קירוב שערים ומשפט סולובי-קיטאייב

1 כמה מדויקים צריכים להיות השערים?

עד כה הרשינו לעצמנו לתכנן מעגלים באמצעות שערים יוניטריים נוחים. אבל במחשב נתון יש אוסף מוגבל של פעולות בסיסיות. האם אפשר להחליף את השערים שבאלגוריתם ברצפים של שערים מתוך האוסף הזה, בלי שהמעגל יתארך יותר מדי? לפני שנענה, נברר איזה דיוק דרוש בכל שער.

לאורך היחידה נשתמש בנורמת האופרטור:

$$\|M\| = \max_{\|v\|_2=1} \|Mv\|_2.$$

נזכיר כי היא תת־כפלית, וכפל במטריצה יוניטרית אינו משנה אותה. בפרט, הנורמה של מטריצה יוניטרית היא אחת.

נניח שהמעגל הרצוי הוא

$$U = U_L U_{L-1} \cdots U_1,$$

ושמימשנו במקומו את המעגל

$$\widetilde{U} = \widetilde{U}_L \widetilde{U}_{L-1} \cdots \widetilde{U}_1, \qquad \|\widetilde{U}_j - U_j\| \le \eta.$$

כל השערים, כולל השערים המקרבים, יוניטריים. שער שפועל רק על חלק מהקיוביטים מורחב על ידי הזהות על האחרים; ההרחבה הזו אינה משנה את נורמת השגיאה.

אפשר לחשוש שהשגיאות יגבירו זו את זו. לשמחתנו, במודל הזה הן מצטברות לכל היותר באופן ליניארי. נסמן $E_j = \widetilde{U}_j - U_j$. הזהות הטלסקופית הבאה נותנת

$$\widetilde{U} - U = \sum_{j=1}^{L} \widetilde{U}_L \cdots \widetilde{U}_{j+1} E_j U_{j-1} \cdots U_1.$$

מכפלות ריקות מתפרשות כזהות. לפי אי־שוויון המשולש והאינווריאנטיות היוניטרית,

$$\|\widetilde{U} - U\| \le \sum_{j=1}^{L} \|E_j\| \le L\eta.$$

לכל קלט מנורמל, גם המרחק בין שני וקטורי הפלט חסום על ידי $L\eta$. כדי לקשור זאת לפלט הקלאסי, יהי P מקרן המתאר אירוע במדידה הסופית, ונסמן את שני מצבי הפלט ב־ $|\psi\rangle, \left|\widetilde{\psi}\right\rangle$. אז

$$\left|\langle\psi| P |\psi\rangle - \left\langle\widetilde{\psi}\right| P \left|\widetilde{\psi}\right\rangle\right| \leq 2\| |\psi\rangle - \left|\widetilde{\psi}\right\rangle \| \leq 2L\eta.$$

לכן, כדי לשנות את הסתברות ההצלחה בלכל היותר δ, מספיק לבחור דיוק לכל שער של $\eta \leq \delta/(2L)$.

זהו ניתוח של *קירוב יוניטרי* לשערים. רעש פיזיקלי כללי, ובפרט אינטראקציה עם הסביבה, אינו בהכרח מהצורה הזו. ההתמודדות איתו שייכת לתיקון שגיאות ולחישוב עמיד לשגיאות, fault-tolerant quantum computation. בהמשך היחידה נניח שאפשר לבצע בדיוק את שערי הבסיס, ונעסוק בשגיאה הנובעת מהחלפת שער רצוי ברצף שלהם.

2 אוניברסליות מדויקת ואוניברסליות בקירוב

אוסף שערים הוא *אוניברסלי במדויק* אם אפשר לממש באמצעותו כל שער יוניטרי רצוי, עד כדי פאזה גלובלית. למשל, כל השערים על קיוביט יחיד יחד עם CNOT מאפשרים זאת. זהו אוסף אינסופי: השערים על קיוביט יחיד תלויים בפרמטרים רציפים.

לעומת זאת, מאוסף סופי אפשר לבנות רק מספר בן־מנייה של מעגלים סופיים, בעוד שיש מספר לא בן־מנייה של שערים, גם לאחר זיהוי פאזות גלובליות. לכן מאוסף סופי לא נצפה לאוניברסליות מדויקת. נבקש *אוניברסליות בקירוב*: לכל שער ולכל דיוק חיובי, קיים רצף משערי האוסף שמקרב אותו עד כדי פאזה גלובלית.

דוגמה חשובה היא

$$\{H, T, \mathsf{CNOT}\}, \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}.$$

לא נוכיח כאן את האוניברסליות של האוסף הזה. שימו לב לסימון: במספר מקורות מגדירים את שער T כ־ $\mathrm{diag}(e^{-i\pi/8}, e^{i\pi/8})$, הנבדל מההגדרה שלנו רק בפאזה גלובלית.

חשוב גם לדייק במונח *שער שוזר*: לא מספיק ששער על שני קיוביטים אינו מכפלה טנזורית. למשל, SWAP אינו מכפלה כזו, אבל הוא שולח כל מצב מכפלה למצב מכפלה. שער שוזר הוא שער שיוצר שזירה עבור לפחות מצב מכפלה אחד.

האוניברסליות מבטיחה שקיים קירוב, אבל עדיין אינה אומרת דבר על אורך הרצף. אולי כדי לקבל דיוק ε נצטרך מיליון שערים? אולי מספר השערים יגדל כמו $1/\varepsilon$? כאן נכנס משפט סולובי--קיטאייב.

3 ניסוח המשפט

נתמקד בממד קבוע d, כלומר בשער על מספר קבוע של קיוביטים. נעבוד בחבורה

$$SU(d) = \{U \in \mathbb{C}^{d\times d} : U^\dagger U = I,\ \det U = 1\}.$$

כל מטריצה יוניטרית ניתנת לכתיבה כ־ $e^{i\theta}V$ עם $V \in SU(d)$. לצורך קירוב מעגל שלם אפשר להזניח את הפאזה הגלובלית. עם זאת, פאזה של שער הופכת לפאזה יחסית אם מוסיפים לו בקרה, ולכן כשמקרבים שער מבוקר יש להתייחס למטריצה המבוקרת כולה.

משפט 3.1 (סולובייב--קיטאייב, הגרסה שנוכיח)**.** *יהי $\mathcal{G} \subseteq SU(d)$ אוסף סופי הסגור ללקיחת הופכי, ונניח שהמכפלות של שערים ממנו צפופות ב־ $SU(d)$. אז לכל $U \in SU(d)$ ולכל $0 < \varepsilon < 1/2$ קיימת מילה $\widetilde{U}$ מעל $\mathcal{G}$ כך ש־*

$$\|U - \widetilde{U}\| \le \varepsilon, \qquad |\widetilde{U}| = O\!\left(\log^{\gamma}\frac{1}{\varepsilon}\right), \qquad \gamma = \frac{\log 5}{\log(3/2)} \approx 3.97.$$

הקבוע בחסם תלוי באוסף השערים ובממד הקבוע. בהנחות החישוביות הרגילות על ייצוג המטריצות וחישובן בדיוק נתון, אפשר גם למצוא את המילה בזמן פולינומי ב־ $\log(1/\varepsilon)$.

ההנחה על הופכיים אומרת שהיפוך מילה אינו מגדיל את אורכה: הופכים את סדר השערים ומחליפים כל שער בהופכי שלו. אפשר גם לצרף מראש לאוסף סופי את ההופכיים שלו.

הממד הקבוע חשוב. המשפט אינו טוען שאפשר לממש שער שרירותי על n קיוביטים במספר שערים פולינומי ב־ n. נשתמש בו כדי לקרב בנפרד את השערים המקומיים של מעגל נתון.

3.1 תוכנית ההוכחה

מצפיפות ומקומפקטיות אפשר להכין מראש רשימה סופית של מילים, כך שכל שער נמצא במרחק לכל היותר ε_0 מאחת מהן. זו רשת בדיוק קבוע, שאותו נבחר קטן מספיק בהמשך. אורך המילים המרבי ברשימה הוא קבוע ℓ_0. הכנת הרשימה יכולה להיות יקרה מאוד, אבל אינה תלויה בדיוק הסופי המבוקש.

נראה כיצד לשפר קירוב בדיוק ε לקירוב בדיוק $K\varepsilon^{3/2}$, תוך הגדלת אורך המילה פי חמישה בלבד. חזרה על השיפור תיתן את המשפט. כל הקבועים בהמשך יכולים להיות תלויים ב־ d.

4 למה דווקא קומוטטור?

נניח שכבר מצאנו קירוב $\widetilde{U}$ לשער הרצוי U, וש־ $\|U-\widetilde{U}\|\le\varepsilon$. נגדיר את *שער התיקון*

$$\Delta = U\widetilde{U}^{-1}.$$

אז

$$U = \Delta\widetilde{U}, \qquad \|\Delta - I\| \le \varepsilon.$$

כלומר, אחרי הקירוב הראשון נשאר לנו לתקן תנועה קטנה מאוד ליד הזהות.

אם פשוט נקרב את Δ בדיוק ε, לא נרוויח דבר. אנחנו מחפשים דרך להרכיב תיקון קטן מתוך שערים שאנחנו יודעים לקרב רק בדיוק הישן, כך שהשגיאות שלהם ישפיעו על התיקון בעוצמה קטנה יותר.

4.1 הלוך, הצידה, חזור

נחשוב על שתי תנועות קטנות, המיוצגות על ידי V ו־ W. נסתכל על הביטוי

$$\mathcal{C}(V,W) = VWV^{-1}W^{-1}.$$

זהו *הקומוטטור החבורתי*. אם התנועות מתחלפות, הוא בדיוק הזהות. אם הן אינן מתחלפות, הוא מודד את השארית שנוצרת מהחלפת סדר הפעולות. אפשר לחשוב עליו כמסלול קצר שחוזר על צעדיו בשני כיוונים, אך אינו נסגר בדיוק מפני שסדר התנועות משנה. כרגיל, כשמפעילים את המכפלה על וקטור, הגורם הימני פועל ראשון.

כדי לראות מה נשאר, נכתוב

$$V = e^{tX}, \qquad W = e^{tY},$$

כאשר X,Y אנטי־הרמיטיות ו־ t קטן. מפיתוח טיילור, עבור מטריצות קבועות,

$$e^{tX}e^{tY} = I + t(X+Y) + t^2\left(\frac{X^2}{2} + XY + \frac{Y^2}{2}\right) + O(t^3),$$
$$e^{-tX}e^{-tY} = I - t(X+Y) + t^2\left(\frac{X^2}{2} + XY + \frac{Y^2}{2}\right) + O(t^3).$$

כשמכפילים, האיברים הליניאריים מתבטלים, ובסדר השני מתקבל

$$\mathcal{C}(e^{tX},e^{tY}) = I + t^2(XY - YX) + O(t^3).$$

הביטוי

$$[X,Y] = XY - YX$$

נקרא *הקומוטטור המטריציוני*, או סוגר לי. הוא שונה מהקומוטטור החבורתי: הראשון הוא הפרש מכפלות, והשני הוא מכפלה של ארבע מטריצות הפיכות. הנוסחה מראה את הקשר ביניהם.

זהו הרמז שחיפשנו: **תנועות בגודל מסדר ראשון יוצרות, באמצעות קומוטטור, תיקון מסדר שני.** כדי ליצור תיקון בגודל ε, טבעי לבחור תנועות בגודל $\sqrt{\varepsilon}$. השארית מסדר שלישי תהיה אז בגודל $\varepsilon^{3/2}$.

4.2 הקשר לאלגבראות לי

כן, זה בדיוק המקום שבו אלגברת לי מופיעה. חבורת המטריצות $SU(d)$ היא מרחב רציף של פעולות, ואלגברת לי שלה מתארת את כיווני התנועה ליד הזהות:

$$\mathfrak{su}(d) = \{X : X^\dagger = -X,\ \operatorname{tr} X = 0\}.$$

למשל, נגזרת של מסלול יוניטרי העובר בזהות חייבת להיות אנטי־הרמיטית: גזירת הזהות $U(t)^\dagger U(t) = I$ בנקודה $U(0) = I$ נותנת $U'(0)^\dagger + U'(0) = 0$. תנאי הדטרמיננטה נותן עקבה אפס.

האקספוננט מחזיר כיוון כזה לפעולה בחבורה: $X \mapsto e^X$. סוגר לי מתאר את הכיוון מסדר שני המתקבל מהמסלול הקטן של הקומוטטור. איננו צריכים כאן את התורה הכללית של אלגבראות לי; פיתוח טיילור והעובדה שנוכיח בהמשך יספיקו.

נוח לנו לכתוב את הכיוונים בתור iB, iC, כאשר B, C הרמיטיות. אז $[iB, iC] = -[B, C]$, ולכן, אם $\|B\|, \|C\| \le r$ ו־ r קטן,

$$e^{iB} e^{iC} e^{-iB} e^{-iC} = I - [B, C] + O(r^3).$$

כל סימוני השארית ביחידה הם בנורמת האופרטור.

4.3 דוגמה: מסיבובים בשני כיוונים לסיבוב בכיוון שלישי

עבור מטריצות פאולי מתקיים $[X, Y] = 2iZ$. לכן

$$e^{itX} e^{itY} e^{-itX} e^{-itY} = I - 2it^2 Z + O(t^3) = e^{-2it^2 Z} + O(t^3).$$

כלומר, ארבעה סיבובים קטנים סביב שני צירים נותנים, בקירוב, סיבוב קטן עוד יותר סביב הציר השלישי. זה מסביר באופן מוחשי איך קומוטטור יכול לייצר כיוון תיקון חדש.

למשל, כדי לקרב e^{iaZ} עבור $a > 0$ קטן, אפשר לבחור

$$B = \sqrt{a/2}\, X, \qquad C = -\sqrt{a/2}\, Y.$$

אז $[B,C] = -iaZ$, ושגיאת הקירוב היא $O(a^{3/2})$.

5 בניית תיקון קטן כקומוטטור

נחזור ל־ $\Delta \in SU(d)$ שמרחקו מהזהות לכל היותר ε. עבור ε קטן מספיק אפשר לכתוב

$$\Delta = e^{iA}, \qquad A = A^\dagger, \qquad \operatorname{tr} A = 0, \qquad \|A\| = O(\varepsilon).$$

כדי לראות זאת, מלכסנים את Δ ובוחרים לכל ערך עצמי $e^{i\theta_j}$ את הזווית הקטנה שלו. אז $|\theta_j| = O(\varepsilon)$. מאחר שהדטרמיננטה היא אחת, $\sum_j \theta_j$ היא כפולה של 2π; עבור ממד קבוע ו־ ε קטן מספיק, הכפולה היחידה האפשרית היא אפס.

כעת נשתמש בעובדה הבאה, שהוכחתה מופיעה בסוף היחידה.

למה 5.1 (קומוטטור מאוזן)**.** *לכל מטריצה הרמיטית חסרת עקבה A קיימות מטריצות הרמיטיות חסרות עקבה B, C כך ש־*

$$[B,C] = -iA, \qquad \|B\|, \|C\| \le c_d \sqrt{\|A\|}.$$

כאן c_d הוא קבוע התלוי רק בממד.

התנאי על העקבה אינו טכני בלבד: לכל זוג מטריצות מתקיים $\operatorname{tr}[B,C] = 0$. לכן לא נוכל לייצר בדרך הזו כיוון שהוא כפולה לא־אפסית של הזהות. זו גם הסיבה לטיפול בפאזה הגלובלית ולמעבר ל־ $SU(d)$. ברמת החבורה, הדטרמיננטה של כל קומוטטור חבורתי היא אחת.

נגדיר

$$V = e^{iB}, \qquad W = e^{iC}.$$

שתי המטריצות שייכות ל־ $SU(d)$, ומרחקן מהזהות הוא $O(\sqrt{\varepsilon})$. לפי פיתוח הקומוטטור,

$$\begin{aligned} \mathcal{C}(V,W) &= I - [B,C] + O(\varepsilon^{3/2}) \\ &= I + iA + O(\varepsilon^{3/2}) \\ &= e^{iA} + O(\varepsilon^{3/2}). \end{aligned}$$

בשורה האחרונה השתמשנו בכך ששארית הפיתוח של e^{iA} היא $O(\|A\|^2) = O(\varepsilon^2)$. לכן

$$\|\Delta - \mathcal{C}(V,W)\| = O(\varepsilon^{3/2}).$$

עד כאן בנינו תיקון מצוין, אבל השערים V, W עדיין אינם בהכרח מילים משערי הבסיס. נותר להבין מדוע אפשר להחליף אותם בקירובים בדיוק הישן, מבלי להרוס את השיפור.

6 למה שגיאות הקירוב אינן הורסות את התיקון?

נניח שהקירובים שלנו מקיימים

$$\|V - \widetilde{V}\|, \|W - \widetilde{W}\| \le \varepsilon.$$

חסם טלסקופי רגיל על ארבעת הגורמים היה נותן רק שגיאה $O(\varepsilon)$. זה לא מספיק! אבל החסם הזה מפספס את המבנה: כל שער מופיע יחד עם ההופכי *של אותו שער*, ושני השערים קרובים לזהות.

הנה דרך ישירה לראות את הרווח. לכל מטריצות יוניטריות,

$$\begin{aligned}\|\mathcal{C}(V,W) - \mathcal{C}(\widetilde{V},W)\| &= \|VWV^\dagger - \widetilde{V}W\widetilde{V}^\dagger\| \\ &= \|V(W-I)V^\dagger - \widetilde{V}(W-I)\widetilde{V}^\dagger\| \\ &\le 2\|V-\widetilde{V}\|\,\|W-I\|.\end{aligned}$$

הוצאת הזהות היא הצעד החשוב: אם $W = I$, הקומוטטור הוא הזהות בלי קשר לבחירת V, ולכן השגיאה ב־ V אינה יכולה להשפיע כלל. ככל ש־ W קרוב יותר לזהות, השפעת השגיאה קטנה יותר.

באופן דומה, באמצעות הכתיבה

$$\mathcal{C}(\widetilde{V},W) = \widetilde{V}(I + W(\widetilde{V}^\dagger - I)W^\dagger),$$

מקבלים

$$\|\mathcal{C}(\widetilde{V},W) - \mathcal{C}(\widetilde{V},\widetilde{W})\| \le 2\|W-\widetilde{W}\|\,\|\widetilde{V}-I\|.$$

כאן

$$\|\widetilde{V} - I\| \le \|V - I\| + \varepsilon = O(\sqrt{\varepsilon}).$$

מצירוף החסמים נובע

$$\|\mathcal{C}(V,W) - \mathcal{C}(\widetilde{V},\widetilde{W})\| = O(\varepsilon\sqrt{\varepsilon}) = O(\varepsilon^{3/2}).$$

זהו היתרון השני של הקומוטטור: לא רק שהוא יוצר תיקון מסדר שני, אלא גם שגיאות בקירוב גורמיו מוכפלות במרחק הקטן של הגורמים האחרים מהזהות.

6.1 צעד השיפור

נגדיר את המילה החדשה

$$U_{\text{new}} = \widetilde{V}\widetilde{W}\widetilde{V}^{-1}\widetilde{W}^{-1}\widetilde{U}.$$

אז

$$\begin{aligned}\|U - U_{\text{new}}\| &= \|\Delta - \mathcal{C}(\widetilde{V}, \widetilde{W})\| \\ &\le \|\Delta - \mathcal{C}(V, W)\| + \|\mathcal{C}(V, W) - \mathcal{C}(\widetilde{V}, \widetilde{W})\| \\ &\le K\varepsilon^{3/2}\end{aligned}$$

עבור קבוע מתאים $K \ge 1$. אם כל אחד מהקירובים הישנים הוא מילה באורך לכל היותר ℓ, אורך המילה החדשה הוא לכל היותר 5ℓ.

חשוב שהמילים $\widetilde{V}^{-1}, \widetilde{W}^{-1}$ מתקבלות על ידי היפוך המילים שכבר בחרנו, ולא על ידי חיפוש קירובים עצמאיים להופכיים. כך נשמר הביטול שעליו מבוסס הניתוח.

7 מהשיפור המקומי למשפט

נסמן ב־ ε_k את חסם השגיאה ברמה k, וב־ ℓ_k את חסם אורך המילים. הבנייה נותנת

$$\varepsilon_{k+1} = K\varepsilon_k^{3/2}, \qquad \ell_{k+1} \le 5\ell_k.$$

נבחר מראש ε_0 קטן מספיק לכל הלמות, ובפרט כך ש־ $K^2\varepsilon_0 < 1$. אם נסמן $q_k = K^2\varepsilon_k$, נקבל

$$q_{k+1} = q_k^{3/2}, \qquad q_k = q_0^{(3/2)^k}, \qquad \ell_k \le 5^k \ell_0.$$

לכן השגיאה קטנה בקצב כפול־מעריכי במספר הרמות, בעוד האורך גדל רק מעריכית.

נבחר את הרמה הראשונה שבה $\varepsilon_k \le \varepsilon$. אז

$$k = \log_{3/2} \log \frac{1}{\varepsilon} + O(1),$$

ומכאן

$$\ell_k \le \ell_0\, 5^k = O\!\left(\log^{\log 5/\log(3/2)} \frac{1}{\varepsilon}\right).$$

זהו החסם שרצינו.

הבנייה גם אלגוריתמית: כדי לקרב שער ברמה חדשה, מוצאים לו קירוב ברמה הקודמת, מחשבים את שער התיקון ואת שני גורמיו, ומקרבים כל אחד מהגורמים ברמה הקודמת. יש שלוש קריאות רקורסיביות; את שני ההופכיים מקבלים ללא קריאות נוספות. הממד קבוע, ועומק הרקורסיה הוא $O(\log\log(1/\varepsilon))$. חישובי המטריצות נעשים בדיוק מספיק כדי שהשגיאות הנומריות ייבלעו בחסמים. בהנחות הייצוג שצוינו במשפט, מתקבל זמן פולינומי ב־ $\log(1/\varepsilon)$, כולל כתיבת המילה המתקבלת.

8 המסקנה למעגלים קוונטיים

נחזור למעגל בעל L שערים מקומיים, שכל אחד מהם פועל על מספר קבוע של קיוביטים. כדי לקבל שגיאה כוללת בנורמה לכל היותר δ, נקרב כל שער בדיוק δ/L. משפט סולובי--קיטאייב מחליף כל שער במילה באורך

$$O\left(\log^{\gamma}\frac{L}{\delta}\right),$$

ולכן מספר השערים הכולל הוא

$$O\left(L\log^{\gamma}\frac{L}{\delta}\right).$$

עבור שגיאה קבועה, או שגיאה שהיא הפוכה לפולינום, התקורה היא פולילוגריתמית בגודל המעגל. זו הסיבה שבחירת אוסף שערים אוניברסלי סביר אינה משנה את מחלקת הבעיות שאפשר לפתור בחישוב קוונטי יעיל.

המעריך $\gamma \approx 3.97$ הוא המעריך שמתקבל מההוכחה הזו, ואינו חסם מיטבי ידוע. קיימים שיפורים כלליים, ועבור אוספי שערים מיוחדים גם בניות קצרות יותר. לא נזדקק להם כאן.

השלמה: הוכחת למת הקומוטטור המאוזן

הדוגמה עם מטריצות פאולי כבר מסבירה את הרעיון עבור קיוביט יחיד. כדי להשלים את ההוכחה בממד קבוע כללי, נראה בנייה אלמנטרית.

נניח $A \neq 0$, ונסמן $\eta = \|A\|$. ראשית נעבור לבסיס שבו כל איברי האלכסון של A הם אפס. אכן, נכתוב

$$A = Q\,\mathrm{diag}(a_1,\dots,a_d)Q^{\dagger}, \qquad \sum_{j=1}^{d} a_j = 0.$$

תהי F מטריצת פורייה המנורמלת, שכל ערכיה בערך מוחלט הם $1/\sqrt{d}$. עבור $R = QF$ המטריצה

$$A' = R^{\dagger}AR = F^{\dagger}\,\mathrm{diag}(a_1,\dots,a_d)F$$

מקיימת

$$A'_{jj} = \frac{1}{d}\sum_{k=1}^{d} a_k = 0.$$

נבחר מטריצה אלכסונית עם ערכים שונים ועקבה אפס:

$$D = \mathrm{diag}(d_1,\dots,d_d), \qquad d_j = j - \frac{d+1}{2}.$$

לכל מטריצה C' מתקיים

$$[D, C']_{jk} = (d_j - d_k) C'_{jk}.$$

זו הסיבה שבחרנו בסיס שבו האלכסון של A' מתאפס: כעת אפשר לפתור את משוואת הקומוטטור איבר־איבר.

נגדיר

$$B' = \sqrt{\eta}\, D, \qquad C'_{jj} = 0, \qquad C'_{jk} = \frac{-iA'_{jk}}{\sqrt{\eta}\,(d_j - d_k)} \quad (j \neq k).$$

אז B', C' הרמיטיות וחסרות עקבה, ומתקיים

$$[B', C'] = -iA'.$$

להרמיטיות של C' משתמשים גם ב־ $A'_{kj} = \overline{A'_{jk}}$ וגם בכך שהמכנה מחליף סימן כאשר מחליפים בין האינדקסים.

לבסוף,

$$\|B'\| \leq \frac{d-1}{2}\sqrt{\eta}.$$

מאחר ש־ $|d_j - d_k| \geq 1$ עבור אינדקסים שונים, אפשר לחסום באמצעות נורמת פרובניוס:

$$\|C'\| \leq \|C'\|_{\mathrm{F}} \leq \frac{\|A'\|_{\mathrm{F}}}{\sqrt{\eta}} \leq \sqrt{d}\,\sqrt{\eta}.$$

כאן $\|M\|_{\mathrm{F}} = (\sum_{j,k} |M_{jk}|^2)^{1/2}$, והשתמשנו באי־השוויון $\|M\|_{\mathrm{F}} \leq \sqrt{d}\,\|M\|$.

נחזיר את שתי המטריצות לבסיס המקורי:

$$B = RB'R^{\dagger}, \qquad C = RC'R^{\dagger}.$$

הצמדה יוניטרית שומרת נורמה, הרמיטיות ועקבה, ולכן קיבלנו את כל הדרישות. אם $A = 0$, פשוט בוחרים $B = C = 0$.

לקריאה נוספת

להצגה אלגוריתמית מפורטת של ההוכחה, ראו את הסקירה של דוסון ונילסן:

C. M. Dawson and M. A. Nielsen, The Solovay–Kitaev algorithm.

לשיפור של המעריך במקרה הכללי, ראו:

G. Kuperberg, Breaking the cubic barrier in the Solovay–Kitaev algorithm.