MATH 1800: Quantum Information Theory with Applications to Cryptography

Final Exam
Review

Solutions

Elliptic curves

In addition to the problems below, take another look at midterms 1&2, the reviews preceding them and homework assignments.

Problem 1. Let P be a point on a smooth elliptic curve over $\mathbb{R}$. Suppose that P is not the point at infinity.

(a) Give a geometric condition that is equivalent to P being a point of order 2.

Solution: the tangent line to E at P is vertical, hence these are the points of intersection of the graph of E with the x-axis (the graph of E is symmetric w.r.t. the x-axis and, as $-P$ is the reflection of P w.r.t. the x-axis, $P = -P$ only for P on the x-axis).

(b) Give a geometric condition (justify your answer) that is equivalent to P being a point of order 3.

Solution: such a point P satisfies $P \oplus P \oplus P = \mathcal{O}$ or $P \oplus P = -P$, which implies that the third point of intersection of the tangent line to E at P with the graph of E is P. Let $F_\ell(x)$ be the restriction of the defining polynomial of E to the tangent line to E at P. Then $F_\ell(x)$ vanishes at P with multiplicity 3, meaning that $F_\ell(x(P)) = F'_\ell(x(P)) = F''_\ell(x(P)) = 0$ (here $x(P)$ is the x-coordinate of P), thus P is an inflection point.

Problem 2. Let E be a smooth elliptic curve over $\mathbb{R}$.

(a) How many points (elements) of order 2 can $G(E)$ have? (justify your answer)

Solution: the cubic polynomial in the defining equation of E has either one or three real zeros and those are precisely the elements of order 2.

(b) Find the equation $\psi(x)$ that the x-coordinate of a point (element) satisfies if and only if it has order 3?[1] (justify your answer)

Solution: using implicit differentiation, we find $2y\dfrac{dy}{dx} = 3x^2 + a$, thus, $\dfrac{dy}{dx} = \dfrac{3x^2+a}{2y}$. Differentiating implicitly one more time gives

$$\frac{d^2y}{dx^2} = \frac{d\left(\dfrac{3x^2+a}{2y}\right)}{dx} = \frac{6x \cdot 2y - 2\dfrac{dy}{dx}(3x^2+a)}{4y^2} = \frac{12xy^2 - (3x^2+a)^2}{4y^3} = \frac{12x(x^3+ax+b) - (3x^2+a)^2}{4y^3},$$

so $\psi(x) = 12x(x^3+ax+b) - (3x^2+a)^2 = 3x^4 + 6ax^2 + 12bx - a^2$.

(c) Let's pick a concrete example with $b = 0, a = 1$, i.e. the defining equation of E is $y^2 = x^3 + x$. Find the inflection points (give both coordinates).

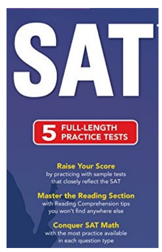
Solution: we have $\psi(x) = 3x^4 + 6x^2 - 1$ and using the substitution $t = x^2 \geq 0$, get the quadratic equation $\psi(t) = 3t^2 + 6t - 1$, which has the zeros $t_{1,2} = \dfrac{-6 \pm 4\sqrt{3}}{6}$. Notice that $t_2 = \dfrac{-6-4\sqrt{3}}{6}$ is less than 0, while

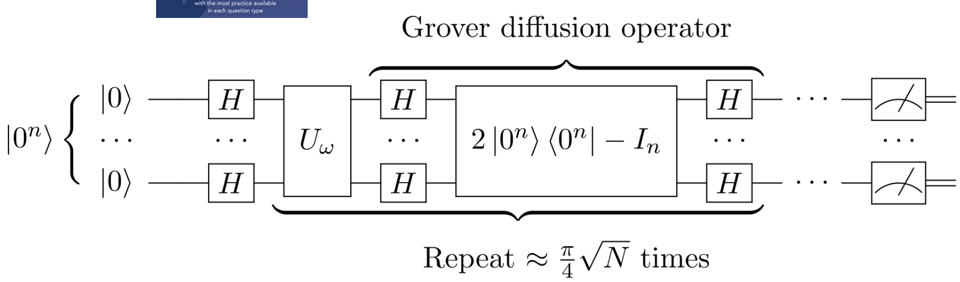
[1]**Hint:** hopefully, you found out that the answer in 1(b) is 'inflection points'. That means a point $P = (P_x, P_y)$ has order 3 iff $y''(P) = \dfrac{d^2y}{dx^2} = 0$. Find the second derivative using implicit differentiation of $y^2 = x^3 + ax + b$, the defining equation of E, twice. Then use the defining equation of E again to get rid of the y terms.

$t_1 = \dfrac{-6+4\sqrt{3}}{6} = \dfrac{-3+2\sqrt{3}}{3}$ is greater. Notice that the domain of E is $x \geq 0$, hence, the only possible value of the x- coordinate is $\sqrt{\dfrac{-3+2\sqrt{3}}{3}}$. The inflection points are

$$P_1 = \left(\sqrt{\frac{-3+2\sqrt{3}}{3}}, \frac{2\sqrt{-3+2\sqrt{3}}}{3}\right)$$
$$P_2 = \left(\sqrt{\frac{-3+2\sqrt{3}}{3}}, -\frac{2\sqrt{-3+2\sqrt{3}}}{3}\right).$$

Hover over Grover





Problem 3. Let r_x be the reflection with respect to the x-axis and r_ℓ the reflection with respect to a line ℓ. Denote the angle between the x-axis and line ℓ by α. Show that the composition $r_\ell \circ r_x$ is the counterclockwise rotation by 2α, while $r_x \circ r_\ell$ is the clockwise rotation by 2α.

Solution: the triangles vOP and $r_x(v)OP$ are equal (a shared side OP and equal sides $vP = r_x(v)P$ because r_x is a reflection together with the angle between these sides being $\frac{\pi}{2}$ in both triangles), implying equality of the angles $\angle POv$ and $\angle POr_x(v)$ (see Figure 1 below). Analogously one shows that the angles $\angle QOr_x(v)$ and $\angle QO(r_x \circ r_\ell(v))$ are equal as well. As $\angle POv + \angle POr_x(v) = \theta$, the assertion follows.

Problem 4. Let $N = 2^n$ and $\xi = H^{\otimes n}(|0\ldots 0\rangle) = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle$ be the generic superposition state. Consider any boolean function $f : \mathbb{B}^n \longrightarrow \mathbb{B}$. Denote the cardinality of the solution set of f by t, i.e. $t = \#\{x \in \mathbb{B}^n \mid f(x) = 1\}$. Let $|G\rangle = \frac{1}{\sqrt{t}}\sum_{i,f(i)=1}|i\rangle$ and $|B\rangle = \frac{1}{\sqrt{N-t}}\sum_{j,f(j)=0}|j\rangle$ be the generic superposition of 'good' (solution) and 'bad' (not solution) states, respectively.

(a) Show that the vectors $|G\rangle$ and $|B\rangle$ are orthogonal.

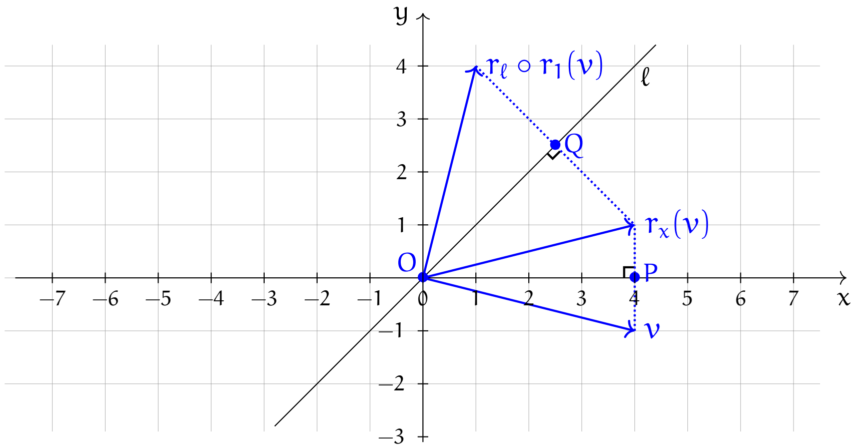


Figure 1: Composition of two reflections is a rotation

Solution: notice that $|G\rangle = \frac{1}{\sqrt{t}}(a_0, a_1, \ldots, a_{N-1})$ and $|B\rangle = \frac{1}{\sqrt{N-t}}(1-a_0, 1-a_1, \ldots, 1-a_{N-1})$ for some $a_i \in \mathbb{B}$, hence, either the i^{th} coordinate of $|G\rangle$ is zero or the i^{th} coordinate of $|B\rangle$ is zero for any $0 \le i \le N-1$ and the result follows.

(b) Compute the angle θ between $|B\rangle$ and $|\xi\rangle$ in the 2-dimensional real plane $\mathbb{R}\langle|G\rangle, |B\rangle\rangle$.[2]

Solution: as $(|B\rangle, |\xi\rangle) = ||B\rangle| \cdot ||\xi\rangle| \cdot \cos(\theta)$ and $||B\rangle| = ||\xi\rangle| = 1$ (unitary vectors), we get $\cos(\theta) = (|B\rangle, |\xi\rangle) = \frac{N-t}{\sqrt{N(N-t)}}$ (recall that $|\xi\rangle = \frac{1}{\sqrt{N}}(1, 1, \ldots, 1)$). As $\sin^2(\theta) = 1 - \cos^2(\theta) = 1 - \left(\sqrt{\frac{N-t}{N}}\right)^2 = 1 - \left(\sqrt{\frac{N-t}{N}}\right) = \frac{t}{N}$, we conclude that $\theta = \arcsin\left(\sqrt{\frac{t}{N}}\right)$.

(c) Use your result in (b) to show that $|\xi\rangle$ can be written as $|\xi\rangle = \sin(\theta)|G\rangle + \cos(\theta)|B\rangle$.

Solution: the projection of $|\xi\rangle$ on $|B\rangle$ is $\cos(\theta)$ and the projection of $|\xi\rangle$ on $|G\rangle$ is $\cos\left(\theta + \frac{\pi}{2}\right) = \sin(\theta)$, the assertion follows.

(d) Conclude that the Grover operator $\mathcal{G} := r_\xi \circ r_B$ rotates ξ by $2\arcsin\left(\sqrt{\frac{t}{N}}\right)$ towards $|G\rangle$ in the 2-dimensional real plane $\mathbb{R}\langle|G\rangle, |B\rangle\rangle$ (use the results in 1(b) and 3(b)).

Solution: if you have done (a) − (c), this is obvious :)

Definition 1. The Boolean **satisfiability (SAT) problem** asks whether there is at least one combination of binary input variables $x \in \mathbb{B}^n$ for which a Boolean logic formula holds. When this is the case, we say the formula is **satisfiable**.

Problem 5. Consider the four Teenage Mutant Ninja Turtles: Leonardo , Michelangelo , Raphael  and Donatello  and their sensei Splinter . Michelangelo  wants to throw a party, however, a recent ' incident' resulted in the following restrictions.

(1) If Leonardo  participates, Donatello  will come to the party only with sensei Splinter .

(2) Raphael  will join only together with Leonardo .

[2]**Hint:** use the dot product to find $\cos(\theta)$

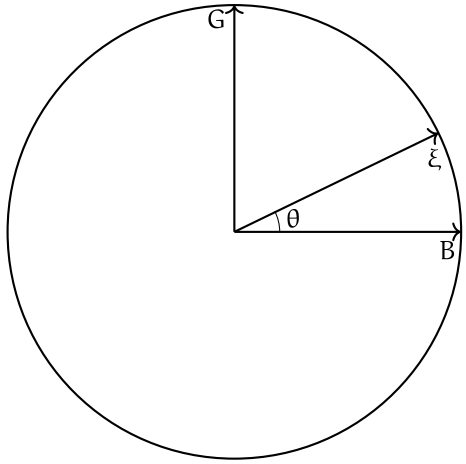


Figure 2: The $|B\rangle, |G\rangle$ and $|\xi\rangle$ states

(3) In turn, Leonardo  will take part only together with Raphael  and without Donatello .

(4) Sensei Splinter  doesn't like when the turtles quarrel, so he will join only if all turtles arrive.

(5) Finally, Michelangelo will cancel the party if no one shows up.
A character does join the party provided his restrictions are not violated.

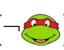
(a) Will the party take place? If 'yes', present possible collection(s) of participants, if 'no', give an explanation.

Solution: Michelangelo , Raphael , Leonardo 

(b) Find the smallest positive integer m for which the Grover operator maps ξ very close to G (use (a)). [3]

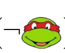
Solution: $\theta = \arcsin\left(\sqrt{\frac{t}{N}}\right) = \arcsin\left(\frac{1}{\sqrt{32}}\right)$ and $m \approx \frac{\pi}{4\theta} - \frac{1}{2} \approx 3.919$ (the closest integer is $\widetilde{m} = 4$).

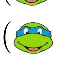
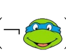
(c) Using the first letters of names to represent participation of corresponding character together with $\neg, \wedge, \vee$ logical operators, write the logical expressions for conditions $(1) - (5)$. For instance, (2) can be written as

$(R \wedge L) \vee (\neg R)$ or ( $\wedge$ ) $\vee$ ($\neg$ )

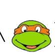
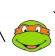
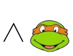
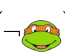
Solution:

(1) $\neg$ ( $\wedge$  $\wedge \neg$ )

(2) ( $\wedge$ ) $\vee$ ($\neg$ )

(3) ( $\wedge$  $\wedge \neg$ ) $\vee$ ($\neg$ )

(4) ( $\wedge$  $\wedge$  $\wedge$  $\wedge$ ) $\vee$ ($\neg$ )

(5) (( $\wedge$ ) $\vee$ ( $\wedge$ ) $\vee$ ( $\wedge$ ) $\vee$ ( $\wedge$ )) $\vee$ ($\neg$ )

[3] **Hint:** Ok, I have to confess that there are solutions:)

Problem 6. Let $f : \mathbb{B}^n \to \mathbb{B}$ be a function and suppose that the number of solutions, t, is known. Give a modification of Grover's algorithm, which finds all t solutions in $\mathcal{O}(t\sqrt{N})$ queries to database (recall that each application of Grover's operator $\mathcal{G}$ requires 1 query).

Solution: suppose that Grover's algorithm collapses to a solution state $|s_1\rangle$ with $s_1 \in \mathbb{B}^n$. Register this solution and consider the function $\widetilde{f}$ given by

$$\widetilde{f}(x) = \begin{cases} f(x), & x \neq s_1 \\ 0, & x = s_1. \end{cases}$$

Notice that the generic solution vectors of f and $\widetilde{f}$ satisfy the relation $\sqrt{t-1}G_{\widetilde{f}} = \sqrt{t}G_f - s_1$, while $\sqrt{N-t+1}B_{\widetilde{f}} = \sqrt{N-t}B_f + s_1$. Apply Grover's algorithm again, but this time with an oracle for $\widetilde{f}$...