Chapter 5

Reserves Recitation.

5.1

Another sorting algorithms, that it's correctness isn't so obivoius.

```
   Result: returns the multiplication x · y where x, y ∈ F_2^n
1  for i ∈ [n] do
2  |  for j ∈ [n] do
3  |  |  if A_j < A_i then
4  |  |  |  swap A_i ↔ A_j
5  |  |  end
6  |  end
7  end
```

Claim 5.1.1. *After the ith iteration, $A_1 \leq A_2 \leq A_3 .. \leq A_i$ and A_i is the maximum of the whole array.*

Proof. By induction on the iteration number i.

1. Base. For $i = 1$, it is clear that when j reaches the position of the maximal element, an exchange will occur and A_1 will be set to be the maximal element. Thus, the condition on line (3) will not be satisfied until the end of the inner loop and indeed, we have that A_1 at the end of the first iteration is the maximum.

2. Assumption. Assume the correctness of the claim for any $i' < i$.

3. Step. Consider the ith iteration. And observes that if $A_i = A_{i-1}$ then A_i is also the maximal elememnt in A, namely no exchange will be made in ith iteration, yet $A_1 \leq A_2 \leq .. \leq A_{i-1}$ by the induction assumption, thus $A_1 \leq A_2 \leq .. \leq A_{i-1} \leq A_i$ and A_i is the maximal element, so the claim holds in the end of the iteration. If $A_i < A_{i-1}$ then there exists $k \in [1, i-1]$ such $A_k > A_i$. Set k to be the minimal position for which the inequlity holds. For Convinet denote by $A^{(j)}$ the array in the begging of the jth iteration of the inner loop. And let's split to cases according to j value.

   (a) $j < k$

(b) $j \geq k$

(c) $j > i - 1$

¡++¿

$\square$

Result: returns the multiplication $x \cdot y$ where $x, y \in \mathbb{F}_2^n$

if $x, y \in \mathbb{F}_2$ **then**
    return $x \cdot y$
end

else
    define $x_l, x_r \leftarrow x$ and $y_l, y_r \leftarrow x$ // $O(n)$.

    calculate $z_0 \leftarrow \text{Karatsuba}(x_l, y_l)$
            $z_2 \leftarrow \text{Karatsuba}(x_r, y_r)$
            $z_1 \leftarrow \text{Karatsuba}(x_r + x_l, y_l + y_r) - z_0 - z_2$

    return $z_0 + 2^{\frac{n}{2}} z_1 + 2^n z_2$ // $O(n)$.
end