**Cesar Leonardo Canales Rivera Grupo 01 Andrés Alberto Aristizábal**

**Carlos Andrés Restrepo Marín Grupo 01 Andrés Alberto Aristizábal**

**Luis Felipe Sánchez Vega Grupo 03 Juan Manuel Reyes**

**Engineering design**

**Phase 1. Identification of the problem**

Venus and Mars have been at war for the last 4 years. In the current year, Venus wants to win the war decisively, to do so they want to predict the positions of Mars’ fleet, having in mind that they archive the positions of past battles.

Identification of necessities and symptoms

* It’s required to multiply matrices.
* Venus’ troops don’t have a way of predicting the exact location of the enemy’s fleet.
* The found location has to be expressed in terms of x and y coordinates.
* The solution to the problem has to be efficient so that Venus can make decisions on time.

Definition of the problem

Venus requires the development of a software that allows them to visualize in a matrix the locations of the ships of the enemy.

The software will have the following functionalities:

1. A graphical interface that allows the user to input the values of the number of rows and columns of the past battle board.
2. A graphical interface that allows the user to input whether the values generated randomly will have repeats or not.
3. A graphical interface that shows the positions of the Martians in the current battle.
4. A graphical interface that allows to generate n matrices that are to be multiplied.

**Phase 2. Recompilation of information**

Matrix: In mathematics, a matrix (plural: matrices) is a rectangular array of numbers, symbols, or expressions, arranged in rows and columns.

Matrix Multiplication: Multiplication of two matrices is defined if and only if the number of columns of the left matrix is the same as the number of rows of the right matrix. If A is an m-by-n matrix and B is an n-by-p matrix, then their matrix product AB is the m-by-p matrix whose entries are given by the dot product of the corresponding row of A and the corresponding column of B.

Formally, the definition of matrix multiplication is that if *C* = *AB* for an *n* × *m* matrix *A* and an *m* × *p* matrix *B*, then *C* is an *n* × *p* matrix with entries



Dot product: In mathematics, the dot product or scalar product is an algebraic operation that takes two equal-length sequences of numbers (usually coordinate vectors) and returns a single number. Algebraically, the dot product is the sum of the products of the corresponding entries of the two sequences of numbers.

Prime number: A prime number (or a prime) is a natural number greater than 1 that cannot be formed by multiplying two smaller natural numbers.

**Phase 3. Looking for creative solutions**

In order to multiply matrices we are considering different algorithms that have proven to do so with matrices of different dimensions. The algorithms to consider are the following:

1. Iterative algorithm: This is the brute force approach which applies the definition of matrix multiplication explained above, applying each dot product and adding the result to each position of the resulting matrix.

Assuming the two input matrices can be multiplied, this algorithm works both for square matrices (matrices with the same number of columns and rows) and for matrices that are not square.

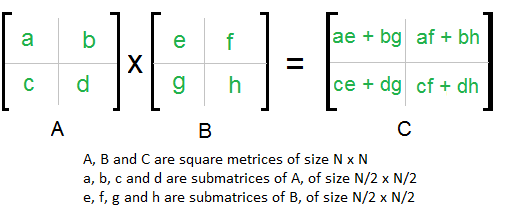
1. Divide and conquer algorithm: This algorithm uses the divide and conquer paradigm which is basically breaking a problem down into two or more subproblems of the same type, until these become simple enough to be solved directly.

All the solutions to the subproblems are then combined to give solution to the original problem.

For the matrix multiplication problem, we can use a divide and conquer approach. Let A and B be two matrices of size N x N we want to multiply and C the result of their multiplication



The algorithm divides A and B in 4 submatrices of size N/2 x N/2 and then calculates the following values recursively: ae + bg, af + bh, ce + dg and cf + dh.

¹

This algorithm works for all square matrices whose dimensions are powers of two, that is, the shapes are 2*n* × 2*n* for some *n*. Matrices that have dimensions that don’t meet the criteria mentioned above can be filled , or padded with zeros until they do.

Using the block matrix identity

²

Here A,B are n×n matrices, and the big matrices are N×N for some N>n. In other words, we add N−n rows and N−n columns of zeroes.

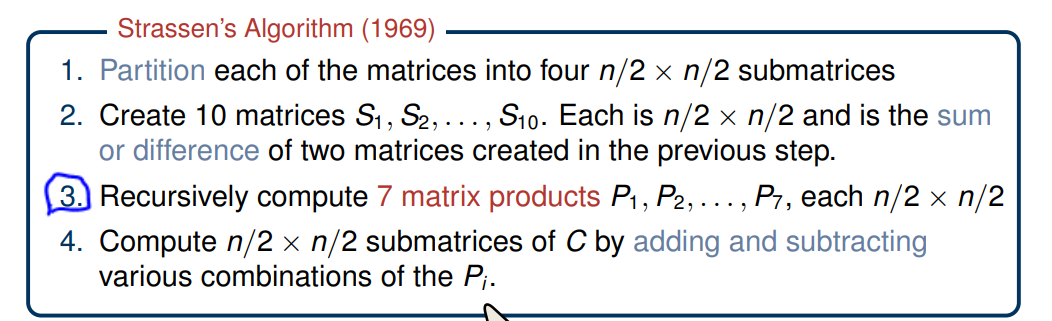
This can be done in two ways:

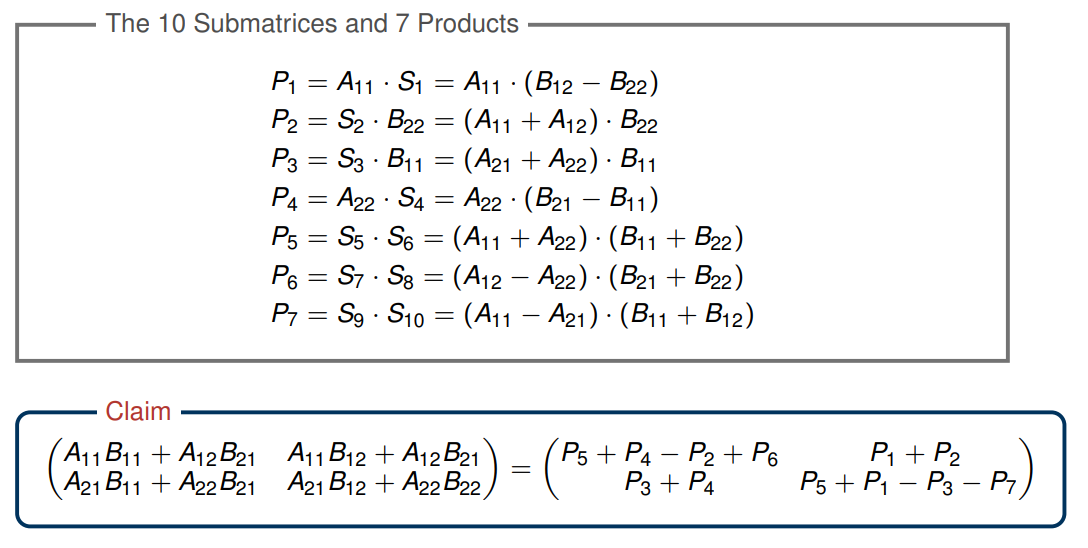
* Pad the original n×n matrices to N×N matrices, where N is the closest power of 2. Note that N<2n, so this doesn't affect the asymptotic complexity.
* Pad the matrices recursively. Whenever a recursive call gets m×m matrices with m>1 odd, we pad them to (m+1)×(m+1) matrices by adding a single row and a single column of zeroes. This also doesn't affect the asymptotic complexity.

Formally, the divide and conquer algorithm consists of eight multiplications of pairs of submatrices, followed by an addition step. The divide and conquer algorithm computes the smaller multiplications recursively, using the scalar multiplication *c*11 = *a*11*b*11 as it’s base case.

A variant of this algorithm that works for matrices of arbitrary shapes and is faster in practice splits matrices in two instead of four submatrices, as follows. Splitting a matrix now means dividing it into two parts of equal size, or as close to equal sizes as possible in the case of odd dimensions.

1. Strassen algorithm: The goal of Strassen’s algorithm is to reduce the number of multiplications in the divide and conquer algorithm. It does so by performing only 7 recursive multiplications of N/2 x N/2 matrices.

³



We iterate this division process *n* times (recursively) until the submatrices degenerate into numbers.

1. Coppersmith-Winograd algorithm: The current *O*(*nk*) algorithm with the lowest known exponent *k* is a generalization of the Coppersmith–Winograd algorithm that has an asymptotic complexity of *O*(*n*2.3728639), by François Le Gall. The Le Gall algorithm, and the Coppersmith–Winograd algorithm on which it is based, are similar to Strassen's algorithm: a way is devised for multiplying two *k* × *k*-matrices with fewer than *k*3 multiplications, and this technique is applied recursively. However, the constant coefficient hidden by the Big O notation is so large that these algorithms are only worthwhile for matrices that are too large to handle on present-day computers.

Another problem we are dealing with is to find prime numbers, some useful algorithms to find prime numbers are the following:

1. Sieve of Eratosthenes: In mathematics, the **Sieve of Eratosthenes** is a simple, ancient algorithm for finding all prime numbers up to any given limit.

It does so by iteratively marking as composite (i.e., not prime) the multiples of each prime, starting with the first prime number, 2. The multiples of a given prime are generated as a sequence of numbers starting from that prime, with constant difference between them that is equal to that prime. This is the sieve's key distinction from using trial division to sequentially test each candidate number for divisibility by each prime.

1. Sieve of Atkins: It’s a modern algorithm for finding all prime numbers up to a specified integer. Compared with the ancient sieve of Eratosthenes, which marks off multiples of primes, the sieve of Atkin does some preliminary work and then marks off multiples of squares of primes, thus achieving a better theoretical asymptotic complexity.

**Phase 4. Transition from ideas to preliminary designs**

Firstly, we’ll mention that we won’t be using the Coppersmith-Winograd algorithm due to its constant factor being to big for small matrices , this renders the algorithm unsuitable for this project.

Revising the other alternatives for the matrix multiplication problem we get:

Iterative algorithm

* Works both for square matrices and not square matrices providing an accurate result every time.
* For large enough matrices, the time it takes grows too fast making this algorithm less efficient.
* This algorithm suggests that arithmetic operations are necessary putting this algorithm at an Θ(*n*3) time complexity.

Divide and conquer algorithm:

* Has one variant for square matrices and another that works in matrices of arbitrary shape that is faster in practice.
* Although the complexity of this algorithm as a function of n is

T(n) = 8T(n/2) + Θ(*n*2), Application of the master theorem for divide-and-conquer recurrences shows this recursion to have the solution Θ(*n*3), the same as the iterative algorithm, also making it less efficient.

Strassen algorithm

* Has reduced execution time in comparison to the other algorithms because it uses a clever mathematical deduction.
* Works for square matrices whose dimensions are powers of two, for matrices that don’t meet this criteria the solution is to pad the matrices with zeros, using the block matrix identity.
* Practical implementations of Strassen's algorithm switch to standard methods of matrix multiplication for small enough submatrices, for which those algorithms are more efficient.
* The asymptotic complexity for multiplying matrices of size N = 2*n* using the Strassen algorithm is O(N*2.8074*)

For the prime finding problem, we revise the next alternative:

Sieve of Eratosthenes

* A number is prime, if none of the smaller prime numbers divides it. Since we iterate over the prime numbers in order, we already marked all numbers, who are divisible by at least one of the prime numbers, as divisible. Hence if we reach a cell and it is not marked, then it isn't divisible by any smaller prime number and therefore has to be prime.
* Sieve of Eratosthenes is an algorithm for finding all the prime numbers in a segment [1;n] using O(nlog⁡log⁡n) operations which is incredibly fast making us able to find primes up to 10 to the 8th power very quickly.
* The biggest weakness of the algorithm is that it “walks” along the memory multiple times, only manipulating single elements. This is not very cache friendly. And because of that, the constant which is concealed in O(nlog⁡log⁡n) is comparably big.
* Despite this, there are plenty of optimizations to reduce the memory problem.

Sieve of Atkins

* This algorithm uses different results of applying modulo of certain numbers, equations and the concept of squarefree to determine whether a number is prime or not.

<https://cp-algorithms.com/algebra/sieve-of-eratosthenes.html>

**Phase 5. Evaluation and selection of solutions**

**Criteria**

Considering the options that remain after going through phase three and four, the following criteria has been proposed in order to choose the best solution. The greater the total score, the higher rated the algorithm will be.

* Criteria A. Efficiency, a fundamental requirement is that the matrix multiplication has to be executed quickly. The complexity of the solution is:
* [3] logarithmic complexity
* [2] less than cubic complexity
* [1] cubic complexity
* Criteria B. Completeness, the solution gives a correct output for any two matrices that can be multiplied. The solution gives a correct result for:
* [2] any pair of matrices
* [1]some specific cases
* Criteria C. Ease of implementation
* [2] the solution can be easily implemented in the programming language
* [1] the implementation of the solution may require more advanced techniques

**Evaluation**

Taking into account the criteria established above, we will carry out the evaluation of the solutions

*For matrix multiplication:*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Solution | Criteria A | Criteria B | Criteria C | Total |
| Solution 1. Iterative algorithm | 1 | 1 | 2 | 4 |
| Solution 2. .Divide and conquer algorithm | 1 | 1 | 2 | 4 |
| Solution 3. Strassen algorithm | 1 | 2 | 2 | 5 |

*For finding prime numbers:*

For the evaluation of these solutions we will only consider criteria A and C.

|  |  |  |  |
| --- | --- | --- | --- |
| Solution | Criteria A | Criteria C | Total |
| Solution A. Sieve of Eratosthenes | 3 | 2 | 5 |
| Solution B. Sieve of Atkins | 3 | 1 | 4 |

**Selection**

The requirements that were assigned indicate that three algorithms should be used to solve the problem of matrix multiplication, given this condition, the three remaining solutions will be implemented. Although it should be mentioned that the third solution (Strassen algorithm) is the best among all of them.

As for the problem of finding prime numbers, according to the evaluation, the best solution is the solution A(Sieve of Eratosthenes). This was chosen mainly because its implementation is already known and it is not too complicated.