Problem Set #9

CMSC/Math 456
Instructor: Daniel Gottesman

Due on Gradscope, Thursday, Dec. 8, 11:59 PM

Problem #1. Different Generators for a Lattice (20 pts.)

For each part of this problem, you are given two sets of vectors, which are specified as row vectors so they look nicer as part of a sentence. Determine if those sets generate the same lattice. If not, say if one of them generates a sub-lattice of the other and which is which (i.e., all the points in one lattice are also points of the other lattice, but not vice-versa), or if neither lattice is a sub-lattice of the other.

a) (10 points) The first set of vectors is $\mathbf{v}_1 = (2, 0)$, $\mathbf{v}_2 = (0, 2)$. The second set of vectors is $\mathbf{w}_1 = (2, 2)$, $\mathbf{w}_2 = (2, -2)$.

b) (10 points) The first set of vectors is $\mathbf{v}_1 = (1, 2, 3)$, $\mathbf{v}_2 = (0, 1, -1)$, $\mathbf{v}_3 = (4, 0, 2)$. The second set of vectors is $\mathbf{w}_1 = (3, -3, 0)$, $\mathbf{w}_2 = (-3, 4, -1)$, $\mathbf{w}_3 = (-2, 4, 4)$.

Problem #2. Noise Level in LWE Encryption (40 pts.)

For this problem, consider the public-key encryption protocol discussed in class and in the textbook Sec. 14.3. For all parts, use $q = 6277$, which is prime. The matrix (A using the notation from class) is square, $n \times n$, with entries chosen to be independent uniformly random elements of $\mathbb{Z}_q$. The "small" n-dimensional vectors $\mathbf{e}$, $\mathbf{f}$, $\mathbf{r}$, and $\mathbf{s}$ and the "small" number x chosen during Gen and Enc are chosen so that their entries are independent random elements from the interval $[-a, a]$.

For a given value of n and the allowed probability of error in Dec, find the largest value of a that is consistent with those parameters. (Larger noise levels means greater security, so you want the largest value that allows reliable decoding.) You may use numerical methods (i.e., programming) or analytic methods (such as statistics) to answer these questions. If you do write some code, you may use any language but do not use any existing libraries containing LWE implementations. Please attach your code to your answers. If you use analytic methods, explain them.

The answers to this problem don't need to be perfectly precise, but should be within 20% of the true answers.

a) (10 points) $n = 10$, zero probability of error

b) (10 points) $n = 100$, zero probability of error

c) (10 points) $n = 10$, 5% chance of error

d) (10 points) $n = 100$, 5% chance of error