MATH 1800: Quantum Information Theory with Applications to Cryptography

Final Exam
Review

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.

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

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

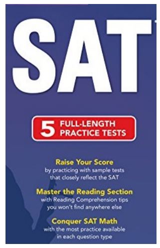
(a) How many points (elements) of order 2 can $G(E)$ have? (justify your answer)

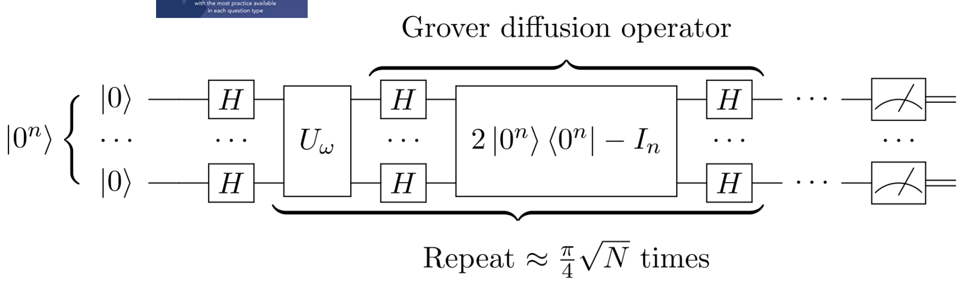
(b) Find the equation $\psi(x)$ that the x-coordinate of a point (element) satisfies if and only if it has order 3?[1] (justify your answer)

(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).

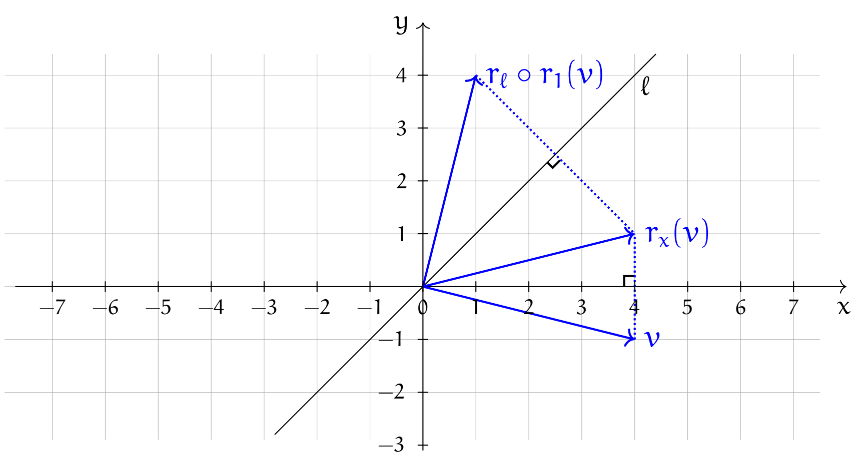
[1]**Hint:** hopefully, you found out that the answer in $1(b)$ is 'inflection points'. That means a point $P = (P_x, P_y)$ has order 3 iff $y''(P) = \frac{d^2y}{dx^2} = 0$. Find the second derivative using implicit differentiation of $y^2 = x^3 + ax + b$, the defining equation of E, twice. Then use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

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.



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 $f : \mathbb{B}^n \to \mathbb{B}$. Denote the cardinality of the solution set of f by t, i.e. $t = \#\{x \in \mathbb{B}^n \mid f(x) = 1\}$. Let $G = \frac{1}{\sqrt{t}} \sum_{i, f(i)=1} |i\rangle$ and $B = \frac{1}{\sqrt{N-t}} \sum_{j, f(j)=0} |j\rangle$ 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.

(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]

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

(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)).

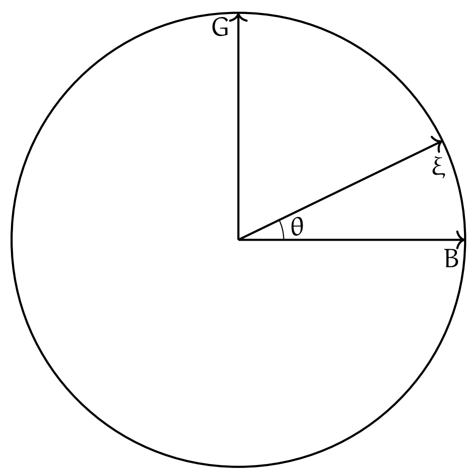


Figure 1: The $|B\rangle, |G\rangle$ and $|\xi\rangle$ states

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.

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

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

(2) Raphael  will join only together with Leonardo .

(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.

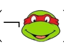
(5) Finally, Michelangelo will cancel the party if no one shows up.

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.

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

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

[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).