

היכרות ראשונה עם קיוביטים**1 הקיוביט**

בִּיט, bit, הוא יחידת המידע הבסיסית בחישוב הקלאסי: אובייקט שערכו אחד משני הערכים 0 או 1. אפשר להפעיל פעולות לוגיות על ביט או על כמה ביטים יחד. ברוב ההקשרים במדעי המחשב אנחנו מתייחסים לביט כאל אובייקט מתמטי מופשט; שאלת המימוש הפיזיקלי שלו נדונה בקורסים אחרים. כל עוד אנחנו עוסקים באלגוריתמים ובמבני נתונים, נוח לנו להשאיר אותה ברקע.

המקבילה הקוונטית לביט היא הקיוביט, qubit. גם כאן נתייחס לאובייקט מתמטי מופשט, אף ששאלת המימוש הפיזיקלי מרתקת במיוחד. חשוב לזכור שקיוביטים אינם רק המצאה של מתמטיקאים: אפשר לממש במעבדה מערכות המתנהגות, בקירוב טוב, בהתאם למודל שנציג. זה אולי נשמע מובן מאליו, אבל משנתחיל להכיר את האובייקט הזה, נראה שהוא מוזר למדי, עד שקל להעלות ספק בקיומו.

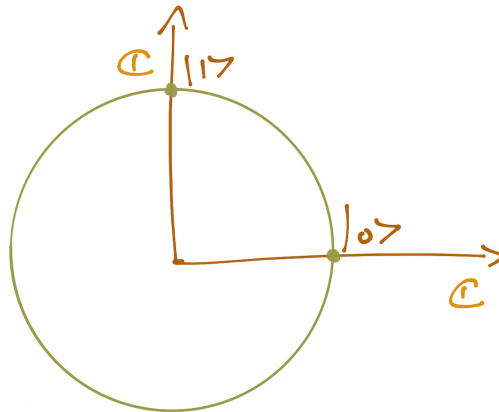
לביט יש שני מצבים אפשריים. גם עבור קיוביט נבחר שני מצבי בסיס, שנסמן $|0\rangle$ ו- $|1\rangle$. זהו סימון של דיראק; לעת עתה נתייחס אליו כסימון בלבד. ההבדל המהותי הוא שמצבי הבסיס אינם ממצים את כל המצבים האפשריים של קיוביט.

1.1 עיקרון הסופרפוזיציה

מצב של קיוביט יכול להיות סופרפוזיציה של שני מצבי הבסיס:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \alpha, \beta \in \mathbb{C}, \quad |\alpha|^2 + |\beta|^2 = 1.$$

כלומר, אנחנו מייצגים את המצב באמצעות וקטור יחידה במרחב $\mathbb{C}^2$. המקדמים α ו- β נקראים **אמפליטודות**, amplitudes. אלה מספרים מרוכבים, ולא הסתברויות; עוד מעט נראה כיצד הם קובעים את הסתברויות המדידה. ליתר דיוק, התיאור הזה הוא של **מצב טהור** של קיוביט. קיים גם מושג כללי יותר של מצב מעורב, שאליו לא נודק כרגע. בהמשך היחידה, כשנאמר "מצב" נתכוון למצב טהור, אלא אם נאמר אחרת.



המצבים $|0\rangle$ ו- $|1\rangle$ מהווים בסיס אורתונורמלי ביחס למכפלה הפנימית הסטנדרטית. הבסיס הזה נקרא הבסיס החישובי. מבחינה מתמטית אין בו משהו קדוש: אפשר לתאר את המצב בכל בסיס אורתונורמלי אחר. במימוש פיזיקלי מסוים, לעומת זאת, ייתכן שבסיס מסוים נוח יותר להכנה ולמדידה. אפשר כמובן לכתוב את אותו המצב בשפה המוכרת מאלגברה לינארית:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad |\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

הסימון $|\psi\rangle$ מציין וקטור, שאפשר לייצג כווקטור עמודה לאחר בחירת בסיס. מה שמופיע בתוך הסוגריים הוא שמו או התווית שלו; למשל, האפס שבסימון $|0\rangle$ אינו אומר שמדובר בווקטור האפס.

כל כך הרבה מידע בקיוביט?

התיאור הזה עלול להישמע בלתי סביר. שני מספרים מרוכבים? הרי התיאור המדויק שלהם עשוי לדרוש אינסוף ביטים. האם קיבלנו זיכרון בנפח אינסופי, ועוד בחלקיק בודד?

צריך להבחין בין המידע הדרוש לתיאור מצב לבין המידע שאפשר לקרוא ממנו. גם במודלים קלאסיים אנחנו משתמשים בגדלים רציפים, בלי להניח שאפשר להכין אותם או למדוד אותם בדיוק אינסופי ובעלות קבועה. במקרה הקוונטי יש מגבלה נוספת: אין מכשיר שמקבל קיוביט במצב לא ידוע ומדפיס את שתי האמפליטודות שלו. כדי להבין מה כן אפשר לעשות, צריך להכיר את כללי המדידה.

2 מדידה

באינטואיציה הקלאסית, מדידה אידאלית מגלה לנו תכונה של המערכת בלי לשנות אותה. במודל הקוונטי, פעולת המדידה כוללת שני מרכיבים: תוצאה קלאסית שאנחנו מקבלים, והמצב שבו המערכת נשארת לאחר קבלת התוצאה. שני המרכיבים חשובים, ובדרך כלל אי אפשר להתעלם מן השני.

המשמעות הפיזיקלית של המעבר הזה עוררה דיונים רבים, ופרשנויות שונות לתורת הקוונטים. לא נצטרך להכריע ביניהן כדי לתכנן אלגוריתמים. נשתמש בכללי החישוב המקובלים: התפתחות אוניטרית בין מדידות, וכלל הסתברותי המתאר את תוצאת המדידה ואת המצב המותנה בה. בפרט, יש בהחלט משמעות למצב הקוונטי לפני המדידה; הוא בדיוק מה שמאפשר לנו לחשב את ההסתברויות לתוצאותיה.

2.1 מדידה של קיוביט בבסיס החישובי

נניח שמצב הקיוביט הוא

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1.$$

מדידה בבסיס החישובי מחזירה אחת משתי תוצאות קלאסיות, 0 או 1. לפי כלל בורן, ההסתברויות הן

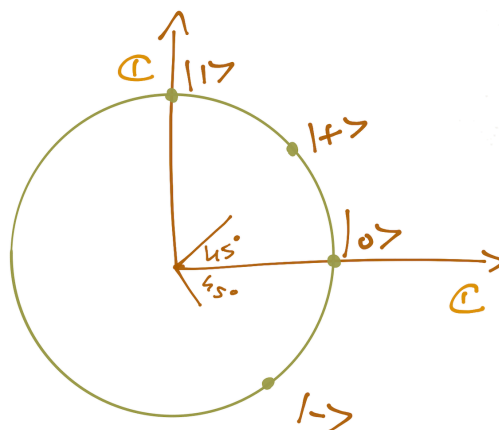
$$\text{Pr}[0] = |\alpha|^2, \quad \text{Pr}[1] = |\beta|^2.$$

במדידה האידיאלית שאנחנו מתארים, אם התקבלה התוצאה 0, מצב הקיוביט לאחר המדידה הוא $|0\rangle$; ואם התקבלה התוצאה 1, המצב הוא $|1\rangle$. לעדכון הזה מקובל לקרוא קריסת המצב. הנרמול שהטלנו על האמפליטודות מבטיח שסכום ההסתברויות הוא 1.

למשל, נגדיר את המצבים

$$|+\rangle \triangleq \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \quad |-\rangle \triangleq \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

מדידה של כל אחד מהם בבסיס החישובי מחזירה 0 או 1 בהסתברויות שוות.



האם סימן המינוס לא משנה דבר? הוא בהחלט משנה, אבל המדידה המסוימת הזו אינה חושפת את ההבדל. המצבים $|+\rangle$ ו- $|-\rangle$ הם שני מצבים שונים, ולמעשה הם אורתוגונליים. נראה מיד שמדידה בבסיס אחר מבחינה ביניהם בוודאות.

2.2 נוטציית דיראק

לפני שנגדיר מדידה בבסיס כללי, נכיר עוד מעט מן הסימון. הווקטור $|\psi\rangle$ נקרא ket, ומצמידים לו את וקטור השורה $\langle\psi|$, הנקרא bra. פורמלית,

$$\langle\psi| \triangleq (|\psi\rangle)^\dagger,$$

כאשר הסימן † מציין שחלוף והצמדה מרוכבת. כלומר,

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \implies \langle\psi| = (\alpha^* \quad \beta^*).$$

המכפלה של וקטור השורה $\langle u|$ בווקטור העמודה $|\psi\rangle$ היא המכפלה הפנימית שלהם. בנוטציית דיראק ממזגים את שני הקווים האנכיים וכותבים

$$\langle u|\psi\rangle \triangleq \langle u|\psi\rangle.$$

במוסכמה הזו המכפלה הפנימית צמודה-לינארית בארגומנט הראשון ולינארית בשני. בפרט,

$$\langle\psi|\psi\rangle = |\alpha|^2 + |\beta|^2 = 1.$$

השמות bra ו- ket נלקחו משני חלקיה של המילה bracket. גם לפיזיקאים מותר לשחק קצת עם מילים.

2.3 מדידה בבסיס אורתונורמלי כללי

נבחר בסיס אורתונורמלי $\{|u\rangle, |v\rangle\}$ של $\mathbb{C}^2$. אפשר לכתוב באופן יחיד

$$|\psi\rangle = a|u\rangle + b|v\rangle, \quad a = \langle u|\psi\rangle, \quad b = \langle v|\psi\rangle.$$

מדידה בבסיס הזה מחזירה אחת משתי תוויות קלאסיות, u או v , בהסתברויות

$$\Pr[u] = |a|^2 = |\langle u|\psi\rangle|^2, \quad \Pr[v] = |b|^2 = |\langle v|\psi\rangle|^2.$$

לאחר המדידה המצב הוא $|u\rangle$ או $|v\rangle$, בהתאם לתוצאה. מאורתונורמליות הבסיס ומנרמול המצב מתקבל $|a|^2 + |b|^2 = 1$, כך ששוב קיבלנו התפלגות הסתברות. התוויות הן שמות לתוצאות, לא תיאור מלא של וקטור שהמכשיר "מדפיס" לנו.

במודל האידאלי מותר למדוד בכל בסיס אורתונורמלי. בהמשך היחידה נראה כיצד שינוי בסיס מתאים מאפשר להסתפק במכשיר מדידה בבסיס החישובי. מדידות מן הסוג הזה נקראות מדידות פרויקטיביות בבסיס אורתונורמלי; יש מדידות קוונטיות כלליות יותר, אבל לא נודק להן כאן.

2.4 דוגמאות: מה המדידה מגלה ומה היא משנה?

נמדוד את המצב $|0\rangle$ בבסיס $\{|+\rangle, |-\rangle\}$. מאחר ש-

$$|0\rangle = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle,$$

נקבל

$$\text{Pr}[+] = |\langle +|0\rangle|^2 = \frac{1}{2}, \quad \text{Pr}[-] = |\langle -|0\rangle|^2 = \frac{1}{2}.$$

לאחר המדידה המצב הוא $|+\rangle$ או $|-\rangle$, בהתאם לתוצאה. לעומת זאת, אם הקלט הוא מלכתחילה אחד משני המצבים האלה, מדידה באותו בסיס מזהה אותו בוודאות. כך אפשר להבחין בין שני מצבים שמדידה בבסיס החישובי אינה מבחינה ביניהם.

נמשיך עוד צעד. אם נכין את המצב $|0\rangle$ ונמדוד פעמיים ברצף בבסיס החישובי, נקבל 0 בשתי המדידות בוודאות. אבל אם נכניס ביניהן מדידה בבסיס $\{|+\rangle, |-\rangle\}$, מדידת הבסיס החישובי שבסוף תחזיר 0 או 1 בהסתברויות שוות. זה נכון בכל אחת משתי התוצאות האפשריות של המדידה שבאמצע. זו דוגמה פשוטה לכך שמדידה אינה רק מגלה מידע: היא יכולה גם לשנות את המצב.

ומה אם ננסה ללמוד את האמפליטודות באמצעות מדידות חוזרות על אותו קיוביט? לאחר המדידה הראשונה כבר אין לנו, בדרך כלל, את המצב המקורי. אם נמדוד שוב באותו בסיס בלי לבצע פעולה נוספת, נקבל שוב את אותה תוצאה. כדי לאמוד מצב לא ידוע משתמשים בעותקים רבים שהוכנו באותו אופן, ומבצעים עליהם מדידות בבסיסים שונים. קיוביט יחיד אינו מספק לנו גישה חופשית לתיאור הרציף של מצבו.

2.5 פאזה גלובלית לעומת פאזה יחסית

יש דיוק חשוב בתיאור מצבים באמצעות וקטורי יחידה: שני וקטורים הנבדלים בכפל בסקלר מרוכב ממודולוס 1 מייצגים את אותו מצב פיזיקלי. כלומר, עבור $\theta \in \mathbb{R}$, הווקטורים $|\psi\rangle$ ו- $e^{i\theta}|\psi\rangle$ מייצגים אותו מצב. הגורם המשותף לכל האמפליטודות נקרא פאזה גלובלית. ואכן, לכל וקטור בסיס $|u\rangle$ מתקיים

$$|\langle u|e^{i\theta}|\psi\rangle|^2 = |e^{i\theta}\langle u|\psi\rangle|^2 = |\langle u|\psi\rangle|^2.$$

בהמשך נראה שגם פעולות אוניטריות אינן הופכות את ההבדל הזה להבדל מדידה.

לעומת זאת, פאזה יחסית בין האמפליטודות עשויה לשנות את המצב. למשל, המצבים $|+\rangle$ ו- $|-\rangle$ נבדלים בסימן של רכיב אחד בלבד, ואינם מתקבלים זה מזה באמצעות כפל כל הווקטור באותו סקלר. כבר ראינו שאפשר להבחין ביניהם בוודאות. בקיצור, סימן מינוס משותף לכל הווקטור אינו משנה את המצב; סימן מינוס על אחד הרכיבים עשוי לשנות אותו מאוד.

הערה לגבי נרמול. גורמי הנרמול מסרבלים לפעמים את הכתיבה, אבל צריך לזכור שהם חלק מן המצב כאשר מחשבים הסתברויות. אם נרצה לציין רק כיוון של וקטור, נוכל לכתוב למשל

$$|+\rangle \propto |0\rangle + |1\rangle.$$

הסימון מציין פרופורציונליות, ולא שוויון בין וקטורים. כאשר משתמשים בכלל בורן יש להחזיר את גורם הנרמול המתאים.

3 איך נראים קיוביטים במעבדה – טעימה קלה

לא נעמיק במימושים הפיזיקליים, אבל כדאי לראות שהמודל אינו תלוי בהתקן מסוים. הנה כמה דוגמאות:

- **אור – קיטוב של פוטון.** עבור פוטון המתקדם בכיוון נתון אפשר לבחור שני מצבי קיטוב מאונכים, למשל אופקי ואנכי, ולזהות אותם עם $|0\rangle$ ו- $|1\rangle$. רכיבים אופטיים מאפשרים להכין סופרפוזיציות של המצבים האלה ולשנות אותן. מפצל מתאים, בצירוף גלאים, מאפשר למדוד באיזה משני מצבי הבסיס התקבל הפוטון.
- **אלקטרון – ספין.** לאלקטרון יש תנע זוויתי פנימי הנקרא ספין. מדידת רכיב הספין בכיוון שנבחר נותנת אחת משתי תוצאות, המכונות לעתים "למעלה" ו"למטה". לא מדובר בכדור קטן שמסתובב סביב עצמו במובן הקלאסי. שתי התוצאות מתאימות לשני מצבי בסיס, ובאמצעות שליטה מתאימה אפשר להכין גם סופרפוזיציות שלהם.
- **אטום או יון – שתי רמות נבחרות.** לאטום יש רמות אנרגיה רבות, אבל אפשר לבחור שתיים מהן שישמשו כמצבי הבסיס של קיוביט. פולסים מתאימים מאפשרים להעביר אוכלוסייה בין הרמות וליצור סופרפוזיציות מבוקרות. למשל, פולס שעוצמתו, משכו והפאזה שלו נבחרו כראוי יכול להכין את המצב $|+\rangle$ מתוך $|0\rangle$. במימושים מסוימים קוראים את המצב באמצעות הארה שגורמת לפלואורסצנציה עבור אחד ממצבי הבסיס, אך לא עבור האחר.

בכל הדוגמאות אנחנו מזהים מרחב מצבים דו-ממדי, שולטים במצב בתוכו ומודדים בבסיס מתאים. המימושים שונים מאוד זה מזה; המתמטיקה שנשתמש בה לתיאור הקיוביט משותפת לכולם.

ומה עם חלקיק שיכול להיות בכל מקום?

תיאור קוונטי של מיקום חלקיק אכן עשיר יותר מתיאור של קיוביט. במקום שני רכיבים, מופיעה פונקציית גל על מרחב המיקומים האפשריים, והמסגרת המתמטית המתאימה היא מרחב הילברט אינסופי-ממדים. באופן גס, זהו מרחב מכפלה פנימית שגם מקיים תנאי של שלמות, כך שלתהליכי גבול מתאימים יש לאן להגיע. גם למדידה יש כאן עדיניות נוספת: מכשיר ממשי מודד מיקום ברזולוציה סופית, ולא מכין וקטור מנורמל שמרוכז בדיוק בנקודה אחת.

הבונוס שלנו כמדעני מחשב הוא שרבים מן הרעיונות המרכזיים בחישוב קוונטי כבר מופיעים במרחבים סופיים־ממדים. נוכל להכיר אותם בלי לשלם כרגע את מלוא המס המתמטי של אנליזה פונקציונלית ותורת המידה. אם כי באופן אישי, אני אוהב את המתמטיקה הזו, ובכלל.

4 הכללה של מושג הקיוביט

כמו שאפשר להכליל ביט ליחידת מידע בעלת יותר משני ערכים, אפשר להחליף את מרחב המצבים $\mathbb{C}^2$ במרחב $\mathbb{C}^d$. מערכת כזו נקראת qudit. המקרה $d = 3$ נקרא qutrit, ולו בסיס חישובי $\{|0\rangle, |1\rangle, |2\rangle\}$. מצב טהור כללי נכתב

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle, \quad |\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1.$$

במדידה בבסיס החישובי מתקבלות התוצאות 0, 1, 2 בהסתברויות $|\alpha|^2, |\beta|^2, |\gamma|^2$, בהתאמה, ולאחר המדידה המצב הוא וקטור הבסיס המתאים לתוצאה.

בחישוב קוונטי נעדיף בדרך כלל לעבוד עם קיוביטים ולהרכיב מהם מערכות גדולות. כמו ששני ביטים מאפשרים לייצג את ארבע המחרוזות 00, 01, 10, 11, למערכת של שני קיוביטים יש ארבעה מצבי בסיס חישוביים:

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle.$$

מצב טהור כללי של המערכת כולה נכתב

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle,$$

כאשר

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1.$$

במדידה של שני הקיוביטים בבסיס החישובי מתקבלת כל מחרוזת בהסתברות שהיא ריבוע המודולוס של האמפליטודה שלה, ולאחר המדידה המצב הוא וקטור הבסיס המתאים. זוהי רק הצצה להמשך: כדי להבין כיצד מצרפים מערכות נלמד על מכפלה טנזורית. בפרט, לא כל מצב של שני קיוביטים אפשר לתאר באמצעות בחירת מצב טהור נפרד לכל אחד מהם.

5 פעולות על קיוביטים

אם מגבילים את עצמנו לפעולות דטרמיניסטיות והפיכות על ביט קלאסי יחיד, יש רק שתי אפשרויות: להשאיר אותו כפי שהוא, או להפוך אותו באמצעות שער NOT. בעולם הקוונטי, אפילו קיוביט אחד מציע מבחר עשיר בהרבה.

נתחיל באנלוג הקוונטי של ההיפוך, שער פאולי X , המוגדר על מצבי הבסיס באמצעות

$$X|0\rangle = |1\rangle, \quad X|1\rangle = |0\rangle.$$

כאן נשתמש בהנחת יסוד של המודל: שער המתאר התפתחות של מערכת סגורה פועל לינארית על וקטור המצב. לכן הגדרת הפעולה על בסיס קובעת אותה על המרחב כולו:

$$X(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle.$$

אין הכוונה שכל תהליך פיזיקלי, ובפרט מדידה או אתחול, מתואר כך. את הפעולות האלה כבר פגשנו בנפרד, וההבחנה ביניהן לבין שערים תהיה חשובה.

בכתיב מטריציוני, ביחס לבסיס החישובי,

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

5.1 אילו טרנספורמציות לינאריות מתארות שערים?

לא כל טרנספורמציה לינארית מתאימה. אם הקלט הוא מצב מנורמל, גם הפלט צריך להיות מצב מנורמל, וזה צריך להתקיים לכל קלט אפשרי. מלינאריות נובע שהתנאי שקול לשימור נורמה של כל וקטור:

$$\|U|\psi\rangle\| = \|\psi\rangle\|.$$

נעלה בריבוע ונקבל, לכל וקטור,

$$\langle\psi|U^\dagger U|\psi\rangle = \langle\psi|\psi\rangle.$$

מכיוון שהמטריצה $U^\dagger U - I$ הרמיטית והצורה הריבועית שלה מתאפסת על כל וקטור, היא חייבת להיות מטריצת האפס. לכן

$$U^\dagger U = I.$$

בממד סופי, כאשר הקלט והפלט שייכים לאותו מרחב, זהו בדיוק התנאי לכך שהמטריצה אוניטרית:

$$U^\dagger U = U U^\dagger = I,$$

או, באופן שקול,

$$U^\dagger = U^{-1}.$$

תנאי שקול נוסף הוא שעמודות המטריצה מהוות בסיס אורתונורמלי. בפרט, כל שער כזה הפיך, וההופכי שלו הוא גם שער חוקי.

מלינאריות נקבל גם

$$U(e^{i\theta}|\psi\rangle) = e^{i\theta}U|\psi\rangle.$$

לכן שני וקטורים הנבדלים בפאזה גלובלית ממשיכים להיבדל רק בפאזה גלובלית גם לאחר הפעלת שערים. כפי שהבטחנו, פעולות כאלה אינן מאפשרות להבחין ביניהם.

במודל המתמטי, כל מטריצה אוניטרית על קיוביט יחיד מגדירה שער מותר. איך מממשים שער מסוים, באיזה דיוק ובאיזו עלות, הן שאלות נוספות. בהמשך הקורס נראה כיצד אפשר להסתפק באוסף קטן של שערים ולקרב בעזרתו שערים אחרים.

5.2 קצת על מטריצות

ננצל את ההזדמנות להיזכר בכמה עובדות מאלגברה לינארית. העובדות הבאות תקפות בממד סופי כללי, ולא רק עבור קיוביט יחיד.

5.2.1 ערכים עצמיים של מטריצות אוניטריות

כל ערך עצמי של מטריצה אוניטרית שוכן על מעגל היחידה. אכן, נניח

$$U|\psi\rangle = \lambda|\psi\rangle, \quad |\psi\rangle \neq 0.$$

משימור הנורמה נקבל

$$\| |\psi\rangle \| = \| U|\psi\rangle \| = \| \lambda|\psi\rangle \| = |\lambda| \| |\psi\rangle \|.$$

חלוקה בנורמה, שאינה אפס, נותנת $|\lambda| = 1$.

5.2.2 מטריצות נורמליות ולכסון אוניטרי

מטריצה ריבועית A מעל $\mathbb{C}$ נקראת נורמלית אם

$$A^\dagger A = AA^\dagger.$$

משפט הפירוק הספקטרלי קובע שהיא נורמלית אם ורק אם יש לה בסיס אורתונורמלי של וקטורים עצמיים. באופן שקול, קיימות מטריצה אוניטרית V ומטריצה אלכסונית D כך ש-

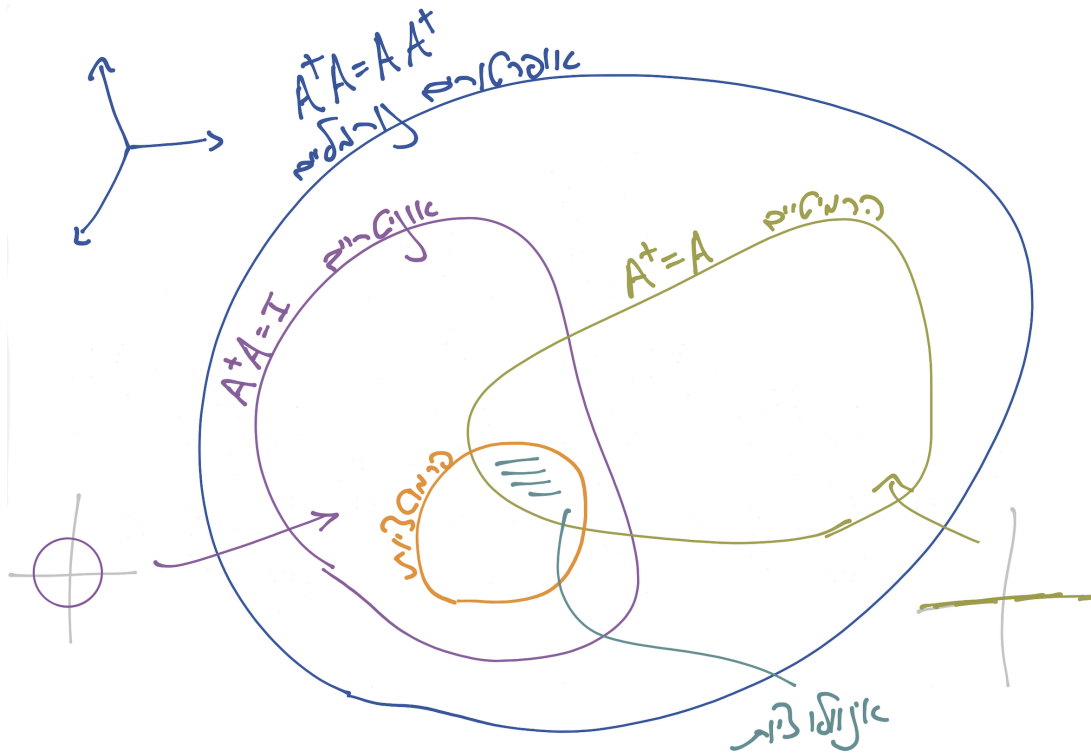
$$A = VDV^\dagger.$$

עמודותיה של V הן וקטורים עצמיים, ועל האלכסון של D מופיעים הערכים העצמיים המתאימים.

כל מטריצה אוניטרית היא נורמלית, ולכן בפרט אפשר לכתוב

$$U = VDV^\dagger, \quad D = \text{diag}(e^{i\theta_1}, \dots, e^{i\theta_d}), \quad (1)$$

כאשר הזוויות $\theta_1, \dots, \theta_d$ ממשייות. גם הכיוון ההפוך נכון: מטריצה נורמלית שכל ערכיה העצמיים על מעגל היחידה היא אוניטרית. הדרישה לנורמליות חשובה; התנאי על הערכים העצמיים לבדו אינו מספיק.



איור 1: משפחת המטריצות הנורמליות

5.2.3 כתיבת מטריצה אוניטרית כאקספוננט

לכל מטריצה אוניטרית U קיימת מטריצה הרמיטית K כך ש-

$$U = e^{iK}.$$

נזכיר שמטריצה הרמיטית מקיימת $K^\dagger = K$, ושלמטריצה ריבועית A מגדירים אקספוננט באמצעות הטור המתכנס

$$e^A \triangleq \sum_{n=0}^{\infty} \frac{A^n}{n!}.$$

כדי לבנות את K , נשתמש בפירוק שב- **משוואה (1)** ונגדיר

$$\Theta = \text{diag}(\theta_1, \dots, \theta_d), \quad K = V\Theta V^\dagger.$$

המטריצה K הרמיטית, משום שהכניסות של Θ ממשייות. מהגדרת האקספוננט ומכך ש- $V^\dagger V = I$ נקבל

$$e^{iK} = V e^{i\Theta} V^\dagger = V D V^\dagger = U.$$

הבחירה אינה יחידה: אפשר להוסיף לכל אחת מן הזוויות כפולה שלמה של 2π . בכיוון ההפוך, האקספוננט e^{iK} של כל מטריצה הרמיטית K הוא אוניטרי, כפי שרואים באותו אופן מן הפירוק הספקטרלי שלה.

כדוגמה, נסו למצוא מטריצה הרמיטית K שעבורה $U = e^{iK}$, כאשר

$$U = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

5.3 בחזרה לשער פאולי X

נשוב לשער X ונגלה שכבר פגשנו את הווקטורים העצמיים שלו:

$$X|+\rangle = |+\rangle, \quad X|-\rangle = -|-\rangle.$$

הערכים העצמיים הם אפוא 1 ו-1, והפירוק המתאים ל- **משוואה (1)** מתקבל עבור

$$D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad V = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \quad (2)$$

שימו לב שהווקטורים $|-\rangle$ ו- $|+\rangle$ מייצגים אותו מצב פיזיקלי, משום שהם נבדלים בפאזה גלובלית בלבד. אבל אין פירוש הדבר שהשער X אינו עושה דבר: על סופרפוזיציה של שני הווקטורים העצמיים הוא משנה את הפאזה היחסית ביניהם.

5.4 שורש של שער

לכל מטריצה אוניטרית יש גם שורש אוניטרי: שער שהפעלתו פעמיים נותנת את השער המקורי. אכן, עבור הפירוק

$$U = V D V^\dagger$$

$$\sqrt{D} \triangleq \text{diag}(e^{i\theta_1/2}, \dots, e^{i\theta_d/2})$$

ונגדיר

$$W \triangleq V\sqrt{D}V^\dagger.$$

או W אוניטרית, וכן

$$W^2 = V\sqrt{D}V^\dagger V\sqrt{D}V^\dagger = VDV^\dagger = U.$$

גם כאן אין בהכרח בחירה יחידה של שורש.

במקרה של X , נבחר את השורשים 1 ו- i לערכים העצמיים 1 ו- -1 , בהתאמה. נקבל

$$\sqrt{X} \triangleq V \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} V^\dagger = \frac{1}{2} \begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}.$$

זהו שורש של פעולת NOT. בעולם הקלאסי, לשער הפיך על ביט יחיד אין אפשרות כזו: האפשרויות הן הזהות וההיפוך, והריבוע של כל אחת מהן הוא הזהות. בעולם הקוונטי, לעומת זאת, אפשר להפעיל "חצי היפוך" פעמיים ולקבל היפוך שלם.

5.5 שני אופרטורים חשובים

שני שערים נוספים שנפגוש שוב ושוב הם **שער פאולי Z** , המוגדר באמצעות

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

ושער האדמרד,

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

שניהם אוניטריים, הרמיטיים, ושווים להופכי של עצמם:

$$Z^2 = H^2 = I.$$

כבר נתקלנו בהם ב-**משוואה (2)**, כאשר לכסנו את X . בפרט,

$$X = HZH.$$

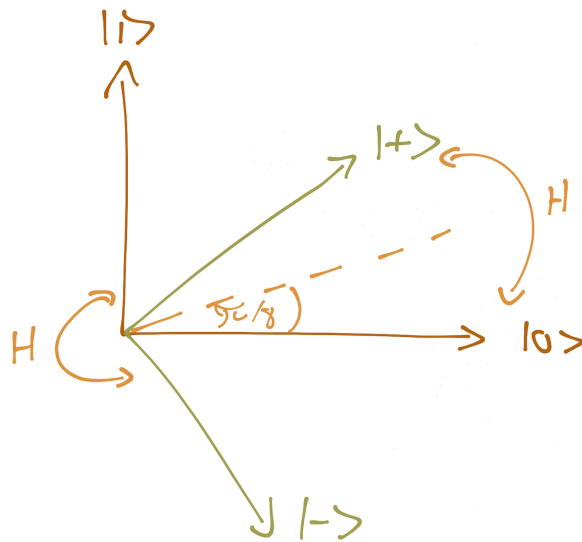
האדמרד ממיר בין הבסיס החישובי לבין הבסיס $\{|+\rangle, |-\rangle\}$:

$$H|0\rangle = |+\rangle, \quad H|1\rangle = |-\rangle, \quad H|+\rangle = |0\rangle, \quad H|-\rangle = |1\rangle.$$

במודל החישובי נניח שאפשר לאתחל קיוביטים למצב $|0\rangle$. אם נרצה להכין את $|+\rangle$, נאתחל כך ואז נפעיל את H .

זהו גם ההסבר להבטחה שלנו לגבי מדידות: אם נרצה למדוד בבסיס $\{|+\rangle, |-\rangle\}$, אפשר להפעיל תחילה H ולמדוד בבסיס החישובי. התוצאה 0 תתאים ל- $+$, והתוצאה 1 תתאים ל- $-$. אם רוצים לשחזר גם את המצב שלאחר המדידה בבסיס המקורי, יש להפעיל שוב את H לאחר המדידה. באופן כללי, עבור בסיס שמרכיב את עמודותיה של מטריצה אוניטרית V , מפעילים תחילה $V^\dagger$, מודדים בבסיס החישובי, ובמידת הצורך מפעילים אחר כך V .

לסיום, אפשר לראות את האדמרד גם באופן גאומטרי. אם מגבילים את תשומת הלב לוקטורים בעלי אמפליטודות ממשיות, הם נמצאים במישור הנפרש על ידי $|0\rangle$ ו- $|1\rangle$. במישור הזה, H הוא שיקוף ביחס לישר היוצר זווית $\pi/8 = 22.5^\circ$ עם הציר $|0\rangle$. זו תמונה נוחה לשער המסוים הזה; באופן כללי, המצבים והאופרטורים שלנו הם מעל המספרים המרוכבים.



איור 2: האדמרד כשיקוף במישור האמפליטודות הממשיות