מדינת ישראל משרד החינוך
מנהל טכנולוגיה
הפיקוח על הוראת מדעי המחשב, הנדסת תכנה וסייבר

תוכנית לימודים - חישוב קוונטי

גרסת אלפא

24.4.2022

ד"ר בועז תמיר, מחבר התכנית

תוכן עניינים (הקלקה על מספר העמוד + לחצן Ctrl ביחד, תקפיץ לעמוד המתאים)

מבוא

המחשב הקוונטי שונה במהותו מהמחשב הקלאסי במבנה הפיזי שלו, בשיטות ההצרנה של בעיות חישוביות המוצגות לו, באלגוריתמים המופעלים עליו וביכולותיו החישוביות. המחשב הקוונטי מהווה כיום אתגר לפיזיקאים למתמטיקאים ולאנשי מדעי המחשב.

אחת המוטיבציות למחשב הקוונטי הינה הניסיון להוריד את סיבוכיות החישוב של בעיות קלאסיות ואכן מספר אלגוריתמים קוונטיים מצליחים בכך. המחשב הקוונטי יכול לפרק מספר לרכיבים הראשוניים שלו בזמן היעיל באופן אקספוננציאלי ביחס לזמן הנדרש ממחשב קלאסי. המחשב הקוונטי יודע לחפש במערך לא ממוין בשורש הזמן הנדרש למחשב קלאסי ועוד.

המחשב הקוונטי עתיד לשמש בבינה מלאכותית כגון בהאצה של חישובי אופטימיזציה של רשתות נוירונים, בלימוד מכונה קוונטי, בתעשייה, בביג דאטה, בהצפנה קוונטית, בפיצוח קודים ועוד. בכל מקום בו נדרש כוח חישובי גדול
עולה מיד האפשרות של שימוש בחישוב קוונטי.

הבנה של פעולתו של מחשב קוונטי דורשת ידע במושגי יסוד בפיזיקה קוונטית. חישוב קוונטי הוא מודל חדש של חישוב, וכמו בכל מודל חדש של חישוב אנו מנסים לזהות תכונות פיזיקליות של המודל או ההתקן אשר ניתן לעשות בהן שימוש לצורך חישוב. במקרה של חישוב קוונטי אנו משתמשים בתכונות קוונטיות כגון סופרפוזיציה, שיזור ומנהור. קיומו של מודל חדש של חישוב מחייב אותנו לבחון ולהגדיר מחדש את כל המושגים הבסיסיים של חישוב ולהחליף אותם במקביליהם הקוונטיים, כך נקבל את הביט הקוונטי או הקיו-ביט, את השערים קוונטיים, המעגלים היוניברסליים הקוונטיים, הרגיסטרים הקוונטיים ועוד.

החשיבה הנדרשת בבנייה של אלגוריתמים קוונטיים משלבת שיקולים פיזיקליים, מתמטיים ושיקולים מתחום מדעי המחשב, היא שונה במהותה מהחשיבה הנדרשת בתכנון קלאסי. חשיבה כזו היא בין תחומית, היא מעודדת חשיבה מחדש על מושגים שהיו נראים מלכתחילה ברורים מאליהם.

מטרות

- חשיפה של התלמיד למושג "מודל החישוב"
- הרחבה של מושג המחשב, חשיבה מחדש של כל מושגי היסוד של מחשב
- הבנה של מושגים בסיסיים של מודלים של חישוב כגון חישוב אנאלוגי/דיגיטלי, חישוב רוורסבילי, חישוב בהסתברות ועוד.
- חשיפה של התלמיד לעקרונות בסיסיים של הפיזיקה הקוונטית שיש להן השלכה לחישוב
- המרה של כל מושגי היסוד של מחשב מהעולם הקלאסי לעולם הקוונטי
- הבנה של פעולתם של רכיבים בסיסיים של מחשב קוונטי
- הבנה של המודל המתמטי של מחשבים קוונטיים
- הבנה של מושג האלגוריתם הקוונטי
- הבנה והדגמה של יעילותם העודפת של מחשבים קוונטיים על מחשבים קלאסיים
- הכרה של סימולטור ה Qiskit לדימוי של מעגלים קוונטיים ולתקשורת עם מחשב קוונטי אמיתי

פרק א: מבוא

הקדמה

לשם מה צריך מחשבים קוונטיים? מהו מודל של חישוב, דוגמאות, סרגל חישוב, מחשב אנלוגי, מחשב דיגיטלי, מחשב DNA, מחשב ככלי עזר לפתרון בעיות חישוב. לעיתים בחירת מכשיר החישוב יכולה לקצר את זמן החישוב.

סיבוכיות של חישוב: בעיות קלות/קשות לפתרון באמצעות מחשב רגיל, דוגמא לבעיה קלה לחישוב, חיפוש במאגר ממוין, דוגמא לבעיה קשה לחישוב, בעיית הסוכן הנוסע. הקושי מוגדר על פי תוספת המשאבים הנדרשים מהמחשב כמו זמן וגודל זיכרון בכדי לפתור בעיה זהה עם מספר גדול יותר של משתנים.

בעיות שמחשב קוונטי פותר בקלות: מחשב קוונטי פותר בקלות בעיות שקשה לפתור באמצעות מחשב קלאסי, לדוגמא פירוק מספר לרכיבים ראשוניים, מדוע בעיה כזו קשה לחישוב במחשב קלאסי?

מחשב קוונטי פותר בעיה של חיפוש במערך לא ממויין בזמן קצר יותר מאשר זמן מחשב קלאסי. במקום זמן של N במחשב קלאסי כאשר N הוא מספר האברים במערך, המחשב הקוונטי מוצא את האיבר הדרוש בזמן של שורש N.

מחשבים משמשים בסימולציה של תופעות טבע: מחשבים קלאסיים משמשים כסימולטורים לתופעות כמו מזג אויר, מנהרת רוח לחקר תעופה ועוד. מחשב קוונטי הוא סימולטור טבעי של תופעות קוונטיות

מושגים

- מודלים אפשריים של חישוב, מכשירי מדידה וחישוב
- סיבוכיות של חישוב כפונקציה של גודל הבעיה
- דוגמאות לבעיות שמחשב קוונטי פותר באופן יעיל יותר
- קשר בין המודל לסיבוכיות החישוב
- המחשב כסימולטור

מטרות ביצועיות

1. התלמיד יגדיר את המושג "סיבוכיות חישוב" ויביא דוגמה.
2. התלמיד יסביר מהי בעיית הסוכן הנוסע.
3. התלמיד יסביר כיצד ניתן לחשב את מספר המסלולים האפשריים בבעיית הסוכן הנוסע.
4. התלמיד יציג דוגמא לבעיית הסוכן הנוסע עם שבעה ערים.

5. התלמיד יגדיר מערך ממוין, חיפוש במערך ממוין, ואלגוריתם לחיפוש במאגר ממוין.
6. התלמיד יגדיר את בעיית החיפוש במערך לא ממוין ויתאר אלגוריתם העושה חיפוש במאגר כזה.
7. התלמיד יביא דוגמאות למחשב אשר משמש כסימולטור.
8. התלמיד יגדיר מהי בעיית פירוק מספר לרכיבים ראשוניים.
9. התלמיד יציע אלגוריתם לפתרון בעיית פירוק מספר לרכיבים ראשוניים שלו, תוך כדי חישוב הסיבוכיות.
10. התלמיד יסביר כיצד סיבוכיות הפתרון שהציע עולה עם הגדלת המספר לפירוק.

דגשים ודרכי הוראה

- להביא לכיתה אבאכוס, סרגל חישוב, טבלת לוגריתמים, אצבעות נאפייר, וכלי חישוב אחרים אם נגישים, להדגים חישוב באמצעותם.
- להסביר את העובדה כי בבעיית הפירוק הוספה של ספרה אחת למספר מגדילה באופן משמעותי את מספר הבדיקות הנדרשות.
- ניתן לעשות תרגיל בזוגות של פירוק מספר לרכיבים, כאשר אחד התלמידים מרכיב מספר והשני מנסה פרק אותו לרכיבים ראשוניים
- להסביר את העובדה שבמערך לא ממוין יש לעבור על כל הרשומות אחד אחד בכדי למצוא אחת מהן, ובמערך ממוין ניתן להשתמש במיון כדי להגיע לרשומה מיד.
- להדגיש את העובדה שסימולטור של תופעה כלשהי טבעי יותר יהיה לבצע אותה עם רכיבים בעלי אותו אופי כמו התופעה שרוצים לדמות.
- להדגיש את העובדה שסיבוכיות של חישוב בעיה יכולה להשתנות אם נשתמש במחשב שונה. לתת דוגמאות
- להדגיש את העובדה שסיבוכיות היא פונקציה של הגדלת מספר הרכיבים בבעיה, והשאלה היא לא כמה משאבי חישוב נדרשים לחשב מקרה מסוים, אלא כיצד אותם משאבים גדלים עם הגדלת מספר הפרמטרים שמגדירים את הבעיה.

לוח זמנים

עבודה על פרק זה צפוייה להימשך 3 שעות.

פרק ב: הגדרה פיזיקלית של מחשב

הקדמה

מכונת טיורינג

מחשב קלאסי מוגדר כמכונת טיורינג. אנו ניתן הרחבה למושג "מחשב".

הגדרה פיזיקלית למחשב

מחשב הוא התקן כלשהו אשר באמצעותו ניתן לעשות חישובים, הדרישות מההתקן הן:

בסיס חישוב בכניסה: מצבים פיזיקליים נפרדים אשר ניתן לזהות כל אחד מהם עם מספר.

בסיס חישוב ביציאה: מצבים פיזיקליים נפרדים אשר ניתן לזהות כל אחד מהם עם מספר.

ההתקן עובר אבולוציה/שינוי, מזמן ראשוני ועד זמן סופי נתון מראש. בתחילת החישוב הנתונים נכתבים באמצעות בסיס החישוב בכניסה ובסיום החישוב התוצאה נקראת מתוך בסיס החישוב ביציאה.

דוגמאות: מחשב תרמודינמי לחישוב ממוצע מספרים, מחשב DNA לחישוב בעיות ריצוף, סוכן נוסע

מסקנה: מציאת תכונות פיזיקליות/כימיות/ביולוגיות בעלות ערך חישובי, ובניית "מחשב" מתאים. הרבה התקנים יכולים לשמש כ"מחשב", כל "מחשב" כזה מתאים לפתרון משפחה של בעיות חישוביות

מושגים

- המחשב כמכונת "טיורינג"
- הגדרה פיזיקלית למחשב
- בסיס חישוב בכניסה וביציאה, אבולוציה בין שתי נקודות זמן ידועות מראש
- כתיבה וקריאה/מדידה של התוצאות
- דוגמאות להתקני חישוב

מטרות ביצועיות

1. התלמיד יסביר מהי מכונת טיורינג
2. התלמיד ידגים כיצד שולחן יכול לשמש כמחשב לצורך חיבור וחיסור מספרים בין 1 ל 4 (או חישוב מודולו 4). התלמיד יסביר מהו בסיס החישוב בכניסה, ביציאה
3. התלמיד יסביר כיצד ניתן לחשב ממוצע של מספרים באמצעות מחשב מבחנות? מהו בסיס החישוב?

4. התלמיד יסביר אילו סוגי בעיות ניתן לחשב באמצעות מחשב DNA.

דגשים ודרכי הוראה

- להדגיש את הרעיון שמחשב יכול להיות כל התקן שהוא ובלבד שהוא יעזור לנו לבצע את החישוב
- להדגיש את העובדה שיש להתאים בין סוג הבעיה לסוג ההתקן שבו משתמשים בחישוב
- להציג חישוב פשוט של מציאת הזוגיות של מספר כלשהו באמצעות מכונת טיורינג.

לוח זמנים

עבודה על פרק זה צפוייה להימשך 3 שעות.

פרק ג: פיזיקה קוונטית

הקדמה

ניסוי שני החריצים:

- שלב א: ניסוי באמצעות תותח של כדורים קלאסיים
- שלב ב: ניסוי באמצעות גלים במים, יצירת גלים משניים, מושג ההתאבכות
- שלב ג: ניסוי באמצעות "תותח" אלקטרונים

המוזרות העולה מהניסוי בשלב ג, אנו יורים אלקטרונים/חלקיקים ומקבלים תוצאה של התאבכות

ניסיון להסביר את המוזרות יוצר בעיות כגון קורלציה של חלקיקים, "מודעות" של החלקיק למצב הניסוי ועוד.

הסבר הניסוי באמצעות "גל". האם האלקטרון הוא גל? אם כן באיזה תווך מתפשט הגל. מושג חדש של "גל הסתברות".

דיון פילוסופי: חלקיק מראה תכונות משתנות בהתאם לניסוי. בניסויים מסוימים הוא מתגלה כחלקיק ובניסויים אחרים הוא מתגלה כגל.

סופרפוזיציה: חלקיק יכול להיות בעת ובעונה אחת בשני מקומות. כיצד ניתן להסביר זאת?

דיון פילוסופי: אם חלקיקים יכולים להיות בסופרפוזיציה מדוע אנחנו לא.

מדידה קוונטית: כל ניסיון למדוד את החלקיקים לאחר שעברו את שני החריצים מביא לקריסה של פונקציית הגל וקבלה של תוצאה קלאסית. כיצד ניתן להסביר זאת?

דיון פילוסופי: מדידה משנה את המציאות, אינטראקציה בין הצופה/המודד לבין האובייקט.

הגדרה: סופרפוזיציה מאוזנת של שני מצבים יקרא קיו ביט q-bit

תופעות נוספות: שיזור של שני חלקיקים. מהו מצב של שני חלקיקים "שזורים". מה קורה לסופרפוזיציה כזו בשעת מדידה. מה ניתן לעשות עם זוגות שזורים. פרוטוקול פשוט של הצפנה ופענוח באמצעות זוגות שזורים.

מנהור קוונטי: חלקיקים קוונטיים יכולים לעבור מחסום שחלקיק קלאסי לא עובד

מושגים

- ניסוי שני החריצים
- דואליות של חלקיק וגל
- סופרפוזיציה

- מדידה קוונטית, קריסה למצב קלאסי
- בעיית המדידה
- קיוביט
- שיזור חלקיקים
- הצפנה קוונטית באמצעות שיזור של חלקיקים
- מנהור קוונטי

מטרות ביצועיות

1. התלמיד יסביר מהי סופרפוזיציה של שני מצבים.
2. התלמיד יסביר מהי המוזרות העולה מניסוי שני החריצים
3. התלמיד יסביר מדוע אנו אומרים שהחלקיק עובר דרך שני החריצים בעת ובעונה אחת
4. התלמיד יסביר מהי דואליות חלקיק גל, מדוע אנחנו צריכים דואליות כזו
5. התלמיד יסביר את ההבדל בין מדידה קלאסית לבין מדידה קוונטית
6. התלמיד יסביר את ההבדל בין מפסק קלאסי שנמצא במצב "כבוי" או "דלוק" למפסק קוונטי שיכול להיות במצב "דלוק" ומצב "כבוי" בעת ובעונה אחת.
7. התלמיד יסביר מדוע מטבע שנזרקת לאוויר לא נמצאת בסופרפוזיציה של "עץ" ו"פלי".
8. התלמיד יסביר את המושג "התאבכות גלים".
9. התלמיד יסביר מהי סופרפוזיציה של ארבע מצבים, מספר כללי של מצבים
10. התלמיד יסביר מה ההבדל בין קיוביט לבין סופרפוזיציה כללית של שני מצבים
11. התלמיד יסביר מהי הצפנה קוונטית באמצעות מספר זוגות שזורים וייתן דוגמה פשוטה עם שש זוגות שזורים

דגשים ודרכי הוראה

- משימה של שרטוט ניסוי שני החריצים ומציאת נקודות החיתוך שלהם במרחק קבוע ממקום יצירת הגלים. ושרטוט דומה למקרה של גלים עם הפרשי מופע של 90 מעלות, 180 מעלות, 270 מעלות
- להדגיש את ההבדל בין מדידה קלאסית שחושפת מציאות שקיימת ממילא, בין אם מודדים או לא, לבין מדידה קוונטית, כשאר עצם המדידה מביאה לשינוי של מצב החלקיק ולקריסה למצב קלאסי

- להדגיש את העובדה שבפיזיקה קוונטית צופה שעושה מדידה איננו מנותק מהגוף בו הוא צופה, ועצם המדידה משפיעה על הגוף הנצפה
- להדגיש את העובדה שבניסויים מסוימים אלקטרון מתנהג כמו חלקיק ובניסויים אחרים מתנהג כמו גל
- להדגיש את העובדה שבפיזיקה קוונטית הסתברות היא חלק אינהרנטי של הפיזיקה ולא רק שיטת תיאור של המציאות כמו במקרה הקלאסי
- להדגיש את "בעיית המדידה", כלומר את העובדה שאנחנו לא יודעים מדוע המערכת קורסת למצב קלאסי וכל מה שנוכל לעשות הוא לתאר את ההסתברויות שדבר כזה יקרה
- להדגיש את העובדה ש"גל" כאן הוא לא גל בתוך תווך כמו מים או אוויר, ולכן לא ברור אם יש לו ממשות פיזיקלית או אם הוא נועד רק לתאר בדיעבד מה קורה כאן
- להדגיש את העובדה שבפיזיקה קוונטית אנחנו לא תמיד יודעים ל"הסביר" את התופעה, ולפעמים אנחנו מחליפים "הסבר" בתיאור
- אפשר לעשות ניסוי במעבדה פשוטה כדי להדגים את תופעת התאבכות הגלים, אפשר ורצוי להציג סרטי וידאו של ניסויים באלו
- להדגיש ולסכם את ההבדלים בין פיזיקה קלאסית לבין פיזיקה קוונטית

לוח זמנים

עבודה על פרק זה צפוייה להימשך 9 שעות.

פרק ד: חזרה והשלמה - אלגברה לינארית

הקדמה

מושגים

- מרחב וקטורי
- אברי בסיס, כתיבה של וקטור כללי באמצעות אברי בסיס
- הטלה של וקטור על אברי בסיס, קואורדינטות
- חיבור וקטורים, מקבילית כוחות
- מרחב דואלי, מרחב שורות ומרחב עמודות
- מכפלה סקלרית של וקטורים
- מספרים מרוכבים, המספר i.
- הצמוד של מספר מרוכב
- הצגה פולארית של מספר מרוכב
- חיבור מספרים מרוכבים
- מכפלה של מרוכבים
- נוסחת דה-מואבר למספרים מרוכבים
- מכפלה סקלרית עם מרחב דואלי צמוד
- אופרטורים במרחב וקטורי
- מטריצה של אופרטור
- הכפלת מטריצה בוקטור
- מכפלת מטריצות

מטרות ביצועיות

1. התלמיד יפתור סדרה של תרגילים בנושא, תרגילים לדוגמה מופיעים בנספח

דגשים ודרכי הוראה

- פתרון התרגילים בביתה

- הצגה של וקטורים בממד 2 בכדי להקל על ההבנה

לוח זמנים

עבודה על פרק זה צפוייה להימשך 15 שעות.

פרק ה: המודל המתמטי של חישוב קוונטי

הקדמה

סופרפוזיציה כוקטור (עמודה) במרחב וקטורי מעל המספרים המרוכבים. קיו-ביט כווקטור מממד 2. ריבוע הערך המוחלט הוא ההסתברות ליפול לענף המתאים של הסופרפוזיציה.

חזרה לניסוי שני החריצים, הסבר של תבנית ההתאבכות באמצעות חיבור של שני מספרים מרוכבים בכל מקום המייצגים את גובה הגל והפאזה המגיעים מכל חריץ. ריבוע הערך המוחלט של סכום המספרים המרוכבים כהסתברות לקבל את החלקיק באותו מקום. האלגוריתם של פיינמן לחישוב האמפליטודה של ההתאבכות.

סופרפוזיציה מאוזנת עם פאזה של 1+ או 1- או i+ או i-, מה המשמעות של כל סופרפוזיציה כזו.

הגדרה של וקטור דואלי, וקטור שורה עם ערכים מרוכבים צמודים כדואלי של וקטור עמודה עם הערכים המקוריים. מכפלה סקלרית של וקטור שורה עם וקטור עמודה. דרישת היוניטריות כדרישה למכפלה סקלרית שווה ל 1. דרישת היונטריות והדרישה לסכום ההסתברויות.

אופרטורים יוניטריים, הגדרה, מדוע אנו משתמשים באופרטורים יוניטריים. אופרטורים יוניטריים כמחשבים קוונטיים, אופרטורים יוניטריים כאופרטורי סיבוב.

מדידה קוונטית: מדידה כאוסף של אופרטורי הטלה. הדגמה על סופרפוזיציה פשוטה עם שני ענפים. הטלה על ציר ה |0> והטלה על ציר ה |1>. ההסתברות לקבל כל ערך מדוד כריבוע הערך המוחלט של אורך ההטלה. נרמול של ההטלה כדי לקבל ווקטור יוניטרי.

מדידה פרוייקטיבית, הגדרות כלליות:

א. ההסתברות לקבל כל ערך רשומה באמצעות אופרטור הטלה

ב. התנאי על סכום של אופרטורי הטלה המבטיח שסכום ההסתברויות יהיה 1

ג. מצב המערכת לאחר המדידה רשום באמצעות אופרטור ההטלה

כתיבה של אופרטורי המדידה במקרה של סופרפוזיציות פשוטות עם שני ענפים ועם ארבע ענפים.

מושגים

- סופרפוזיציה כוקטור במרחב וקטורי מעל המרוכבים
- ההסתברויות לקריסה לכל ענף כריבוע הערך המוחלט של המספר המרוכב שהוא מקדם הענף
- חישוב ההסתברות בניסוי שני החריצים
- מקדמים של ענפי הסופרפוזיציה ומשמעותם, המקדמים 1- i- ,i

- אופרטורים יוניטריים
- אופרטורים יוניטריים כסיבובים במרחב
- התנאי לאופרטור יוניטרי
- מדידה פרוייקטיבית
- אופרטורים של הטלה, כתיבה באמצעות הסימון $|\psi><\psi|$
- מצב המערכת לאחר מדידה פרוייקטיבית, נרמול המצב
- ההסתברות לקבל כל ערך מדידה

מטרות ביצועיות

1. התלמיד יסביר את המשמעות של הצגת הסופרפוזיציה כוקטור במרחב, את משמעות הקואורדינטות ואת משמעות המקדמים
2. התלמיד יסביר מה המשמעות של הדרישה לאופרטור יוניטרי
3. התלמיד יחשב פעולה של אופרטור יוניטרי כלשהו מממד 2 על וקטור כללי. התלמיד יחשב את הוקטור הדואלי לוקטור שהתקבל.
4. התלמיד יראה את השוויון $<\psi|U = U|\psi>$
5. התלמיד יגדיר את כל רכיבי המדידה הקוונטית
6. התלמיד יסביר את חישוב ההסתברות ליפול לכל ענף של הסופרפוזיציה
7. התלמיד יסביר מהו מצב המערכת לאחר מדידה
8. התלמיד יפתור תרגיל במושגי יסוד במדידות קוונטיות כדוגמת התרגיל המופיע בנספחים

דגשים ודרכי הוראה

- להציג את האלגוריתם של פיינמן לחישוב סכום האמפליטודות כפי שפיינמן הראה אותו כחיבור וקטוריאלי של שני מחוגי "שעונים" והעלאה בריבוע של אורך סכום המחוגים.
- להסביר שהתוצאות ההסתברותיות, גם במקרה של קריסה לענף מסוים וגם במקרה של שני החריצים הם תוצאות ניסוי.
- להזכיר מהי הטלה של וקטור לאחד מוקטורי הבסיס. להראות שהטלה מתמטית מובילה לוקטור שלא מייצג מצב פיזיקלי ולכן יש לנרמל את הוקטור שהתקבל, להראות כיצד מנרמלים וקטור כזה
- להשוות בין כל רכיבי ההגדרה המתמטית של מדידה לבין המקרה הפשוט של סופרפוזיציה עם שני ענפים, להציג ולהדגיש כל רכיב

לוח זמנים

עבודה על פרק זה צפוייה להימשך 9 שעות.

פרק ו: שערים/מעגלים קוונטיים בסיסיים

הקדמה

שערים של קיוביט אחד X, Y, Z :

- בדיקה של תנאי היוניטריות
- פעולה על וקטורי הבסיס |0> ו |1>

שער הדמרד: **Hadamard**

- בדיקה של תנאי היוניטריות,
- פעולה על אברי הבסיס |0> ו |1>
- יצירה של סופרפוזיציה

שער של שני קיוביטים:CNOT

- בדיקה של תנאי היוניטריות
- פעולה על אברי הבסיס
- פעולה על סופרפוזיציה
- מטריצה של CNOT

שרשור של מעגלים קוונטיים, הגדרה, שרשור משמאל לימין והרכבה של המטריצות מימין לשמאל.

שערים של סיבוב, סיבוב וקטור סופרפוזיציה בסיסית סביב ציר הX, סביב ציר הY וסביב ציר הZ.

תיאור מטריצות הסיבוב. בדיקה של יוניטריות המטריצות.

קבוצה אוניברסלית של מעגלים קוונטיים, מהי ומדוע צריך קבוצה כזו. קבוצה יוניברסלית במחשבים קלאסיים. תיאור סכמטי של שיטת ההוכחה של משפט כזה מבלי להיכנס לפרטים.

מושגים

- שער קוונטי
- שער קוונטי על סופרפוזיציה מממד 2
- שערים X, Y, Z
- שער הדמרד Hadamard
- שערים קוונטיים על סופרפוזיציה מממד 4
- שער XOR
- קבוצה יוניברסלית של שערים קוונטיים
- בדיקת יוניטריות של שערים קוונטיים

מטרות ביצועיות

1. חישוב והוכחה של יוניטריות של המעגלים הקוונטיים
2. חישוב פעולת המעגלים על קיוביט
3. שרשור של פעולות יוניטריות
4. סימולציה של מעגלים בסיסיים בעזרת Qiskit.

דגשים ודרכי הוראה

- להבהיר את העובדה ששרשור מעגלים קוונטיים משמאל לימין הוא כמו הכפלה של המטריצות המתאימות מימין לשמאל
- להבהיר את הרעיון שלכל שער כזה ניתן להכניס סופרפוזיציה ולא רק מצב קלאסי
- להבהיר את החשיבות של קבוצה יוניברסלית של שערים, גם במקרה הקלאסי וגם במקרה הקוונטי.
- להבהיר איזה קבוצה של מעגלים קוונטיים הינה יוניברסלית

לוח זמנים

עבודה על פרק זה צפוייה להימשך 9 שעות.

פרק ז: שימושים בסיסיים בשערים קוונטיים

הקדמה

בנייה של סופרפוזיציה מאוזנת של מספר קיוביטים באמצעות מעגלי הדמרד

מושג של טנזור של מצבים קוונטיים, טנזור ומכפלה, מושג של טנזור של אופרטורים. חישוב של טנזור של אופרטורי הדמרד. נוסחת הטנזור במקרה הכללי של שני אופרטורים. חישוב המטריצות של טנזור כללי.

יצירת שיזור, יצירת כל מצבי בל באמצעות מעגל הדמרד ומעגל CNOT.

הפרדה בין מצבי בל שונים על ידי מדידה מתאימה.

מעגל SWAP בין שני קיוביטים המורכב ממעגלי CNOT

מעגל סימון בפאזה המורכב מהדמרדים וCNOT

פרוטוקול של טלפורטציה קוונטית. העברה של סופרפוזיציה פשוטה על ידי שתי מדידות והעברה של שני ביטים קלאסיים.

מושג ה no-cloning , הוכחה של העיקרון

מושגים

- טנזור של מצבים
- טנזור של אופרטורים
- יצירת סופרפוזיציה מאוזנת ראשונית
- מצבי Bell
- טלפורטציה קוונטית
- עיקרון ה no cloning
- בנייה של מצבי Bell והפרדה ביניהם על ידי מדידה
- מעגל SWAP

מטרות ביצועיות

1. כניסה לסימולטור של Qiskit בהנחיה של המורה והכרה שלו
2. בנייה ב Qiskit של סופרפוזיציה מאוזנת של שני קיוביטים על ידי שני מעגלי הדמארד
3. בנייה ב Qiskit של צירוף CNOT והדמארד בכדי לייצר זוגות שזורים

4. בנייה ב Qiskit של מעגל הפרדה של מצבי Bell על ידי מדידה
5. בנייה ב Qiskit של מעגל טלפורטציה קוונטית
6. בנייה ב Qiskit של מעגל SWAP בין שני קיוביטים
7. חישוב המטריצה של טנזור של שני הדמרדים
8. חישוב המטריצה של טנזור של שני אופרטורים יוניטריים כלליים, רישום הכלל

דגשים ודרכי הוראה

- חשובה מאוד כניסה לסימולטור של מעגלים קוונטיים ובנייה של מעגלים קוונטים בסיסיים.
- יש להדגיש את העובדה שטלפורטציה קוונטית אפשרית רק לאחר שידור של אינפורמציה קלאסית, ולכן אי אפשר להעביר סופרפוזיציה קוונטית במהירות גדולה ממהירות האור
- יש להדגיש את העובדה כי בטלפורטציה קוונטית הסופרפוזיציה הראשונית נעלמה מהקלט והופיעה רק בפלט, בכפוף לעיקרון ה no cloning
- יש להסביר את משמעות עיקרון ה no-cloning אשר מחייב כל פעם הפעלה של המחשב הקוונטי מחדש.
- יש להדגיש כי תוצאת החישוב הקוונטי היא בהרבה מקרים תוצאה הסתברותית
- יש להסביר את הקשר בין "טנזור" או "מכפלה" של מצבים לבין ריבוי של החלקיקים בלתי תלויים המרכיבים את המעגל הקוונטי

לוח זמנים

עבודה על פרק זה צפוייה להימשך 9 שעות.

פרק ח: אלגוריתמים קוונטיים ראשוניים

הקדמה

אלגוריתם של דויטש, מושג האלגוריתם קוונטי מעל אורקל. הבעיה הקלאסית: הפרדה בין פונקציה קבועה לפונקציה מאוזנת. יתרונות של האלגוריתם של דויטש על אלגוריתם קלאסי. מעבר על כל רכיבי האלגוריתם.

הרחבה של האלגוריתם למקרה כללי (דויטש ג'וזה). כתיבה של האלגוריתם למקרה של n=2, למקרה של n=3.

חישוב קוונטי של מכפלה סקלרית (זווית) בין שני וקטורים. חזרה על מעגל של SWAP למקרה כללי. יתרונות מעל חישוב קלאסי של מכפלה סקלרית. שימושים של אלגוריתם כזה בבינה מלאכותית.

מושגים

- אלגוריתם של דויטש, דויטש ג'וזה
- אלגוריתם קוונטי מעל אורקל
- סימון בפאזה של רכיבים
- היתרון הקוונטי של האלגוריתם של דויטש על אלגוריתם קלאסי
- אלגוריתם לחישוב מכפלה סקלרית של שני וקטורים

מטרות ביצועיות

1. בנייה של האלגוריתם של דויטש על גבי סימולטור Qiskit למקרה של n=4.
2. בנייה של אלגוריתם למכפלה סקלרית של שני וקטורים מממד 2 על גבי סימולטור Qiskis
3. מציאה של שימוש לאלגוריתם של חישוב מכפלה סקלרית
4. התלמיד יסביר את היתרון העודף של אלגוריתם קוונטי מעל אלגוריתם קלאסי בפתרון בעיית דויטש
5. התלמיד יסביר את היתרון העודף של אלגוריתם קוונטי מעל אלגוריתם קלאסי בחישוב מכפלה סקלרית של וקטורים

דגשים ודרכי הוראה

- להדגיש את המושג של אלגוריתם מעל אורקל, ואת הבעייתיות של בנייה בפועל של אלגוריתם כזה ביום
- להדגיש את העובדה שענף של סופרפוזיציה המסומן בפאזה כלשהי שקול לענף עם גל שנמצא בהפרש מופע מתאים

- להדגיש את העובדה שבאלגוריתמים קוונטיים אנו מנסים לחלץ אינפורמציה גלובלית על כל ערכי הקלט
- להדגיש את העובדה שבאלגוריתמים קוונטיים כל הפעולות המותרות הינן על כל ענפי הסופרפוזיציה בבת אחת ולא על כל ענף בנפרד

לוח זמנים

עבודה על פרק זה צפוייה להימשך 12 שעות.

פרק ט: אלגוריתמים קוונטיים מתקדמים - **GROVER**

הקדמה

תיאור סכימטי של גרובר כמגבר הסתברות באלגוריתם של "חיפוש מחט בערימת שחת". כל איטרצית גרובר מורכבת מסימון בפאזה ושיקוף סביב ממוצע האמפליטודות, דוגמה של שני קיוביטים

כתיבת רכיבי גרובר.

מעגל סימון

מעגל שיקוף סביב הממוצע

דוגמה שלמה של גרובר על שני קיוביטים

תיאור גיאומטרי של איטרציות גרובר וחישוב הסיבוכיות הנדרשת.

הרחבה של גרובר למקרה של כמה פתרונות או כמה ענפים מסומנים, הסיבוכיות כפונקציה של מספר הפתרונות. שימושים באלגוריתם גרובר להאצה של חישובים.

מושגים

- גרובר כאלגוריתם מעל אורקל
- איטרציות גרובר
- שיקוף סביב ממוצע האמפליטודות
- הצגה גיאומטרית של איטרציות גרובר
- חישוב מספר האיטרציות הנדרש
- האצת חישובים קלאסיים

מטרות ביצועיות

1. התלמיד יסביר את כל רכיבי מעגל השיקוף ויחשב את הפעולה על וקטור כללי
2. בנייה באמצעות סימולטור Qiskit של מעגל גרובר למקרה פשוט של 2=n.
3. חישוב מטריצת השיקוף למקרה של n=2, 3
4. התלמיד יתאר מבנה סכימטי כללי של אלגוריתם גרובר
5. התלמיד יציע שימוש בגרובר לשם האצת חישוב קלאסי
6. התלמיד יסביר את יתרון האלגוריתם ביחס לאלגוריתם קלאסי של חיפוש במערך לא ממוין

דגשים ודרכי הוראה

- יש להדגיש כי בפועל קשה היום לבנות את אלגוריתם גרובר בהיותו אלגוריתם מעל אורקל קוונטי
- יש להדגיש את העובדה כי אלגוריתם גרובר ניתן להכללה למקרה שבו ישנם כמה פתרונות או רכיבים מסומנים
- יש להדגיש את העובדה כי לאלגוריתם כזה יש משפחה רחבה של יישומים

לוח זמנים

עבודה על פרק זה צפוייה להימשך 12 שעות.

פרק י: אלגוריתם טרנספורם פורייה

הקדמה

מושגים

-

מטרות ביצועיות

1. התלמיד יריץ

דגשים ודרכי הוראה

-

לוח זמנים

עבודה על פרק זה צפוייה להימשך 9 שעות.

פריסת שעות

פרק	הנושא	בכיתה	סה"כ שעות
1	מבוא	3	3
2	הגדרה פיזיקלית של מחשב	3	3
3	פיזיקה קוונטית	9	9
4	אלגברה לינארית	15	15
5	המודל המתמטי של חישוב קוונטי	9	9
6	שערים/מעגלים קוונטיים בסיסיים	9	9
7	שימושים בסיסיים בשערים קוונטיים	9	9
8	אלגוריתמים קוונטיים ראשוניים	12	12
9	אלגוריתמים קוונטיים מתקדמים: GROVER	12	12
10	אלגוריתם טרנספורם פורייה	9	9
	סה"כ שעות		90