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, תהי P הטלה אורתוגונלית המתארת אירוע במדידה הסופית, ונסמן את שני מצבי הפלט ב־ $\left|\widetilde{\psi}\right\rangle, |\psi\rangle$. נרצה לחסום את ההפרש בין ההסתברויות של האירוע בשני המצבים. נסמן את וקטור ההפרש ב־

$$|e\rangle = |\psi\rangle - \left|\widetilde{\psi}\right\rangle .$$

נוסיף ונחסיר את האיבר $\left\langle\widetilde{\psi}\right| P |\psi\rangle$, ונקבל

$$\begin{aligned}
\left|\langle\psi| P |\psi\rangle - \left\langle\widetilde{\psi}\right| P \left|\widetilde{\psi}\right\rangle\right| &= \left|\langle e| P |\psi\rangle + \left\langle\widetilde{\psi}\right| P |e\rangle\right| \\
&\leq |\langle e| P |\psi\rangle| + \left|\left\langle\widetilde{\psi}\right| P |e\rangle\right| \\
&\leq \| |e\rangle \| \|P |\psi\rangle \| + \| \left|\widetilde{\psi}\right\rangle \| \|P |e\rangle \| \\
&\leq 2\| |e\rangle \| \\
&\leq 2L\eta.
\end{aligned}$$

אי־השוויון הראשון הוא אי־שוויון המשולש, והשני הוא קושי--שוורץ. בשלישי השתמשנו בכך ששני מצבי הפלט מנורמלים ושהטלה אורתוגונלית אינה מגדילה נורמה: $\| |v\rangle \| \leq \| P |v\rangle \|$. לבסוף השתמשנו בחסם על המרחק בין מצבי הפלט שהוכחנו לעיל.

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

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.

הוכחת הטענה הזו דורשת לא מעט עבודה טכנית. לא נפרט אותה בקורס: הפרטים הטכניים אינם מוסיפים הרבה תובנה לצורך הדיון שלנו, ונעדיף להתמקד ברעיונות שמאחורי משפט סולובייב--קיטאייב, שהוא הנושא המרכזי ביחידה הזו. הרעיון הוא לפרק מטריצה יוניטרית כללית למכפלה של פעולות, שכל אחת מהן פועלת רק על שני וקטורים מהבסיס הסטנדרטי ומשאירה את האחרים ללא שינוי. לאחר מכן ממשים כל פעולה כזו באמצעות שערים מבוקרים, ומפרקים גם אותם לשערים על קיוביט יחיד ולשערי CNOT. הבנייה נותנת מימוש מדויק, אך מספר השערים הדרוש למימוש שער כללי על n קיוביטים אינו בהכרח פולינומי ב־ n.

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.

אוניברסליות בקירוב מבטיחה שלכל שער רצוי ולכל שגיאה מותרת $\varepsilon > 0$ קיים רצף של שערי בסיס שמקרב אותו עד כדי שגיאה זו. אבל מה קורה לאורך הרצף כשמקטינים את השגיאה המותרת? נניח, למשל, שנרצה שגיאה לכל היותר 2^{-k}. האם ייתכן שנזדקק למספר שערים מעריכי ב־ k, או שתמיד יספיק מספר שערים פולינומי ב־ k? משפט סולוביי--קיטאייב מראה שבתנאים שנפרט מיד, מספר פולינומי אכן מספיק.

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 $V \in SU(d)$ (למה?). לצורך קירוב מעגל אפשר להזניח את הפאזה הגלובלית.

נקבע אוסף סופי של שערי בסיס $\mathcal{G} \subseteq SU(d)$. לרצף סופי של שערים מתוך $\mathcal{G}$ נקרא *מילה*. אם המילה w מורכבת מן השערים $G_1, \dots, G_m$ לפי סדר הפעלתם, אז אורכה הוא מספר השערים ברצף, ונסמן $|w| = m$. המטריצה שהמילה מייצגת היא המכפלה $G_m \cdots G_1$. נשתמש באותו סימון למילה ולמטריצה שהיא מייצגת. למשל, אם נקרב שער U באמצעות מילה $\widetilde{U}$, אז $|\widetilde{U}|$ הוא אורך המילה, ואילו $\|U - \widetilde{U}\|$ היא שגיאת הקירוב בנורמת האופרטור.

כשאומרים שהמילים מעל $\mathcal{G}$ *צפופות* ב־ $SU(d)$, הכוונה היא שלכל שער $U \in SU(d)$ ולכל שגיאה מותרת $\varepsilon > 0$ קיימת מילה $\widetilde{U}$ המקיימת $\|U - \widetilde{U}\| < \varepsilon$. הצפיפות מבטיחה שקיימת מילה כזו, אך אינה נותנת חסם על אורכה. זה מה שנותן המשפט הבא.

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־*

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

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.

4 ההוכחה: מקירוב גס לקירוב מדויק

נתחיל משאלה מעט שונה: נניח שאנחנו כבר יודעים לקרב *כל* שער עד כדי שגיאה ε, במילה באורך לכל היותר ℓ. איך נשתמש ביכולת הזו כדי להשיג דיוק טוב יותר? נראה שמספיק לשפר את השגיאה ל־ $K\varepsilon^{3/2}$ במחיר של חמש מילים ישנות. אז נוכל להפעיל את אותה בנייה שוב, הפעם עם המילים המשופרות.

4.1 נקודת ההתחלה

נבחר דיוק התחלתי קבוע $\varepsilon_0 > 0$, קטן מספיק כפי שיתברר בהמשך. נכין טבלה סופית שמכילה קירוב לכל שער בדיוק הזה. מדוע די בטבלה סופית אף שיש אינסוף שערים? כל חלק ממשי או מדומה של כניסה במטריצה יוניטרית שייך לקטע $[-1, 1]$. נחלק את הקטע למספר סופי של קטעים קטנים ונמיין את המטריצות לפי הקטעים שאליהם נופלות הכניסות שלהן. מאחר שהממד קבוע, אפשר לבחור את הקטעים קטנים מספיק כדי שכל שתי מטריצות באותו תא יהיו במרחק קטן מ־ $\varepsilon_0/2$ בנורמת האופרטור.

נחשוב על כל מטריצה ב־ $SU(d)$ כעל נקודה בקובייה $[-1, 1]^{2d^2}$: לכל אחת מכניסות המטריצה יש שתי קואורדינטות, החלק הממשי והחלק המדומה. נחלק כל ציר לקטעים קצרים. בכך חילקנו את הקובייה למספר סופי של קופסאות קטנות. שתי מטריצות נמצאות באותה קופסה אם בכל קואורדינטה הערכים שלהן שייכים לאותו קטע. נבחר את הקטעים קצרים מספיק כך שהמרחק בנורמת האופרטור בין כל שתי מטריצות באותה קופסה יהיה לכל היותר $\varepsilon_0/2$.

חלוקת הקובייה לקופסאות מחלקת גם את השערים ב־ $SU(d)$ לקבוצות: שני שערים שייכים לאותה קבוצה אם הנקודות המייצגות אותם נמצאות באותה קופסה. מספר הקבוצות סופי, כי מספר הקופסאות סופי. בכל קבוצה נבחר אחד מהשערים שבה ונקרא לו *נציג הקבוצה*.

לפי הנחת הצפיפות, לכל נציג יש מילה מעל $\mathcal{G}$ שמקרבת אותו עד כדי שגיאה $\varepsilon_0/2$. נשמור בטבלה מילה אחת כזו לכל נציג. כעת, בהינתן שער שאותו נרצה לקרב, נשתמש במילה ששמרנו עבור הקבוצה שלו. המרחק מהשער לנציג הוא לכל היותר $\varepsilon_0/2$, כי שניהם באותה קופסה. גם המרחק מהנציג למילה ששמרנו הוא לכל היותר $\varepsilon_0/2$, ולכן המילה מקרבת את השער עד כדי שגיאה ε_0.

4.2 מה נשאר לתקן?

נניח שכבר מצאנו קירוב $\widetilde{U}$ לשער הרצוי U, וש־ $\|U-\widetilde{U}\| \leq \varepsilon$. אנחנו רוצים לשפר את הקירוב שכבר בנינו. השגיאה נתונה לנו בצורה חיבורית, באמצעות ההפרש $U-\widetilde{U}$, אבל כשמוסיפים שער למעגל, הפעולה המתאימה על המטריצות היא כפל. לכן נשאל: איזה שער היינו רוצים להפעיל אחרי $\widetilde{U}$ כדי לקבל בדיוק את U?

נסמן את השער המבוקש ב־ Δ. הדרישה היא

$$\Delta\widetilde{U} = U,$$

ומכאן, בכפל מימין בהופכי של $\widetilde{U}$, נקבל את *שער התיקון*:

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

מה הרווחנו מהמעבר הזה? אם הקירוב היה מדויק, לא היה צורך לתקן דבר, ושער התיקון היה הזהות. לכן טבעי לצפות שאם השגיאה קטנה, שער התיקון יהיה קרוב לזהות. ואכן,

$$\begin{aligned}\|\Delta - I\| &= \|U\widetilde{U}^{-1} - \widetilde{U}\widetilde{U}^{-1}\| \\ &= \|(U-\widetilde{U})\widetilde{U}^{-1}\| \\ &= \|U-\widetilde{U}\| \\ &\leq \varepsilon.\end{aligned}$$

השוויון האחרון נובע מכך שהמטריצה $\widetilde{U}^{-1}$ יוניטרית, וכפל מימין במטריצה יוניטרית שומר על נורמת האופרטור. אי־השוויון הוא הנחת הקירוב.

נניח שמצאנו מילה D המקרבת את שער התיקון Δ. אם נפעיל אותה אחרי המעגל שכבר בנינו, נקבל את הקירוב החדש $D\widetilde{U}$. עד כמה הוא טוב? מכיוון ש־ $U = \Delta\widetilde{U}$, מתקיים

$$\|U - D\widetilde{U}\| = \|(\Delta - D)\widetilde{U}\| = \|\Delta - D\|,$$

כאשר השוויון האחרון נובע מכך שכפל מימין במטריצה יוניטרית שומר על נורמת האופרטור. כלומר, השגיאה בקירוב שער התיקון היא בדיוק השגיאה שתישאר במעגל כולו.

כאן מתעורר הקושי: בשלב הנוכחי אנחנו יודעים לקרב כל שער עד כדי שגיאה ε. אם נפעיל את הבנייה הזו ישירות על Δ, נקבל שוב את אותו חסם על השגיאה. למעשה, את הדיוק הזה כבר משיגה מילת הזהות, שהרי $\|\Delta - I\| \leq \varepsilon$. כדי להבטיח שיפור נצטרך לנצל את העובדה ששער התיקון קרוב לזהות.

אסטרטגיית ההוכחה. נחפש תחילה קירוב לשער התיקון בעל מבנה מתמטי מתאים, ורק אחר כך נעבור למימוש באמצעות שערי הבסיס. לשם כך נשתמש בביטוי

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

הנקרא *קומוטטור חבורתי*, כאשר $V, W \in SU(d)$ הן מטריצות יוניטריות כלליות. בשלב זה איננו דורשים שיהיו שייכות לאוסף שערי הבסיס, או שיהיה להן מימוש מדויק כמילים מעליו. ההוכחה תיעשה בשני צעדים:

- **קירוב התיקון באמצעות קומוטטור.** נבחר שתי מטריצות יוניטריות $V, W \in SU(d)$, שכל אחת מהן נמצאת במרחק $O(\sqrt{\varepsilon})$ מהזהות, כך ש־

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

  זהו צעד העוסק במטריצות בלבד, ללא שימוש באוסף שערי הבסיס. הוא מראה שאת התיקון הדרוש אפשר לקרב באמצעות ביטוי מהצורה המיוחדת הזו, עם שני גורמים קרובים לזהות.

- **ניצול המבנה כדי לעבור למילים מעל שערי הבסיס.** כעת נשתמש ביכולת הקירוב שכבר בנינו כדי למצוא מילים $\widetilde{V}, \widetilde{W}$ המקרבות את המטריצות V, W עד כדי שגיאה ε. נרכיב מהן את המילה

$$\widetilde{V}\widetilde{W}\widetilde{V}^{-1}\widetilde{W}^{-1},$$

  כאשר ההופכיים הם ההופכיים המדויקים של אותן מילים. בזכות מבנה הקומוטטור והקרבה של V, W לזהות, נראה שהמילה הזו עדיין מקרבת את Δ עד כדי שגיאה $O(\varepsilon^{3/2})$. זו ההפתעה המרכזית: אף שהמטריצות מוחלפות בקירובים ששגיאתם עלולה להיות מסדר ε, שגיאת התיקון כולו נשארת מסדר $\varepsilon^{3/2}$. לפי החסם על הצטברות שגיאות שהוכחנו בתחילת היחידה, החלפת ארבעת הגורמים בקירובים הייתה נותנת חסם של 4ε על השינוי בקומוטטור. (גם שגיאת הקירוב של כל גורם הפוך היא לכל היותר ε, שכן עבור מטריצות יוניטריות מתקיים $\|V^{-1} - \widetilde{V}^{-1}\| = \|V - \widetilde{V}\|$, ובדומה עבור W.) לחסם על השינוי בקומוטטור יש להוסיף את שגיאת הקירוב מהצעד הראשון. החסם הזה אינו מספיק כדי להבטיח שיפור; המבנה שמצאנו בצעד הראשון הוא שמאפשר לשמר שגיאה כוללת מסדר $\varepsilon^{3/2}$.

לבסוף נפעיל את מילת התיקון אחרי הקירוב $\widetilde{U}$ שכבר בנינו, ונקבל את המילה הכוללת

$$\widetilde{V}\widetilde{W}\widetilde{V}^{-1}\widetilde{W}^{-1}\widetilde{U}.$$

זהו בדיוק השרשור של חמש מילים מהרמה הקודמת שעליו דיברנו בתחילת ההוכחה. אם כל אחת מהמילים $\widetilde{U}, \widetilde{V}, \widetilde{W}$ היא באורך לכל היותר ℓ, אז גם המילים ההופכיות הן באורך לכל היותר ℓ, ולכן אורך המילה החדשה הוא לכל היותר 5ℓ. כך נשתמש ביכולת הקירוב הישנה כדי לקבל קירוב מדויק יותר.

4.3 בחירת שני השערים המתקנים

למה 4.1. *יהי $\Delta \in SU(d)$ שער המקיים*

$$\|\Delta - I\| \le \varepsilon, \qquad 0 < \varepsilon \le \frac{1}{d}.$$

אז קיימת מטריצה הרמיטית חסרת עקבה A כך ש־

$$\Delta = e^{iA}, \qquad \|A\| \le \frac{\pi}{2}\varepsilon.$$

הוכחה. מכיוון ש־Δ יוניטרית, אפשר ללכסן אותה באמצעות מטריצה יוניטרית Q ולכתוב

$$\Delta = Q\,\mathrm{diag}(e^{i\theta_1}, \dots, e^{i\theta_d})Q^\dagger,$$

כאשר לכל ערך עצמי בחרנו את הזווית $\theta_j \in (-\pi, \pi]$. נגדיר

$$A = Q\,\mathrm{diag}(\theta_1, \dots, \theta_d)Q^\dagger.$$

הזוויות ממשיות, ולכן A הרמיטית, ולפי הבנייה $e^{iA} = \Delta$. נותר לחסום את הנורמה שלה ולבדוק שעקבתה אפס. ראשית, באותו בסיס שבו לכסנו את Δ, המטריצה $\Delta - I$ אלכסונית אף היא. לכן

$$\max_j |e^{i\theta_j} - 1| = \|\Delta - I\| \le \varepsilon.$$

כדי לעבור מחסם על המרחק לחסם על הזווית, נשים לב שלכל j מתקיים

$$|e^{i\theta_j} - 1| = 2\sin\left(\frac{|\theta_j|}{2}\right) \ge \frac{2}{\pi}|\theta_j|,$$

כאשר השתמשנו באי־השוויון $\sin t \ge 2t/\pi$ עבור $0 \le t \le \pi/2$. מכאן

$$\|A\| = \max_j |\theta_j| \le \frac{\pi}{2}\varepsilon.$$

כעת נבדוק את העקבה. מכיוון ש־ $\det \Delta = 1$, מתקיים

$$e^{i\sum_{j=1}^{d}\theta_j} = \prod_{j=1}^{d} e^{i\theta_j} = 1.$$

מכאן שסכום הזוויות הוא כפולה של 2π. כדי להסיק שהסכום הוא אפס, נשתמש בהנחה $\varepsilon \le 1/d$:

$$\left|\sum_{j=1}^{d}\theta_j\right| \le \sum_{j=1}^{d}|\theta_j| \le \frac{\pi}{2}d\varepsilon \le \frac{\pi}{2}.$$

הכפולה היחידה של 2π בתחום הזה היא אפס, ולכן

$$\operatorname{tr} A = \sum_{j=1}^{d}\theta_j = 0.$$

□

בבחירת הדיוק ההתחלתי נדרוש אפוא גם $\varepsilon_0 \le 1/d$. מכיוון שהשגיאה רק קטנה מרמה לרמה, נוכל להפעיל את הלמה בכל שלב של הרקורסיה.

כעת נשתמש בעובדה הבאה, שהוכחתה מופיעה בסוף היחידה.

למה 4.2 (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.

מספר הערות לפני שנמשיך: מדוע היה חשוב להראות שהעקבה של A היא אפס? אנחנו רוצים למצוא מטריצות B, C המקיימות $[B, C] = -iA$. אבל העקבה של כל קומוטטור היא אפס, שכן

$$\operatorname{tr}[B, C] = \operatorname{tr}(BC) - \operatorname{tr}(CB) = 0.$$

לכן, אם העקבה של A אינה אפס, למשוואה הזו אין פתרון.

מה הקשר לפאזה גלובלית? כל מטריצה הרמיטית A ניתנת לכתיבה בצורה

$$A = A_0 + \alpha I, \qquad \alpha = \frac{\operatorname{tr} A}{d}, \qquad \operatorname{tr} A_0 = 0.$$

מכיוון שמטריצת הזהות מתחלפת עם A_0, נקבל

$$e^{iA} = e^{i\alpha} e^{iA_0}.$$

כלומר, האיבר αI תורם לשער רק פאזה גלובלית. זו הסיבה שבחרנו מלכתחילה לעבוד ב־ $SU(d)$: לאחר שמפרידים את הפאזה הגלובלית, הלמה הקודמת מבטיחה שלשער התיקון הקרוב לזהות יש ייצוג $\Delta = e^{iA}$ עם $\operatorname{tr} A = 0$, כפי שנדרש בבניית הקומוטטור.

אפשר לראות את אותה מגבלה גם ישירות במכפלת השערים:

$$\det(VWV^{-1}W^{-1}) = \det(V)\det(W)\det(V)^{-1}\det(W)^{-1} = 1.$$

לכן כל תיקון שנבנה כקומוטטור חבורתי שייך בהכרח ל־ $SU(d)$.

נחזור לשער התיקון $\Delta = e^{iA}$. לפי הלמה, מצאנו מטריצות הרמיטיות חסרות עקבה B, C המקיימות

$$[B, C] = -iA, \qquad \|B\|, \|C\| = O(\sqrt{\varepsilon}).$$

כעת נגדיר שני שערים

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

ונראה שהקומוטטור החבורתי שלהם מקרב את Δ עד כדי שגיאה $O(\varepsilon^{3/2})$.

ראשית, נשים לב שגם V, W שייכים ל־ $SU(d)$: האקספוננטים יוניטריים משום ש־ B, C הרמיטיות, והדטרמיננטה שלהם היא אחת משום שהעקבות של B, C הן אפס. נסמן

$$r = \max\{\|B\|, \|C\|\}.$$

מפיתוח האקספוננט נקבל $V = I + iB + O(r^2)$ ובדומה עבור W. לכן שני השערים נמצאים במרחק $O(r) = O(\sqrt{\varepsilon})$ מהזהות.

כעת נחשב עד כמה הקומוטטור שלהם שונה מהזהות. לשם כך נשים לב לזהות

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

אכן, האיבר הראשון באגף ימין נותן את הקומוטטור, והשני נותן את הזהות. לכן נתחיל מהשוואה בין שתי המכפלות VW ו־ WV.

נפתח את האקספוננטים עד סדר שני:

$$e^{iB} = I + iB - \tfrac{1}{2}B^2 + O(r^3), \qquad e^{iC} = I + iC - \tfrac{1}{2}C^2 + O(r^3).$$

בכפל לפי שני הסדרים מתקבל

$$VW = I + i(B+C) - \tfrac{1}{2}(B^2+C^2) - BC + O(r^3),$$
$$WV = I + i(B+C) - \tfrac{1}{2}(B^2+C^2) - CB + O(r^3).$$

כאן רואים מדוע פיתחנו עד סדר שני: בסדר הראשון שתי המכפלות זהות. בסדר השני מופיע לראשונה איבר שתלוי בסדר הכפל: במכפלה הראשונה זהו $(iB)(iC) = -BC$, ובשנייה זהו $(iC)(iB) = -CB$. לכן, בחיסור נקבל

$$VW - WV = CB - BC + O(r^3) = -[B,C] + O(r^3).$$

נותר לכפול מימין ב־ $V^{-1}W^{-1}$. שני ההופכיים קרובים לזהות עד כדי $O(r)$, ולכן גם מכפלתם היא $I + O(r)$. מאחר ש־ $\|[B,C]\| \le 2\|B\|\|C\| \le 2r^2$, הכפל הזה משנה את התוצאה רק בסדר שלישי:

$$\mathcal{C}(V,W) - I = (-[B,C] + O(r^3))(I + O(r)) = -[B,C] + O(r^3).$$

עכשיו נשתמש בבחירה של B, C. בחרנו אותם כך ש־ $-[B,C] = iA$, ולכן

$$\mathcal{C}(V,W) = I + iA + O(r^3).$$

נשווה זאת לשער התיקון שאותו רצינו לממש:

$$\Delta = e^{iA} = I + iA + O(\|A\|^2).$$

בשני הפיתוחים קיבלנו אותו איבר $I + iA$, ולכן נותר לחסום רק את השאריות. מכיוון ש־ $r = O(\sqrt{\varepsilon})$ ו־ $\|A\| = O(\varepsilon)$, נקבל

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

בכך השלמנו את הצעד הראשון: מצאנו שני שערים קרובים לזהות שהקומוטטור שלהם נותן את התיקון בדיוק המשופר. אלא שבינתיים V, W הם שערים שבחרנו מתמטית; עדיין אין לנו מילים מעל אוסף שערי הבסיס שממממשות אותם בדיוק. בצעד הבא נראה שדי לקרב כל אחד מהם בדיוק הישן ε כדי לשמור על הדיוק המשופר של הקומוטטור.

5 למה שגיאות הקירוב אינן הורסות את התיקון?

בצעד הראשון בחרנו את V, W כך שהקומוטטור שלהם מקרב את שער התיקון ברמת הדיוק החדשה. כעת נפעיל על כל אחד מהם את אלגוריתם הקירוב ברמה הישנה. נקבל שתי מילים המקיימות

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

חסם טלסקופי רגיל על ארבעת הגורמים היה נותן רק שגיאה $O(\varepsilon)$. חסם כזה אינו מבטיח שום שיפור: הוא מתייחס לארבע שגיאות כאילו נבחרו בנפרד. אבל החסם הזה מפספס את המבנה: כל שער מופיע יחד עם ההופכי *של אותו שער*, ושני השערים קרובים לזהות.

נחליף תחילה רק את V ונשאיר את W קבוע. מה יקרה אם $W = I$? במקרה הזה שתי המכפלות שוות בדיוק לזהות, תהיה השגיאה בקירוב הראשון אשר תהיה. לכן כדאי להפריד את תרומת הזהות מתוך W עוד לפני שלוקחים חסם על הנורמה. לכל מטריצות יוניטריות,

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

בשורה הראשונה השמטנו גורם יוניטרי משותף מימין. כדי לראות את אי־השוויון האחרון, נסמן $E = W - I$ ונוסיף ונחסיר את $\widetilde{V}EV^\dagger$:

$$VEV^\dagger - \widetilde{V}E\widetilde{V}^\dagger = (V - \widetilde{V})EV^\dagger + \widetilde{V}E(V^\dagger - \widetilde{V}^\dagger).$$

מתת־כפליות ומכך שלקיחת צמוד הרמיטי שומרת על הנורמה, כל אחד משני האיברים חסום בנורמה על ידי $\|V - \widetilde{V}\|\,\|E\|$. זהו הרווח שחיפשנו: השגיאה בקירוב השער הראשון מוכפלת במרחק של השער השני מהזהות.

באופן דומה, באמצעות הכתיבה

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

מקבלים

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

כאן

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

נעבור אפוא מהקומוטטור המקורי לקומוטטור של שתי המילים דרך קומוטטור הביניים $\mathcal{C}(\widetilde{V}, W)$. לפי אי־שוויון המשולש, השגיאה הכוללת חסומה בסכום שתי שגיאות ההחלפה שחישבנו. בשתיהן מופיעה מכפלה של שגיאה בגודל לכל היותר ε במרחק מהזהות בגודל $O(\sqrt{\varepsilon})$. לכן

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

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

5.1 צעד השיפור

כעת יש לנו מילה עבור התיקון. נזכור שהמטרה המקורית הייתה לקרב את $U = \Delta\widetilde{U}$, ולכן נפעיל קודם את הקירוב הישן ואחריו את התיקון. בסימון של מכפלת מטריצות סדר זה נותן

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

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.

6 מהשיפור המקומי למשפט

נסמן ב־ ε_k את חסם השגיאה ברמה k, וב־ ℓ_k את חסם אורך המילים. ברמה אפס משתמשים בטבלה הסופית שהכנו מראש. הטענה האינדוקטיבית היא שכל שער בממד הנתון ניתן לקירוב ברמה k, ולכן מותר להפעיל את הבנייה של אותה רמה גם על שני השערים המתקנים. צעד השיפור שהוכחנו נותן

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

נבחר מראש ε_0 כך שיתקיימו כל הדרישות עד כה, ובפרט $\varepsilon_0 \le 1/d$ עבור הלמה על הלוגריתם של שער התיקון. נדרוש גם ש־ $K^2\varepsilon_0 < 1$. אם נסמן $q_k = K^2\varepsilon_k$, אז $q_0 < 1$, והבחירה בגורם הנרמול מבטלת את הקבוע ברקורסיה:

$$K^2\varepsilon_{k+1} = K^3\varepsilon_k^{3/2} = (K^2\varepsilon_k)^{3/2}.$$

מכאן

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

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

נבחר את הרמה הראשונה שבה $\varepsilon_k \le \varepsilon$. כדי למצוא אותה ניקח לוגריתם בזהות עבור q_k:

$$\log(1/q_k) = (3/2)^k \log(1/q_0).$$

לכן, עבור דיוק יעד קטן מספיק, דרושה הרמה הראשונה שבה אגף ימין מגיע ל־ $\log(1/(K^2\varepsilon))$. מאחר שהדיוק ההתחלתי קבוע, מתקבל

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

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.

7 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. לפי החסם הטלסקופי מתחילת היחידה, סכום השגיאות של כל ההחלפות הוא לכל היותר $L \cdot (\delta/L) = \delta$. מכיוון שמספר הקיוביטים שעליהם פועל כל שער קבוע, גם הממד שבו מפעילים את המשפט קבוע. משפט סולוביי--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, והוא אינו מיטבי. קיימים שיפורים כלליים, ועבור אוספי שערים מיוחדים גם בניות קצרות יותר. לא נזדקק להם כאן.

8 אחרי ההוכחה: איך מגיעים לקומוטטור?

בהוכחה עברנו מתיאור חיבורי של השגיאה לתיקון כפלי: השווינו בין שני שערים על ידי הכפלת האחד בהופכי של האחר. כעת נשאל איך אפשר היה לנחש באילו שני שערים כדאי להשתמש כדי לקבל תיקון שקרוב במיוחד לזהות. אם נשווה שער לעצמו, נקבל את הזהות בדיוק. מה שנחוץ לנו הוא זוג שערים שמסכימים בסדר הראשון, אבל ההבדל ביניהם בסדר השני ניתן לבחירה.

ננסה להשוות שתי דרכים להשתמש באותם שני שערים: פעם בסדר VW ופעם בסדר WV. כדי למדוד את ההבדל ביניהן נכפול את הראשונה בהופכית של השנייה, בדיוק כפי שהגדרנו קודם את שער התיקון. נקבל

$$(VW)(WV)^{-1} = VWV^{-1}W^{-1}.$$

עכשיו ברור מדוע חוזרים בסדר הזה: אילו חזרנו בדיוק על עקבותינו, היינו מקבלים את הזהות לכל בחירה של השערים. כאן נשאר הבדל אם השערים אינם מתחלפים.

מה גודל ההבדל? נכתוב $V = e^{tX}$ ו־ $W = e^{tY}$, כאשר X, Y אנטי־הרמיטיות. לשתי הדרכים יש אותו איבר ליניארי, $t(X+Y)$, אבל באחת מופיע בסדר השני t^2XY ובשנייה t^2YX. לכן החישוב מההוכחה נותן

$$\mathcal{C}(e^{tX}, e^{tY}) = I + t^2[X, Y] + O(t^3).$$

כדי לקבל תיקון בגודל ε נבחר אפוא צעדים בגודל $t = \sqrt{\varepsilon}$. הלמה על הקומוטטור המאוזן הבטיחה שנוכל לבחור גם את *כיוון* התיקון. כעת רואים את המקור של המעריך: לאחר שהתאמנו את האיבר הריבועי, השארית הראשונה היא מסדר $t^3 = \varepsilon^{3/2}$.

8.1 הקשר לאלגבראות לי

לחישוב הזה יש שם ופירוש גאומטרי. 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 $U'(0)^\dagger + U'(0) = 0$. כדי לראות מה מוסיף תנאי הדטרמיננטה, נכתוב $U(t) = I + tX + O(t^2)$ עבור מסלול חלק בעל נגזרת X באפס. בפיתוח הדטרמיננטה, האיברים מסדר ראשון מתקבלים מבחירת איבר אלכסוני יחיד מתוך tX ואיברי זהות בכל יתר המקומות. לכן

$$\det U(t) = 1 + t \operatorname{tr} X + O(t^2).$$

אם הדטרמיננטה נשארת אחת לאורך המסלול, המקדם הליניארי חייב להתאפס.

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 ולמת הקומוטטור המאוזן נתנו לנו את כל מה שנדרש.

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.

8.2 דוגמה: מסיבובים בשני כיוונים לסיבוב בכיוון שלישי

בסעיף זה האותיות X, Y, Z מציינות את מטריצות פאולי ההרמיטיות; היוצרים האנטי־הרמיטיים של הסיבובים הם המטריצות הללו כפול i. 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 $O(a^{3/2})$.

השלמה: הוכחת למת הקומוטטור המאוזן

הדוגמה עם מטריצות פאולי כבר מסבירה את הרעיון עבור קיוביט יחיד. בממד כללי נשתמש ברעיון אחר: אם אחת משתי המטריצות אלכסונית, קל מאוד לחשב את הקומוטטור שלה עם המטריצה השנייה. הקושי היחיד הוא שבבסיס הזה אלכסון הקומוטטור בהכרח מתאפס. לכן נתחיל מבחירת בסיס שבו גם למטריצת המטרה יש אלכסון אפס.

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

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

מקיימת

$$A'_{jj} = \sum_{k=1}^{d} |F_{kj}|^2 a_k = \frac{1}{d}\sum_{k=1}^{d} a_k = 0.$$

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.

נותר לבחור את הגדלים של שני הגורמים. אם נכפול גורם אחד בסקלר ואת השני בהופכי שלו, הקומוטטור לא ישתנה. כדי ששניהם יהיו בגודל מסדר שורש של נורמת המטרה, 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,

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

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

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

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

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.