University of Freiburg
Dept. of Computer Science
Prof. Dr. F. Kuhn
S. Faour, M. Fuchs, A. Malyusz

Algorithm Theory
Sample Solution Exercise Sheet 2

Due: Friday, 3rd of November 2023, 10:00 am

Exercise 1: Faster Polynomial Multiplication *(14 Points)*

Let $p(x) := -3x^2 + x + 6$ and $q(x) := 2x^2 + 4$. The goal is to compute $p(x) \cdot q(x)$ with the help of the FFT algorithm. Please, make use of the following sketch:

1. Illustrate the **divide** procedure of the algorithm (for both functions p and q). More precisely, for the i-th divide step (with focus on $p(x)$), write down all the polynomials p_{ij} for $j \in \{0, ..., 2^i - 1\}$ that you obtain from further dividing the polynomials from the previous divide step $i - 1$ (we define $p_{00} := p$, and the first split is into p_{10} and p_{11} and so on...).

2. Illustrate the **combine** procedure of the algorithm (for both functions p and q). That is, starting with the polynomials of the smallest degree as base cases, compute the DFT of p_{ij} (respectively q_{ij}) bottom up with the recursive formula given in the lecture. The recursion stops when $DFT_8(p_{00})$ (respectively $DFT_8(q_{00})$) is computed i.e., we know the function's values at the (8-th) roots of unity.

3. **Multiply** the polynomials. More specific, give the point value representation of $p(x) \cdot q(x)$, i.e., $(w_8^0, y_0), (w_8^1, y_1), \ldots, (w_8^7, y_7)$.

4. Use the **inverse** DFT procedure from the lecture to get the final coefficients for $p(x) \cdot q(x)$. To do that efficiently, first compute the $DFT_8(f)$ where $f(x) := y_0 + y_1 \cdot x + ... + y_7 \cdot x^7$ and then compute the coefficients a_k for $k \in \{0, 1, ..., 7\}$ of $p(x) \cdot q(x)$ (using that $a_k = 1/8 \cdot f(w_8^{-k})$).

Write down all intermediate results to get partial points in the case of a typo.

Sample Solution

1. Note that for the divide step we want to preserve that $p(x) = p_0(x^2) + x \cdot p_1(x^2)$ where p_0 contains the even coefficients and p_1 the odds.
   divide p:

$$
\begin{aligned}
p_{00} &= -3x^2 + x + 6 \\
p_{10} &= -3x + 6 \\
p_{11} &= 1 \\
p_{20} &= 6 \\
p_{21} &= -3 \\
p_{22} &= 1 \\
p_{23} &= 0
\end{aligned}
$$

divide q:

$$
\begin{aligned}
q_{00} &= 2x^2 + 4 \\
q_{10} &= 2x + 4 \\
q_{11} &= 0 \\
q_{20} &= 4 \\
q_{21} &= 2 \\
q_{22} &= 0 \\
q_{23} &= 0
\end{aligned}
$$

2. In the combine step we compute the required values in a bottom-up fashion using the following formula from the lecture:

$$
p(w_N^k) := \begin{cases} p_0\left(w_{N/2}^k\right) + w_N^k \cdot p_1\left(w_{N/2}^k\right) & \text{if } k < N/2 \\ p_0\left(w_{N/2}^{k-N/2}\right) + w_N^k \cdot p_1\left(w_{N/2}^{k-N/2}\right) & \text{if } k \geq N/2 \end{cases}
$$

combine p:

$$
\begin{aligned}
p_{10}(w_4^0) &= p_{20}(w_2^0) + w_4^0 \cdot p_{21}(w_2^0) = 6 + 1 \cdot (-3) = 3 \\
p_{10}(w_4^1) &= p_{20}(w_2^1) + w_4^1 \cdot p_{21}(w_2^1) = 6 + i \cdot (-3) = 6 - 3i \\
p_{10}(w_4^2) &= p_{20}(w_2^0) + w_4^2 \cdot p_{21}(w_2^0) = 6 - 1 \cdot (-3) = 9 \\
p_{10}(w_4^3) &= p_{20}(w_2^1) + w_4^3 \cdot p_{21}(w_2^1) = 6 - i \cdot (-3) = 6 + 3i
\end{aligned}
$$

$$
\begin{aligned}
p_{11}(w_4^0) &= p_{22}(w_2^0) + w_4^0 \cdot p_{23}(w_2^0) = 1 \\
p_{11}(w_4^1) &= p_{22}(w_2^1) + w_4^1 \cdot p_{23}(w_2^1) = 1 \\
p_{11}(w_4^2) &= p_{22}(w_2^0) + w_4^2 \cdot p_{23}(w_2^0) = 1 \\
p_{11}(w_4^3) &= p_{22}(w_2^1) + w_4^3 \cdot p_{23}(w_2^1) = 1
\end{aligned}
$$

Now we can go to the next recursion level. Note that we have $w_8^0 = 1$, $w_8^1 = \frac{1+i}{\sqrt{2}}$, $w_8^2 = i$, $w_8^3 = \frac{-1+i}{\sqrt{2}}$, $w_8^4 = -1$, $w_8^5 = -w_8^1$, $w_8^6 = -i$, $w_8^7 = -w_3^8$.

$$
\begin{aligned}
p_{00}(w_8^0) &= p_{10}(w_4^0) + w_8^0 \cdot p_{11}(w_4^0) = 3 + 1 = 4 \\
p_{00}(w_8^1) &= p_{10}(w_4^1) + w_8^1 \cdot p_{11}(w_4^1) = 6 - 3i + \frac{1+i}{\sqrt{2}} = 6 + \frac{1}{\sqrt{2}} + \left(-3 + \frac{1}{\sqrt{2}}\right) \cdot i \\
p_{00}(w_8^2) &= p_{10}(w_4^2) + w_8^2 \cdot p_{11}(w_4^2) = 9 + i \cdot 1 = 9 + i \\
p_{00}(w_8^3) &= p_{10}(w_4^3) + w_8^3 \cdot p_{11}(w_4^3) = 6 + 3i + \frac{-1+i}{\sqrt{2}} = 6 - \frac{1}{\sqrt{2}} + \left(3 + \frac{1}{\sqrt{2}}\right) \cdot i \\
p_{00}(w_8^4) &= p_{10}(w_4^0) - w_8^0 \cdot p_{11}(w_4^0) = 3 - 1 = 2 \\
p_{00}(w_8^5) &= p_{10}(w_4^1) - w_8^1 \cdot p_{11}(w_4^1) = 6 - 3i - \frac{1+i}{\sqrt{2}} = 6 - \frac{1}{\sqrt{2}} + \left(-3 - \frac{1}{\sqrt{2}}\right) \cdot i \\
p_{00}(w_8^6) &= p_{10}(w_4^2) - w_8^2 \cdot p_{11}(w_4^2) = 9 - i \\
p_{00}(w_8^7) &= p_{10}(w_4^3) - w_8^3 \cdot p_{11}(w_4^3) = 6 + 3i - \frac{-1+i}{\sqrt{2}} = 6 + \frac{1}{\sqrt{2}} + \left(3 - \frac{1}{\sqrt{2}}\right) \cdot i
\end{aligned}
$$

combine q:

$$q_{10}(w_4^0) = q_{20}(w_2^0) + w_4^0 \cdot q_{21}(w_2^0) = 4 + 1 \cdot 2 = 6$$
$$q_{10}(w_4^1) = q_{20}(w_2^1) + w_4^1 \cdot q_{21}(w_2^1) = 4 + i \cdot 2 = 4 + 2i$$
$$q_{10}(w_4^2) = q_{20}(w_2^0) + w_4^2 \cdot q_{21}(w_2^0) = 4 - 1 \cdot 2 = 2$$
$$q_{10}(w_4^3) = q_{20}(w_2^1) + w_4^3 \cdot q_{21}(w_2^1) = 4 - i \cdot 2 = 4 - 2i$$

$$q_{11}(w_4^0) = q_{22}(w_2^0) + w_4^0 \cdot q_{23}(w_2^0) = 0$$
$$q_{11}(w_4^1) = q_{22}(w_2^1) + w_4^1 \cdot q_{23}(w_2^1) = 0$$
$$q_{11}(w_4^2) = q_{22}(w_2^0) + w_4^2 \cdot q_{23}(w_2^0) = 0$$
$$q_{11}(w_4^3) = q_{22}(w_2^1) + w_4^3 \cdot q_{23}(w_2^1) = 0$$

$$q_{00}(w_8^0) = q_{10}(w_4^0) + w_8^0 \cdot q_{11}(w_4^0) = 6$$
$$q_{00}(w_8^1) = q_{10}(w_4^1) + w_8^1 \cdot q_{11}(w_4^1) = 4 + 2i$$
$$q_{00}(w_8^2) = q_{10}(w_4^2) + w_8^2 \cdot q_{11}(w_4^2) = 2$$
$$q_{00}(w_8^3) = q_{10}(w_4^3) + w_8^3 \cdot q_{11}(w_4^3) = 4 - 2i$$
$$q_{00}(w_8^4) = q_{10}(w_4^0) - w_8^0 \cdot q_{11}(w_4^0) = 6$$
$$q_{00}(w_8^5) = q_{10}(w_4^1) - w_8^1 \cdot q_{11}(w_4^1) = 4 + 2i$$
$$q_{00}(w_8^6) = q_{10}(w_4^2) - w_8^2 \cdot q_{11}(w_4^2) = 2$$
$$q_{00}(w_8^7) = q_{10}(w_4^3) - w_8^3 \cdot q_{11}(w_4^3) = 4 - 2i$$

3. **Multiply:**

$$p_{00}(w_8^0) \cdot q_{00}(w_8^0) = 4 \cdot 6 = 24$$
$$p_{00}(w_8^1) \cdot q_{00}(w_8^1) = \left(6 + \frac{1}{\sqrt{2}} + \left(-3 + \frac{1}{\sqrt{2}}\right) \cdot i\right)(4 + 2i) = 30 + \sqrt{2} + 3\sqrt{2} \cdot i$$
$$p_{00}(w_8^2) \cdot q_{00}(w_8^2) = (9 + i) \cdot 2 = 18 + 2i$$
$$p_{00}(w_8^3) \cdot q_{00}(w_8^3) = \left(6 - \frac{1}{\sqrt{2}} + \left(3 + \frac{1}{\sqrt{2}}\right) \cdot i\right) \cdot (4 - 2i) = 30 - \sqrt{2} + 3\sqrt{2} \cdot i$$
$$p_{00}(w_8^4) \cdot q_{00}(w_8^4) = 2 \cdot 6 = 12$$
$$p_{00}(w_8^5) \cdot q_{00}(w_8^5) = \left(6 - \frac{1}{\sqrt{2}} + \left(-3 - \frac{1}{\sqrt{2}}\right) \cdot i\right) \cdot (4 + 2i) = 30 - \sqrt{2} - 3\sqrt{2} \cdot i$$
$$p_{00}(w_8^6) \cdot q_{00}(w_8^6) = (9 - i) \cdot 2 = 18 - 2i$$
$$p_{00}(w_8^7) \cdot q_{00}(w_8^7) = \left(6 + \frac{1}{\sqrt{2}} + \left(3 - \frac{1}{\sqrt{2}}\right) \cdot i\right) \cdot (4 - 2i) = 30 + \sqrt{2} - 3\sqrt{2} \cdot i$$

Thus, $p(x) \cdot q(x)$ has the following point value representation

$$(w_8^0, 24),$$
$$(w_8^1, 30 + \sqrt{2} + 3\sqrt{2} \cdot i),$$
$$(w_8^2, 18 + 2i),$$
$$(w_8^3, 30 - \sqrt{2} + 3\sqrt{2} \cdot i),$$
$$(w_8^4, 12),$$
$$(w_8^5, 30 - \sqrt{2} - 3\sqrt{2} \cdot i),$$
$$(w_8^6, 18 - 2i),$$
$$(w_8^7, 30 + \sqrt{2} - 3\sqrt{2} \cdot i)$$

4. **Inverse DFT:** To efficiently compute the inverse DFT, we again have to do some bottom-up computation, now based on the polynomial $f(x) := y_7x^7 + y_6x^6 + ... + y_0$, where the y_i values are the y-values in the point value representation of $p(x) \cdot q(x)$.

$$
\begin{aligned}
f_{00} &= f \\
f_{10} &= y_6x^3 + y_4x^2 + y_2x + y_0 \\
f_{11} &= y_7x^3 + y_5x^2 + y_3x + y_1 \\
f_{20} &= y_4x + y_0 \\
f_{21} &= y_6x + y_2 \\
f_{22} &= y_5x + y_1 \\
f_{23} &= y_7x + y_3 \\
f_{30} &= y_0 = 24 \\
f_{31} &= y_4 = 12 \\
f_{32} &= y_2 = 18 + 2i \\
f_{33} &= y_6 = 18 - 2i \\
f_{34} &= y_1 = 30 + \sqrt{2} + 3\sqrt{2} \cdot i \\
f_{35} &= y_5 = 30 - \sqrt{2} - 3\sqrt{2} \cdot i \\
f_{36} &= y_3 = 30 - \sqrt{2} + 3\sqrt{2} \cdot i \\
f_{37} &= y_7 = 30 + \sqrt{2} - 3\sqrt{2} \cdot i
\end{aligned}
$$

$$
\begin{aligned}
f_{20}(w_2^0) &= f_{30}(w_1^0) + w_2^0 \cdot f_{31}(w_1^0) = 24 + 12 = 36 \\
f_{20}(w_2^1) &= f_{30}(w_1^0) + w_2^1 \cdot f_{31}(w_1^0) = 24 - 12 = 12 \\
f_{21}(w_2^0) &= f_{32}(w_1^0) + w_2^0 \cdot f_{33}(w_1^0) = 18 + 2i + 18 - 2i = 36 \\
f_{21}(w_2^1) &= f_{32}(w_1^0) + w_2^1 \cdot f_{33}(w_1^0) = 18 + 2i - 18 + 2i = 4i \\
f_{22}(w_2^0) &= f_{34}(w_1^0) + w_2^0 \cdot f_{35}(w_1^0) = 30 + \sqrt{2} + 3\sqrt{2} \cdot i + 30 - \sqrt{2} - 3\sqrt{2} \cdot i = 60 \\
f_{22}(w_2^1) &= f_{34}(w_1^0) + w_2^1 \cdot f_{35}(w_1^0) = 30 + \sqrt{2} + 3\sqrt{2} \cdot i - (30 - \sqrt{2} - 3\sqrt{2} \cdot i) = 2\sqrt{2} + 6\sqrt{2}i \\
f_{23}(w_2^0) &= f_{36}(w_1^0) + w_2^0 \cdot f_{37}(w_1^0) = 30 - \sqrt{2} + 3\sqrt{2} \cdot i + 30 + \sqrt{2} - 3\sqrt{2} \cdot i = 60 \\
f_{23}(w_2^1) &= f_{36}(w_1^0) + w_2^1 \cdot f_{37}(w_1^0) = 30 - \sqrt{2} + 3\sqrt{2} \cdot i - (30 + \sqrt{2} - 3\sqrt{2} \cdot i) = -2\sqrt{2} + 6\sqrt{2}i
\end{aligned}
$$

$$
\begin{aligned}
f_{10}(w_4^0) &= f_{20}(w_2^0) + w_4^0 \cdot f_{21}(w_2^0) = 36 + 36 = 72 \\
f_{10}(w_4^1) &= f_{20}(w_2^1) + w_4^1 \cdot f_{21}(w_2^1) = 12 + i \cdot 4i = 8 \\
f_{10}(w_4^2) &= f_{20}(w_2^0) + w_4^2 \cdot f_{21}(w_2^0) = 36 - 36 = 0 \\
f_{10}(w_4^3) &= f_{20}(w_2^1) + w_4^3 \cdot f_{21}(w_2^1) = 12 - i \cdot 4i = 16
\end{aligned}
$$

$$
\begin{aligned}
f_{11}(w_4^0) &= f_{22}(w_2^0) + w_4^0 \cdot f_{23}(w_2^0) = 60 + 60 = 120 \\
f_{11}(w_4^1) &= f_{22}(w_2^1) + w_4^1 \cdot f_{23}(w_2^1) = 2\sqrt{2} + 6\sqrt{2}i + i(-2\sqrt{2} + 6\sqrt{2}i) = -4\sqrt{2} + 4\sqrt{2}i \\
f_{11}(w_4^2) &= f_{22}(w_2^0) + w_4^2 \cdot f_{23}(w_2^0) = 60 - 60 = 0 \\
f_{11}(w_4^3) &= f_{22}(w_2^1) + w_4^3 \cdot f_{23}(w_2^1) = 2\sqrt{2} + 6\sqrt{2}i - i(-2\sqrt{2} + 6\sqrt{2}i) = 8\sqrt{2} + 8\sqrt{2}i
\end{aligned}
$$

And finally:

$$
\begin{aligned}
f_{00}(w_8^0) &= f_{10}(w_4^0) + w_8^0 \cdot f_{11}(w_4^0) = 72 + 120 = 192 \\
f_{00}(w_8^1) &= f_{10}(w_4^1) + w_8^1 \cdot f_{11}(w_4^1) = 8 + \frac{1+i}{\sqrt{2}}(-4\sqrt{2} + 4\sqrt{2}i) = 0 \\
f_{00}(w_8^2) &= f_{10}(w_4^2) + w_8^2 \cdot f_{11}(w_4^2) = 0 + i \cdot 0 = 0 \\
f_{00}(w_8^3) &= f_{10}(w_4^3) + w_8^3 \cdot f_{11}(w_4^3) = 16 + \frac{-1+i}{\sqrt{2}}(8\sqrt{2} + 8\sqrt{2}i) = 0 \\
f_{00}(w_8^4) &= f_{10}(w_4^0) - w_8^0 \cdot f_{11}(w_4^0) = 72 - 120 = -48 \\
f_{00}(w_8^5) &= f_{10}(w_4^1) - w_8^1 \cdot f_{11}(w_4^1) = 8 - \frac{1+i}{\sqrt{2}}(-4\sqrt{2} + 4\sqrt{2}i) = 16 \\
f_{00}(w_8^6) &= f_{10}(w_4^2) - w_8^2 \cdot f_{11}(w_4^2) = 0 - i \cdot 0 = 0 \\
f_{00}(w_8^7) &= f_{10}(w_4^3) - w_8^3 \cdot f_{11}(w_4^3) = 16 - \frac{-1+i}{\sqrt{2}}(8\sqrt{2} + 8\sqrt{2}i) = 32
\end{aligned}
$$

As stated in slide 10 of the lecture, one can compute the coefficients by $a_k = 1/8 \cdot f(w_8^{-k})$, so:

$$
\begin{aligned}
a_0 &= 192/8 = 24 \\
a_1 &= 32/8 = 4 \\
a_2 &= 0/8 = 0 \\
a_3 &= 16/8 = 2 \\
a_4 &= -48/8 = -6 \\
a_5 &= 0/8 = 0 \\
a_6 &= 0/8 = 0 \\
a_7 &= 0
\end{aligned}
$$

$\Rightarrow p(x) \cdot q(x) = -6x^4 + 2x^3 + 4x + 24.$

Exercise 2: FFT Application *(6 Points)*

Let A, B be two sets of integers between 0 and n i.e., $A, B \subseteq \{0, 1, 2, \ldots, n\}$. We define two random variables X_A and X_B, where X_A is obtained by choosing a number uniformly at random from A and X_B is obtained by choosing a number uniformly at random from B. We further define the random variable $Z := X_A + X_B$. Note that Z can take values in the range $0, \ldots, 2n$.
Give an $O(n \log n)$ algorithm to compute the distribution of Z. Hence, the algorithm should compute the probability $P(Z = z)$ for all $z \in \{0, \ldots, 2n\}$. Note that $\sum_{z=0}^{2n} P(Z = z) = 1$. You can use the algorithms of the lecture as a black box. State the correctness of your algorithm and also explain the runtime!

Sample Solution

Our algorithm works as follows, first we construct a polynomial $p_A(x) = \sum_{i=0}^{n} a_i x^i$ where $a_i := 1$ if $i \in A$ and $a_i := 0$ otherwise. In the same manner we construct the polynomial $p_B(x) = \sum_{i=0}^{n} b_i x^i$. Note that those constructions require only linear time.
Now we multiply those polynomials i.e., $p_Z(x) = p_A(x) \cdot p_B(x) = \sum_{i=0}^{2n} c_i x^i$. Using FFT, this multiplication can be computed in $O(n \log n)$ time. This gives us the coefficients of $p_Z(x) : c_0, \ldots, c_{2n}$.
The resulting distribution will be determined in the following way, for some given $z \in \{0, \ldots, 2n\}$: $P(Z = z) := \frac{c_z}{|A| \cdot |B|}$. Computing this value for each z also takes linear time. It follows that the overall runtime is dominated by the FFT step and therefore is $O(n \log n)$.

It remains to show that $P(Z = z) = \frac{c_z}{|A| \cdot |B|}$ is true. First take note that we have $P(X_A = k) = \frac{a_k}{|A|}$, and similarly $P(X_B = k) = \frac{b_k}{|B|}$. Further, by the definition of the multiplication of polynomials, we have $c_k = \sum_{i=0}^{k} a_i \cdot b_{k-i}$. It then follows:

$$\begin{aligned}
P(Z = z) &= P(X_A + X_B = z) \\
&= \sum_{i=0}^{z} P(X_A = i \wedge X_B = z - i) \\
&= \sum_{i=0}^{z} P(X_A = i) \cdot P(X_B = z - i) \\
&= \frac{1}{|A| \cdot |B|} \cdot \sum_{i=0}^{z} a_i \cdot b_{z-i} \\
&= \frac{1}{|A| \cdot |B|} \cdot c_z
\end{aligned}$$