Multiplication in F[x] using the FFT

Input $a, b \in F[x]$ where $a = \sum_{i=0}^{d} a_i x^i$ and $b = \sum_{i=0}^{m} b_i x^i$.
Output $c = a \times b = \sum_{i=0}^{d+m} c_i x^i \in F[x]$.

1 Pick smallest $n = 2^k > d + m$.
Find $\omega \in F$ with $\omega^n = 1$ and $\omega^i \neq 1$ for $1 \leq i < n$.

Idea: interpolate $c(x)$ from $[\ c(\omega^i) = a(\omega^i) b(\omega^i)\ :\ 0 \leq i < n\ ]$.

2 Compute $W = [\omega^i : 0 \leq i < n/2]$.

3 FFT ($n, W, A = [a_0, a_1, \ldots, a_d, 0, \ldots, 0]$) # $A = [a(1), a(\omega), \ldots, a(\omega^{n-1})]$

FFT ($n, W, B = [b_0, b_1, \ldots, b_m, 0, \ldots, 0]$) # $B = [b(1), b(\omega), \ldots, b(\omega^{n-1})]$

4 Compute $C = [\ A_i \times B_i\ :\ 0 \leq i < n\ ]$ # $C = [c(1), c(\omega), \ldots, c(\omega^{n-1})]$

5 Compute $W = [\omega^{-i}\ :\ 0 \leq i < n/2]$.

FFT (n, W, C) # $C = n[c_0, c_1, \ldots, c_{d+m}, 0, \ldots, 0]$

6 Return $\sum_{i=0}^{d+m} \frac{1}{n} C_i x^i \in F[x]$

Cost