرات گاز ایده‌آل محبوس در یک محفظه. بنابراین گسسته بودن یا پیوسته بودن، به خودی خود یک خاصیت منحصربه فرد میکروسکوپی نیست.

تمام اطلاعات ذرات را که می‌توان در چارچوب مکانیک کوانتومی استخراج کرد، در ماتریس چگالی آن نهفته است، به همین دلیل ماتریس چگالی[1] را ماتریس حالت این ذرات می گوییم. حتی برای یک ذره هم می‌توان از ماتریس چگالی سخن گفت [۲].

۱.۵.۱ حالت‌های یک کیوبیت

یک کیوبیت، ساده‌ترین سیستم کوانتومی با فضای هیلبرت دو بعدی است. این فضا را با $\mathbb{C}^2$ نشان می‌دهیم که فضای بردارهای دو بعدی مختلط است. حالت یک کیوبیت ψ را معمولا به صورت [۲]:

$$|\psi\rangle = a|\circ\rangle + b|1\rangle$$

می‌نویسیم که در آن $|\circ\rangle = (1,\circ)$ و $|1\rangle = (\circ,1)$ پایه‌های محاسباتی خوانده می‌شوند.

[1] Density matrix

ماتریس‌های پائولی یا عملگرهای $\{I, X, Y, Z\}$ از عملگرهای پرکاربرد در فضای کوانتومی هستند که روی یک کیوبیت اثر می‌کنند و به صورت

$$I := \begin{pmatrix} ۱ & ۰ \\ ۰ & ۱ \end{pmatrix}, \quad X := \begin{pmatrix} ۰ & ۱ \\ ۱ & ۰ \end{pmatrix}, \quad Y := \begin{pmatrix} ۰ & -i \\ i & ۰ \end{pmatrix}, \quad Z := \begin{pmatrix} ۱ & ۰ \\ ۰ & -۱ \end{pmatrix}$$

تعریف می‌شوند. مربع ماتریس‌های فوق برابر همانی است. یعنی:

$$X^۲ = Y^۲ = Z^۲ = I^۲ = I.$$

اثر عملگرها روی یک کیوبیت را در ادامه بررسی می‌کنیم. عملگر همانی هیچ تغییری در کیوبیت ایجاد نمی‌کند. اگر $q = (\alpha, \beta) \in \mathbb{C}^۲$ یک کیوبیت باشد، آنگاه

$$\begin{aligned} |q'\rangle &= I|q\rangle \\ &= \begin{pmatrix} ۱ & ۰ \\ ۰ & ۱ \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \\ &= \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \equiv \alpha|۰\rangle + \beta|۱\rangle, \end{aligned} \tag{۱.۱}$$

ماتریس X به صورت:

$$\begin{aligned} |q'\rangle &= X|q\rangle \\ &= \begin{pmatrix} ۰ & ۱ \\ ۱ & ۰ \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \qquad (۲.۱) \\ &= \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \equiv \beta|۰\rangle + \alpha|۱\rangle \qquad (۳.۱) \end{aligned}$$

عمل می‌کند. مشاهده می‌شود که عملگر X حالت (α, β) را به حالت (β, α) می‌نگارد که دراینصورت به اصطلاح خطای بیت‌ـ برگردان اتفاق افتاده است. به طور مشابه عملگرهای Y و Z به ترتیب به صورت زیر روی یک کیوبیت $|q\rangle$ اثر می‌کند که به اصطلاح خطای بیت‌ـ فاز برگردان وفازبرگردان نامیده می شوند.

$$|q'\rangle = Y|q\rangle = -i(\beta|۰\rangle - \alpha|۱\rangle),$$

$$|q'\rangle = Z|q\rangle = \alpha|۰\rangle - \beta|۱\rangle.$$

همچنین روابط زیر بین ماتریس‌های پائولی برقرار است:

$$\begin{cases} XY = -YX = iZ \\ YZ = -ZY = iX \\ ZX = -XZ = iY \end{cases}$$

۶.۱ کدگذاری کانال

در نظریه کدگذاری کدهای کنترل و تصحیح خطا عمدتا به دو زیرکلاس کدهای بلوکی[1] و کدهای پیچشی[2] تقسیم می‌شوند. تفاوت اساسی کدهای پیچشی در مقایسه با کدهای بلوکی، با حافظه بودن آنها است. در کدهای بلوکی دنباله اطلاعات خارج شده از منبع به بلوک‌های مجزایی تقسیم شده و پردازش هر بخش داده به‌صورت جداگانه انجام می‌گیرد. از سوی دیگر در کدهای پیچشی یک کدواژه n بیتی در خروجی به k بیت متناطر در ورودی کدگذار و m بخش k بیتی قبلی از دنباله اطلاعات بستگی دارد [۱۱].

۱.۶.۱ کد بلوکی

تعریف ۱.۶.۱. فرض کنید $A = \{a_1, a_2, \ldots, a_q\}$ یک مجموعه متناهی باشد که الفبای کد نامیده می‌شود و فرض کنید A^n تمامی رشته‌های به طول n روی A باشد، یعنی:

$$A^n = \{b_1 b_2 \ldots b_n \mid b_i \in A\}.$$

هر زیرمجموعه ناتهی C از A^n یک کد بلوکی q ـ تایی نامیده می‌شود. هر عضو C یک کدکلمه نامیده می‌شود. اگر $C \subseteq A^n$ دارای M کدواژه باشد، آنگاه گوییم C دارای طول n و اندازه M است و آن را یک (n, M) ـ کد می‌نامیم.

تعریف ۲.۶.۱. نرخ یک کد، میزان درصد اطلاعات در هر سمبل است که برای یک (n, M) ـ کد برابر $R = \frac{\log_q M}{n}$ می‌باشد. در واقع می‌دانیم هر چه نرخ کد بیشتر باشد، کد حاصل بهتر خواهد بود.

[1] Block codes
[2] Convolutional codes

تعریف ۳.۶.۱. فرض کنید F_q یک میدان متناهی از q است. یک کد بلوکی qتایی C که مجموعه کدواژه های آن، زیرفضایی k بعدی از فضای برداری F_q^n باشد را یک کد خطی q تایی می‌گوییم. کد C را یک (n,k)ـ کد خطی می‌نامند.

تعریف ۴.۶.۱. تعداد مکان‌هایی را که دو بردار $\mathbf{x}=(x_1,x_2,\ldots,x_n)$ و $\mathbf{y}=(y_1,y_2,\ldots,y_n)$ از F_q^n با هم متفاوت هستند را فاصله همینگ[1] بین دو بردار $\mathbf{x}$ و $\mathbf{y}$ می‌نامند و آن را با نماد $d(x,y)$ نشان می‌دهند و در صورتی که پارامتر d که در ادامه معرفی می‌شود، معلوم باشد کد C را یک (n,k,d)ـ کد خطی می‌نامند.

کمترین فاصله همینگ یک کد بلوکی C به صورت زیر تعریف می‌شود که کمینه فاصله نام دارد.

$$d(C)=\min\{d(x,y)\mid x,y\in C, x\neq y\}. \qquad (۱.۱)$$

تعریف ۵.۶.۱. اگر C یک کد خطی باشد، آنگاه وزن همینگ[2] یک کد کلمه

$$x=(x_1,x_2,\ldots,x_n)\in C$$

برابر با تعداد مؤلفه‌های ناصفر x است و با نماد $wt(x)$ نشان داده می‌شود. همچنین کمترین وزن کد C به صورت زیر تعریف می‌شود:

$$wt(C)=\min\{wt(x)\mid x\in C, x\neq 0\}. \qquad (۲.۱)$$

۲.۶.۱ ماتریس مولد و ماتریس بررسی توازن

یک (n,k)ـ کد خطی C زیرفضایی k بعدی از F_q^n است. بنابراین می‌توان k کدواژه مستقل خطی g_0، g_1، ...، g_{k-1} را در C پیدا کرد به طوری‌که هر کدواژه v در C ترکیبی خطی از این k کدواژه باشد. این k کدواژه تشکیل یک پایه برای کد خطی C می‌دهند. به عبارت‌دیگر، اگر هر کدام از اعضای این پایه را به عنوان سطری از یک ماتریس $k\times n$ در نظر بگیریم، ماتریس

[1] Hamming distance
[2] Hamming weight

مولد G ماتریسی است که هر سطر آن یکی از اعضای پایه است که به‌صورت زیر نمایش داده می‌شود [۱]:

$$G = \begin{pmatrix} g_0 \\ g_1 \\ \vdots \\ g_{k-1} \end{pmatrix} = \begin{pmatrix} g_{0,0} & g_{0,1} & \cdots & g_{0,n-1} \\ g_{1,0} & g_{1,1} & \cdots & g_{1,n-1} \\ \vdots & \vdots & \vdots & \vdots \\ g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,n-1} \end{pmatrix}.$$

اگر $u = (u_0, u_1, \ldots, u_{k-1})$ یک دنباله اطلاعات ورودی باشد، کدواژه متناظر آن یعنی v به شکل زیر است:

$$v = uG = (u_0, u_1, \ldots, u_{k-1}) \begin{pmatrix} g_0 \\ g_1 \\ \vdots \\ g_{k-1} \end{pmatrix} = u_0 g_0 + u_1 g_1 + \ldots + u_{k-1} g_{k-1}.$$

ماتریس G ماتریس مولد[1] کد C نامیده می‌شود. از آنجایی که که کد خطی C بیشتر از یک پایه دارد، ماتریس مولد کد یکتا نیست و به همین دلیل می‌توان با استفاده از جایگشت ستون‌ها و اعمال سطری مقدماتی، ماتریس G را به شکل استاندارد $G = (I_{k\times k}|P_{k\times(n-k)})$ بازنویسی کرد. در فرآیند کدگشایی از ماتریس بررسی توازن[2] استفاده می‌شود که از روی ماتریس مولد به صورت زیر به‌دست می‌آید:

$$H = \left(-P^T_{(n-k)\times k} \mid I_{(n-k)\times(n-k)} \right) \qquad (۳.۱)$$

هر بردار در فضای سطری ماتریس G بر سطرهای H عمود است. بنابراین یک n تایی v یک کدواژه در C است اگر و تنها اگر $vH^T = 0$. از این رو C فضای پوچ ماتریس H است. تمام ترکیبات خطی سطرهای ماتریس H تشکیل یک $(n, n-k)$ـ کدخطی می‌دهد که آن را کد دوگان C نامیده و با نماد $C^\perp$ نشان می‌دهیم. کد $C^\perp$ فضای پوچ ماتریس مولد کد C است [۱].

قضیه ۱.۶.۱. [۱] اگر کد C یک کد بلوکی خطی با ماتریس بررسی توازن H باشد، آنگاه کمینه فاصله کد C برابر با کمترین تعداد ستون‌های وابسته خطی در ماتریس H است.

[1] generator matrix
[2] parity check matrix

مثال ۱.۶.۱. ماتریس مولد زیر یک کد بلوکی خطی باینری با نرخ $R = \frac{۳}{۷}$ و طول $n = ۷$ را تعریف می‌کند. این ماتریس بیام با طول سه را به کدواژه‌های با طول هفت تبدیل می‌کند:

$$G = \begin{pmatrix} ۱ & ۰ & ۰ & ۰ & ۱ & ۱ & ۱ \\ ۰ & ۱ & ۰ & ۱ & ۰ & ۱ & ۱ \\ ۰ & ۰ & ۱ & ۱ & ۱ & ۰ & ۱ \end{pmatrix}$$

پیام $u = ۰۰۱$ به صورت زیر کدگذاری می‌شود:

$$v = uG = (۰۰۱) \begin{pmatrix} ۱ & ۰ & ۰ & ۰ & ۱ & ۱ & ۱ \\ ۰ & ۱ & ۰ & ۱ & ۰ & ۱ & ۱ \\ ۰ & ۰ & ۱ & ۱ & ۱ & ۰ & ۱ \end{pmatrix} = ۰۱۱۰۱۱۰$$

ماتریس بررسی توازن این کد دارای نمایشی به صورت زیر است :

$$H = \begin{pmatrix} ۰ & ۱ & ۱ & ۱ & ۰ & ۰ & ۰ \\ ۱ & ۰ & ۱ & ۰ & ۱ & ۰ & ۰ \\ ۱ & ۱ & ۰ & ۰ & ۰ & ۱ & ۰ \\ ۱ & ۱ & ۱ & ۰ & ۰ & ۰ & ۱ \end{pmatrix}$$

گیرنده دنباله (۰۱۱۰۱۱۰) را دریافت می‌کند و کدواژه بودن آن را به صورت زیر تایید میکند:

$$vH^T = (۰۱۱۰۱۱۰) \begin{pmatrix} ۰ & ۱ & ۱ & ۱ \\ ۱ & ۰ & ۱ & ۱ \\ ۱ & ۱ & ۰ & ۱ \\ ۱ & ۰ & ۰ & ۰ \\ ۰ & ۱ & ۰ & ۰ \\ ۰ & ۰ & ۱ & ۰ \\ ۰ & ۰ & ۰ & ۱ \end{pmatrix} = ۰۰۰۰۰۰۰$$

۳.۶.۱ کدهای دوری و شبه‌دوری

کدهای دوری[1] دسته‌ای مهم از کدهای خطی هستند که برای اولین بار توسط پرانگ در سال ۱۹۵۷ مورد مطالعه قرار گرفتند. کشف این کدها نقطه عطفی در نظریه کدگذاری می‌باشد [۴۶].

[1] cyclic codes

تعریف ۱.۶.۱. به زیرمجموعه S از F_q^n دوری گویند اگر $(a_{n-1}, a_0, a_1, \ldots, a_{n-2}) \in S$ به طوری‌که $(a_0, a_1, \ldots, a_{n-1}) \in S$.

یک کد خطی C کد دوری نامیده می‌شود اگر C یک مجموعه دوری باشد.

قضیه ۲.۶.۱. [۳۹] اگر C یک (n,k)ـ کدخطی qـ تایی باشد و هر کدواژه $(c_0, c_1, \ldots, c_{n-1})$ به صورت چندجمله‌ای $c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}$ نمایش داده شود، آنگاه کد C دوری است اگر و تنها اگر یک ایده‌آل در حلقه خارج قسمتی $R_n = \frac{F_q[x]}{\langle x^n - 1 \rangle}$ باشد.

توجه داشته باشید که حلقه خارج قسمتی R_n شامل همه چندجمله‌ای‌های از درجه کمتر از n روی میدان F_q است که جمع و ضرب بین هر دو چندجمله‌ای از این حلقه به پیمانه $x^n - 1$ روی میدان F_q محاسبه می‌شود.

قضیه ۳.۶.۱. [۳۹] اگر C یک کد دوری باشد، در این صورت:

- یک چندجمله‌ای تکین یکتا مانند $g(x)$ از کمترین درجه در C موجود است که C را تولید می‌کند. این چندجمله‌ای را چندجمله‌ای مولد می‌گویند.
- $g(x) | x^n - 1$.
- اگر $\deg g(x) = r$، آنگاه بعد کد C برابر $n - r$ است و کد C به صورت زیر تعریف می‌شود:

$$C = \langle g(x) \rangle = \{u(x) g(x) | \deg g(x) = r\}. \qquad (۴.۱)$$

- اگر $g(x) = g_0 + g_1 x + \ldots + g_r x^r$، آنگاه ماتریس مولد کد C دارای نمایشی به صورت زیر است که در آن هر سطر یک انتقال از سطر قبلی است.

$$G = \begin{pmatrix} g_0 & g_1 & \ldots & g_r & & \\ & g_0 & g_1 & \ldots & g_r & \\ & & \ddots & \ddots & \ddots & \ddots \end{pmatrix}.$$

مثال ۲.۶.۱. کد دوری $(۷,۴)$ همینگ توسط چندجمله‌ای مولد $g(x) = ۱ + x^۲ + x^۳$ تولید می‌شود. جدول ۱.۱ کلمات پیام و کدواژه های این کد را به دو صورت دنباله‌ای و چندجمله‌ای از درجه شش یا کمتر نشان می‌دهد.

جدول ۱.۱: نمایش پیام و کدواژه های کد دوری $(۷,۴)$ همینگ به دو شکل باینری و چندجمله‌ای

u	$u(x)$	$u(x)g(x)$	v
۰۰۰۰	۰	۰	۰۰۰۰۰۰۰
۱۰۰۰	۱	$۱+x^۲+x^۳$	۱۰۱۱۰۰۰
۰۱۰۰	x	$x+x^۳+x^۴$	۰۱۰۱۱۰۰
۱۱۰۰	$۱+x$	$۱+x+x^۲+x^۴$	۱۱۱۰۱۰۰
۰۰۱۰	$x^۲$	$x^۲+x^۴+x^۵$	۰۰۱۰۱۱۰
۱۰۱۰	$۱+x^۲$	$۱+x^۳+x^۴+x^۵$	۱۰۰۱۱۱۰
۱۱۱۰	$۱+x+x^۲$	$۱+x+x^۵$	۱۱۰۰۰۱۰
۰۰۰۱	$x^۳$	$x^۳+x^۵+x^۶$	۰۰۰۱۰۱۱
۱۰۰۱	$۱+x^۳$	$۱+x^۲+x^۵+x^۶$	۱۰۱۰۰۱۱
۰۱۰۱	$x+x^۳$	$x+x^۴+x^۵+x^۶$	۰۱۰۰۱۱۱
۱۱۰۱	$۱+x+x^۳$	$۱+x+x^۳+x^۴+x^۵+x^۶$	۱۱۰۱۱۱۱
۰۰۱۱	$x^۲+x^۳$	$x^۲+x^۳+x^۴+x^۶$	۰۰۱۱۱۰۱
۱۰۱۱	$۱+x^۲+x^۳$	$۱+x^۴+x^۶$	۱۰۰۰۱۰۱
۰۱۱۱	$x+x^۲+x^۳$	$x+x^۲+x^۶$	۰۱۱۰۰۰۱
۱۱۱۱	$۱+x+x^۲+x^۳$	$۱+x+x^۳+x^۶$	۱۱۰۱۰۰۱

تعریف ۷.۶.۱. ماتریس مربعی A را دوری گویند اگر و تنها اگر هر سطر آن انتقال دوری سطر بالایی و سطر اولی انتقال آخرین سطر باشد.

تعریف ۸.۶.۱. کد خطی C به طول n را شبه‌دوری[۱] (QC) می‌نامند هرگاه بخش‌کننده‌ای از n مانند $n_۰$ موجود باشد به طوری‌که انتقال به چپ یا راست هر کدواژه به اندازه $n_۰$ سمبل کد کلمه‌ای در C باشد.

یک کد QC با پارامتر $(n=n_۰N, k=k_۰q)$ دارای افزونگی برابر با $r=(n_۰-k_۰)q$ است. ماتریس بررسی این کد نمایشی به صورت زیر دارد که در آن هر زیرماتریس $H^c_{i,j}$ یک ماتریس دوری از اندازه $q\times q$ است.

$$H=\begin{pmatrix} H^c_{۰,۰} & H^c_{۰,۱} & \cdots & H^c_{۰,n-۱} \\ H^c_{۱,۰} & H^c_{۱,۱}\cdots & H^c_{۱,n-۱} & \\ \vdots & \vdots & \ddots & \ddots \\ H^c_{r_۰-۱,۰} & H^c_{r_۰-۱,۱} & \cdots & H^c_{r_۰-۱,n-۱} \end{pmatrix}.$$

[1] quaci cyclic

ملاحظه ۱.۶.۱. یک کد QC که تحت انتقال به چپ یا راست پایا باشد، یک کد دوری است.

۴.۶.۱ کدهای LDPC

کدهای بررسی توازن تنک[1] (LDPC) خانواده مهمی از کدهای بلوکی هستند که نخستین بار توسط گالاگر در سال ۱۹۶۰ معرفی گردید [۲۸]. به دلیل پیچیده بودن این کدها و اینکه پردازنده‌های آن زمان توانایی پیاده‌سازی این کدها را نداشتند این کدها به مدت چندین دهه به دست فراموشی سپرده شدند. تنر در سال ۱۹۸۱ یک نمایش گرافی برای کدهای LDPC ارائه داد. پس از معرفی کدهای توربو در سال ۱۹۹۳ و الگوریتم کدگشایی تکراری[2] رویکردی دوباره به کدهای LDPC در سال ۱۹۹۵ توسط مک‌کی و نیل آغاز شد و نشان داده شد که کدهای LDPC نیز با استفاده از روش‌های کدگشایی تکراری می‌توانند عملکرد خطائی نزدیک به حد شانون داشته باشند [۳۸].

کدهای LDPC توسط نمایش گرافی موسوم به گراف تنر[3] که توسط تنر ابداع شده است، نمایش و کدگشایی می‌شوند.

تعریف ۹.۶.۱. گراف G را دو بخشی گوییم هرگاه بتوان V را به دو مجموعه U و W چنان افراز کرد که هر یال از G یک رأس از U را به رأسی از W وصل کند.

تعریف ۱۰.۶.۱. به یک ماتریس بررسی توازن $m \times n$، می‌توان یک گراف دوبخشی با مجموعه رأس‌های V_1 و V_2 نسبت داد به قسمی که مجموعه‌های V_1 و V_2 به ترتیب متناظر با n ستون و m سطر ماتریس H می‌باشند. هر عضو مجموعه V_1 رأس متغیر و متقابلا هر عضو مجموعه V_2 رأس بررسی نامیده می‌شود. یک عضو V_1 به عضوی از V_2 متصل است اگر و فقط اگر درایه متناظر در ماتریس بررسی توازن ناصفر باشد. با توجه به اینکه تنر اولین بار از این گراف برای نمایش کدهای LDPC استفاده نمود، آن را گراف تنر می‌نامند. کمر گراف تنر برابر طول کوتاه‌ترین دور این گراف است. در حالت کلی انتظار این است که گراف تنر دورهایی به طول کوتاه، به ویژه دور به طول ۴ نداشته باشد. در گراف تنر کدهای LDPC دورها دارای طول زوج

[1] low- density parity check codes
[2] iteration decoding algoritm
[3] Tanner graph

می‌باشند، زیرا گراف دوبخشی است. از نماد $TG(H)$ برای نمایش گراف تنر استفاده می‌شود. دورهایی از طول کوتاه ممکن است کارایی کد LDPC را با استفاده از الگوریتم کدگشایی تکراری کاهش دهند.

تعریف ۱.۶.۱۱. نسبت تعداد درایه‌های ناصفر یک ماتریس به کل درایه‌های آن را چگالی[1] ماتریس و یک ماتریس با چگالی کم را یک ماتریس خلوت[2] گویند.

تعریف ۱.۶.۱۲. یک کد LDPC یک کد بلوکی خطی است که ماتریس بررسی توازن آن خلوت باشد. در صورتی‌که سطرها و ستون‌های ماتریس بررسی توازن این کدها به ترتیب دارای وزن k و j باشند، آنها را کدهای LDPC (j,k) منظم و در غیراین صورت آنها را کدهای LDPC نامنظم می‌نامند. k و j را باید طوری انتخاب کنیم که در مقابل طول ستون‌های H اعداد کوچکی باشند.

۵.۶.۱ ساخت کدهای LDPC

کدهای LDPC براساس شیوه طراحی، به دو دسته کلی کدهای تصادفی و کدهای ساختاری تقسیم می‌شوند. کدهای تصادفی توسط رایانه پدید می‌آیند و در مقایسه با کدهای ساختاری کارایی نرخ خطای بیت[3] (BER) بهتری دارند ولی به دلیل نبود ساختار، پیچیدگی کدگذاری بالایی دارند. از روش‌های ساختاری برای طراحی کدهای LDPC می‌توان به روش مک‌کی–نیل و روش گالاگر اشاره نمود. در زیر به ساخت کدهای LDPC شبه دوری می‌پردازیم که نوعی کد ساختاری است که در مرجع [۳۲] ارائه شده است.

۶.۶.۱ کدهای LDPC شبه‌دوری

تعریف ۱.۶.۱۳. میدان متناهی F_q را در نظر بگیرید. عناصر ناصفر این میدان تشکیل یک گروه ضربی می‌دهند. فرض کنید a و b دو عنصر ناصفر در این میدان باشند به طوری‌که $o(b)=r_\circ$ و $o(a)=n_\circ$. در این صورت یک کد QC-LDPC با ماتریس بررسی توازن H موجود

[1] density
[2] low- density parity check matrix
[3] Bit error rate

است که H متشکل از $r_\circ \times n_\circ$ زیرماتریس است که در آن هر زیرماتریس I_x یک ماتریس همانی از اندازه $N \times N$ است به قسمی که سطرهای آن به اندازه x مکان به سمت چپ انتقال داده شده‌اند. ماتریس H دارای نمایشی به صورت زیر است:

$$H = \begin{pmatrix} I_1 & I_a & I_{a^2} & \dots & I_{a^{n_\circ-1}} \\ I_b & I_{ab} & I_{a^2 b} & \dots & I_{a^{n_\circ-1}b} \\ \vdots & \vdots & & \ddots & \vdots \\ I_{b^{r_\circ-1}} & I_{ab^{r_\circ-1}} & I_{a^2 b^{r_\circ-1}} & \dots & I_{a^{n_\circ-1}b^{r_\circ-1}} \end{pmatrix}$$

یک کد C با ماتریس بررسی توازن به فرم H دارای نرخ $R > 1 - (\frac{r_\circ}{n_\circ})$ است. می‌توان دید که حداقل $r_\circ - 1$ سطر وابسته در H وجود دارد. از ساختار ماتریس H واضح است که در هر سطر و ستون به ترتیب به تعداد $n_\circ$ و $r_\circ$ درایه یک وجود دارد. بنابراین C یک کد LDPC منظم است.

مثال ۱.۶.۳. یک کد QC-LDPC با ماتریس توازن زیر را در نظر بگیرید. این کد پارامترهای $(۱۵۵,۶۴,۲۰)$ دارد به طوری‌که $N = ۳۱$، $a = ۲$ و $b = ۵$.

$$H = \begin{pmatrix} I_1 & I_2 & I_4 & I_8 & I_{16} \\ I_5 & I_{10} & I_{20} & I_9 & I_{18} \\ I_{25} & I_{19} & I_7 & I_{14} & I_{28} \end{pmatrix}$$

نرخ این کد برابر $R = \frac{۶۴}{۱۵۵}$ است.

مثال ۱.۶.۴. کد QC-LDPC با پارامترهای $(۲۱,۸,۶)$ و ماتریس ارائه شده در زیر را در نظر بگیرید که $m = ۷$، $b = ۶$ و $a = ۲$.

$$H = \begin{pmatrix} I_1 & I_2 & I_4 \\ I_6 & I_5 & I_3 \end{pmatrix}$$

این ماتریس، ماتریس بررسی توازن یک $(۲,۳)$ـ کد منظم است.

گالاگر در [۲۸] نشان داده که برای $j > ۲$، کمینه فاصله (n, j, k)ـ کدهای LDPC با افزایش n (طول کد) به طور خطی افزایش می‌یابد. به علاوه گالاگر نشان داده است که برای $j > ۲$، نسبت کمترین فاصله همینگ کد به طول کد، به یک عدد ثابت α که به انتخاب k و j وابسته است، میل می‌کند.

برای کدگشایی کدهای LDPC می‌توان از روش‌های کدگشایی تعویض بیت[۱] (BF)، الگوریتم کدگشایی جمع‌ـضرب[۲] (SPA) و همینطور الگوریتم کدگشایی نشر اعتماد [۳] (BP) استفاده کرد. الگوریتم‌های کدگشایی کدهای LDPC به الگوریتم‌های تکراری عبور پیام معروف هستند.

[1]Bit fip decoding
[2]Sum- product algoritm
[3]Belief propagation algoritm

فصل ۲

کدهای تصحیح خطای کوانتومی

۱.۲ مقدمه

کدهای تصحیح خطای کوانتومی[1]، نقش بسیار مهمی در حفاظت اطلاعات کوانتومی ایفا می‌کنند. در سال‌های قبل، تلاش‌های بسیاری در جهت دستیابی به کدهای کوانتومی با پارامترهای مناسب بر روی میدان‌های مختلف شده است. ساختار کدهای کوانتومی به دست آمده از کدهای کلاسیک بر روی $\mathbb{F}_2$، اولین بار توسط کالدربنک–شور استین [۱۵] در سال ۱۹۶۶ ارائه شدند. این روش که به ساختار CSS شناخته می‌شود، با اقبال زیادی مواجه شده و امکان به دست آوردن کدهای پایدارساز کوانتومی بسیاری را فراهم کرده است، به عنوان مثال کدهای بررسی توازن کم چگالی یکی از زیر کلاس های شناخته شده کدهای پایدار ساز هستند که می‌توانند با استفاده از روش های تکراری براساس بردار سندروم کدگشایی شوند. به مرور زمان، کتکار[2] و همکارانش [۳۹] ساختار کدهای کوانتومی با الفبای گسترده‌ای از کدهای کلاسیک خطی بر روی $\mathbb{F}_q$ را شناسایی کردند.

[1] Quantum error correction Codes
[2] Ketkar

۲.۲ الفبا و زبان

هر مجموعه‌ای از علائم[1]، یک الفبا[2] خوانده می‌شود. به هر کدام از اعضای این مجموعه یک حرف و به هر دنباله‌ای از حروف یک رشته[3] یا یک کلمه[4] گویند. ۰۰۰۱۱۱ و ۰۱۰۱۰۱ هر دو رشته‌هایی از الفبای Σ هستند. معمولا برای نشان‌دادن رشته‌ها، از حروف s، w و نظیر آنها استفاده می‌شود و به صورت $s = s_1 s_2 \dots s_n$ نوشته می‌شود که در آن s_iها حروف الفبا هستند. عدد n طول رشته است که به صورت $|s| = n$ بیان می‌شود. مجموعه تمام رشته‌های ممکن از الفبای Σ با Σ^* نشان داده می‌شود. واضح است که Σ^* یک مجموعه نامتناهی عضوی است. رشته تهی، رشته‌ای است که شامل هیچ حرفی نباشد. این رشته را با ε نشان می‌دهند. طول رشته ε برابر با صفر می‌باشد. هرگاه w یک رشته باشد، w^R معکوس آن رشته است [۳۹]. به عنوان مثال، اگر $w = ۰۰۱۱۲$، آنگاه $w^R = ۲۱۱۰۰$.

تعریف ۱.۲.۲. [۳۹] یک زیرمجموعه از Σ^* را یک زبان روی الفبای Σ می‌نامیم.

۳.۲ غلبه بر موانع تصحیح خطای کوانتومی

تفاوت‌های کدهای کلاسیک با کدهای کوانتومی یا به عبارتی موانع کدهای کوانتومی درسالهای اولیه طرح اطلاعات کوانتومی باعث شده بود عده‌ای فکر کنند هرگز نمی توان اطلاعات کوانتومی را تصحیح کرد، اما امروزه یک نظریه کامل برای آشکارسازی و تصحیح خطای کوانتومی تدوین شده است که می تواند برتمام موانع غلبه کند. خطاهای کوانتومی برخلاف خطاهای کلاسیک پیوسته هستند اما اگر بتوانیم خطای بیت‌ـ برگردان[5]، فاز‌ـبرگردان[6] و بیت‌ـفاز‌ـبرگردان یعنی خطاهای پائولی را اصلاح کنیم آنگاه هر نوع خطایی حتی خطاهای پیوسته را نیز می‌توانیم اصلاح کنیم.

[1] symbols
[2] alphabet
[3] string
[4] word
[5] Bit-flip
[6] Phase-flip

عملگر پائولی و عملگر واحد، یک پایه برای تمام ماتریس‌ها با عملگرهای فضای دو بعدی کیوبیت می‌سازند:

$$U = I \otimes U_0 + X \otimes U_1 + Y \otimes U_2 + Z \otimes U_3.$$

نکته ۱.۳.۲. تمام نکته کدهای کوانتومی این است که چگونه حالت یک کیوبیت را کد کرد تا حالت‌های فوق بر هم عمود باشند و بتوان آنها را از هم جدا کرد.

البته خطا می‌تواند روی دو کیوبیت یا بیشتر رخ دهد ولی در صورتی که کیوبیت‌ها به خوبی از اثر محیط محافظت شوند، احتمال ایجاد خطا روی دو کیوبیت از ایجاد خطا روی یک کیوبیت کمتر است. همچنین احتمال ایجاد خطا روی تعداد بیشتری از کیوبیت‌ها، ناچیز خواهد بود.

۴.۲ کدهای کوانتومی

کدهایی وجود دارند که هرکدام قادرهستند خطاهای بیت_برگردان، فاز_برگردان و بیت_فاز برگردان را اصلاح کنند. به عنوان مثال درادامه به کد ۳ کیوبیتی که قادر است خطای بیت_برگردان را تشخیص دهد و اصلاح کند می‌پردازیم.

فرض کنید تنها امکانی که برای خطا وجود دارد، برگردان یک کیوبیت است به این معنا که در طول کانال ممکن است عملگر X روی کیوبیت اثر کند. در این صورت هرگاه یک کیوبیت در ابتدای کانال به صورت

$$|\psi\rangle = a|0\rangle + b|1\rangle,$$

ارسال شده باشد، در اثر خطای احتمالی ممکن است به صورت زیر دریافت شود:

$$X|\psi\rangle = a|1\rangle + b|0\rangle.$$

برای آشکارسازی وتصحیح این نوع خطا کیوبیت های $|0\rangle$ و $|1\rangle$ به صورت زیر کد می‌شود:

$$|0\rangle \to |0\rangle_E = |000\rangle, \quad |1\rangle \to |1\rangle_E = |111\rangle,$$

که علامت E از کدگذار گرفته می‌شود.

در نتیجه حالت یک کیوبیت به صورت زیر کد می‌شود:

$$|\psi\rangle = a|۰\rangle + b|۱\rangle \rightarrow |\psi\rangle_E = a|۰۰۰\rangle + b|۱۱۱\rangle.$$

این حالت ویژه، حالت مشترک عملگرهای $Z_۱Z_۲$ و $Z_۱Z_۳$ با مقادیر ویژه ۱ است. به عبارت دیگر:

$$Z_۱Z_۲|\psi\rangle_E, Z_۱Z_۳|\psi\rangle_E = |\psi\rangle_E.$$

حال اگر خطای $X_۱$، $X_۲$ و $X_۳$ رخ دهد، حالت $|\psi\rangle_E$ تبدیل به حالتی می‌شود که مقدار ویژه‌اش برای عملگرهای فوق تغییر خواهد کرد:

$$I|\psi\rangle_E = a|۰۰۰\rangle + b|۱۱۱\rangle \rightarrow Z_۱Z_۲ = ۱ \quad Z_۱Z_۳ = ۱$$

$$X_۱|\psi\rangle_E = a|۱۰۰\rangle + b|۰۱۱\rangle \rightarrow Z_۱Z_۲ = -۱ \quad Z_۱Z_۳ = -۱$$

$$X_۲|\psi\rangle_E = a|۰۱۰\rangle + b|۱۰۱\rangle \rightarrow Z_۱Z_۲ = -۱ \quad Z_۱Z_۳ = ۱$$

$$X_۳|\psi\rangle_E = a|۰۰۱\rangle + b|۱۱۰\rangle \rightarrow Z_۱Z_۲ = ۱ \quad Z_۱Z_۳ = -۱$$

این عملگرها که مقادیر ویژه آنها خطا را آشکار می‌کند، سندرم‌های خطا[1] نامیده می‌شود. زیرفضای کد یعنی C در اثر خطاهای متفاوت، به زیرفضاهای متعامد نگاشته می‌شود و در نتیجه با تعیین این که در کدام زیرفضا هستیم، می‌توان به خطای ایجاد شده پی برد. بعد از اینکه مشخص شد خطای بیت‌ـ برگردان در چه نقطه‌ای روی داده است، می‌توان با اعمال عملگر تصحیح کننده، خطا را اصلاح کرد.

نکته ۱.۴.۲. تمام کدهایی که خطا را تشخیص می‌دهند، لزوما نمی‌توانند آنها را تصحیح کنند. به عنوان مثال کد دوکیوبیتی زیر رادر نظربگیرید

$$|\psi\rangle = a|۰\rangle + b|۱\rangle \rightarrow |\psi\rangle_E = a|۰۰\rangle + b|۱۱\rangle.$$

[1] error syndrome

حال اگر یک خطای X_1،X_2 رخ دهد حالت $|\psi\rangle_E$ تبدیل به حالت های زیر می شود:

$$X_1|\psi\rangle_E = a|10\rangle + b|01\rangle$$

$$X_2|\psi\rangle_E = a|01\rangle + b|10\rangle$$

براحتی می توان با مقایسه ی این دوحالت از حالت اولیه تشخیص داد که خطایی رخ داده است.این کار بااندازه گیری Z_1 Z_2 که مقدارش برای هردوحالت بالا منفی یک است قابل انجام است.امااشکال این کد این است که تنها می تواند خطارا تشخیص دهد و نمی تواند تصحیح کند زیرامشخص نیست که خطای بیت_برگردان در کیوبیت اول رخ داده است یا کیوبیت دوم.

نکته ۲.۴.۲. فضای برداری حالت‌های n کیوبیت، یک فضای 2^n بعدی است که با $V = (\mathbb{C}^2)^{\otimes n}$ نشان داده می‌شود به طوری‌که $\mathbb{C}^2$، یک فضای دو بعدی مختلط با بردارهای پایه $|0\rangle$ و $|1\rangle$ است. کد C چیزی جز انتخاب یک زیرفضای مناسب از V نیست. هرگاه این زیرفضا دارای بعد 2^k باشد، گوییم کد مربوطه برای نوشتن k کیوبیت در n کیوبیت به کار رفته است. در حالت کلی، کدگذاری به صورت زیر می‌باشد:

$$|\psi\rangle = \sum_{x=0}^{2^k-1} \psi_x|x\rangle \to |\psi\rangle_E = \sum_{x=0}^{2^k-1} \psi_x|x\rangle_E,$$

به طوری‌که $\{|x\rangle_E\}$ پایه‌ای برای زیرفضای C از V می‌باشد. در مثالی که در بالا به آن پرداختیم فضای V یک فضای ۸بعدی است و زیرفضایی که انتخاب کرده‌ایم یک فضای ۲ بعدی است، لذا کدی که نوشته‌ایم یک کیوبیت را در سه کیوبیت می‌نگارد.

نکته ۳.۴.۲. هر کدی که می‌نویسیم تنها قادر است مجموعه‌ای از خطاها را اصلاح کند. این مجموعه را خطاهای قابل تصحیح توسط کد نامیده و با $\varepsilon_C = E_1, E_2, \ldots$ نمایش می‌دهیم. به عنوان مثال کدی که درقسمت بالا به آن پرداختیم تنها قادر است خطاهای تک بیتی را اصلاح کند.

نکته ۴.۴.۲. کدی که پیش‌تر نوشته شد، یک زیرفضای مشخص از زیرفضای مربوط به سه کیوبیت است. این زیرفضای دوبعدی زیرفضایی است با مقادیر ویژه ۱ برای دو عملگر Z_1Z_2

و Z_1Z_3. این دو عملگر را عملگرهای پایدارساز مربوط به این زیرفضا گویند. عملگر Z_2Z_3 نیز یک عملگر پایدارساز برای این فضا می‌باشد و مستقل از دو عملگر قبلی نیست. در واقع مجموعه عملگرهایی که این فضا را پایدار نگه می‌دارند، تشکیل یک گروه می‌دهند که به آن گروه پایدارساز می‌گویند. برای این کد، این گروه عبارت است از $S = \{Z_1Z_2, Z_1Z_3, Z_2Z_3, I\}$.

در این کد خطاهایی که روی کیوبیت رخ می‌دهد سه نوع عملگر پائولی X_1، X_2 و X_3 هستند. این خطاها با بعضی از عملگرها جابجا می‌شوند و با بعضی از آنها جابجا نمی‌شوند و دقیقا همین رابطه است که مقادیر ویژه عملگرهای پایدارکننده را از ۱ به ۱− تبدیل می‌کند و باعث می‌شود که ما بتوانیم وقوع خطا را تشخیص بدهیم. فرض کنید که S یک عملگر پایدارساز و E یک خطاست که با S جابجا نمی‌شود. هرگاه $|\psi\rangle$ یک حالت متعلق به کد باشد. بنابر تعریف می‌دانیم که

$$S|\psi\rangle = |\psi\rangle, \longrightarrow S(E|\psi\rangle) = -E(S|\psi\rangle) = -E|\psi\rangle. \qquad (۱.۲)$$

بنابراین وقتی که یک خطای E رخ می دهد تمام عملگرهای پایدارسازی که با E جابجا نمی‌شوند مقادیر ویژشان از ۱ به ۱− تغییر می‌کند. جدول زیر رابطه جابجایی عملگرهای خطا و سندروم‌های خطا را نشان می‌دهد. علامت مثبت به معنای جابجایی و علامت منفی به معنای پادجابجایی است.

X_3	X_2	X_1	I	
$+$	$-$	$-$	$+$	Z_1Z_2
$-$	$+$	$-$	$+$	Z_1Z_3

همانطور که از جدول بالا پیداست، سندروم‌های مربوط به خطاها همه با هم متفاوت‌اند و همین موضوع باعث تمیزدادن خطاها و در نتیجه تصحیح آنها می‌شود.

۵.۲ فرمالیزم پایدارساز

تعریف ۱.۵.۲. ضرب تانسوری عملیاتی است که طی آن یک فضای برداری بزرگتر از دو فضای برداری کوچکتر تشکیل می‌شود. اگر دوفضای برداری V و W با ابعاد به ترتیب m و n باشند

آنگاه $W \otimes V$ یک فضای برداری mn بعدی است که مولفه های آن ترکیب خطی از ضرب تانسوری مولفه‌های $|v\rangle \in V$ و $|w\rangle \in W$ هستند.

برای مثال ضرب تانسوری دو بردار $(۱,۲)$ و $(۳,۴)$ برداری است به صورت:

$$\begin{pmatrix} ۱ \\ ۲ \end{pmatrix} \otimes \begin{pmatrix} ۳ \\ ۴ \end{pmatrix} = \begin{pmatrix} ۱ \times ۳ \\ ۱ \times ۴ \\ ۲ \times ۳ \\ ۲ \times ۴ \end{pmatrix} = \begin{pmatrix} ۳ \\ ۴ \\ ۶ \\ ۸ \end{pmatrix}$$

در این مثال ضرب تانسوری روی بردارهایی از فضای دو بعدی انجام شد در حالی‌که این عملیات می تواند روی عملگرهای خطی نیز انجام شود. فرض کنید $A : V \longrightarrow V'$ و $B : W \longrightarrow W'$ آنگاه $A \otimes B : V \otimes W \longrightarrow V' \otimes W'$ خواهد بود. A را یک ماتریس $m \times n$ بعدی و B را یک ماتریس $p \times q$ بعدی در نظر بگیرید. نمایش ماتریس حاصلضرب تانسوری به صورت زیر است:

$$A \otimes B = \begin{pmatrix} A_{۱۱}B & \cdots & A_{۱n}B \\ \vdots & \ddots & \vdots \\ A_{m۱}B & \cdots & A_{mn}B \end{pmatrix}$$

که $A_{۱۱}B$ بیانگر یک زیرماتریس $p \times q$ بعدی است. برای مثال ضرب تانسوری ماتریس‌های پائولی X و Y به صورت زیر خواهد بود:

$$X \otimes Y = \begin{pmatrix} ۰Y & ۱Y \\ ۱Y & ۰Y \end{pmatrix} = \begin{pmatrix} ۰ & ۰ & ۰ & -i \\ ۰ & ۰ & i & ۰ \\ ۰ & -i & ۰ & ۰ \\ i & ۰ & ۰ & ۰ \end{pmatrix}$$

مجموعه عملگرهای پائولی به تنهایی تشکیل گروه نمی‌دهند چون ویژگی بسته بودن راندارند،اما اگر این مجموعه را در اعداد $\pm i$ و ± ۱ ضرب کنیم، آنگاه تشکیل یک گروه می‌دهند. این گروه را گروه پائولی روی یک کیوبیت می‌نامیم.

تعریف ۲.۵.۲. گروه پائولی روی یک کیوبیت عبارت است از:

$$\mathcal{P}_۱ = \{\pm ۱, \pm i\} \times \{I, X, Y, Z\}$$

گروه پائولی روی N کیوبیت به صورت زیر تعریف می‌شود:

$$\mathcal{P}_N = \{\pm ۱, \pm i\} \times \{\sigma_{i_۱} \otimes \sigma_{i_۲} \otimes \ldots \otimes \sigma_{i_n} \mid i_۱, i_۲, \ldots, i_n = ۰, ۱, ۲, ۳\}.$$

تعداد اعضای این گروه برابر است با $|\mathcal{P}_N| = ۴^{N+۱}$.

نکته ۱.۵.۲. هر دو عضو گروه پائولی با هم جابه‌جا می‌شوند.

نکته ۲.۵.۲. مربع هر عضو گروه پائولی برابر $+۱$ یا -۱ است.

تعریف ۳.۵.۲. هر زیرگروه از گروه $\mathcal{P}_N$ که عناصر آن ۱) هرمیتی باشند، ۲) جابه‌جا شوند، ۳) زیرگروه شامل -۱ نباشد، یک گروه پایدارساز خوانده می‌شود.

۶.۲ کدهای پایدارساز

فرض کنید $\mathcal{H} = \{|\psi\rangle\}$ فضای پایدار کوانتومی ۲^nـ بعدی از N کیوبیت باشد و

$$\mathcal{P}_۱ := i^c\{I = \begin{bmatrix} ۱ & ۰ \\ ۰ & ۱ \end{bmatrix}, X = \begin{bmatrix} ۰ & ۱ \\ ۱ & ۰ \end{bmatrix}, Z = \begin{bmatrix} ۱ & ۰ \\ ۰ & -۱ \end{bmatrix}, Y = iXZ\}$$

گروه پائولی باشد که روی یک کیوبیت عمل می‌کند و i واحد موهومی و i^c عامل فازی با $c \in \{۰, ۱, ۲, ۳\}$ می‌باشد. عملگرهای غیرهمانی که روی کیوبیت واحد عمل می‌کنند، به‌ترتیب دلالت بر عملگر بیت‌ـ برگردان (X)، عملگر فازـ برگردان (Z) یا هر دو (Y) دارد. در این صورت ضرب تانسوری $(\otimes)$ از $\mathcal{P}_۱$ تشکیل یک گروه پائولی Nـ کیوبیت می‌دهد که با $\mathcal{P}_N = i^c\{I, X, Y, Z\}^{\otimes N}$ نشان می‌دهند. برای هر دو عملگر $E, F \in \mathcal{P}_N$ تعریف می‌کنیم:

$$E \circ F := \prod_{j=۰}^{N-۱} E_j \circ F_j, \qquad (۱.۲)$$

به طوری‌که $E_j \circ F_j = +۱$ اگر $E_j F_j = F_j E_j$ و $E_j \circ F_j = -۱$ اگر $E_j F_j = -E_j F_j$. لذا دو عملگر پائولی یا جابه‌جایی‌اند $(E \circ F = +۱)$ یا غیرجابه‌جایی $(E \circ F = -۱)$ [۵۹].

تعریف ۱.۶.۲. [۵۹] کد پایدارساز $[[N, K, d^Q]]$ یک زیرفضای یکتای ۲^Kـ بعدی $\mathcal{H}_S$ از $\mathcal{H}$ است که توسط زیرگروه‌های آبلی $\mathcal{S}$ از گروه پائولی Nـ کیوبیت $\mathcal{P}_N$ با $-I^{\otimes N} \notin \mathcal{S}$ پایدار می‌شود به

طوری‌که همه عضوهای $\mathcal{S}$ به طور همزمان مقدار ویژه ۱+ را ایجاد می‌کنند ، یعنی [۲۵]:

$$S|\psi\rangle = |\psi\rangle, \quad \forall S \in \mathcal{S}, \quad |\psi\rangle \in \mathcal{H}_{\mathcal{S}}. \tag{۲.۲}$$

تعریف ۲.۶.۲. [۵۹] وزن یک عملگر پائولی S برابر با تعداد مؤلفه‌های غیر همانی تعریف می‌شود که توسط $wt(S)$ نشان داده می‌شود.

تعریف ۳.۶.۲. [۵۹] کمینه فاصله d^Q از کدهای پایدارساز به صورت زیر تعریف می‌شود:

$$d^Q = \min\{wt(E)|E \in \mathcal{N}_{\mathcal{S}} \backslash \mathcal{S}Z(\mathcal{P}_N)\}, \tag{۳.۲}$$

به طوری‌که

$$\mathcal{N}_S = \{E \in \mathcal{P}_N | E \circ S = +۱, \ \ \forall S \in \mathcal{S}\}$$

شامل همه عملگرهای جابه‌جایی $\mathcal{S}$ است و $Z(\mathcal{P}_N)$ مرکز گروه پائولی $\mathcal{P}_N$ است به طوری‌که $\mathcal{S} \subseteq Z(\mathcal{P}_N)$.

هنگامی که عملگر خطای E روی حالت $|\psi\rangle \in \mathcal{H}_{\mathcal{S}}$ عمل می‌کند، حالت تخریب شده $E|\psi\rangle$ با اندازه‌گیری مقادیر ویژه مجموعه مستقل $m = N - K$ مولدهای پایدارساز $\mathbf{g} = \{g_۰, g_۱, \ldots, g_{m-۱}\} \in \mathbf{S}$ مشخص می‌شود. در نتیجه بردار

$$\mathbf{M} = \{g_i \circ E | ۰ \leq i < m\} \in \{+۱, -۱\}^m$$

حاصل می‌شود که هنگام اندازه‌گیری خطای سندروم $s = \{+۱ \to ۰, -۱ \to ۱\}^m$ ایجاد می‌شود.

۱.۶.۲ فرم استاندارد ماتریس بررسی توزان برای کدهای پایدارساز

یک فرم استاندارد برای کدهای پایدارساز کواترنری می‌تواند انجام محاسبات کوانتومی را ساده نماید. هر ماتریس بررسی توازن برای کدهای پایدارساز را می‌توان با انجام عملیات حذفی گاوس به صورت یک حالت استاندارد نوشت. در زیر شکل استاندارد برای ماتریس بررسی توازن کدهای پایدارساز کوانتومی نشان داده شده است [۵۹].

$$\left(\begin{array}{ccc|ccc} \overbrace{I}^{r} & \overbrace{A_۱}^{n-k-r} & \overbrace{A_۲}^{k} & \overbrace{B}^{r} & \overbrace{C_۱}^{n-k-r} & \overbrace{C_۲}^{k} \\ ۰ & ۰ & ۰ & D & I & E \end{array}\right)$$

که در آن r رتبه‌ای از قسمت X ماتریس مولد پایدارساز است.

۷.۲ کدهای کالدربنک- شور-استین

کدهای کالدربنک-شور-استین یا به اختصار کدهای CSS از روی دو کد کلاسیک C_1 و C_2 به ترتیب با مشخصات $[n, k_1]$ و $[n, k_2]$ و با اندازه $|C_2| < |C_1|$ که دارای شرایط زیر هستند ساخته می‌شوند:

۱. کد C_1 شامل کد C_2 باشد، یعنی $C_2 \subset C_1$.

۲. کدهای C_1 و $C_2^{\perp}$ (کد دوگان C_2) هر دو قابلیت تصحیح t خطا را داشته باشند.

کدهای کلاسیک را به صورت $[n, k, d]$ نمایش می‌دهند. همچنین کدهای کوانتومی نیز به صورت $[[n, k, d]]$ نمایش داده می‌شوند که n طول کد، k بعد کد و d کمینه فاصله کد می‌باشد[۴].

۸.۲ کدهای کوانتومی غیر- CSS

کد پایدارساز کواترنری را می‌توان با استفاده از نظریه کدهای کوانتومی کلاسیک از طریق یکریختی بین گروه پائولی کیوبیت منحصربفرد $\mathcal{P}_1 = \{I, X, Z, Y = XZ\}$ (عامل‌های فازی تحت یکریختی نادیده گرفته می‌شوند) و میدان گالوای $GF(4) = \{0, 1, \omega, \overline{\omega} = \omega^2\}$ توصیف کرد. یکریختی شامل دو جنبه است [۵۹]:

عضوهای شناسایی $I \leftrightarrow 0$، $X \leftrightarrow 1$، $Z \leftrightarrow \omega$ و $Y \leftrightarrow \overline{\omega}$ و عملگر شناسایی جمعی $\leftrightarrow$ ضربی، ضرب داخلی اثر $\leftrightarrow$ جابه‌جایی. تحت این یکریختی، جابه‌جایی بین عملگر پائولی در (۱.۲) نشان داده شده است که با ضرب داخلی اثر[1] بین دو عضو از $GF(4)$ معادل است، یعنی:

$$E \circ F \equiv tr(\sigma_E \overline{\sigma}_F), \quad E, F \in \mathcal{P}_1 \longleftrightarrow \sigma_E, \sigma_F \in GF(4), \tag{۱.۲}$$

[1] trace inner product

به طوری‌که تابع اثر $tr(x) = x + x^{۲}$ روی $GF(۲)$ و $\overline{\sigma}_F = \sigma_{F^{۲}}$ اعمال می‌شود. برای دو عملگر پائولی Nـ کیوبیت $E = E_{۱}E_{۲}\dots E_N$ و $F = F_{۱}F_{۲}\dots F_N$ که به بردارهای

$$\sigma_E = (\sigma_{E_{۱}}, \sigma_{E_{۲}}, \dots, \sigma_{E_N})$$

و

$$\sigma_F = (\sigma_{F_{۱}}, \sigma_{F_{۲}}, \dots, \sigma_{F_N})$$

نگاشته می‌شود، خواهیم داشت $\sigma_E\overline{\sigma}_F = \sum_i \sigma_{E_i} \times \overline{\sigma}_{F_i}$ که به عنوان ضرب داخلی بین دو بردار تعریف می‌شود. لذا E و F جابه‌جایی‌اند اگر $tr(\sigma_E\overline{\sigma}_F) = ۰$ و غیرجابه‌جایی‌اند اگر $tr(\sigma_E\overline{\sigma}_F) = ۱$. فرض کنید $H_{GF(۴)}$ بیانگر ماتریس بررسی توازن کد پایدارساز باشد که شامل یکریختی m مؤلفه پایدارساز مولد g باشد. در این صورت $H_{GF(۴)}$ یک کد پایدارساز $[[N, K]]$ تعریف می‌شود [۵۹].

از طرف دیگر، با توجه به این واقعیت که هر عضو $GF(۴)$ را می‌توان در یک ۲ـتایی [۱] دودویی با استفاده از $۰۰ \longleftrightarrow ۰$، $۱۰ \longleftrightarrow ۱$، $۰۱ \longleftrightarrow \omega$ و $۱۱ \longleftrightarrow \overline{\omega}$ نشان داد، کد پایدارساز نیز می‌تواند از کدهای دودویی کلاسیک ساخته شود. نگاشت $\Phi : \mathcal{P}_N \longleftrightarrow GF(۲)^{۲N}$ تعریف می‌شود. این نشان می‌دهد که عملگر پائولی Nـ کیوبیتی که تنها با یک فاز تفاوت دارد می‌تواند به عنوان یک $۲N$ـ تایی دودویی از طریق نگاشت زیر بیان شود [۵۹]:

$$\Phi(E) = (a|b), \qquad (۲.۲)$$

به طوری‌که $a = (a_{۱}, a_{۱}, \dots, a_{N-۱})$ و $b = (b_{۰}, b_{۱}, \dots, b_{N-۱})$ دو Nـ تایی دودویی هستند که در کنار هم قرار گرفته‌اند. در اینجا، $a_j = ۱$ یک خطای بیتـ برگردان روی jـ امین کیوبیت را نشان می‌دهد، $b_j = ۱$ یک خطای فازـبرگردان روی jـ امین کیوبیت را نشان می‌دهد و دو خطا روی کیوبیت‌های یکسان توسط $a_j = b_j = ۱$ بیان می‌شود.

برای هر دو عملگر پائولی مجزای $E = (a|b)$ و $F = (a'|b')$، آنها یا جابه‌جا می‌شوند یا غیرجابه‌جایی‌اند، یعنی $E \circ F = \pm ۱$. این علامت توسط $(-۱)^{(a\cdot b')+(a'\cdot b)}$ تعیین می شود. به طوری‌که $(a \cdot b') + (a' \cdot b)$ ضرب داخلی پیچشی می‌باشد.

[۱] هر دوتایی توسط یک چندجمله‌ای به فرم $a + b\omega$ بیان می‌شود به طوری‌که $a, b \in \{۰, ۱\}$.

قضیه ۱.۸.۲. دو عضو جابه‌جایی‌اند اگر و تنها اگر ۲ـ تایی‌های متناظر آنها $(a \mid b)$ و $(a' \mid b')$ در شرط زیر صدق کنند:

$$(a \cdot b') + (a' \cdot b) = ۰ \pmod ۲, \tag{۳.۲}$$

به طوری‌که $\cdot$ ضرب نقطه‌ای $a \cdot b' = \sum_j a_j b'_j$ است.

برای گروه پایدارساز $\mathcal{S}$ تولید شده از مجموعه مولدهای پایدارساز مستقل $\mathbf{g} = \{g_۰, g_۱, \ldots, g_{m-۱}\}$، ماتریس بررسی توازن H از $\mathcal{S}$ توسط هر سطر متناظر از $\mathbf{H}$ به عنوان $\Phi(g_j)$ برای $۰ \le j < m$ و $g_j \in g$ تعریف می‌شود. در این صورت $\mathbf{H}$ از اندازه $m \times ۲N$ به فرم $\mathbf{H} = [\mathbf{H}_۱ \mid \mathbf{H}_۲]$ است به طوری‌که:

$$\mathbf{H}_۱ = \begin{bmatrix} \mathbf{a}_{g_۰} \\ \mathbf{a}_{g_۱} \\ \vdots \\ \mathbf{a}_{g_{m-۱}} \end{bmatrix}, \quad \mathbf{H}_۲ = \begin{bmatrix} \mathbf{b}_{g_۰} \\ \mathbf{b}_{g_۱} \\ \vdots \\ \mathbf{b}_{g_{m-۱}} \end{bmatrix}. \tag{۴.۲}$$

فرض کنید $\mathbf{h}_i = (\mathbf{a}_{g_i} \mid \mathbf{b}_{g_i})$ و $\mathbf{h}_{i'} = (\mathbf{a}_{g_{i'}} \mid \mathbf{b}_{g_{i'}})$ دو سطر از H باشند به طوری‌که $۰ \le i, i' < m$ و $i \neq i'$. چون هر دو عضو $\mathcal{S}$ باید جابه‌جا شوند، h_i و $h_{i'}$ با در نظر گرفتن ضرب داخلی پیچیده در (۳.۲) باید متعامد باشند. این نتیجه می‌دهد که برای m مؤلفه مولد پایدارساز باید در شرط زیر صدق کنند:

$$\mathbf{H}_۱\mathbf{H}_۲^T + \mathbf{H}_۲\mathbf{H}_۱^T = ۰^{m \times m} \pmod ۲, \tag{۵.۲}$$

که در آن $۰^{m \times m}$ ماتریس صفر $m \times m$ بعدی است و $(\cdot)^T$ دلالت بر ترانهاده ماتریس دارد. رابطه (۵.۲) قید SIP برای کد پایدارساز کوانتومی نامیده می‌شود [۴۰].

از (۳.۲) یادآوری می‌شود که وزن عملگر پائولی تعداد عضوهای غیرهمانی است. در این صورت وزن عملگر $E \in \mathcal{P}_N$ نشان داده شده در $۲N$ـ تایی دودویی $\Phi(E) = (\mathbf{a} \mid \mathbf{b})$ به صورت $wt(a)$ و $wt(b)$ دلالت بر تعداد یک‌ها در Nـ تایی دودویی تعریف می‌شود. فرض کنید C فضای پوچ تولید شده توسط $\mathbf{H} = [\mathbf{H}_۱ \mid \mathbf{H}_۲]$ روی میدان $GF(۲)$ باشد. همچنین فرض کنید:

$$\mathcal{C}^{\perp} := \{(\mathbf{v}|\mathbf{w}) \mid \forall (\mathbf{a}|\mathbf{b}) \in \mathcal{C} : (\mathbf{a} \cdot \mathbf{w}) + (\mathbf{v} \cdot \mathbf{b}) = ۰ \pmod ۲\}, \tag{۶.۲}$$

فضای دوگان سیمپلکتیک از $\mathcal{C}$ باشد [۲۶]. مینیمم فاصله از کد پایدارساز تعریف شده در (۳.۲) معادل است با

$$d^Q = \min\{wt(\mathbf{e} \mid \mathbf{f}) \mid (\mathbf{e} \mid \mathbf{f}) \in \mathcal{C}^\perp \setminus \mathcal{C}\}. \tag{۷.۲}$$

کدها با داشتن $\mathbf{H} = [\mathbf{H}_۱ \mid \mathbf{H}_۲]$ به عنوان ماتریس بررسی توازن در $GF(۲)$ یا $\mathbf{H}_{GF(۴)}$ در $GF(۴)$ غیر CSS هستند. کدهای پایدارساز شبه دوری (QCS) هستند اگر $\mathbf{H}_{GF(۴)}$ دارای ساختار شبه دوری باشند که از کدهای QC-LDPC کلاسیک به دست آمده‌اند، به طوری‌که ماتریس بررسی توزان با یکریختی تعریف شده در (۱.۲) برابر است با $\mathbf{H} = [\mathbf{H}_۱ \mid \mathbf{H}_۲]$. خانواده‌ی مهمی از کدهای CSS کوانتومی به فرم زیر می‌باشند[۵۱، ۱۵]:

$$[\mathbf{H}_۱ \mid \mathbf{H}_۲] = \left[\begin{array}{c|c} \mathbf{A} & \circ \\ \circ & \mathbf{B} \end{array}\right], \tag{۸.۲}$$

که در آن $\mathbf{A}$ و $\mathbf{B}$ ماتریس‌های بررسی توازن از دو کد بلوکی خطی با طول یکسان می‌باشند. ساختار SIP در (۵.۲) به $\mathbf{AB}^T = \circ$ کاهش می‌یابد. به علاوه، اگر $\mathbf{A} = \mathbf{B}$، قید $\mathbf{AA}^T = \circ$، به یک کد CSS حاوی دوگان کاهش می‌یابد. توجه داشته باشید که خانواده CSS از کدهای کوانتومی زیرکلاسی از کدهای پایدارساز است که می‌تواند روی فضای اقلیدسی ساخته شود.

فصل ۳

ساختار جدید از کدهای LDPC کوانتومی

۱.۳ مقدمه

در این بخش، سه ساختار از کدهای LDPC کوانتومی براساس روش‌های ساختار جبری مانند استقرا و الحاق ماتریس‌ها و جایگشت دوری ارائه می‌شود. ساختارهای موجود در این بخش، مبتنی بر ماتریس پایه کدهای زمینه QC-LDPC هستند. توجه داشته باشید که مجموعه QR و مجموعه غیر QR از گروه ضربی اول دارای هیچ عضو اشتراک نیست. ماتریس بررسی توزان از کد QCS دارای یک ستون ثابت و سطر وزنی است [۵۹].

فرض کنید $B = [b_{i,j}]_{0 \le i < D, 0 \le j < L}$ یک ماتریس صحیح $D \times L$ باشد. با جایگذاری هر درایه

B با یک ماتریس جایگشت چرخشی (CPMs) $P^{b_{i,j}}$ از مرتبه $v \times v$ به طوری‌که

$$P := \begin{bmatrix} ۰ & ۱ & ۰ & \dots & ۰ \\ ۰ & ۰ & ۱ & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & ۰ \\ ۰ & \ddots & \ddots & \ddots & ۱ \\ ۱ & ۰ & \dots & ۰ & ۰ \end{bmatrix} \tag{۱.۳}$$

و $P^v = P^۰ = I$ یک آرایه $D \times L$ از CPMs $H = [P^{b_{i,j}}]_{۰ \le i < D, ۰ \le j < L}$ به دست می‌آید. بنابراین B به عنوان ماتریس پایه H شناخته می‌شود و فضای پوچ H یک کد LDPC شبه دوری (D, L, v) منظم با ستون وزنی D، سطر وزنی L را تعریف می‌کند و مرتبه P برابر v می‌باشد. ماتریس دودویی H به عنوان پراکندگی آرایه B شناخته می‌شود.

به عبارت دیگر، یک ماتریس جایگشت چرخشی دوری $P^{b_{i,j}}$ را می‌توان به عنوان یک چندجمله‌ای $a(x) = x^{b_{i,j}}$ به صورت فشرده نشان داد. فرض کنید $f(x) = \sum_{i=۰}^{l-۱} x^{r_i}$ چندجمله‌ای با l مؤلفه باشد به طوری‌که $۰ \le r_۰ < r_۱ < \ldots < r_{l-۱} < v$. در این صورت $A = f(P) = \sum_{i=۰}^{l-۱} P^{r_i}$ ماتریس جایگشت چرخشی وزن l است که به کمک l اندیس $r_۱, \ldots, r_l$ از ماتریس‌های جایگشت چرخشی ساخته می‌شود به طوری‌که هر ماتریس جایگشت چرخشی P^{r_i} یک ماتریس همانی است که r واحد سطر آن منتقل شده‌اند. ترانهاده ماتریس A به صورت A^T تعریف می‌شود و با صورت چندجمله‌ای $f(P^{-۱}) = \sum_{i=۰}^{l-۱} P^{-r_i} = \sum_{i=۰}^{l-۱} P^{v-r_i}$ معادل است [۵۹].

تعریف ۱.۱.۳. (کدهای پایدارساز شبه دوری) فرض کنید $H = [A \mid B]$ یک ماتریس بررسی توازن از اندازه $m \times ۲N$ باشد که در آن A و B آرایه‌های ماتریس جایگشت چرخشی به دست آمده از $Q^{\mathcal{R}}$ و $Q^{\mathcal{NR}}$ همراه با پراکندگی آرایه می‌باشد. در این صورت $H = [A \mid B]$ یک $[[N, N-m]]$ کد پایدارساز شبه دوری با وزن سطری w_r و وزن ستونی w_c (w_c, w_r) در ماتریس بررسی توازن $H_{GF(۴)}$ تعریف می‌کند.

۲.۳ ماتریس پایه برای کدهای QCS پیشنهادی

فرض کنید $Q^{\mathcal{R}}$ و $Q^{\mathcal{NR}}$ مجموعه باقی‌مانده و غیرباقی‌مانده مربعی از Z_p^* باشند به طوری‌که $p = ۴n \pm ۱$ یک عدد اول فرد است. فرض کنید $\beta = \alpha^۲$ و $k = (p-۱)/۲$ که در آن α یک عضو اولیه از میدان متناهی $GF(p)$ باشد. چون $\alpha^۲ \in Q^{\mathcal{R}}$، β ریشه kـ ام اولیه واحد و $Q^{\mathcal{R}}$ تحت ضرب توسط β بسته است، $Q^{\mathcal{R}}$ را می‌توان به صورت زیر بیان کرد:

$$Q^{\mathcal{R}} = \{\beta^۰ = ۱, \beta, \ldots, \beta^{k-۱}\}. \tag{۱.۳}$$

برای نمایش $Q^{\mathcal{NR}}$ در عبارت β، عدد اول p را با دو حالت در نظر می‌گیریم [۱۱]:

۱. $p = ۴n - ۱$: با اولین مکمل متقابل درجه دوم، برای عدد اول $p = ۴n - ۱$ خواهیم داشت $-۱ \in Q^{\mathcal{NR}}$. لذا با در نظر گرفتن لم ۲.۳.۱، داریم:

$$Q^{\mathcal{NR}} = -۱ \times \{۱, \beta, \ldots, \beta^{k-۱}\} \equiv -Q^{\mathcal{R}}, \tag{۲.۳}$$

و برای $۰ \leq i < k$، $\beta^i + (-\beta^i) = ۰$. به علاوه، بردارهای صحیح $h_{Q^{\mathcal{R}}}$ و $h_{Q^{\mathcal{NR}}}$ به صورت زیر ساخته می‌شوند:

$$h_{Q^{\mathcal{R}}} = [Q^{\mathcal{R}}(۰), Q^{\mathcal{R}}(۱), \ldots, Q^{\mathcal{R}}(k-۱)] = [۱, \beta, \ldots, \beta^{k-۱}], \tag{۳.۳}$$

و

$$h_{Q^{\mathcal{NR}}} = -h_{Q^{\mathcal{R}}}, \tag{۴.۳}$$

به طوری‌که برای $۰ \leq j < k$، $Q^{\mathcal{R}}(j)$ (به ترتیب $Q^{\mathcal{NR}}(j)$) بیانگر jـ امین عضو از $Q^{\mathcal{R}}$ (به ترتیب $Q^{\mathcal{NR}}$) می‌باشد.

۲. $p = ۴n + ۱$ [۱۱]: زمانی که $p = ۴n + ۱$ یک عدد اول فرد است، با استفاده از اولین مکمل متقابل درجه دوم، $\pm ۱ \in Q^{\mathcal{R}}$. لذا

$$Q^{\mathcal{R}} = \{۱, \beta, \ldots, \beta^{k-۱}\} \equiv \pm\{۱, \beta, \ldots, \beta^{k/۲-۱}\}. \tag{۵.۳}$$

فرض کنید

$$h_{Q^{\mathcal{R}}} = \left[1, \beta, \ldots, \beta^{k/2-1}, -1, -\beta, \ldots, -\beta^{k/2-1}\right]. \qquad (۶.۳)$$

بنابه لم ۲.۳.۱، برای $0 \leq i < k$ می‌دانیم که $\alpha^{2i} \in Q^{\mathcal{R}}$ که در آن $\alpha^{2i+1} \cdot \alpha^{2i} \in Q^{\mathcal{NR}}$ و $\alpha^{2i+1} \in Q^{\mathcal{NR}}$. بنابراین برای هر $\gamma \in Q^{\mathcal{NR}}$:

$$h_{Q^{\mathcal{NR}}} = \gamma h_{Q^{\mathcal{R}}}. \qquad (۷.۳)$$

در ادامه $k-1$ جایگشت از $h_{Q^{\mathcal{R}}}$ و $h_{Q^{\mathcal{NR}}}$ را به دست می‌آوریم. چون برای $0 \leq i < k$، $\beta^k = \beta^0 = 1$ و $\beta^k \beta^i \equiv \beta^{k+i} \equiv \beta^i$، iـ امین جایگشت با iـامین انتقال دوری از $h_{Q^{\mathcal{R}}}$ و $h_{Q^{\mathcal{NR}}}$ به سمت چپ معادل است. بنابراین یک زوج از ماتریس‌های پایه $k \times k$، H_{1b} و H_{2b} به دست می‌آید به طوری‌که iـامین سطر H_{1b} و H_{2b} به ترتیب برابر است با $\beta^i h_{Q^{\mathcal{R}}}$ و $\beta^i h_{Q^{\mathcal{NR}}}$ و H_{1b} و H_{2b} مربع لاتین جابه‌جایی هستند که برای $0 \leq i, j < k$ و $\gamma \in Q^{\mathcal{NR}}$ می‌توان به صورت زیر بیان کرد:

$$H_{1b}(i,j) = \beta^{i+j}, \quad H_{2b}(i,j) = \gamma\beta^{i+j}. \qquad (۸.۳)$$

توجه داشته باشید هر دو H_{1b} و H_{2b} ماتریس‌های مربعی هستند که سطرها به ترتیب k جایگشت متفاوت از $Q^{\mathcal{R}}$ و $Q^{\mathcal{NR}}$ هستند. چون برای $0 \leq i, j < k$، $H_{1b}(i,j) = H_{1b}(j,i)$ و $H_{2b}(i,j) = H_{2b}(j,i)$ خواهیم داشت $H_{1b} = H_{1b}^T$ و $H_{2b} = H_{2b}^T$. لذا بنابه تعریف ۱.۴.۱، H_{1b} ، H_{2b} مربع لاتین جابه‌جایی از مرتبه k هستند . به علاوه چون، $(H_{1b}(i,j), H_{2b}(i,j))$ و $(H_{1b}(i',j'), H_{2b}(i',j'))$ برای $i' = i \pm 1 \pmod k$ و $j' = j \pm 1 \pmod k$ یکسان هستند بنابه تعریف ۲.۴.۱، H_{1b} و H_{2b} مربع‌های لاتین غیرمتعامد هستند.

۳.۳ کدهای QCS نوع $I-A$ از مجموعه‌های QR از اندازه عدد اول $p = 4n - 1$

فرض کنید $A = [a_{i,j}]_{0 \leq i < c, 0 \leq j < d}$ و $B = [b_{i,j}]_{0 \leq i < c, 0 \leq j < d}$ دو ماتریس پایه از اندازه $c \times d$ باشند. همچنین فرض کنید $A_p = [P^{a_{i,j}}]_{0 \leq i < c, 0 \leq j < d}$ و $B_p = [P^{b_{i,j}}]_{0 \leq i < c, 0 \leq j < d}$ به ترتیب آرایه‌های

$c\times d$ متناظر از CPMs باشند. در این صورت انطباق A_p و B_p به صورت $V_p=A_p+B_p$ داده می‌شود که (i,j)ـامین عضو برابر است با $P^{a_{i,j}}+P^{b_{i,j}}$ و یک ماتریس دوری از وزن دو است. برای سادگی، تعریف می‌کنیم $P^{a_{i,j}}+P^{b_{i,j}}=P^{v_{i,j}}$ به طوری‌که $v_{i,j}=a_{i,j}\boxplus b_{i,j}$. در این صورت ماتریس پایه V_p را به صورت $V=[v_{i,j}]_{۰\le i<c,۰\le j<d}$ خواهیم داشت که می‌توان به صورت $V=A\boxplus B$ بیان کرد.

فرض کنید $\mathbf{O}_k$ ماتریس پایه $k\times k$ تمام صفر باشد. $H'_{۲b}=H_{۲b}\boxplus\mathbf{O}_k$ را می‌سازیم که برای $۰\le i,j<k$، (i,j)ـامین درایه برابر است با $H_{۲b}(i,j)\boxplus ۰$. بنابراین ماتریس بررسی توزان پراکنده شده از $H'_{۲b}$ یک آرایه $k\times k$ دوری از وزن دو است.

لم ۱.۳.۳. برای عدد صحیح مثبت n و $p=۴n-۱$ که در آن p یک عدد اول فرد است فرض کنید $H=[H_۱\mid H'_۲]$ $H_b^{IA}=[H_{۱b}\mid H'_{۲b}=H_{۲b}\boxplus\mathbf{O}_k]$ و $v=p$. در این صورت ماتریس بررسی توزان پراکنده شده از H_b^{IA} با در نظر گرفتن SIP خود متعامد می‌باشد.

برهان. برای سادگی، ماتریس دودویی $H=[H_۱\mid H'_۲]$ را به فرم چندجمله‌ای در نظر می‌گیریم. برای $۰\le i,j<k$، فرض می‌کنیم $\mathbb{F}=[f_{i,j}(x)]$ و $\mathbb{T}=[t_{i,j}(x)]$ به ترتیب ماتریس چندجمله‌ای $k\times k$ از $H_۱$ و $H'_۲$ باشند به طوری‌که $f_{i,j}(x)=x^{H_{۱b}(i,j)}$ و $t_{i,j}(x)=x^{H_{۲b}(i,j)}$ و $x^۰=۱$. توجه داشته باشید اثبات خود متعامد بودن H تحت SIP معادل با این است که نشان دهیم چندجمله‌ای‌ها در $\mathbb{F}\mathbb{T}^T+\mathbb{T}\mathbb{F}^T$ باید دارای ضریب زوج باشند، چون $H_{۱b}=-H_{۲b}$، اولین سطر $\mathbb{F}\mathbb{T}^T+\mathbb{T}\mathbb{F}^T$ به صورت زیر است:

$$\Big[\sum_{j=۰}^{k-۱}\Big(x^{\beta^j}(۱+x^{\beta^j})+x^{-\beta^j}(۱+x^{-\beta^j})\Big),\sum_{j=۰}^{k-۱}\Big(x^{\beta^j}(۱+x^{\beta^{j+۱}})+x^{-\beta^j}(۱+x^{-\beta^{j-۱}})\Big),\dots,$$
$$\sum_{j=۰}^{k-۱}\Big(x^{\beta^j}(۱+x^{\beta^{j+k-۱}})+x^{-\beta^j}(۱+x^{-\beta^{j-k-۱}})\Big)\Big]. \qquad (۱.۳)$$

بقیه $k-۱$ سطر تغیرات دوری از معادله (۱.۳) به سمت راست هستند. به علاوه، برای $۰\le i<k$، جملات در معادله (۱.۳) را می‌توان به صورت زیر بیان کرد:

$$\sum_{j=۰}^{k-۱}\Big(x^{\beta^j}+x^{(\beta^j+\beta^j\beta^i)}+x^{-\beta^j}+x^{(-\beta^j-\beta^j\beta^{-i})}\Big). \qquad (۲.۳)$$

چون برای عدد اول $p = ۴n - ۱$، $Q^{\mathcal{R}} \cup Q^{\mathcal{NR}} = Z_p^*$، چند جمله‌ای $\sum_{j=۰}^{k-۱}(x^{\beta^j} + x^{-\beta^j})$ بیانگر ماتریس $\mathcal{I}_k - I_k$ می‌باشد به طوری‌که $\mathcal{I}_k$ و I_k به ترتیب بیانگر ماتریس $k \times k$ تمام یک و ماتریس همانی $k \times k$ هستند. به علاوه می‌نویسیم:

$$\sum_{j=۰}^{k-۱} x^{(\beta^j + \beta^j \beta^i)} + x^{-\beta^j - \beta^j \beta^{-i})} = \sum_{j=۰}^{k-۱} x^{\beta^j + \beta^{j+i}} + x^{-(\beta^j + \beta^{k-i+j})}. \qquad (۳.۳)$$

با بسط برای $۰ \le i < k$، مجموعه‌های توانی

$$\{\beta^j + \beta^{i+j} \mid ۰ \le j < k\}, \quad \{\beta^j + \beta^{k-i+j} \mid ۰ \le j < k\}$$

در (۳.۳) به عنوان $\beta^{k+j} = \beta^j$ یکسان هستند و اندیس i فقط جهت تغییرات دوری β را تعیین می‌کند. این بدان معنی است که

$$\{\beta^j + \beta^{i+j}\} \cup \{-(\beta^j + \beta^{k-i+j})\} = Z_p^*$$

ایجاب می‌کند چندجمله‌ای

$$\sum_{j=۰}^{k-۱}(x^{\beta^j(۱+\beta^i)} + x^{-\beta^j(۱+\beta^{-i})})$$

نیز بیانگر ماتریس $\mathcal{I}_k - I_k$ باشد. لذا $\mathbb{F}\mathbb{T}^T + \mathbb{T}\mathbb{F}^T = ۰ \pmod ۲$ و زوج ماتریس‌های دودویی $H_۱$ و $H'_۲$ با در نظر گرفتن SIP خودمتعامد می‌باشند. □

تعریف ۱.۳.۳. (کدهای QCS نوع $I - A$) فرض کنید $k = (p-۱)/۲ \ge \rho'$ و $H_۱^{sub}$ و $H_۲'^{sub}$ به ترتیب زیرماتریس‌های $\rho' \times k$ از $H_{۱b}$ و $H'_{۲b}$ باشند. ماتریس بررسی توزان H پراکنده شده از $H_b^{IA} = [H_{۱b}^{sub} \mid H_{۲b}'^{sub}]$ کد QCS از نوع $I - A$، $\mathcal{C}_{IA}(H_b'^{IA}, ۳\rho', ۳k, v)$ را به طول kv و نرخ $۱ - \rho'/k$ تعریف می‌کند که در آن $v = p$، $۳\rho'$ و $۳k$ ستون‌ها و سطرهای وزنی $H_{GF(۴)}$ می‌باشد.

توجه داشته باشید ماتریس بررسی توزان از کد QCS نوع $I - A$ یک ماتریس مربعی با kp سطر می‌باشد. با توجه به ساختار اساسی جبر از مجموعه‌های QR، ماتریس بررسی توزان دارای رتبه کامل نیست و بعد دقیق $\mathcal{C}_{IA}(H_b'^{IA}, ۳\rho', ۳k, p)$ از گزاره زیر به دست می‌آید.

گزاره ۱.۳.۳. برای هر عدد صحیح و مثبت n و عدد اول $p=۴n-۱$، فرض کنید $v=p$. بعد کد QCS از نوع $I-A$، $[[N,K]]$ برابر است با $N-\mathrm{Rank}(H)$ به طوری‌که $N=p(p-۱)/۲$ و وقتی n فرد است، $\mathrm{Rank}(H)=(p-۱)^۲/۲+۱$ و وقتی n زوج است، $\mathrm{Rank}(H)=(p-۱)(p-۲)/۲+۱$.

برهان. فرض کنید $\{d_۰,d_۱,\ldots,d_{k-۱}\}$، k عضو از مجموعه باقی‌مانده مربعی Q^R باشد. ماتریس بررسی توازن $H_۱$، روی $\mathbb{F}_۲$ را می‌توان به صورت زیر بیان کرد:

$$H_۱=\begin{bmatrix} P_{۰,۰}^{d_{\sigma_۰(۰)}} & \cdots & P_{۰,k-۱}^{d_{\sigma_۰(k-۱)}} \\ \vdots & \ddots & \vdots \\ P_{k-۱,۱}^{d_{\sigma_{k-۱}(۰)}} & \cdots & P_{k-۱,k-۱}^{d_{\sigma_{k-۱}(k-۱)}} \end{bmatrix}, \tag{۴.۳}$$

به طوری‌که $\sigma_۰$ یک جایگشت از $\{۰,۱,\ldots,k-۱\}$ و σ_j که $۱\le j<k$ یک انتقال دوری چپ از $(\sigma_۰(۰),\ldots,\sigma_۰(k-۱))$ با j موقعیت است، یعنی

$$(\sigma_j(۰),\ldots,\sigma_j(k-۱))=(\sigma_۰(j),\ldots,\sigma_۰(k-۱),\sigma_۰(۰),\ldots,\sigma_۰(j-۱))$$

و هر P_{ij}^d دلالت بر dـامین توان P است. فرض کنید α، pـامین ریشه اولیه واحد و $\mathbb{F}_۲(\alpha)$ میدان متناهی مینیمال شامل هر دو $\mathbb{F}_۲$ و α باشد. با استفاده از عملکرد [۶۰]، برای تحلیل کدهای LDPC شبه دوری، می‌توان عبارت P^d را که $۰\le d<p$ به صورت زیر نوشت:

$$P^d=V_p\cdot\mathcal{D}(\alpha^d)\cdot V_p^{-۱}, \tag{۵.۳}$$

به طوری‌که V_p دلالت بر ماتریس واندرموند $p\times p$ تولید شده توسط α روی $\mathbb{F}_۲(\alpha)$، $V_p^{-۱}$ معکوس V_p و $\mathcal{D}(\alpha^i)$ ماتریس قطری $p\times p$ با درایه‌های قطری $\{۱,\alpha^i,\ldots,\alpha^{i(p-۱)}\}$ می‌باشد. ماتریس $H_۱$ را می‌توان به صورت زیر تجزیه کرد:

$$H_۱=\mathrm{Diag}(V_p)\cdot\tilde{H}_۱\cdot\mathrm{Diag}(V_p^{-۱}), \tag{۶.۳}$$

که در آن

$$\tilde{H}_۱=\begin{bmatrix} \mathcal{D}(\alpha^{d_{\sigma_۰(۰)}}) & \cdots & \mathcal{D}(\alpha^{d_{\sigma_۰(k-۱)}}) \\ \vdots & \ddots & \vdots \\ \mathcal{D}(\alpha^{d_{\sigma_{k-۱}(۰)}}) & \cdots & \mathcal{D}(\alpha^{d_{\sigma_{k-۱}(k-۱)}}) \end{bmatrix}$$

و

$$\mathrm{Diag}(\mathcal{F}) = \begin{bmatrix} \mathcal{F} & \circ & \circ \\ & \ddots & \circ \\ \circ & \circ & \mathcal{F} \end{bmatrix}$$

برای $\mathcal{F} = V_p$ و V_p^{-1}. چون هر دو $\mathrm{Diag}(V_p)$ و $\mathrm{Diag}(V_p^{-1})$ دارای رتبه کامل k_p هستند، $\mathrm{Rank}(H_1) = \mathrm{Rank}(\tilde{H}_1)$.

توجه داشته باشید که $\tilde{H}_1$ را می‌توان به عنوان ماتریس بلوکی با بلوک‌های $k \times k$ در نظر گرفت که هر کدام ماتریس بلوکی $p \times p$ است. سپس می‌توان ستون‌ها و سطرهای $\tilde{H}_1$ به فرم یک ماتریس قطری بلوکی $\tilde{\tilde{H}}_1$ با هر بلوک از اندازه $k \times k$ مرتب کرد و jـامین بلوک قطری که $\circ \leq j \leq p$ برابر است با C_j به طوری‌که

$$C_j = \begin{bmatrix} \alpha^{jd_{\sigma_\circ(\circ)}} & \dots & \alpha^{jd_{\sigma_\circ(k-1)}} \\ \vdots & \vdots & \vdots \\ \alpha^{jd_{\sigma_{k-1}(\circ)}} & \dots & \alpha^{jd_{\sigma_{k-1}(k-1)}} \end{bmatrix}. \tag{۷.۳}$$

مشاهده می‌کنیم که $\mathrm{Rank}(\tilde{H}_1) = \mathrm{Rank}(\tilde{\tilde{H}}_1) = \sum_{j=\circ}^{p-1} \mathrm{Rank}(C_j)$. لذا خواهیم داشت:

$$\mathrm{Rank}(H_1) = \sum_{i=\circ}^{p-1} \mathrm{Rank}(C_j). \tag{۸.۳}$$

به ویژه، C_j یک ماتریس گردشی روی $\mathbb{F}_2(\alpha)$ است. بنابراین، بنابه قضیه ۱.۶.۳، رتبه C_j برابر است با $k-z$ به طوری‌که z تعداد ریشه‌های چندجمله‌ای $\sum_{i=\circ}^{k-1} \alpha^{jd_{\sigma_\circ(i+1)}} x^i$ است که شامل $\{1, \beta, \dots, \beta^{k-1}\} \subset \mathbb{F}_2(\beta)$ می‌باشد به طوری‌که β، kـامین ریشه اولیه واحد است. هنگامی که $j = \circ$ همه β و β^{k-1} ریشه‌های $f_\circ(x) = 1 + x + \ldots + x^{k-1}$ است، بنابراین $\mathrm{Rank}(C_\circ) = 1$. فرض کنید $j > \circ$. ابتدا $f_j(\beta^l)$ را برای $1 \leq l < k$ در نظر بگیرید. می‌نویسیم $\mathbb{F}_2(\alpha)(\beta) = \mathbb{F}_{2^r}$ و فرض کنید γ دلالت بر عضوهای اولیه $\mathbb{F}_{2^r}$ باشد. در این صورت $\alpha = \gamma^{\frac{2^r-1}{p}}$، $\beta = \gamma^{\frac{2^r-1}{k}}$ و

$$f_j(\beta^l) = \sum_{i=\circ}^{k-1} \alpha^{jd_{\sigma_\circ(i+1)}} \beta^{il} = \sum_{i=\circ}^{k-1} \gamma^{\frac{2^r-1}{p} jd_{\sigma_\circ(i+1)} + \frac{2^r-1}{k} il}.$$

چون p اول و $k = (p-1)/2$ با p اول می‌باشد، اعداد صحیح i_1 و i_2 که $1 \leq i_1, i_2 < k$ مشمول $\gamma^{\frac{2^r-1}{p}} = \gamma^{\frac{2^r-1}{k} i_2}$ وجود ندارد. در نتیجه، عدد صحیح i که $1 \leq i < k$ وجود ندارد به طوری‌که

$\gamma^{\frac{2^r-1}{p}2jd_{\sigma_0}(1)}=\gamma^{\frac{2^r-1}{p}jd_{\sigma_0(i+1)}+\frac{2^r-1}{k}il}$. بنابراین

$$\Big\{\frac{2^r-1}{p}jd_{\sigma_0(i+1)}+\frac{2^r-1}{k}il\ :\ 0\le i<k\Big\}\subset \mathbf{Z}^*_{2^r-1}$$

تحت ضرب توسط ۲ بسته نیست. در نتیجه خواهیم داشت:

$$\begin{aligned} f_j(\beta^l)^2 &= \Big(\sum_{i=0}^{k-1}\gamma^{\frac{2^r-1}{p}jd_{\sigma_0(i+1)}+\frac{2^r-1}{k}il}\Big)^2 \\ &= \sum_{i=0}^{k-1}\gamma^{2\left(\frac{2^r-1}{p}jd_{\sigma_0(i+1)}+\frac{2^r-1}{k}il\right)} \neq \sum_{i=0}^{k-1}\gamma^{\frac{2^r-1}{p}jd_{\sigma_0(i+1)}+\frac{2^r-1}{k}il}=f_j(\beta^l), \end{aligned} \qquad (۹.۳)$$

که ایجاب می‌کند $f_j(\beta^l)\neq 0$.

در ادامه $l=0$ را در نظر بگیرید به طوری‌که $f_j(\beta^0)=f_j(1)=\sum_{i=1}^{k}\alpha^{jd_{\sigma_0}(i+1)}$. چون برای هر $1\le j<p$، p اول است، $f_j(1)$ یا برابر است با $\sum_{d\in Q^{\mathcal{R}}}\alpha^d$ یا $\sum_{i=1}^{k}\alpha^{d_i}=\sum_{d\in Q^{\mathcal{NR}}}\alpha^d$. چون $\sum_{i=0}^{p-1}\alpha^i=0$، $\sum_{d\in Q^{\mathcal{R}}}\alpha^d+\sum_{d\in Q^{\mathcal{NR}}}\alpha^d=1$، لذا $\sum_{d\in Q^{\mathcal{R}}}\alpha^d\neq\sum_{d\in Q^{\mathcal{NR}}}\alpha^d$. فرض کنید n فرد باشد. در این حالت، $p\equiv 3 \bmod 8$. بنابه قانون تقابل درجه دوم، ۲ در $\mathbf{Z}_p^*$ باقی‌مانده مربعی نیست. در نتیجه، $\{2d\ :\ d\in Q^{\mathcal{R}}\}=Q^{\mathcal{NR}}$ و لذا

$$\Big(\sum_{d\in Q^{\mathcal{R}}}\alpha^d\Big)^2=\sum_{d\in Q^{\mathcal{R}}}\alpha^{2d}=\sum_{d\in Q^{\mathcal{NR}}}\alpha^d\neq\sum_{d\in Q^{\mathcal{R}}}\alpha^d. \qquad (۱۰.۳)$$

این ایجاب می‌کند که هر دو $\sum_{d\in Q^{\mathcal{R}}}\alpha^d$ و $\sum_{d\in Q^{\mathcal{NR}}}\alpha^d$ شامل $\mathbb{F}_2$ نباشد و برابر با صفر نیست. در نتیجه برای هر $1\le j<p$، $f_j(1)\neq 0$. فرض کنید n زوج باشد. در این حالت، $p\equiv -1 \bmod 8$ و p با یک به پیمانه ۴ همنهشت نیست. بنابه قانون مربعی درجه دوم، ۲ در $\mathbf{Z}_p^*$ باقی‌مانده lvfud است. در این صورت $\mathcal{Q}^{\mathcal{R}}=\{d_0,\dots,d_{k-1}\}$ تحت ضرب توسط ۲ بسته است. در نتیجه:

$$\Big(\sum_{d\in Q^{\mathcal{R}}}\alpha^d\Big)^2=\sum_{d\in Q^{\mathcal{R}}}\alpha^{2d}=\sum_{d\in \mathcal{Q}^{\mathcal{R}}}\alpha^d. \qquad (۱۱.۳)$$

این ایجاب می‌کند که یا $\sum_{d\in Q^{\mathcal{R}}}\alpha^d$ یا $\sum_{d\in Q^{\mathcal{NR}}}\alpha^d$ برابر با صفر باشد. لذا می‌توان برای $1\le j<p$ ادعا کرد که $f_j(1)$ یا $f_{p-j}(1)$ برابر با صفر است، یعنی k انتخاب از j بین ۱ و $p-1$ وجود دارد

به طوری‌که $f_j(۱) = ۰$. حال می‌توان به دست آورد:

$$\begin{aligned}\mathrm{Rank}(H_۱) &= \mathrm{Rank}(C_۰) + \ldots + \mathrm{Rank}(C_{p-۱}) \\ &= \begin{cases} (p-۱)^۲/۲ + ۱, & n = \text{فرد} \\ (p-۱)(p-۱)/۲ + ۱, & n = \text{زوج} \end{cases}\end{aligned} \tag{۱۲.۳}$$

به طوری‌که $k = (p-۱)/۲$. به طور مشابه می‌توان ثابت کرد که رتبه $H'_۲$ برابر یک است که متفاوت از رتبه $H_۱$ می‌باشد. چون هر دو $P^d_{i,j}$ از $H'_۲$ دارای وزن ۲ می‌باشند، یعنی $(P^d + P^۰)$ ماتریس قطری $\mathcal{D}$ به فرم زیر خواهد بود:

$$\mathcal{D}(۱ + \alpha^i) = \begin{bmatrix} ۰ & ۰ & \ldots & ۰ \\ ۰ & ۱ + \alpha^i & \ddots & \vdots \\ \vdots & \ddots & \ddots & ۰ \\ ۰ & \ldots & ۰ & ۱ + \alpha^{i(p-۱)} \end{bmatrix}. \tag{۱۳.۳}$$

لذا $\tilde{H}_۲$ را می‌توان برای $\gamma \in \mathcal{Q}^{\mathcal{NR}}$ به صورت زیر نوشت:

$$\tilde{H}_۲ = \begin{bmatrix} \mathcal{D}(۱ + \alpha^{\gamma d_{\sigma_۰}(۰)}) & \ldots & \mathcal{D}(۱ + \alpha^{\gamma d_{\sigma_۰}(k-۱)}) \\ \vdots & \ddots & \vdots \\ \mathcal{D}(۱ + \alpha^{\gamma d_{\sigma_{k-۱}}(۰)}) & \ldots & \mathcal{D}(۱ + \alpha^{\gamma d_{\sigma_{k-۱}}(k-۱)}) \end{bmatrix}. \tag{۱۴.۳}$$

توجه داشته باشید که همیشه اولین درایه قطری $\mathcal{D}(۱ + \alpha^i)$ برابر صفر است. با مرتب کردن سطرها و ستون‌های $\tilde{H}_۲$، $\tilde{H}_۲$ به یک ماتریس قطری بلوکی $\tilde{\tilde{H}}_۲$ با فرم یکسان $\tilde{\tilde{H}}_۱$ با $\mathrm{Rank}(C_۰) = ۰$ تبدیل می‌شود. چون کدهای پیشنهادی QCS LDPC کدهای غیر CSS هستند، سطرهای $(a \mid b)$ از H با $a = ۰$ یا $b = ۰$ وجود ندارد. در این صورت رتبه ماتریس دودویی H می‌تواند بزرگتر از k_p باشد. به علاوه، زیرماتریس H^{sub} از H از اندازه $\mathrm{Rank}(H_۱) \times \mathrm{Rank}(H_۱)$ با دترمینان غیرصفر وجود دارد که رتبه H روی $\mathbb{F}_۲$ برابر است با $\mathrm{Rank}(H_۱)$. لذا اثبات کامل می‌شود. □

۴.۳ کدهای QCS نوع $I-B$ از مجموعه‌های QR از اندازه عدد اول $p = ۴n - ۱$

برای عدد اول فرد $p = ۴n - ۱$ و $k = (p-۱)/۲ = ۲n - ۱$، k تعداد قطر پراکنده

$$\{\mathcal{T}_i=\{(j,j+i) \bmod k\} \mid ۰\le j<k\}$$

برای $۰\le i<k$ از $H_{۱b}$ یا $H_{۲b}$ براساس تعریف ۳.۴.۱ به دست می‌آوریم. فرض کنید

$$\mathscr{S}_{I_B}=\{R_{I_v}\pi\tau_i\equiv R_{I_v}P^i \mid ۰\le i<v, v=k\}$$

مجموعه ماتریس‌های جایگشتی به دست آمده از k قطر پراکنده باشد که در آن P، CPM تعریف شده در (۱.۳) است و

$$R_{I_v}:=\begin{bmatrix} ۰ & ۰ & \dots & ۰ & ۱ \\ ۰ & ۰ & \dots & ۱ & ۰ \\ \vdots & ۰ & ۱ & ۰ & ۰ \\ ۰ & \ddots & ۰ & \vdots & \vdots \\ ۱ & ۰ & \dots & ۰ & ۰ \end{bmatrix} \tag{۱.۳}$$

ماتریس همانی معکوس $v\times v$ و $\pi\tau_i$، iـ امین انتقال دوری راست از یک ماتریس همانی است.

لم ۱.۴.۳. برای عدد صحیح و مثبت n و $p=۴n-۱$ به طوری‌که p یک عدد اول فرد است، فرض کنید $H_b^{IB}=\left[\begin{array}{cc|cc} H_{۱b} & DH_{۲b} & H_{۲b} & DH_{۱b}\end{array}\right]$ به طوری‌که $D\in\mathscr{S}_{IB}$. همچنین فرض کنید v عدد صحیح و مثبت باشد. در این صورت ماتریس دودویی

$$H=[A_۱ \mid A_۲]=[H_۱\ H_۲'\mid H_۲\ H_۱']$$

پراکنده شده از H_b^{IB} با در نظر گرفتن SIP خودمتعامد است.

برهان. برای $۰\le i,j<k$، فرض کنید $\mathbb{F}=[f_{i,j}(x)]$ و $\mathbb{T}=[t_{i,j}(x)]$ به ترتیب ماتریس چندجمله‌ای $k\times k$ از $H_۱$ و $H_۲$ باشند به طوری‌که $f_{i,j}(x)=x^{H_{۱b}(i,j)}$ و $t_{i,j}(x)=x^{H_{۲b}(i,j)}$. فرض کنید $\mathbb{A}_۱=[\mathbb{F}\ \hat{\mathbb{T}}]$ و $\mathbb{A}_۲=[\mathbb{T}\ \hat{\mathbb{F}}]$ به ترتیب ماتریس چندجمله‌ای از $A_۱$ و $A_۲$ باشند به طوری‌که $\hat{\mathbb{F}}=D\mathbb{F}$، $\hat{\mathbb{T}}=D\mathbb{T}$ و $D\in\mathscr{S}_{I_B}$. در این صورت خواهیم داشت:

$$\mathbb{A}_۱\mathbb{A}_۲^T+\mathbb{A}_۲\mathbb{A}_۱^T=\left(\mathbb{F}\mathbb{T}^T+\hat{\mathbb{T}}\hat{\mathbb{F}}^T\right)+\left(\mathbb{T}\mathbb{F}^T+\hat{\mathbb{F}}\hat{\mathbb{T}}^T\right). \tag{۲.۳}$$

با بسط (۲.۳)، می‌توان با جایگشت سطری یکسان روی هر دوی $\mathbb{F}$ و $\mathbb{T}$ ادعا کرد که $\mathbb{F}\mathbb{T}^T=\hat{\mathbb{F}}\hat{\mathbb{T}}^T$ و $\mathbb{T}\mathbb{F}^T=\hat{\mathbb{T}}\hat{\mathbb{F}}^T$. لذا $A_۱A_۲^T+A_۲A_۱^T=۰ \pmod ۲$ و $H=[A_۱ \mid A_۲]$ با در نظر گرفتن SIP خودمتعامد هستند. □

تعریف ۱.۴.۳. (کدهای QCS نوع $I-B$) فرض کنید $k=(p-1)/2$. $\rho' \leq k$. زیرماتریس $H_b'^{IB}=[H_{1b}^{sub}H_{2b}'^{sub} \mid H_{2b}^{sub}H_{1b}'^{sub}]$ از مرتبه $\rho' \times 4k$ ماتریس پایه از کد QC-LDPC $(\rho', 4k, v)$ می‌باشد. در این صورت ماتریس بررسی توزان H پراکنده شده از $H_b'^{IB}$ یک کد QCS نوع $I-B$، $\mathcal{C}_{I_B}(H_b'^{IB}, 2\rho', 4k, v)$ با طول $2kv$، نرخ $1-\rho'/2k$ و با وزن‌های ستونی و سطری $2\rho'$ و $4k$ از $H_{GF(4)}$ تعریف می‌کند.

در زیر نشان می‌دهیم که ماتریس پایه $H_b'^{IB}$ یک گروه $(2\rho', 4k)$ از کدهای QCS نوع $I-B$ تعریف می‌کند به طوری‌که زوج ماتریس‌های بررسی توازن آنها با در نظر گرفتن SIP برای هر مقادیر v خودمتعامد می‌باشند.

نتیجه ۱.۴.۳. فرض کنید $v \in \mathbb{Z}^+$ عدد صحیح مثبت باشد. ماتریس پایه $H_b'^{IB}$ خانواده‌ای از کدهای QCS نوع $I-B$ را تعریف می‌کند به طوری‌که هر کد $\mathcal{C}_{I_B}(H_b'^{IB}, 2\rho', 4k, v)$ با در نظر گرفتن SIP خودمتعامد می‌باشد.

برهان. از لم ۱.۴.۳ یادآوری می‌کنیم که $\mathbb{F}\mathbb{T}^T$ (به ترتیب $\mathbb{T}\mathbb{F}^T$) و $\hat{\mathbb{F}}\hat{\mathbb{T}}^T$ (به ترتیب $\hat{\mathbb{T}}\hat{\mathbb{F}}^T$) زوج‌های یکسان هستند به طوری‌که $\mathbb{F}$ و $\mathbb{T}$ ماتریس‌های چندجمله‌ای $k \times k$ و $\hat{\mathbb{F}}=D\mathbb{F}$ و $\hat{\mathbb{T}}=D\mathbb{T}$ با $D \in \mathscr{S}_{I_B}$ می‌باشند. در این صورت با گرفتن پیمانه v روی توان چندجمله‌ای می‌توان نتیجه گرفت که $\mathbb{F}\mathbb{T}^T=\hat{\mathbb{F}}\hat{\mathbb{T}}^T$ (به ترتیب $\mathbb{T}\mathbb{F}^T=\hat{\mathbb{T}}\hat{\mathbb{F}}^T$). لذا $H=[A_1 \mid A_2]$ همیشه با در نظر گرفتن SIP برای v دلخواه خودمتعامد است. □

گزاره ۱.۴.۳. برای عدد صحیح مثبت $k=(p-1)/2$ و $\rho' \leq k$ و هر عدد صحیح مثبت v، ماتریس بررسی توزان پراکنده شده از زیرماتریس $H_b'^{IB}$ از مرتبه $\rho' \times k$ یک کد QCS نوع $I-B$، $[[N,K]]=[[(p-1)v, K]]$ را برقرار می‌سازد به طوری‌که $K \geq (p-1)v-\rho'(v-1)-1$.

برهان. با حذف سطرهای $k-\rho'$ از H_b^{IB}، زیرماتریس‌های A_1^{sub} و A_2^{sub} از اندازه $\rho'v \times 2kv$ یک کد QCS را با نرخ حداقل $R^Q=1-\rho'/2k$ تعریف می‌کند. چون مجموع v سطر A_1 وهمچنین مجموع v سطر A_2 برابر بردار تمام یک است، رتبه A_1^{sub} و A_2^{sub} حداکثر برابر است با $\rho'(v-1)+1$ [۲۴]. بنابراین بعد کد حداقل برابر است با $(p-1)v-\rho'(v-1)-1$. □

۵.۳ کدهای QCS نوع II از مجموعه‌های QR از اندازه عدد اول $p = ۴n + ۱$

یادآوری می‌شود که برای $p = ۴n + ۱$ یک عدد اول فرد و $k = (p - ۱)/۲ = ۴n/۲ = ۲n$ یک عدد صحیح زوج $h_{Q^{\mathcal{R}}} = [۱, \beta, \ldots, \beta^{k/۲-۱}, -۱, -\beta, \ldots, -\beta^{k/۲-۱}]$ می‌باشد. ماتریس پایه متناظر $H_{۱b}$ یک مربع لاتین جابه‌جایی به فرم زیر است:

$$H_{۱b} = \left[\begin{array}{ccc|ccc} ۱ & \ldots & \beta^{\frac{k}{۲}-۱} & -۱ & \ldots & -\beta^{\frac{k}{۲}-۱} \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \beta^{\frac{k}{۲}-۱} & \ddots & -\beta^{\frac{k}{۲}-۲} & -\beta^{\frac{k}{۲}-۱} & \ddots & \beta^{\frac{k}{۲}-۲} \\ \hline -۱ & \ddots & \beta^{\frac{k}{۲}-۱} & ۱ & \ddots & \beta^{\frac{k}{۲}-۱} \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ -\beta^{\frac{k}{۲}-۱} & \ldots & \beta^{\frac{k}{۲}-۲} & \beta^{\frac{k}{۲}-۱} & \ldots & -\beta^{\frac{k}{۲}-۲} \end{array}\right] \equiv \begin{bmatrix} W_{۱۱} & W_{۱۲} \\ W_{۲۱} & W_{۲۲} \end{bmatrix}, \tag{۱.۳}$$

که در آن $W_{۲۲} = W_{۱۱}$، $W_{۲۱} = W_{۱۲}$ و $W_{۱۱} = -W_{۱۲}$. فرض کنید $\gamma \in Q^{\mathcal{NR}}$ و $\mathscr{S}_{II} = \{R_{I_v} P^i \mid ۰ \leq i < v, v = k\}$ مجموعه ماتریس‌های جایگشت باشد به طوری‌که R_{I_v} معکوس ماتریس همانی در (۱.۳) است. $H'_{۲b}$ به صورت زیر ساخته می‌شود:

$$H'_{۲b} = (\gamma H_{۱b}) D, \tag{۲.۳}$$

به طوری‌که $D \in \mathscr{S}_{II}$.

لم ۱.۵.۳. برای عدد صحیح مثبت n و $p = ۴n + ۱$ به طوری‌که p عدد اول فرد باشد فرض کنید $H_b^{II} = [H_{۱b} \mid H'_{۲b}]$ که در آن $H_{۱b}$ و $H'_{۲b}$ به ترتیب در (۱.۳) و (۲.۳) تعریف شده‌اند. در این صورت ماتریس دودویی $H = [H_۱ \mid H'_۲]$ پراکنده شده از H_b^{II} با در نظر گرفتن SIP خودمتعامد است.

برهان. فرض کنید $\mathbb{Y} = [y_{i,j}(x)]$ و $\mathbb{U} = [u_{i,j}(x)]$ به ترتیب ماتریس $k \times k$ چندجمله‌ای از $H_۱$ و $H'_۲$ باشند که در آن برای $۰ \leq i, j < k$، $y_{i,j}(x) = x^{H_{۱b}(i,j)}$ و $u_{i,j}(x) = x^{H'_{۲b}(i,j)}$. لذا بنابه روابط

(۱.۳) و (۲.۳) خواهیم داشت:

$$\mathbb{Y}=\begin{bmatrix}\mathbb{Y}_1 & \mathbb{Y}_2\\ \mathbb{Y}_2 & \mathbb{Y}_1\end{bmatrix},\quad \mathbb{U}=\begin{bmatrix}\mathbb{U}_1 & \mathbb{U}_2\\ \mathbb{U}_2 & \mathbb{U}_1\end{bmatrix} \tag{۳.۳}$$

به طوری‌که زیرماتریس‌های $\mathbb{Y}_1$، $\mathbb{Y}_2$، $\mathbb{U}_1$ و $\mathbb{U}_2$ ماتریس‌های $k/2\times k/2$ چندجمله‌ای هستند. در این صورت:

$$\mathbb{Y}\mathbb{U}^T=\begin{bmatrix}\mathbb{Y}_1\mathbb{U}_1^T+\mathbb{Y}_2\mathbb{U}_2^T & \mathbb{Y}_1\mathbb{U}_2^T+\mathbb{Y}_2\mathbb{U}_1^T\\ \mathbb{Y}_2\mathbb{U}_1^T+\mathbb{Y}_1\mathbb{U}_2^T & \mathbb{Y}_2\mathbb{U}_2^T+\mathbb{Y}_1\mathbb{U}_1^T\end{bmatrix} \tag{۴.۳}$$

و

$$\mathbb{U}\mathbb{Y}^T=\begin{bmatrix}\mathbb{U}_1\mathbb{Y}_1^T+\mathbb{U}_2\mathbb{Y}_2^T & \mathbb{U}_2\mathbb{Y}_1^T+\mathbb{U}_1\mathbb{Y}_2^T\\ \mathbb{U}_1\mathbb{Y}_2^T+\mathbb{U}_2\mathbb{Y}_1^T & \mathbb{U}_2\mathbb{Y}_2^T+\mathbb{U}_1\mathbb{Y}_1^T\end{bmatrix}. \tag{۵.۳}$$

با بسط، می‌توان ادعا کرد که

$$\begin{aligned}&\mathbb{Y}_1\mathbb{U}_1^T=\mathbb{U}_2\mathbb{Y}_2^T,\quad \mathbb{Y}_2\mathbb{U}_1^T=\mathbb{U}_2\mathbb{Y}_1^T\\ &\mathbb{Y}_1\mathbb{U}_2^T=\mathbb{U}_1\mathbb{Y}_2^T,\quad Y_2\mathbb{U}_2^T=\mathbb{U}_1\mathbb{Y}_1^T.\end{aligned} \tag{۶.۳}$$

بنابراین $\mathbb{Y}\mathbb{U}^T=\mathbb{U}\mathbb{Y}^T$ ایجاب می‌کند که H_1 و H_2' با در نظر گرفتن SIP خودمتعامد باشند. □

تعریف ۱.۵.۳. (کدهای QCS نوع‌ـ II) فرض کنید $k=(p-1)/2\geq\rho'$. زیرماتریس $H_b'^{II}=[H_{1b}^{sub}\mid H_{2b}^{tsub}]$ از مرتبه $\rho'\times 2k$ ماتریس پایه از کد QC-LDPC $(\rho',2k,v)$ است. در این صورت ماتریس بررسی توزان H پراکنده شده از $H_b'^{II}$ یک کد QCS نوع‌ـ II، $\mathcal{C}_{II}(H_b'^{II},2\rho',2k,v)$ با طول kv، نرخ $1-\rho'/k$ و با وزن‌های ستونی و سطری $2\rho'$ و $2k$ از $H_{GF(4)}$ تعریف می‌کند.

گزاره ۱.۵.۳. برای عدد صحیح مثبت n، $k=(p-1)/2\geq\rho'$ که $p=4n+1$ عدد اول و هر عدد صحیح مثبت v، ماتریس بررسی توازن پراکنده شده از زیرماتریس $H_b'^{II}$ از مرتبه $\rho'\times k$ کد QCS نوع II، $[[N,K]]=[[(p-1)v/2,K]]$ برقرار می‌سازد به طوری‌که $K\geq(p-1)v/2-\rho'(v-1)-1$.

برهان. به اثبات گزاره ۱.۴.۳ مراجعه کنید. □

با در نظر گرفتن (۱.۲)، می‌دانیم که هر زوج جابه‌جایی از عملگرها در پایدارساز $\mathcal{S}$ باید دارای تعداد یکسانی از موقعیت‌های مشترک با عضوهای غیرهمانی باشد. بنابراین، $H_{GF(4)}$ از

کد QCS شامل دورهای بدیهی به طول چهار است. به عبارت دیگر، تعداد دورهایی به طول چهار در $H_{GF(۴)}$ ممکن است با ساختن کدهای دودویی QC-LDPC بدون دورهایی به طول چهار کاهش می‌یابد. در ادامه، کمر کدهای QC-LDPC برای این سه نوع کدهای QCS مورد بحث قرار می‌گیرد. چون همه کدهای QC-LDPC در این پایان‌نامه، کدهای دودویی در نظر گرفته شده است، تجزیه و تحلیل دور بعد براساس دامنه دودویی می‌باشد.

در [۲۴]، نشان داده شد که دور در گراف تنر از کد QC-LDPC را می‌توان به عنوان دنباله‌ی متناظر با CPMs، $v \times v$ در نظر گرفت. بنابراین دور به طول $۲i$ در کد پیچشی دودویی QC-LDPC را می‌توان به صورت دنباله

$$(j_۰, l_۰); (j_۱, l_۱); \ldots; (j_k, l_k); \ldots; (j_{i-۱}, l_{i-۱}); (j_۰, l_۰)$$

توصیف کرد به طوری‌که (j_k, l_k) نشان‌دهنده j_kـامین سطر و l_kـامین ستون از ماتریس پایه H_b است و نقطه ویرگول بین (j_k, l_k) و $(j_{k+۱}, l_{k+۱})$ را می‌توان به عنوان $(j_{k+۱}, l_k)$ در نظر گرفت. واضح است که $j_k \neq j_{k+۱}$ و $l_k \neq l_{k+۱}$. بنابراین شرط لازم و کافی برای وجود دورهایی به طول $۲i$ برابر است با [۲۴]:

$$\sum_{k=۰}^{i-۱} (h_{j_k, l_k} - h_{j_{k+۱}, l_k}) = ۰ \pmod{v}, \qquad (۷.۳)$$

که در آن هر h_{j_k, l_k} یک عضو در H_b بیان می‌کند.

کد QCS ـ نوع $I - A$، $\mathcal{C}_{IA}(H_b'^{IA}, ۳\rho', ۳k, v)$ را در نظر بگیرید به طوری‌که $H_b'^{IA} = [H_{۱b}^{sub} \mid H_{۲b}'^{sub}]$. ماتریس دودویی $H = [H_۱^{sub} \mid H_۲'^{sub}]$ بعد از پراکندگی $H_۲'^{sub}$ شامل دورهایی به طول چهار است که از ماتریس پایه O_k تمام صفر تولید می‌شود. علاوه‌براین، کد QCS نوع $I - B$، $\mathcal{C}_{IB}(H_b'^{IB}, ۲\rho', ۴k, v)$ را در نظر بگیرید که در آن

$$H_b'^{IB} = [H_{۱b}^{sub} H_{۲b}'^{sub} \mid H_{۲b}^{sub} H_{۱b}'^{sub}].$$

چون برای $p = ۴n - ۱$، $H_{۲b} = -H_{۱b}$ برای $i \neq i'$ و $۰ \leq i, i' < k$ خواهیم داشت:

$$(H_{۱b}(i, j) - H_{۱b}(i', j)) + (-H_{۱b}(i, j) - (-H_{۱b}(i', j)) = ۰.$$

لذا برای هر مقدار v، ماتریس دودویی H از کد QCS نوع $I-B$ شامل دورهایی به طول چهار هستند. در مقایسه با کدهای QCS نوع $I-A$ و نوع $I-B$، ماتریس دودویی H از کدهای QCS نوع II پیشنهادی دارای دوری به طول چهار نیست. در ادامه شرط کافی روی v برای H برای داشتن کمر شش ثابت شده است.

لم ۲.۵.۳. برای عدد صحیح و مثبت v و عدد اول $p=۴n+۱$ شرط کافی روی v برای ماتریس دودویی H پراکنده شده از $H_b^{\prime II}=[H_{۱b}^{sub} \mid H_{۲b}^{\prime sub}]$ برای داشتن کمر شش برابر است با $v=p$ یا

$$v > ۲\max\{\max(Q^{\mathcal{R}})-۱, \max(Q^{\mathcal{NR}}-\min(Q^{\mathcal{NR}})\}. \qquad (۸.۳)$$

برهان. فرض کنید $\mathscr{D}_{i_۱,i_۲}$ اختلاف بین سطر $i_۱$ و $i_۲$ از H_b^{II} باشد به طوری‌که $۰ \le i_۱, i_۲ < k$. در این صورت $\mathscr{D}_{i_۱,i_۲}=[(\beta^{i_۱}-\beta^{i_۲})h_{Q^{\mathcal{R}}}(\beta^{i_۱}-\beta^{i_۲})\hat{h}_{Q^{\mathcal{NR}}}]$ به طوری‌که $\hat{h}_{Q^{\mathcal{NR}}}$ یک جایگشت ستونی از $h_{Q^{\mathcal{NR}}}$ پس از اعمال ماتریس جایگشت D به $H_{۲b}^{\prime}$ می‌باشد.

حالت $v=p$ را در نظر بگیرید. برای دو عضو مجزای $a,b \in \mathscr{D}_{i_۱,i_۲}$ خواهیم داشت

$$.a-b \neq ۰ (\mathrm{mod}\ p)$$

این به این دلیل است که برای هر کدام

$$(\beta^{i_۱}-\beta^{i_۲})(\mathrm{mod}\ p) \in Q^{\mathcal{R}}$$

یا

$$(\beta^{i_۱}-\beta^{i_۲})(\mathrm{mod}\ p) \in Q^{\mathcal{NR}}$$

با در نظر گرفتن لم ۲.۳.۱، $\mathscr{D}_{i_۱,i_۲}=Q^{\mathcal{R}} \cup Q^{\mathcal{NR}}=Z_p^*$. بنابراین $\mathscr{D}_{i_۱,i_۲}$ برداری است که شامل $p-۱$ عضو مجزای Z_p^* می‌باشد.

علاوه براین، حالت $v \neq p$ را در نظر بگیرید. در این حالت اگر برای برخی عدد صحیح c، $(a-b) \neq cv$ خواهیم داشت $a-b \neq ۰ (\mathrm{mod}\ v)$. توجه داشته باشید بیشترین اندازه $a-b$ زمانی اتفاق می‌افتد که $a=-b$ برای $b=\max(\mathscr{D}_{i_۱,i_۲})$. بنابراین، اگر $v > ۲\max(\mathscr{D}_{i_۱,i_۲})$، $a-b \neq$

$\max\{\max(h_{Q^{\mathcal{R}}}) - \min(h_{Q^{\mathcal{R}}})\} \circ (\mathrm{mod}\ v)$. چون بیشترین اندازه $\mathscr{D}_{i_1,i_2}$ برای i_1 و i_2 دلخواه از $\max(\hat{h}_{Q^{\mathcal{NR}}}) - \min(\hat{h}_{Q^{\mathcal{NR}}})$ و $\min(h_{Q^{\mathcal{R}}}) = 1$ تعیین می‌شود، کافی است برای

$$v > 2 \cdot \max\{\max(Q^{\mathcal{R}} - 1m, \max(Q^{\mathcal{NR}} - \min(Q^{\mathcal{NR}}\}, \qquad (۹.۳)$$

مشاهده کنید که ماتریس دودویی پراکنده شده H دارای دوری از طول چهار نیست چون هیچ دنباله‌ای $(j_0, l_0); (j_1, l_1); (j_0, l_0)$ در H_b^{II} وجود ندارد به طوری‌که شرط در (۷.۳) بتواند برقرار شود. □

۶.۳ کمینه فاصله از کدهای QCS نوع II

کمینه فاصله برای کد کوانتومی (غیر CSS و CSS) ساخته شده از کدهای کلاسیک خود- متعامد یا شامل دوگان، پایین‌ترین کران توسط کمینه فاصله از کد کلاسیک می‌باشد. به ویژه، فرض کنید C_1 و C_2 دو کد بلوکی خطی کلاسیک به ترتیب با پارامترهای $[n, k_1, d_1]$ و $[n, k_2, d_2]$ باشند به طوری‌که $C_2^{\perp} \subset C_1$. در این صورت فاصله d^Q از کد کوانتومی به صورت زیر بیان می‌شود:

$$d^Q \geq \min\{d_1, d_2\},$$

به طوری‌که:

$$d_1 = \min\{wt(c), c \in \mathcal{C}_1 \setminus \mathcal{C}_2^{\perp}\},$$

$$d_2 = \min\{wt(c), c \in \mathcal{C}_2 \setminus \mathcal{C}_1^{\perp}\},$$

و $wt(c)$ وزن c می‌باشد که تعداد عضوهای غیرصفر در کد کلمات c را نشان می‌دهد.

چون کدهای QCS نوع II پیشنهادی غیر- CSS هستند و ماتریس بررسی توزان متناظر با کمر شش ساختار شبه دوری دارند، قضیه زیر روی کمینه فاصله از کدهای QCS نوع- II بیان می‌شود.

قضیه ۱.۶.۳. برای عدد صحیح n و $p = ۴n + ۱$ به طوری‌که p یک عدد اول فرد است، فرض کنید $\rho' \leq k = (p-۱)/۲$ و v مرتبه CPMs باشد که در یکی از شرایط لم ۲.۵.۳ صدق می‌کند. در این صورت فضای پوچ ماتریس بررسی توزان $H = [H_۱^{sub} \mid H_۲'^{sub}]$ یک کد QCS نوع II برای کمینه فاصله $d^Q \geq \rho' + ۱$ تعریف می شودکه در آن ماتریس‌های $H_۱^{sub}$ و $H_۲'^{sub}$ به ترتیب زیرماتریس‌های $\rho' v \times kv$ از $H_۱$ و $H_۲'$ هستند.

از بخش‌های قبل، یادآوری می‌کنیم که کمینه فاصله از کد LDPC کوانتومی غیرـ CSS به صورت زیر تعریف می‌شود:

$$\begin{aligned} d^Q &= \min\{wt(a \mid b) \mid (a \mid b) \in \mathcal{C}^\perp \setminus \mathcal{C}\} \\ &\equiv \min\{wt(a) + wt(b) - wt(a \cap b) \mid (a \mid b) \in \mathcal{C}^\perp \setminus \mathcal{C}\}, \end{aligned} \tag{۱.۳}$$

به طوری‌که $a, b \in GF(۲)^N$. بنابه روش حدفی گاوس روی $H = [A \mid B]$ ماتریس زیر را خواهیم داشت:

$$H_{GE} = \left[\begin{array}{cc|cc} I & C & E & F \end{array}\right], \tag{۲.۳}$$

که در آن I و E از اندازه $(N-K) \times (N-K)$ و C و F از اندازه $(N-K) \times K$ می‌باشند. فرض کنید $\mathcal{C}$ فضای کد باشد که توسط H_{GE} تولید می‌شود. فضای دوگان $C^\perp$ از $\mathcal{C}$ می‌تواند توسط

$$\left[\begin{array}{c} H_{GE} \\ \overline{X}_۱ \\ \overline{Z}_۱ \end{array}\right], \tag{۳.۳}$$

تولید شود که در آن

$$\overline{X}_۱ = \left[\begin{array}{cc|cc} \circ & I & F^T & \circ \end{array}\right], \quad \overline{Z}_۱ = \left[\begin{array}{cc|cc} \circ & \circ & C^T & I \end{array}\right]. \tag{۴.۳}$$

توجه داشته باشید $'\circ'$ دلالت بر ماتریس تمام صفر است و می‌توان ادعا کرد که هر دوی $\overline{X}_۱$ و $\overline{Z}_۱$ به H_{GE} با در نظر گرفتن SIP متعامد هستند. با این وجود، چون عملگرهای پائولی X و Z غیرجابه‌جایی هستند، می‌توان مشاهده کرد که $\overline{X}_۱$ و $\overline{Z}_۱$ غیرجابه‌جایی می‌باشند.

علاوه براین، چون $\overline{X}_۱, \overline{Z}_۱ \in \mathcal{C}^{\perp} \setminus \mathcal{C}$، کدکلمات غیرصفر $(a \mid b)$ به طوری‌که a یا b بردار صفر از طول N هستند، وجود دارد. چون زوج کدهای QC-LDPC تحت ضرب اسکالر از ماتریس‌های پایه یکریخت هستند، دو کد QC-LDPC معادل با کمینه فاصله یکسان هستند. فرض کنید $d_۱$ و $d_۲$ کمینه فاصله از زوج کدهای QC-LDPC باشند. از آنجا که گراف‌های تنر هر دو کد LDPC بدون دور به طول چهار هستند، در این صورت $d_۱ \geq \rho' + ۱$ و $d_۲ \geq \rho' + ۱$ [۲۹]. لذا کمینه فاصله کدهای QCS از نوع II دارای کران پایین $d^Q \geq (\rho' + ۱)$ می‌باشد به طوری‌که یا a یا b بردار غیرصفر از طول N برای کدکلمه $(a \mid b)$ می‌باشد. در زیر یک مثال از QCS نوع‌ـ II پیشنهادی بیان می‌شود.

مثال ۱.۶.۳. پارامترهای $n = ۱$، $p = ۵$ و $v = ۵$ را در نظر بگیرید. مجموعه‌های $Q^{\mathcal{R}} = \{۱, ۴\}$ و $Q^{\mathcal{NR}} = \{۲, ۳\}$ برای ساخت $H_۱$ و $H_۲'$ مورد استفاده قرار می‌گیرند. فرض کنید $\rho' = k = ۲$. رتبه‌های $H_۱$ و $H_۲'$ برابر است با $\rho' v - ۱ = ۹$. بنابراین $H_۱$ و $H_۲'$ یک کد QCS نوع II تعریف می‌کنند. بنابه روش حذفی گاوس روی $H = [H_۱ \mid H_۲']$، $\overline{X}_۱$ و $\overline{Z}_۱$ به صورت زیر به دست می‌آیند:

$$\overline{X}_۱ = (۰۰۰۰۰۰۰۰۰۱ \mid ۱۰۰۱۱۱۱۱۱۰),$$
$$\overline{Z}_۱ = (۰۰۰۰۰۰۰۰۰۰ \mid ۱۱۱۱۱۱۱۱۱۱). \qquad (۵.۳)$$

با در نظر گرفتن بحث فوق، کمینه فاصله از این کد حداقل برابر است با $\rho' + ۱ = ۳$. توجه داشته باشید این کوچکترین کد QCS نوع II ساخته شده از زوج کدهای LDPC با بعد یک می‌باشد. با بسط (۳.۳)، می‌توان مشاهده کرد که کمینه فاصله از این کد برابر با سه می‌باشد. لذا این یک کد QCS نوع II، $[[۱۰, ۱, ۳]]$ است.

توجه داشته باشید نرخ کد QC-LDPC (D, L, v) توسط $R = ۱ - D/L$ داده می‌شود به طوری‌که D و L به ترتیب بیانگر وزن ستون و وزن سطر از ماتریس بررسی توزان متناظر است. همچنین از طرح پیشنهادی کدهای QCS نوع II می‌دانیم که ماتریس‌های پایه از کدهای QC-LDPC دارای وزن سطری k و وزن ستونی $\rho' \leq k$ می‌باشد. بنابراین، کدهای QC-LDPC دارای نرخ کد $R = ۱ - \rho'/k$ می‌باشند. این نتیجه می‌دهد که برای نرخ کد ثابت R، ρ' با اندازه

k مجموعه QR افزایش می‌یابد. علاوه براین، خواهیم داشت $k=(p-۱)/۲\equiv(۴n)/۲=۲n$ به طوری‌که $p=۴n+۱$، ρ' با p نیز افزایش می‌یابد. بنابراین، برای نرخ کد ثابت، کران پایین فاصله از کدهای QCS ـ نوع II با اندازه k مجموعه باقی‌مانده مربعی افزایش می‌یابد.

۷.۳ مثال‌ها

مثال ۱.۷.۳. (کد QCS نوع $I-A$) برای $n=۳$ و $p=۴n-۱=۱۱$ خواهیم داشت $Q^R=\{۱,۳,۴,۵,۹\}$ و $Q^{\mathcal{NR}}=-Q^{\mathcal{R}}=\{۱۰,۸,۷,۶,۲\}$. فرض کنید $v=p$ و $H'_{۲b}=H_{۲b}\boxplus O_۵$. خواهیم داشت $H=[H_۱\mid H'_۲]$ پراکنده شده از $H_b^{IA}=[H_{۱b}\mid H'_{۲b}]$ و آن یک کد QCS نوع $I-A$، $[[kp,kp-k(p-۱)-۱]]=[[۵۵,۴]]$ است. توجه داشته باشید که $H'_۲$ شامل دوری به طول چهار با توجه به ماتریس تمام صفر $O_۵$ است.

مثال ۲.۷.۳. (کد QCS ـ نوع $I-B$) $Q^{\mathcal{R}}$ و $Q^{\mathcal{NR}}$ در مثال ۱.۷.۳ را در نظر بگیرید. $D\in\mathscr{S}_{I_B}$ را به صورت زیر در نظر بگیرید:

$$D=\begin{bmatrix}۰&۰&۱&۰&۰\\۰&۱&۰&۰&۰\\۱&۰&۰&۰&۰\\۰&۰&۰&۰&۱\\۰&۰&۰&۱&۰\end{bmatrix},$$

و فرض کنید $H'_{۱b}=DH_{۱b}$ و $H'_{۲b}=DH_{۲b}$. انتخاب کنید $\rho'=k=۵$ و $v=۳۱$، ماتریس پایه $H_b'^{IB}=[H_{۱b}H'_{۲b}\mid H_{۲b}H'_{۱b}]$ نشان داده شده در معادله

$$H_b'^{IB}=\left[\begin{array}{cccccccccc|cccccccccc}۱&۳&۹&۵&۴&۲&۶&۷&۱۰&۸&۱۰&۸&۲&۶&۷&۹&۵&۴&۱&۳\\۳&۹&۵&۴&۱&۸&۲&۶&۷&۱۰&۸&۲&۶&۷&۱۰&۳&۹&۵&۴&۱\\۹&۵&۴&۱&۳&۱۰&۸&۲&۶&۷&۲&۶&۷&۱۰&۸&۱&۳&۹&۵&۴\\۵&۴&۱&۳&۹&۷&۱۰&۸&۲&۶&۶&۷&۱۰&۸&۲&۴&۱&۳&۹&۵\\۴&۱&۳&۹&۵&۶&۷&۱۰&۸&۲&۷&۱۰&۸&۲&۶&۵&۴&۱&۳&۹\end{array}\right]\tag{۱.۳}$$

یک کد QCS نوع $I-B$، $[[۳۱۰,۱۵۹]]$ تعریف می‌کند.

توجه داشته باشید در این مثال، گراف تنر از ماتریس بررسی توزان H پراکنده شده از H_b^{IIB} داده شده در معادله (۱.۳) شامل دورهایی به طول چهار است. برای این منظور، دنباله $(j_\circ, l_\circ); (j_1, l_1); (j_\circ, l_\circ) = (1,1); (2,1\circ); (1,1)$ را در نظر بگیرید. چون

$$1 - 3 + 1\circ - 8 = \circ \pmod{v}$$

برای v دلخواه، این دنباله چرخه‌ای از دور به طول چهار را نشان می‌دهد.

مثال ۳.۷.۳. (کد QCS ـ نوع II) برای $n = 3$ و $p = 13$ خواهیم داشت $Q^{\mathcal{R}} = \{1,3,4,9,1\circ,12\}$ و $Q^{\mathcal{NR}} = \{2,5,6,7,8,11\}$ با $k = (p-1)/2 = 6$. فرض کنید $\beta = 4$ و $\gamma = 2 \in Q^{\mathcal{NR}}$. در این صورت:

$$\begin{aligned} h_{Q^{\mathcal{R}}} &= \{1,4,3,12,9,1\circ\} \\ &\equiv \{1,4,3,-1,-4,-3\} \pmod{13} \\ h_{Q^{\mathcal{NR}}} &= \gamma h_{Q^{\mathcal{R}}} = \{2,8,6,11,5,7\} \\ &\equiv \{2,8,6,-2,-8,-6\} \pmod{13}. \end{aligned}$$

فرض کنید $H'_{2b} = H_{2b} R_{I_v}$ به طوری‌که $v = k$. فرض کنید $\rho' = 3$ و $v = 61$. رتبه H_1 و H_2 برابر است با:

$$\rho'(v-1) + 1 = 3(61-1) + 1 = 181,$$

و کمینه فاصله کد برابر است با کران پایین $d^Q \geq 4$. لذا ماتریس پایه $H_b^{'II}$ نشان داده شده در معادله

$$H_b^{'II} = \left[\begin{array}{cccccc|cccccc} 1 & 4 & 3 & 12 & 9 & 1\circ & 7 & 5 & 11 & 6 & 8 & 2 \\ 4 & 3 & 12 & 9 & 1\circ & 1 & 2 & 7 & 5 & 11 & 6 & 8 \\ 3 & 12 & 9 & 1\circ & 1 & 4 & 8 & 2 & 7 & 5 & 11 & 6 \end{array}\right] \qquad (۲.۳)$$

کد QCS نوع II، $[[366, 185, n \geq 4]]$ با نرخ $R^Q > 0.5$ را تعریف می‌کند.

ماتریس دودویی H از کد دارای هیچ دوری به طول چهار نیست که می‌توان از (۲.۳) ادعا کرد. علاوه براین، زمانی که $i = 3$، دنباله

$$(j_۰, l_۰); (j_۱, l_۱); (j_۲, l_۲); (j_۰, l_۰) = (۱, ۱); (۳, ۴); (۲, ۵); (۱, ۱)$$

تشکیل دور به طول شش می‌دهد، یعنی:

$$\sum_{k=۰}^{۲} (h_{j_k, l_k} - h_{j_{k+۱}, l_k}) = ۱ - ۳ + ۱۰ - ۹ + ۱۰ - ۹ = ۰ \pmod{v}.$$

بنابراین، ماتریس بررسی توازن دودویی H از کد دارای کمر شش است.

فصل ۴

کدهای ساخته شده و نتایج عددی

۱.۴ کدهای ساخته شده

در این بخش کدهای LDPC کوانتومی براساس روش پیشنهادی ارائه می‌شود. فرض کنید $H_b^{IA} = [H_{۱b}|H'_{۲b}]$ به طوری که $H'_{۲b} = H_{۲b} \boxplus \mathbf{O}_k$. با حذف $(k+۱)/۲ \times k$ سطرهای پایینی H_b^{IA}، زیرماتریس $H_b'^{IA}$ از مرتبه $(k-۱)/۲ \times k$ به دست می‌آید. سپس زیرماتریس با استفاده از CPM، $\mathbf{P}$ از مرتبه $v = p$ پراکنده می‌شود. برای $n = ۵,۶$و۸، ماتریس بررسی توزان H کد QCS نوع $I - A$ مانند $[[۱۷۱,۹۸]]$، $[[۲۵۳,۱۴۲]]$ و $[[۴۶۵,۲۵۴]]$ به ترتیب با نرخ ۰٪۵۷۳، ۰٪۵۶۱ و ۰٪۵۴۶ تعریف می‌کند. پارامترهای آنها در جدول ۱.۴ نشان داده شده است.

جدول ۱.۴: پارامترهای کدهای QCS از نوع $I-A$

$p=۴n-۱$، $\rho'=(k-۱)/۲$ و $\upsilon=p$				
n	**k**	**N**	**K**	(w_c,w_r)
۵	۹	۱۷۱	۹۸	$(۱۲,۲۷)$
۶	۱۱	۲۵۳	۱۴۲	$(۱۵,۳۳)$
۸	۱۵	۴۶۵	۲۵۴	$(۲۱,۴۵)$

جدول‌های ۲.۴ و ۳.۴ مجموعه‌هایی از کدهای QCS نوع $I-B$ و نوع II ساخته شده از ثابت υ و مقادیر متفاوت n می‌باشند. برای کدهای QCS نوع $I-B$ نشان داده شده در جدول ۲.۴، فرض کنید $\rho'=k$، $\upsilon=۶۱$ و ماتریس پایه $H_b^{IB}=[H_{۱b}\ \ H'_{۲b}\mid H_{۲b}\ \ H'_{۱b}]$ به طوری‌که $H'_{۱b}=DH_{۱b}$ و $H'_{۲b}=DH_{۲b}$ با انجام ضرب چپ به ترتیب روی $H_{۱b}$ و $H_{۲b}$ با ماتریس جایگشت $D\in\mathscr{S}_{I_B}$ به دست آمده‌اند. برای ۸ و$n=۳,۵,۶$، کدهای QCS نوع $I-B$ به طول $N=۲kv$، بعد $K=(p-۱)\upsilon-\rho'(\upsilon-۱)-۱$ و نرخ کد حداقل برابر است با ۰٫۵.

جدول ۲.۴: پارامترهای کدهای QCS از نوع $I-B$ با $\upsilon=۶۱$

$p=۴n-۱$، $\rho'=k$ و $\upsilon=۶۱$				
n	**k**	**N**	**K**	(w_c,w_r)
۳	۵	۶۱۰	۳۰۹	$(۱۰,۲۰)$
۵	۹	۱۰۹۸	۵۵۷	$(۱۸,۳۶)$
۶	۱۱	۱۳۴۲	۶۸۱	$(۲۲,۴۴)$
۸	۱۵	۱۸۳۰	۹۲۹	$(۳۰,۶۰)$

جدول ۳.۴: پارامترهای کدهای QCS از نوع II با $\upsilon = ۷۹$

$p = ۴n + ۱$، $\rho' = k/۲$ و $\upsilon = ۷۹$					
n	**k**	**N**	**K**	(w_c, w_r)	d^Q
۳	۶	۴۷۴	۲۳۹	$(۱۶, ۱۲)$	≥ ۴
۴	۸	۶۳۲	۳۱۹	$(۸, ۱۶)$	≥ ۵
۷	۱۴	۱۱۰۶	۵۵۹	$(۱۴, ۲۸)$	≥ ۸
۱۰	۲۰	۱۵۸۰	۷۹۹	$(۲۰, ۴۰)$	≥ ۱۱

برای کدهای QCS نوع II نشان داده شده در جدول ۳.۴، فرض کنید $\rho' = k/۲$، $\upsilon = ۷۹$ و $H_b'^{II} = [H_{۱b}^{sub} \mid H_{۲b}^{sub}]$ به طوری‌که $D = R_{I_k} \in \mathscr{S}_{II}$. برای ۱۰ و $n = ۳, ۴, ۷$ نیمی از کدهای QCS نوع II به طول $k\upsilon$، بعد $K = (p-۱)\upsilon/۲ - \rho'(\upsilon - ۱) - ۱$ و کران پایین کمینه فاصله با استفاده از $\rho' + ۱$ به دست می‌آیند.

۲.۴ کدگشایی کدهای QCS روی $GF(۴)$

از آنجا که گروه پائولی $\mathcal{P}_۱$ را می‌توان به عضوهای $GF(۴)$ از طریق یکریختی توصیف شده در بخش قبل نگاشت، کدگشایی کد LDPC کوانتومی با کدگشایی کدهای چهارتایی کلاسیک روی کانال ۴ـ پرتویی مشابه است [۴۴، ۵۵].

در این پایان‌نامه، الگوریتم جمعی‌ـضربی مبنی بر سندرم (SPA) را مورد استفاده قرار می‌دهیم. ورودی کدگشا بردار سندروم $\mathbf{s} = \{۰, ۱\}^{N-K}$ است که توسط ضرب داخلی اثر بین دنباله دریافتی و ماتریس بررسی توازن $\mathbf{H}_{GF(۴)}$ می‌باشد که در (۱.۲) تعریف شده است. فرض کنید کدگشا پیام منتقل شده در امتداد یال‌های گراف تنر از هر گره کیوبیت یک بردار احتمال $[۱ - f, f/۳, f/۳, f/۳]$ است و هر مقدار از چپ به راست در بردار بیانگر وجود احتمال یک خطای واحد پائولی $E \in \mathcal{P}_۱$ روی jـامین گره کیوبیت است، یعنی:

$$Pr(E_{q_j} = I) = ۱ - f,$$
$$Pr(E_{q_j} = X) = Pr(E_{q_j} = Z) = Pr(E_{q_j} = Y) = f/۳. \qquad (۱.۴)$$

فرض کنید $u_{qj\to S_i}(E_j)$ و $u_{S_i\to q_j}(E_j)$ به ترتیب پیام‌های ارسالی از گره کیوبیت j به گره بررسی i و پیام‌های ارسالی از گره بررسی i به گره کیوبیت j باشند. همچنین $N(q_j)$ بیانگر همسایگی‌های گره کیوبیت j و $N(S_i)$ بیانگر همسایگی‌های گره بررسی i می‌باشند. پس از دریافت پیام‌ها، هر گره بررسی براساس معادله

$$u_{S_i\to q_j}(E_{q_j}) \propto \sum_{E_{q_{j'}}, q_{j'}\in N(S_i)\backslash q_j} \Big(\mathfrak{B}(\mathbf{E}\circ S_i = s_i \mid E_{q_j}\in\mathcal{P}_1) \prod_{q_{j'}\in N(S_i)\backslash q_j} u_{q_j\to S_i}(E_{q_{j'}})\Big) \tag{۲.۴}$$

به گره کیوبیت همسایه خود پیامی ارسال می‌کند به طوری‌که $N(S_i)\backslash q_j$ دلالت بر همه همسایگی‌های گره بررسی S_i به جز گره کیوبیت q_j و مجموع همه عملگرهای خطای احتمالی $\mathbf{E}\in\mathcal{P}_N$ است. احتمال شرطی $\mathfrak{B}(E\circ S_i = s_i \mid E_{qj}\in\mathcal{P}_1)$ بسته به اینکه سندرم s_i برای $E_{q_j}\in\mathcal{P}_1$ صدق کند یا یک است یا صفر. سپس هر گره کیوبیت پیامی را به بررسی‌های همسایگی خود ارسال می‌کند که به صورت زیر داده می‌شود:

$$u_{q_j\to S_i}(E_{q_j}) \propto p_{q_j}(E_{q_j}) \prod_{S_{i'}\in N(q_j)\backslash S_i} u_{S_{i'}\to q_j}(E_{q_j}), \tag{۳.۴}$$

به طوری‌که $N(q_j)\backslash S_i$ دلالت بر همه همسایگی‌های گره کیوبیت q_j به جز گره برسی S_i و $p_{q_j}(E_{q_j})$ که در (۱.۴) تعریف شده است. در این صورت $b_{q_j}(E_{q_j})$ معادل است با:

$$b_{q_j}(E_{q_j}) = p_{q_j}(E_{q_j}) \prod_{S_i\in N(q_j)} u_{S_i\to q_j}(E_{q_j}). \tag{۴.۴}$$

معادلات (۲.۴) و (۳.۴) تا زمانی که پیام به درستی کدگشایی نشود یا به حداکثر تعداد تکرار از پیش تعیین شده برسد، به صورت تکراری کار می‌کند. خروجی کدگشا زمانی که عملگر خطای $\hat{\mathbf{E}} = \bigotimes_{j=1}^{N} \hat{E}_{q_j}$ دارای سندرم یکسان مانند $\mathbf{s} = (s_1, \ldots, s_m)$ باشد به طوری‌که $\hat{E}_{q_j} = \arg\max_{E_{q_j}\in\mathcal{P}_1}\{b_{q_j}(E_{q_j})\}$ به صورت آزمایشی تصمیم می‌گیرد.

فرآیند کدگشایی تکراری تا زمان کدگشایی صحیح عملگر خطا یا رسیدن به حداکثر تعداد تکرار ادامه می‌یابد. فرض کنید δ_X، δ_Z و δ_Y متغیرهای تصادفی باشند که به طور یکنواخت در دامنه $[0, \Delta]$ برای برخی قدرت اختلال ثابت Δ توزیع شده‌اند. برای هر تکرار کدگشایی،

احتمالات قبلی گره‌های کیوبیت از هر بررسی غیرقابل قبول به صورت زیر آشفته می‌شود:

$$Pr(E_j = I) = Pr(E_j = I),$$
$$Pr(E_j = \phi) = (۱ + \delta_\phi)PR(E_j = \phi), \quad \phi = X, Y, Z. \tag{۵.۴}$$

احتمالات قبلی آشفته برای تعداد ثابتی از تکرارهای کدگشایی قبل از اینکه روند اختلال تصادفی دوباره انجام شود، استفاده می‌شود. این روند تا زمانی که یک عملگر خطا به درستی کدگشایی شود و یا به حداکثر تعداد تکرار برای کدگشایی جمعی‌ـ ضربی برسد، تکرار می‌شود. قدرت اختلال تصادفی به صورت $\Delta = ۰/۱$ در نظر گرفته می‌شود و حداکثر تعداد تکرار برای کدگشایی جمعی‌ـ ضربی ۵۰ است. برای اثربخشی محاسبه عملکرد گره بررسی در (۲.۴)، SPA مبنی بر FFT در شبیه‌سازی‌ها استفاده می‌شود [۲۰].

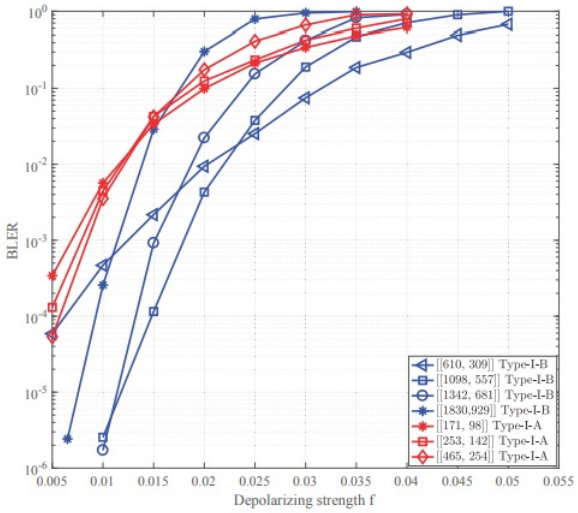
۳.۴ نتایج عددی

کمینه فاصله کدهای CSS ساخته شده از کدهای کلاسیک شامل دوگان با وزن سطر ماتریس بررسی توازن از بالاکراندار می‌شود [۴۰، ۳۴]. به این دلیل که کدکلمات وزنی برابر با وزن سطر ماتریس بررسی توازن است، وجود دارد و این کدکلمات نمی‌تواند در دوگان باشد. علاوه براین، با توجه به کراندار شدن کمینه فاصله، برای N بزرگ دوگان یک کد LDPC نمی‌تواند تعدادی از خطاهای متناسب با N را تصحیح کند. زمانی که کدها دارای طول بلوکی بزرگی باشند و با کدگشایی تحت پیام تکراری کدگشایی شود، به طبقه‌هایی با خطای بالا منجر می‌شوند. این ویژگی همچنین در مورد کدهای پیشنهادی غیر CSS اعمال می‌شود زیرا آنها از کدهای کلاسیک QC-LDPC خود متعامد نیز ساخته می‌شوند. توجه داشته باشید برای $\rho' \leq k$ داده شده، کدهای QCS نوع $I - A$، $I - B$ و نوع II دارای $H_{GF(۴)}$ به ترتیب با وزن‌های ستونی و سطری $(۳\rho', ۳k)$، $(۲\rho', ۴k)$ و $(۲\rho', ۲k)$ هستند. بنابراین، کدهای QCS پیشنهادی نسبت به اکثر کدهای کوانتومی موجود دارای وزن سطری بسیار بزرگتری هستند. علاوه براین، برای نرخ کد ثابت، وزن‌های ستونی و سطری کدهای QCS را می‌توان با تغییر اندازه مجموعه باقی‌مانده مربعی k افزایش داد که به طور بالقوه کران بالای کمینه فاصله را افزایش می‌دهد.

علاوه براین، می‌دانیم که مجموعه کدهای بلوکی خطی منظم از نظر جانبی خوب هستند، یعنی $d_{\min} \geq N_\phi$ یعنی کمینه فاصله با کدی به طول N به صورت خطی رشد می‌کند. نماد ϕ بیانگر نرخ رشد کمینه فاصله است. علاوه براین با افزایش چگالی مجموعه کد منظم، نشان داده می‌شود که ϕ به کران گیلبرت–ورشاموف [۴۱] نزدیک می‌شود.

در مقابل، یک مجموعه کد منظم با چگالی بالا منجر به آستانه کدگشایی تکراری با فاصله بیشتر از ظرفیت در مقایسه با مجموعه کد منظم پراکنده می‌شود [۴۸]. چون کدهای QCS پیشنهادی، مجموعه کدهای منظمی هستند که دارای وزن سطری و ستونی بالایی می‌باشند، کمینه فاصله کد QCS پیشنهادی زیاد است. لذا با کاهش سطح آستانه کدگشایی، سطح خطای بهتر و عملکرد آبشار تند به وجود می‌آید.

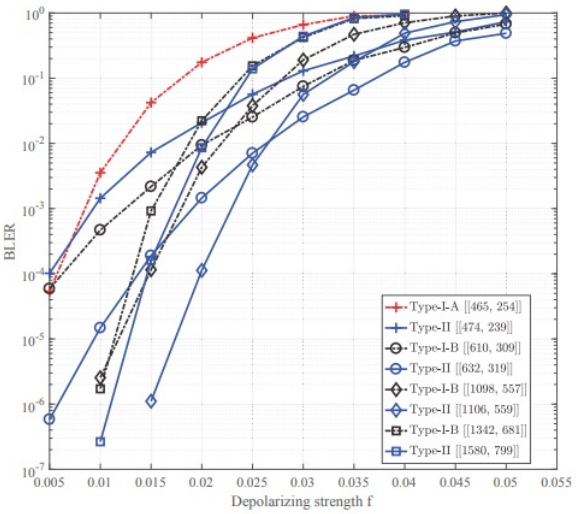
شکل ۱.۴ کارایی BLER از کدهای QCS نوع $I-A$ و نوع $I-B$ را که در جدول‌های ۱.۴ و ۲.۴ بیان شده‌اند، نشان می‌دهد. از شکل، می‌توان مشاهده کرد که مجموعه QR با اندازه $k = ۲n-۱$ افزایش می‌یابد، منحنی BLER برای کدهای QCS نوع $I-A$ دارای یک سقوط آب تندتری هستند. به همین ترتیب، با افزایش n ناحیه سقوط آب برای کدهای QCS نوع $I-B$ تندتر می‌شود.



شکل ۱.۴: BLER از کدهای QCS نوع $I-A$ و نوع $I-B$ از جدول‌های ۱.۴ و ۲.۴

علاوه براین، کدهای QCS نوع II با کدهای QCS نوع I مقایسه گردید و عملکرد BLER در شکل ۲.۴ نشان داده شد. مشاهده می‌شود که کدهای QCS نوع II پیشنهادی از کدهای QCS

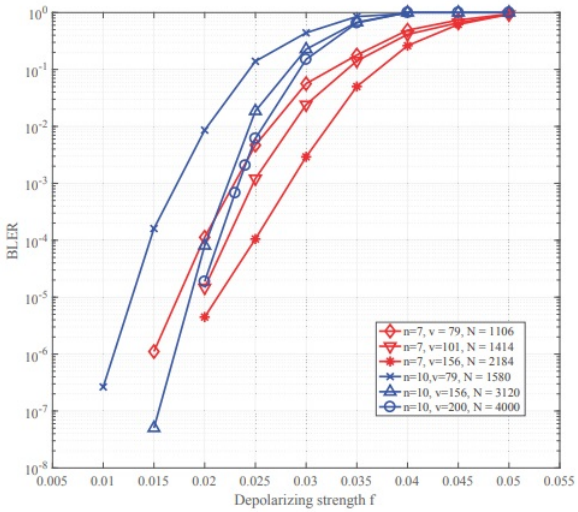
نوع I با طول‌ها و نرخ‌های مشابه بهتر عمل می‌کنند. به ویژه، برای طول کد مشابه و نرخ کد، کدهای پیشنهادی QCS نوع II دارای $\mathbf{H}_{GF(۴)}$ بسیار پراکنده‌تر از $\mathbf{H}_{GF(۴)}$ کدهای QCS پیشنهادی نوع I هستند. لذا کدهای QCS نوع II دارای آستانه کدگشایی بهتری هستند.



شکل ۲.۴: مقایسه BLER برای کدهای QCS پیشنهادی

شکل ۳.۴ نشان می‌دهد که کارایی BLER از کدهای QCS نوع II تحت تاثیر مرتبه‌های متفاوت υ قرار می‌گیرد. مشاهده می‌شود که برای مجموعه باقی‌مانده مربعی از اندازه $k = ۲n$، آستانه کدگشایی تکراری از کدهای QCS نوع II با افزایش υ بهبود می‌یابد. زیرا برای وزن‌های ستونی و سطری ثابت $(w_c, w_r) = (۲\rho', ۲k)$ به طوری‌که $\rho' \leq k$، افزایش υ باعث افزایش طول کد N می‌شود که باعث کاهش قدرت ماتریس می‌شود. به علاوه، اگر υ به طور پیوسته برای ثابت (w_c, w_r) افزایش یابد، خطا در کف به نظر می‌رسد. زیرا کمینه فاصله از کدهای QCS پیشنهادی با وزن سطری کراندار می‌شود که وقتی طول کد N بسیار بزرگ است، منجر به کف خطا می‌شود. برای این منظور، از شکل ۳.۴، کد QCS نوع II با $n = ۷$ و $\upsilon = ۱۵۶$ و $(w_c, w_r) = (۱۴, ۲۸)$ دارای کف خطا در $f = ۰/۰۲$ است. افزایش وزن‌های ستونی و سطری (w_c, w_r) با افزایش مجموعه باقی‌مانده مربعی ممکن است کف خطا را از بین ببرد. این در شکل ۳.۴ با کد QCS نوع II به طول $N = ۳۱۲۰$ از $k = ۲n$ و $\upsilon = ۱۵۶$ ساخته شده است به طوری‌که $n = ۱۰$. کد دارای وزن‌های ستونی و سطری $(w_c, w_r) = (۲۰, ۴۰)$ می‌باشد. منحنی BLER برای این کد دارای یک آبشار تیزتر و بدون کف خطا تا $۱۰^{-۷}$ می‌باشد، اما آستانه کدگشایی

بدتری در مقایسه با کد با $n = ۷$ و $n = ۱۵۶$ دارد.

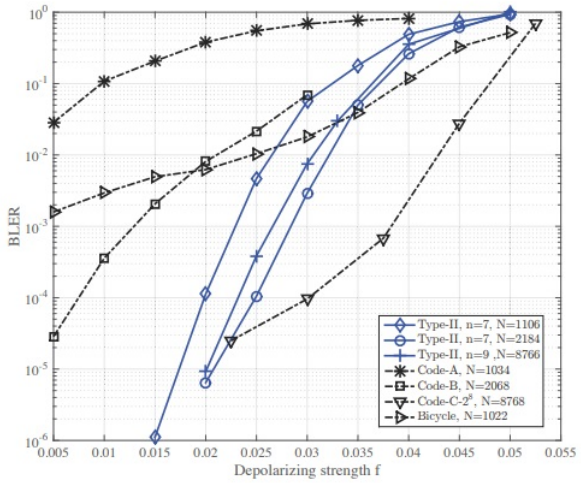


شکل ۳.۴: مقایسه عملکرد کدهای QCS نوع II با $n = ۷$، $v = ۷۹, ۱۰۱, ۱۵۶$ و $n = ۱۰$، $v = ۷۹, ۱۵۶, ۲۰۰$

کدهای پیشنهادی QCS نوع II را با کدهای CSS و غیرـ CSS موجود از نرخ‌ها و طول‌های مشابه مقایسه کردیم. عمکرد خطا از دو کد LDPC کوانتومی از [۵۳] در شکل ۴.۴ نشان داده شده است. دو کد بیان شده به صورت کد A و کد B به طول‌های $N = ۱۰۳۴$ و $N = ۲۰۶۸$ به ترتیب با الحاق CPMهای چند وزنی و با تلاش ماتریس ساخته می شوند [۵۳]. از شکل می‌توان مشاهده کرد که کدهای QCS نوع II با $N = ۱۱۰۶$ و $N = ۲۱۸۴$ عملکرد قابل توجهی به ترتیب نسبت به کد A و کد B در منطقه آبشار دارند. توجه داشته باشید کد A و کد B دارای ساختار غیر CSS هستند و نصف آنها با وزن‌های ستونی و سطری $(۸, ۱۶)$ هستند در حالی که کدهای QCS نوع II به طول $N = ۱۱۰۶, ۲۱۸۴$ دارای وزن‌های ستونی و سطری $(۱۴, ۲۸)$ می‌باشند. همچنین کدهای QCS نوع II به طول ۱۱۰۶ با کدهای دوچرخه‌ای مک‌کی[1] مقایسه می‌شوند. ساختار کد دوچرخه‌ای از ماتریس دوری با استفاده از روش بیان شده در [۴۰] به دست آمده است و کد دوچرخه‌ای ساخته شده داری نرخ ۰/۵، طول ۱۰۲۲ است و در شکل ۴.۴ به عنوان «دوچرخه» نشان داده شده است. این کد، کد CSS است و دارای وزن سطری ۱۶ و وزن ستونی متوسط ۸ می‌باشد. از شکل می‌توان مشاهده کرد که BLER برای کدهای

[1] MacKay's Bicycle codes

پیشنهادی QCS نوع II بهتر از کدهای دوچرخه در هر منطقه آبشار و خطا عمل می کنند. در حالی که کد دوچرخه با طول ۱۰۲۲ دارای کف خطای اولیه است که از $f \approx$ ۰/۰۳ شروع می‌شود. همچنین در شکل ۴.۴، کد QCS نوع II دیگری با نرخ ۰/۵ و $N =$ ۸۷۶۶ ساخته شده و با کد CSS از ۸۷۶۸ کیوبیت در [۳۴] مقایسه گردید. کد در [۳۴] در شکل ۴.۴ با کد $C -$ ۲۸ مشخص شده و کدگشایی در سطح نمادی روی $GF($۲۸$)$ انجام شده است به طوری‌که هر نماد با یک باند ۸ـ تایی مشخص شده است. کد QCS نوع II ساخته شده دارای وزن‌های ستونی و سطری $(18,36)$ هستند در حالی که وزن‌های ستونی و سطری کد $C -$ ۲۸، $(4,8)$ است. از شکل ۴.۴ مشاهده می‌شود که عملکرد کد $C -$ ۲۸ دارای آستانه کدگشایی بهتری در مقایسه با ساختار کد QCS نوع II می‌باشند. در حالی که کد QCS نوع II ساخته شده دارای یک آبشار واضح و عملکرد کف خطای کمتری است.



شکل ۴.۴: مقایسه عملکرد بین کدهای QCS نوع II و کدهای LDPC کوانتومی. توجه داشته باشید BLER رسم شده در اینجا برای کد $C -$ ۲۸ تابع $f = ۳f_m/۲$ است به طوری‌که f_m احتمال مرزی استفاده شده در [۳۴] است. برای مقایسه، LBER از کدهای CSS کلی $\text{Cod} - C -$ ۲۸ از $۱ - (۱ - P_{BSC})^۲$ محاسبه می‌شود [۴۰] به طوری‌که P_{BSC} دلالت بر BLER برای کد منحصربفرد روی کانال متقارن دودویی کلاسیک (BSC) می‌باشد

به علاوه کدهای QCS پیشنهادی از طریق یک کانال دپولاریز کوانتومی که همان کانال ۴ـ تایی کلاسیک است، کدگشایی می‌شوند. در طول کدگشایی پیام تکراری، هر گره کیوبیت گراف تنر بردار ۴ احتمال را عبور کی‌دهد. پس از دریافت بردار، فرآیند پیچیده گره بررسی

می‌تواند از طریق تبدیل سریه فوریه (FFT) محاسبه شود که به ضرب و جمع $\mathcal{O}(N_q \log(q))$ نیاز دارد که در آن $N = ۲^۲ = ۴$ و N طول کد می‌باشد.

در مقابل، معمولا کدهای QCS روی $GF(۲)$ با نمایش یک کانال ۴ـ تایی با دو کانال متقارن دودویی مستقل (BSC) کدگشایی می‌شوند. بنابراین برای کدگشایی احتمالی BP، فرآیند گره بررسی هنگام انجام FFT به ضرب و جمع $\mathcal{O}(N_q \log(q))$ نیاز دارد. بر این اساس، پیچیدگی FFT برای کد $C - ۲^۸$، $\mathcal{O}(۲^۸(N/۸)\log(۲^۸))$ است که حدود $۲^۵$ برابر بیشتر از کدگشایی کد QCS نوع II با طول ۸۷۶۶ روی $GF(۴)$ است.

نتیجه‌گیری

در این پایان‌نامه، سه نوع کد LDPC کوانتومی از ساختار شبه‌دوری با استفاده از مجموعه QR معرفی گردید. با طراحی ماتریس پایه از ساختار مربع لاتین با استفاده از مجموعه‌های QR از پیمانه اول و جایگشت وانطباق ماتریس ها،روش های ساخت پیشنهادی طیف وسیعی از کدهای LDPC کوانتومی را با نرخ‌ها و طول‌های متفاوتی ارائه می کنند. کران‌های پایینی روی کمینه فاصله از کدهای پیشنهادی QCS نوع II از کمینه فاصله از کدهای QC-LDPC به دست آوردیم. عملکرد خطا از کدهای QCS پیشنهادی نسبت به کانال‌های دپولاریز کننده کوانتومی، هیچ کف خطایی را در BLER از $\sim ۱۰^{-۷}$ نشان نمی‌دهد که عملکرد بهتری نسبت به برخی از کدهای LDPC کوانتومی موجود دارد.

واژه‌نامه انگلیسی به فارسی

پراکندگی آرایه ..... Array Dispersion

مربع لاتین ..... Latin Square

انطباق ماتریس ..... Matrix Concatenation

الحاق ماتریس ..... Matrix Superposition

مجموعه باقی مانده مربعی ..... Quadratic Residue Set

خودمتعامد ..... Self Orthogonal

کد پایدارساز ..... Stabilizer Code

قطر پراکنده ..... Transversal

ضرب داخلی پیچیده ..... Twisted Inner Product

واژه‌نامه فارسی به انگلیسی

الحاق ماتریس ..... Matrix Superposition

انطباق ماتریس ..... Matrix Concatenation

پراکندگی آرایه ..... Array Dispersion

خود متعامد ..... Self Orthogonal

ضرب داخلی پیچیده ..... Twisted Inner Product

قطر پراکنده ..... Transversal

کد پایدارساز ..... Stabilizer Code

مجموعه باقی مانده مربعی ..... Quadratic Residue Set

مربع لاتین ..... Latin Square

مراجع

[۱] م. احمدیان عطاری، کدهای کنترل و تصحیح خطا در سامانه‌های مخابراتی، انتشارات دانشگاه صنعتی خواجه‌نصیرالدین طوسی، ۱۳۹۲.

[۲] م. حسین‌زاده، کدهای کوانتومی به وجود آمده بر روی برخی حلقه‌های گروهی، پایان‌نامه کارشناسی ارشد، دانشگاه تربیت مدرس، ۱۳۹۶.

[۳] دکتر ح. دوستی، نظریه‌ی گراف و کاربردهای آن، انتشارات مبتکران.

[4] M., Andrew Steane, **Enlargement of Calderbank-Shor-Steane quantum codes**, IEEE Transactions on information theory, VOL. 45,NO. 7, NOVEMBER 1999.

[5] I. Andriyanova, D. Maurice, and J. P. Tillich, **Quantum LDPC codes obtained by non-binary constructions**, In Proc. IEEE Int. Symp. Inf. Theory, pp. 343-347, 2012.

[6] I. Andriyanova, D. Maurice, and J. P. Tillich, **Spatially coupled quantum LDPC codes**, In Proc. IEEE Inf. Theory. Workshop, pp. 327-331, 2012.

[7] S. A. Aly, **A class of quantum LDPC codes derived from Latin squares and combinatorial objects**, Techn. report, 2007.

[8] S. A. Aly, **A class of quantum LDPC codes constructed from finite geometries**, in Proc. IEEE GlobeComm., pp. 1-5, 2008.

[9] Z. Babar, S. X. Ng and L. Hanzo, **EXIT-chart-aided near-capacity quantum turbo code design**, IEEE Trans. Vehi. Tech., vol. 64, pp. 866- 875, 2015.

[10] Z. Babar, P. Botsinis, D. Alanis, S. X. Ng, L. Hanzo, **Construction of Quantum LDPC Codes From Classical Row-Circulant QC-LDPCs**, IEEE Comm. Lett. vol. 20, No. 1, pp 9-12, 2016.

[11] E. R. Berlekamp, **Algebraic coding theory**, McGraw-Hill, 1st edition, 1968.

[12] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, R.A. Wilson, **Theory of Finite Groups**, Oxford Univ. Press (Clarendon), Oxford and New York, 1985.

[13] Cover, J. A. **Thomas, elbfents of information theory**, John Wiley Sons, Inc. 2006.

[14] T. Camara, H. Ollivier, and J. P. Tillich. **Constructions and performance of classes of quantum LDPC codes**, [Online] arXiv:quant ph/0502086v2, 2005.

[15] A. R. Calderbank and P. W. Shor, **Good quantum error-correcting codes exist**, Phys. Rev. A, vol. 54, pp. 1098-1105, 1996.

[16] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, **Quantum error correction and orthogonal geometry**, Phys. Rev. Lett., vol. 78, pp. 405-409, 1997.

[17] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, **Quantum error correction via codes over** $GF(4)$, IEEE Trans. Inf. Theory, vol. 44, No. 4, pp. 1369-1387, 1998.

[18] S.-Y. Chung, G. Forney, T. Richardson, and R. Urbanke, **On the design of low-density parity-check codes within 0.0045 db of the shannon limit**, IEEE Comm. Lett., vol. 5, pp. 58-60, 2001.

[19] D. Donovan, R.A.H. Gower and A. khodkar, **Latin interchanges and direct products**, Ars Combin 64 (2002), 271-287.

[20] D. Declercq and M. Fossorier, **Decoding algorithms for nonbinary LDPC codes over** $GF(q)$, IEEE Trans. Comm., vol. 55, no. 4, pp. 633- 643, 2007.

[21] I. B. Djordjevic. **Quantum LDPC codes from incomplete block designs**, IEEE Comm. Lett., vol. 12, pp. 389-391, 2008.

[22] P., Elias, **Coding for noisy channels**, IRE Conv. Rec, pt. 4, pp. 37-46, Mar. 1955.

[23] Jr., G.D., Forney, 1970. **Convolutional codes I: algebraic structure**. IEEE Trans. Inf. Theory16 (6), 720-738.

[24] M. P. C. Fossorier, **Quasi-cyclic low-density parity-check codes from circulant permutation matrices**, IEEE Trans. Inf. Theory, vol 50, no. 8, pp. 1788-1793, 2004.

[25] D. Gottesman, **A class of quantum error-correcting codes saturating the quantum Hamming bound**, Phys. Rev. A, vol. 54, pp. 1862-1868, 1996.

[26] M. Grassl, and M. Rotteler, **On optimal quantum codes,** Int. Journal. of Quant. Info., vol. 2, No. 1, pp. 55-64, 2004.

[27] J., Gomez-Torrecillas, F.J., Lobillo, G., Navarro, 2016. **Convolutional codes with a matrix-algebra word ambient**. Adv. Math. Com-mun.10 (1), 29-43.

[28] R. G., Gallager, **Low-density parity-check codes**, IRE Trans. Inf.Theory, vol. IT-8, pp. 21-28, Jan. 1962.

[29] Q. Huang, Q. Diao, S. Lin and K. Abdel-Ghaffar, **Cyclic and quasicyclic LDPC codes on constrained parity-check matrices and their trapping sets**, IEEE Trans. Inf. Theory, vol. 58, no. 5, pp. 2648-2671, 2012.

[30] M. Hagiwara and H. Imai, **Quantum quasi-cyclic LDPC codes**, in Proc. IEEE Int. Symp. Inf. Theory, pp. 806-810, 2007.

[31] M. Hagiwara, K. Kasai, H. Imai, and K. Sakaniwa, **Spatially coupled quasi-cyclic quantum LDPC codes**, in Proc. IEEE Int. Symp. Inf. Theory, pp. 638-642, 2011.

[32] A. , Jimenez Felstrom, and K. S., Zigangirov, **Time-varying periodic convolutional codes with low- density parity-check matrix**, IEEE Trans. Inf. Theory, vol. 45, no. 6, pp. 2181–2191, Sep. 1999.

[33] K. Kasai, M. Hagiwara, H. Imai and K. Sakaniwa, **Non-binary quasicyclic quantum LDPC codes**, in Proc. IEEE Int. Symp. Inf. Theory, pp. 653-657, 2011.

[34] K. Kasai, M. Hagiwara, H. Imai, and K. Sakaniwa, **Quantum error correction beyond the bounded distance decoding limit**, IEEE Trans. Inf. Theory, vol. 58, no. 2, pp. 1223-1230, 2012.

[35] A. Ketkar, A. Klappenecker, S. Kumar and P. k. Sarvepalli , **Nonbinary stabilizer codes over finite fields**, IEEE Transactions on information theory, VOL. 52,NO. 11, NOVEMBER 2006.

[36] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, **Perfect quantum error correcting code**, Phys. Rev. Lett., vol. 77, no. 1, pp. 198 - 201, 1996.

[37] S.R., Lopez-Permouth, S., Szabo, 2013. **Convolutional codes with additional algebraic structure**. J. Pure Appl. Algebra217 (5), 958-972.

[38] D. J. C. , MacKay, and R. M., Neal, **Near Shannon limit performance of low density parity check codes**, Electron. Lett, vol. 32, pp. 1645–1646, Aug. 1996.

[39] F.J., MacWilliams, N.J.A., Sloane, **The Theory of Error-Correcting Codes, North-Holland Publishing**, Company 1977.

[40] D. MacKay, G. Mitchison, and P. McFadden, **Sparse-graph codes for quantum error correction**, IEEE Trans. Inf. Theory, vol. 50, pp. 2315- 2330, 2004.

[41] D. MacKay, **Good error-correcting codes based on very sparse matrices**, IEEE Trans. Inf. Theory, vol. 45, pp. 399-431, 1999.

[42] M. A. Nielsen and I. L. Chuang, **Quantum computation and quantum information**, Cambridge Uni. Press, 2000.

[43] M. Newman, **Circulants and difference sets**, Proceedings of the American Mathbfatical Society, vol. 88, no. 1, pp. 184-188, 1983.

[44] D. Poulin and Y. Chung, **On the iterative decoding of sparse quantum codes**, Quantum Information Computation, vol. 8, pp. 987-1000, 2008.

[45] M. S. Postol, **A proposed quantum low-density parity-check codes**, [Online] arXiv:quant-ph/0108131, 2001.

[46] E., Prange, **Cyclic error-correcting codes in two symbols**, Air Force Cambridge Research Center, Cambridge, 57-103, MA. 195.

[47] T. Richardson, R. Urbanke, **Modern Coding Theory**, Cambridge University Press 2008.

[48] T. Richardson, M. Shokrollahi, and R. Urbanke, **The capacity of low-density parity-check codes under message-passing decoding**, IEEE Trans. Inf. Theory, vol. 47, No. 2, pp. 599-618, 2001.

[49] H. Robert Morelos-Zaragoza, **The Art of Error Correcting Coding**, John Wiley Sons Ltd. 2006.

[50] P. W. Shor, **Schbfe for reducing decoherence in quantum mbfory**, Phys. Rev. A, vol. 52, pp. 2493-2496, 1995.

[51] A. Steane, **Multiple particle interference and quantum error correction**, Proc. Royal Society of London, vol. 452, no. 1954, pp. 2551 - 2577, 1996.

[52] K. Todd Moon, **Error Correction Coding**, John Wiley Sons, Inc. 2005.

[53] P. Tan and J. Li, **Efficient quantum stabilizer codes: LDPC and LDPC-convolutional constructions**, IEEE Trans. Inf. Theory, vol. 56, pp. 476- 491, 2010.

[54] R. M. Tanner, D. Sridhara, A. Sridharan, T. E. Fuja, and D. J., Costello, **LDPC block and convolutional codes based on circulant matrices**, IEEE Trans. Inf. Theory, vol. 50, no. 12, pp. 2984, Dec. 2004.

[55] Y.-J. Wang, B. C. Sanders, B.-M. Bai and X.-M. Wang, **Enchanced feedback iterative decoding of sparse quantum codes**, IEEE Trans. on Info. Theory, vol. 58, no. 5, pp. 1231-1241, 2012.

[56] Y. Xie, J. Yuan and R. Malaney, **Quantum stabilizer codes from difference sets**, in Proc. IEEE Int. Symp. Inf. Theory, pp. 524-528, 2013.

[57] Y. Xie and J. Yuan, **Proto-graph quantum LDPC codes from tensor product of parity-check matrices**, in Proc. IEEE Global Comm. Workshop, 2015.

[58] Y. Xie and J. Yuan, **Reliable Quantum LDPC Codes Over GF(4),** in Proc. IEEE Global Comm. Workshop, 2016.

[59] Y. Xie and J. Yuan, **Quantum LDPC Codes from Quadratic Residue Sets**, School of Electrical Engineering and Telecommunications, University of New South Wales, Australia, 2017.

[60] L. Zhang, Q. Huang, S. Lin, K. Abdel-Ghaffar, and I. F. Blake, **Quasicyclic LDPC codes: an algebraic construction, rank analysis, and codes on latin squares**, IEEE Trans. Commun., vol. 58, no. 11, pp. 3126-3139, 2010.

Abstract

We design classes of quantum low-density parity-check (LDPC) codes, called quasi-cyclic stabilizer (QCS) codes, from conventional QC-LDPC codes. The proposed QCS codes belong to the family of non-CSS stabilizer codes. The QC-LDPC codes are self-orthogonal with respect to the symplectic inner product (SIP), and are constructed from submatrices of non-orthogonal Latin squares via array dispersion. The Latin squares are constructed using quadratic (non)-residue sets of prime modulus p, where $p = 4n \pm 1$. For $p = 4n - 1$, two constructions, namely Type-I-A and Type-I-B QCS codes, are proposed based on matrix superposition and matrix concatenation, respectively. For $p = 4n + 1$, Type-II QCS codes are proposed based on permutations of a base matrix. We show that the parity-check matrix for Type-I-B and Type-II QCS codes is self-orthogonal with respect to the SIP for all orders of circulant permutation matrix. This results in designing some QCS codes characterized by a single base matrix. We show that the minimum distance of Type-II QCS codes can be lower bounded by the minimum distance of the QC-LDPC codes. Simulation results show that the proposed QCS codes outperform some codes in the literature with a noteworthy low error floor, below 10^{-7}, over quantum depolarizing channels.

Faculty Of Mathematical Sciences

MSc Thesis in Cryptography and Coding

Investigation of methods for constructing quantum LDPC codes using classical codes

By: Maede Najafi

Supervisor:

Dr. Meysam Alishahi

Advisor:

Dr. Farzane Amirzade Dana

December 2021