MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Lightweight Introduction to Lattices – Part 2

Author: M. Dimitrov, B. Esslinger

June 2020

Introduction (1/5)

This challenge series accompanies the basic theory from a chapter called "LIGHTWEIGHT INTRODUCTION TO LATTICES". The chapter is part of the CrypTool Book [1].

Some lattice-based cryptography schemes are secure against quantum computers. Therefore, these constructions are relevant for current post-quantum cryptography research.

This challenge uses vectors to hide a famous quote in modern art. Can you reveal it?

Introduction (2/5)

We can represent a system of linear equations by a product of matrices. Let's consider the following system of equations:

$$\begin{cases} x + 9y + 3z = 61 \\ 2x + 4y + 8z = 94 \\ 5x + 7y + 6z = 128 \end{cases}$$

We can transfer the same system of equations into a product of matrices:

$$\begin{pmatrix} 1 & 9 & 3 \\ 2 & 4 & 8 \\ 5 & 7 & 6 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 61 \\ 94 \\ 128 \end{pmatrix}$$

Introduction (3/7)

We can further automate this process by using *SageMath* [2]:

```
sage: M = matrix([[1,9,3], [2,4,8], [5,7,6]])
sage: r = matrix([[61],[94],[128]])
sage: M.solve_right(r)
```

Which yields the final solutions $x = 13$, $y = 3$, and $z = 7$.

Introduction (4/5)

A matrix is arranged in rows and columns. The matrix M here is a 3×3-matrix, since it has 3 rows and 3 columns, and the matrix r is a 1×3 matrix, since is has 1 row and 3 columns. Furthermore, r can be viewed as a vector, since it consists of only 1 row.

Definition A directed line from the point $P(x_1, x_2)$ to the point $Q(y_1, y_2)$ is a **vector** with the following components:

$$\overrightarrow{PQ} = \overrightarrow{OS} = (s_1, s_2) = (y_1 - x_1, y_2 - x_2)$$

The starting point of the vector $\overrightarrow{OP} = (x_1, x_2)$ is at the origin $O = (0, 0)$ and the end point is $P = (x_1, x_2)$.

Introduction (5/7)

Let's express the vectors $\overrightarrow{PQ}$ and $\overrightarrow{RQ}$ having the three points $P(0, 1)$, $Q(2, 2)$ and $R(1.5, 1.5)$ with the use of *SageMath*:

```
sage: vOP = vector([0,1])
sage: vOQ = vector([2,2])
sage: vOR = vector([1.5,1.5])
sage: vPQ = vOQ - vOP
sage: vRQ = vOQ - vOR
sage: print(vPQ, vRQ)
(2,1) (0.5, 0.5)
```

Introduction (6/7)

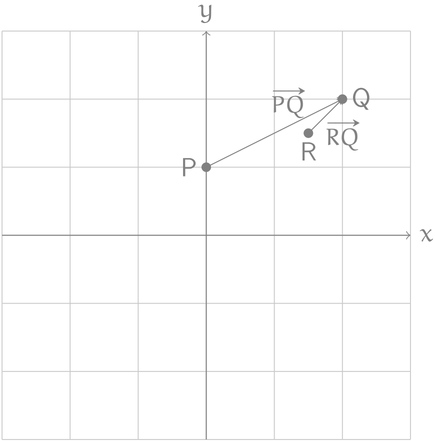

Figure: Finding vectors

Introduction (7/7)

Addition of vectors, multiplication of a scalar with a vector

For any two vectors $x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$, $y = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$ in $\mathbb{R}^2$ and a scalar k,

the sum of $x + y$ and the product kx are defined as follows:

$$x + y = \begin{bmatrix} x_1 + y_1 \\ x_2 + y_2 \end{bmatrix} \text{ and } kx = \begin{bmatrix} kx_1 \\ kx_2 \end{bmatrix}$$

.

Challenge (1/2)

Can you find the famous (English) quote hidden in the puzzle challenge in the figure of the following slide? Please hand in the solution without spaces.

Hint: ASCII (American Standard Code for Information Interchange) is involved.

Challenge (2/2)

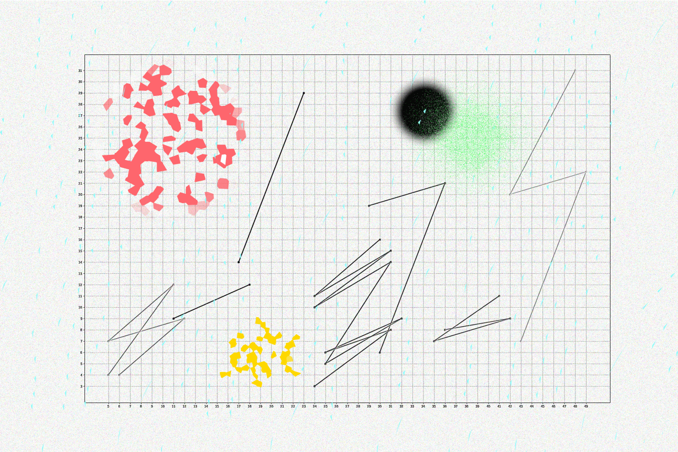

Figure: Puzzle Challenge

References

1. The CrypTool Book, Chapter 12.
   https://www.cryptool.org/en/ctp-documentation/ctbook

2. SageMath can either be downloaded or used online.
   - Download SageMath: https://www.sagemath.org/
   - SageMathCell: https://sagecell.sagemath.org/
   - CoCalc: https://cocalc.com/