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

Algorithm Theory
Sample Solution Exercise Sheet 2

Due: Wednesday, 9th of November, 2022, 11:59 pm

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

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

1. Illustrate the **divide** procedure of the algorithm. More precisely, for the i-th divide step, 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. That is, starting with the polynomials of smallest degree as base cases, compute the DFT of p_{ij} bottom up with the recursive formula given in the lecture. The recursion stops when $DFT_8(p_{00})$ is computed.
3. **Multiply** the polynomials. More specific, give the point value representation of $p^2(x)$, 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 $p(x)^2$. To do that efficiently, first compute the $DFT_8(q)$ where $q(x) := y_0 + y_1 \cdot x + ... + y_7 \cdot x^7$ and then compute the coefficients a_k for $k \in \{0, 1, ..., 7\}$.

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

Sample Solution

1. **divide:**

$$\begin{aligned}
p_{00} &= 2x^3 - x^2 + 4x + 4 \\
p_{10} &= -x + 4 \\
p_{11} &= 2x + 4 \\
p_{20} &= 4 \\
p_{21} &= -1 \\
p_{22} &= 4 \\
p_{23} &= 2
\end{aligned}$$

2. **combine:** Bottom up using previous values:

$$\begin{aligned}
p_{10}(w_4^0) &= p_{20}(w_2^0) + w_4^0 \cdot p_{21}(w_2^0) = 4 + 1 \cdot (-1) = 3 \\
p_{10}(w_4^1) &= p_{20}(w_2^1) + w_4^1 \cdot p_{21}(w_2^1) = 4 + i \cdot (-1) = 4 - i \\
p_{10}(w_4^2) &= p_{20}(w_2^0) + w_4^2 \cdot p_{21}(w_2^0) = 4 - 1 \cdot (-1) = 5 \\
p_{10}(w_4^3) &= p_{20}(w_2^1) + w_4^3 \cdot p_{21}(w_2^1) = 4 - i \cdot (-1) = 4 + i
\end{aligned}$$

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

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

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

3. **Multiply:** Now $p^2(x)$ has the following point value representation

$$
\begin{aligned}
&(w_8^0, 81), \\
&(w_8^1, 14\sqrt{2} - 1 + i \cdot (22\sqrt{2} + 4)), \\
&(w_8^2, 21 + 20i), \\
&(w_8^3, -14\sqrt{2} - 1 + i \cdot (22\sqrt{2} - 4)), \\
&(w_8^4, 9), \\
&(w_8^5, -14\sqrt{2} - 1 + i \cdot (-22\sqrt{2} + 4)), \\
&(w_8^6, 21 - 20i), \\
&(w_8^7, 14\sqrt{2} - 1 + i \cdot (-22\sqrt{2} - 4))
\end{aligned}
$$

4. **Inverse DFT:** To efficiently compute the inverse DFT, we again have to do some bottom-up computation, now based on the polynomial $q(x) = y_7 x^7 + y_6 x^6 + ... + y_0$, where the y_i values are the y-values in the point value representation of p^2.

$$
\begin{aligned}
q_{00} &= q \\
q_{10} &= y_6x^3 + y_4x^2 + y_2x + y_0 \\
q_{11} &= y_7x^3 + y_5x^2 + y_3x + y_1 \\
q_{20} &= y_4x + y_0 \\
q_{21} &= y_6x + y_2 \\
q_{22} &= y_5x + y_1 \\
q_{23} &= y_7x + y_3 \\
q_{30} &= y_0 = 81 \\
q_{31} &= y_4 = 9 \\
q_{32} &= y_2 = 21 + 20i \\
q_{33} &= y_6 = 21 - 20i \\
q_{34} &= y_1 = 14\sqrt{2} - 1 + i \cdot (22\sqrt{2} + 4) \\
q_{35} &= y_5 = -14\sqrt{2} - 1 + i \cdot (-22\sqrt{2} + 4) \\
q_{36} &= y_3 = -14\sqrt{2} - 1 + i \cdot (22\sqrt{2} - 4) \\
q_{37} &= y_7 = 14\sqrt{2} - 1 + i \cdot (-22\sqrt{2} - 4)
\end{aligned}
$$

$$
\begin{aligned}
q_{20}(w_2^0) &= q_{30}(w_1^0) + w_2^0 \cdot q_{31}(w_1^0) = 81 + 9 = 90 \\
q_{20}(w_2^1) &= q_{30}(w_1^0) + w_2^1 \cdot q_{31}(w_1^0) = 81 - 9 = 72 \\
q_{21}(w_2^0) &= q_{32}(w_1^0) + w_2^0 \cdot q_{33}(w_1^0) = 21 + 20i + 21 - 20i = 42 \\
q_{21}(w_2^1) &= q_{32}(w_1^0) + w_2^1 \cdot q_{33}(w_1^0) = 21 + 20i - 21 + 20i = 40i \\
q_{22}(w_2^0) &= q_{34}(w_1^0) + w_2^0 \cdot q_{35}(w_1^0) = -2 + 8i \\
q_{22}(w_2^1) &= q_{34}(w_1^0) + w_2^1 \cdot q_{35}(w_1^0) = 28\sqrt{2} + 44\sqrt{2}i \\
q_{23}(w_2^0) &= q_{36}(w_1^0) + w_2^0 \cdot q_{37}(w_1^0) = -2 - 8i \\
q_{23}(w_2^1) &= q_{36}(w_1^0) + w_2^1 \cdot q_{37}(w_1^0) = -28\sqrt{2} + 44\sqrt{2}i
\end{aligned}
$$

$$
\begin{aligned}
q_{10}(w_4^0) &= q_{20}(w_2^0) + w_4^0 \cdot q_{21}(w_2^0) = 90 + 42 = 132 \\
q_{10}(w_4^1) &= q_{20}(w_2^1) + w_4^1 \cdot q_{21}(w_2^1) = 72 + 40i^2 = 32 \\
q_{10}(w_4^2) &= q_{20}(w_2^0) + w_4^2 \cdot q_{21}(w_2^0) = 90 - 42 = 48 \\
q_{10}(w_4^3) &= q_{20}(w_2^1) + w_4^3 \cdot q_{21}(w_2^1) = 72 - 40i^29 = 112
\end{aligned}
$$

$$
\begin{aligned}
q_{11}(w_4^0) &= q_{22}(w_2^0) + w_4^0 \cdot q_{23}(w_2^0) = -4 \\
q_{11}(w_4^1) &= q_{22}(w_2^1) + w_4^1 \cdot q_{23}(w_2^1) = -16\sqrt{2} + 16\sqrt{2}i \\
q_{11}(w_4^2) &= q_{22}(w_2^0) + w_4^2 \cdot q_{23}(w_2^0) = 16i \\
q_{11}(w_4^3) &= q_{22}(w_2^1) + w_4^3 \cdot q_{23}(w_2^1) = 72\sqrt{2} + 72\sqrt{2}i
\end{aligned}
$$

And finally:

$$\begin{aligned}
q_{00}(w_8^0) &= q_{10}(w_4^0) + w_8^0 \cdot q_{11}(w_4^0) = 128 \\
q_{00}(w_8^1) &= q_{10}(w_4^1) + w_8^1 \cdot q_{11}(w_4^1) = 0 \\
q_{00}(w_8^2) &= q_{10}(w_4^2) + w_8^2 \cdot q_{11}(w_4^2) = 48 + 16i^2 = 32 \\
q_{00}(w_8^3) &= q_{10}(w_4^3) + w_8^3 \cdot q_{11}(w_4^3) = -32 \\
q_{00}(w_8^4) &= q_{10}(w_4^0) - w_8^0 \cdot q_{11}(w_4^0) = 132 + 4 = 136 \\
q_{00}(w_8^5) &= q_{10}(w_4^1) - w_8^1 \cdot q_{11}(w_4^1) = 64 \\
q_{00}(w_8^6) &= q_{10}(w_4^2) - w_8^2 \cdot q_{11}(w_4^2) = 48 - i(16i) = 64 \\
q_{00}(w_8^7) &= q_{10}(w_4^3) - w_8^3 \cdot q_{11}(w_4^3) = 256
\end{aligned}$$

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

$$\begin{aligned}
a_0 &= 128/8 = 16 \\
a_1 &= 256/8 = 32 \\
a_2 &= 64/8 = 8 \\
a_3 &= 64/8 = 8 \\
a_4 &= 136/8 = 17 \\
a_5 &= -32/8 = -4 \\
a_6 &= 32/8 = 4 \\
a_7 &= 0
\end{aligned}$$

$\Rightarrow p^2(x) = 4x^6 - 4x^5 + 17x^4 + 8x^3 + 8x^2 + 32x + 16.$

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:

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