CSS codes

Reza Haghshenas

قضیه‌ی اساسی تصحیح خطای کوانتومی

Basis of $C = \{ |c_1\rangle, |c_2\rangle, \dots |c_k\rangle \}$

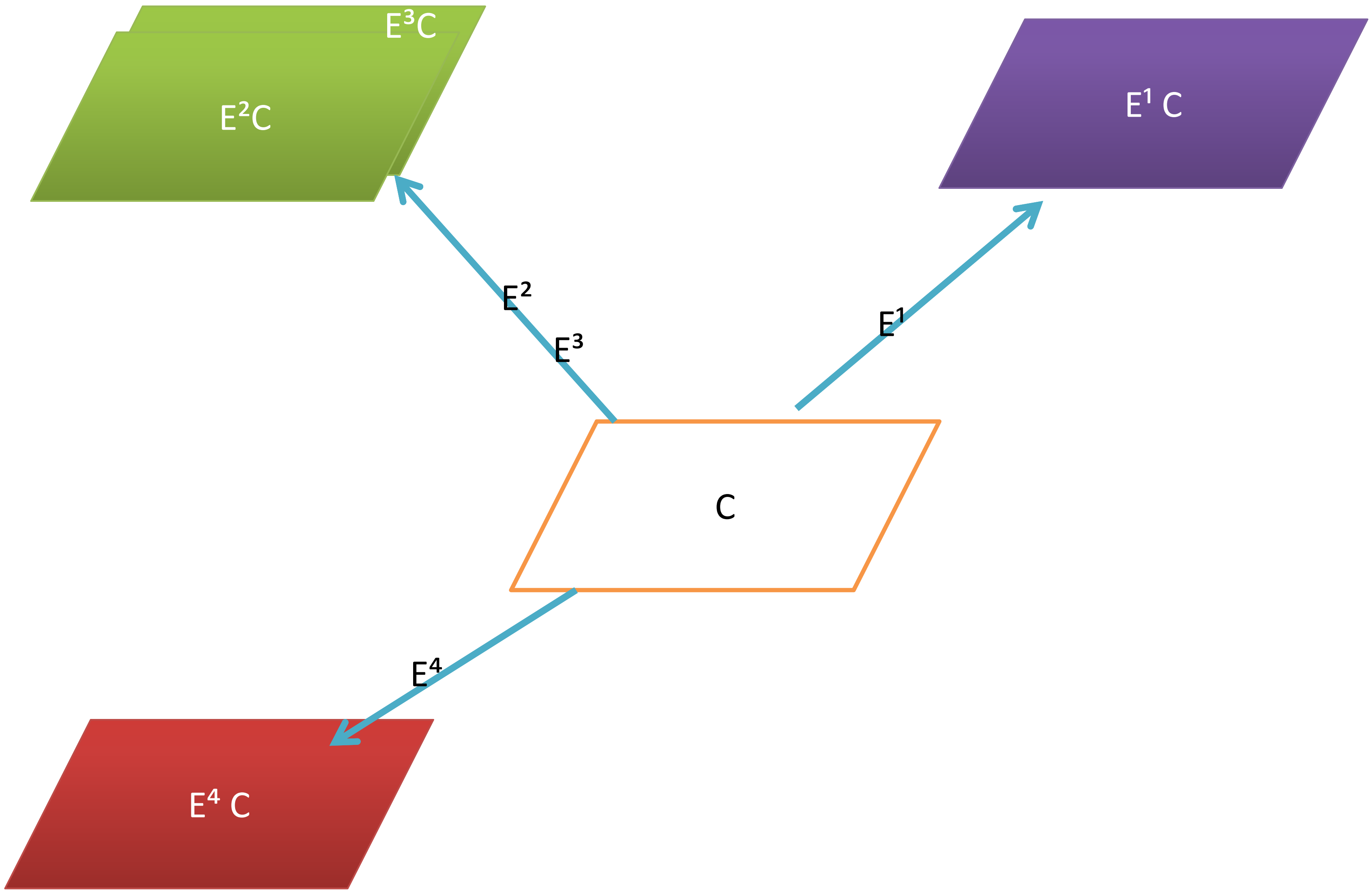
قضیه : C یک کد کوانتومی تصحیح کننده‌ی خطا در کانال Q است اگر و فقط اگر

$\forall\ E_k, E_l \ \ \&\ \ \forall\ i, j$

$$\langle c_i | E_k^\dagger E_l | c_j \rangle = 0 \qquad \text{if } i \neq j$$

$$\langle c_i | E_k^\dagger E_l | c_i \rangle = \alpha_{kl} \qquad \forall\ i$$

قضیه‌ی اساسی تصحیح خطای کوانتومی



We know about necessary and sufficient conditions of quantum error correction codes,
But what can we construct a class of quantum error correction codes?

Answer is CSS codes that use of classical linear codes

Calderbank-Shor-Steane codes

CSS codes:

فرض کنید که $C_۱$ یک کد کلاسیک خطی $[n, k_۱]$ و $C_۲$ یک کد کلاسیک خطی $[n, k_۲]$ است به نحوی که $C_۲ \subset C_۱$ و کد $C_۱$ و $C_۲^{\perp}$ بتوانند t خطا را تصحیح کنند. می خواهیم نشان بدهیم که کد کوانتومی $CSS(C_۱, C_۲)$ که توسط حالت های

$$|x + C_۲\rangle \equiv \frac{۱}{\sqrt{|C_۲|}} \sum_{y \in C_۲} |x + y\rangle$$

ابتدا باید ببینبم این کد معرف فضای چند کیوبیتی است؟

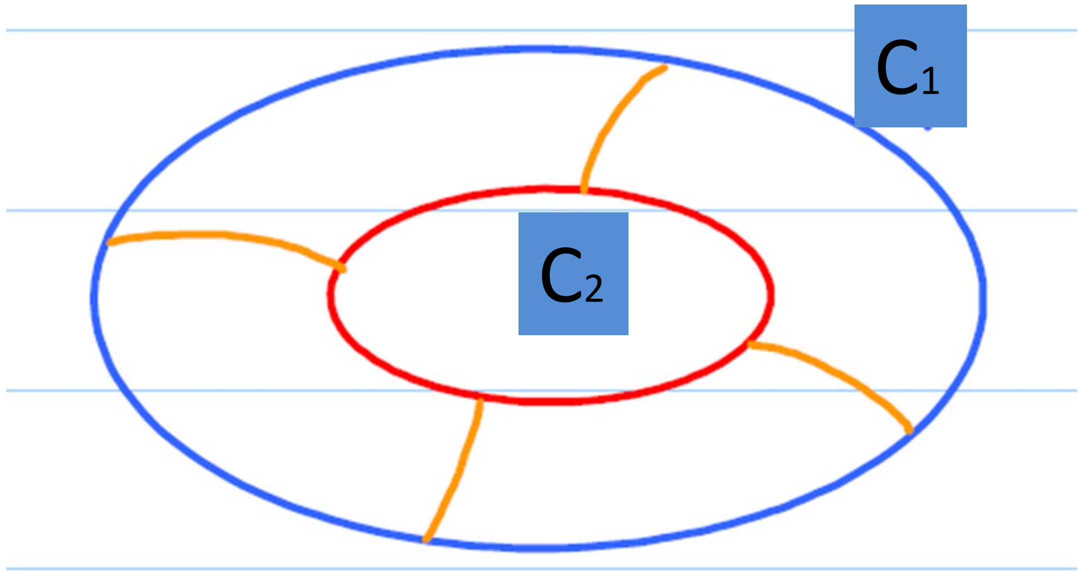
$$x - x' \in C_۲ \longrightarrow |x + C_۲\rangle = |x' + C_۲\rangle$$

$$x - x' \notin C_۲ \longrightarrow |x + C_۲\rangle \neq |x' + C_۲\rangle, |x + C_۲\rangle \perp |x' + C_۲\rangle.$$

$$|x + C_{\text{۲}}\rangle \equiv \frac{\text{۱}}{\sqrt{|C_{\text{۲}}|}} \sum_{y \in C_{\text{۲}}} |x + y\rangle$$

$$x - x' \in C_{\text{۲}} \longrightarrow |x + C_{\text{۲}}\rangle = |x' + C_{\text{۲}}\rangle$$

$$x - x' \notin C_{\text{۲}} \longrightarrow |x + C_{\text{۲}}\rangle \neq |x' + C_{\text{۲}}\rangle, |x + C_{\text{۲}}\rangle \perp |x' + C_{\text{۲}}\rangle.$$



از معادلات بالا در می یابیم که تعداد پایه های کد $CSS(C_1, C_2)$ برابراست با تعداد هم مجموعه های C_2 در C_1 (C_1/C_2) ، که تعداد اعضای ان برابر است با $\frac{|C_1|}{|C_2|}$. بنابرای تعداد پایه های کد $CSS(C_1, C_2)$ برابر است با $2^{k_1-k_2}$. تا اینجا نشان داده ایم که این یک کد $[n, k_1 - k_2]$ است.

حال باید نشان بدهیم که این کد می تواند t خطا را تصحیح کند

خطای بیت برگردان را با یک nتایی مرتب e_1 و خطای فاز برگردان را با n تایی مرتب e_2 نشان می دهیم

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)\cdot(e_2)} |x + y + e_1\rangle$$

برای اشکار کردن خطای بیت برگردان از یک حالت کمکی $|۰\rangle$ و عملگر یونیتاری U استفاده می کنیم:

$$|x+y+e_۱\rangle|۰\rangle \xrightarrow{U} |x+y+e_۱\rangle|H_۱(x+y+e_۱)\rangle = |x+y+e_۱\rangle|H_۱(e_۱)\rangle$$

$$\frac{۱}{\sqrt{|C_۲|}}\sum_{y\in C_۲}(-۱)^{(x+y)\cdot(e_۲)}|x+y\rangle$$

برای اشکار کردن خطای فاز برگردان ابتدا روی هر یک از بیت ها عملگر هادامارد را اثر می دهیم

$$(H)^{\otimes n}\frac{۱}{\sqrt{|C_۲|}}\sum_{y\in C_۲}(-۱)^{(x+y)\cdot(e_۲)}|x+y\rangle = \frac{۱}{\sqrt{|C_۲|۲^n}}\sum_{z}\sum_{y\in C_۲}(-۱)^{(x+y)\cdot(e_۲+z)}|z\rangle.$$

$$(H)^{\otimes n}|x+y\rangle = \frac{۱}{\sqrt{۲^n}}\sum_{z}(-۱)^{(x+y)\cdot z}|z\rangle$$

$$(H)^{\otimes n}\frac{۱}{\sqrt{|C_۲|}}\sum_{y\in C_۲}(-۱)^{(x+y)\cdot(e_۲)}|x+y\rangle = \frac{۱}{\sqrt{|C_۲|۲^n}}\sum_{z}\sum_{y\in C_۲}(-۱)^{(x+y)\cdot(e_۲+z)}|z\rangle.$$

قرار می دهیم $z' = z + e_۲$

$$\boxed{\frac{۱}{\sqrt{|C_۲|۲^n}}\sum_{z'}\sum_{y\in C_۲}(-۱)^{(x+y)\cdot(z')}|z'+e_۲\rangle.}$$

قضیه:

برای کد های C و $C^{\perp}$ داریم

$$\sum_{\nu\in C}(-۱)^{\tilde{\nu}u} = \begin{cases} ۲^k & u\in C^{\perp} \\ ۰ & u\notin C^{\perp} \end{cases}$$

با توجه به قضیه صفحه قبل اگر $z' \in C_2^{\perp}$ پس $|C_2| = \sum_{y \in C_2}(-1)^{y \cdot z'}$، و هنگامی که $z' \neq C_2$
داریم $\sum_{y \in C_2}(-1)^{y \cdot z'} = |C_2|$. بنابراین حالت ما به شکل مقابل در می اید

$$\frac{1}{\sqrt{\frac{2^n}{|C_2|}}} \sum_{z' \in C_2^{\perp}} (-1)^{(x)\cdot(z')} |z' + e_2\rangle$$

همانند قسمت گذشته با استفاده از حالت کمکی $|0\rangle$ و عملگر یونیتاری U داریم:

$$|z' + e_2\rangle|0\rangle \longrightarrow |z' + e_2\rangle|H_2(z' + e_2)\rangle = |z' + e_2\rangle|H_2(e_2)\rangle$$

لذا بدست می اوریم

$$\frac{1}{\sqrt{\frac{2^n}{|C_2|}}} \sum_{z' \in C_2^{\perp}} (-1)^{(x)\cdot(z')} |z'\rangle.$$

با به کار بردن عملگر هادامارد به هر یک از بیت ها، حالت اولیه بدست می اید

$$\boxed{\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle.}$$

مثال:

به عنوان یک مثال، کد $[[۷, ۱, ۳]]$ را بررسی میکنیم. این کد معروف به کد استین است. برای ساختن این کد از کد کلاسیک خطی $[۷, ۴, ۳]$ که توسط ماتریس پاریته زیر تولید می شود به عنوان کد $C_۱$ استفاده می کنیم

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

کد $C_۲$ را برابر با $C_۱^{\perp}$ می گیریم. برای اینکه نشان دهیم این دو کد به عنوان کد CSS کار می کنند باید ابتدا نشان دهیم که $C_۲ \subset C_۱$. برای این کار ابتدا ماتریس پاریته $C_۲$ را بدست می اوریم که برابر است با

$$H(C_۲) = \tilde{G}(C_۱) = \begin{pmatrix} ۱ & ۰ & ۱ & ۰ & ۱ & ۰ & ۱ \\ ۰ & ۱ & ۰ & ۰ & ۱ & ۰ & ۱ \\ ۰ & ۱ & ۱ & ۰ & ۰ & ۱ & ۱ \\ ۰ & ۰ & ۰ & ۱ & ۱ & ۱ & ۱ \end{pmatrix}.$$

پایه های این کد برابراند با:

$$|0 + C_2\rangle = |\bar{0}\rangle = |0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle$$
$$|0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle.$$

و برای پیدا کردن پایه دیگر کافی است عضوی از C_1 را پیدا کنیم که در C_2 نباشد

$$|(1, 1, 1, 1, 1, 1, 1)+C_2\rangle = |\bar{1}\rangle = |1111111\rangle + |0101011\rangle + |1001100\rangle + |0011001\rangle$$
$$|1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle.$$