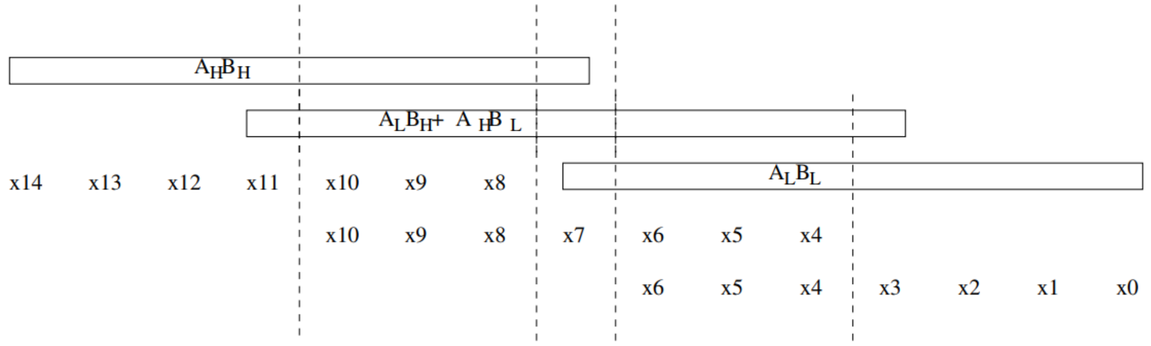
Question 1: In this question we shall explore this overlap-free Karatsuba multiplier. We shall mainly focus on multiplications in $GF(2)[x]$ here, i.e for $A = \sum_{i=0}^{n-1} a_i x^i$ and $B = \sum_{i=0}^{n-1} b_i x^i$ we shall compute AB. In standard Karatsuba the recursive formula for AB is:

$A_H B_H x^{2m} + \{[(A_H + A_L)(B_H + B_L)] - [A_H B_H + A_L B_L]\}x^m + A_L B_L$



where $m = n/2$. More specifically we divide the polynomial A and B in "most significant half" and "less significant half" as: $A = x^m A_H + A_L$ and so for B. Apart from the XOR delays for the components within the {} (which requires delay of 2 XOR computation) we have another XOR gate delay for adding the overlapped coefficients of the partial products. For example, if $m = 4$ and $n = 8$, the overlap can be represented as shown in Fig. 1. In overlap-free Karatsuba multiplication we try to get rid of these XOR gate delay corresponding to the overlaps. Your task is to find an expression for overlap-free Karatsuba multiplier.

Question 2. Let $A \in GF(q^m)^*$ and $r = (q^m - 1)/(q - 1)$. Here, $GF(q^m)^*$ is a subgroup of $GF(q^m)$ and $A - 1$ denotes the multiplicative inverse of A. Prove that $A^{-1} = (A^r)^{-1} \cdot A^{r-1}$.