Exercise 1

Task 1
Prove that the *Vandermonde*-Matrix

$$V(a_0, \dots, a_{n-1}) = \begin{pmatrix} 1 & a_0 & a_0^2 & \dots & a_0^{n-1} \\ 1 & a_1 & a_1^2 & \dots & a_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_{n-1} & a_{n-1}^2 & \dots & a_{n-1}^{n-1} \end{pmatrix}$$

is ivertible if and only if the numbers $a_0, \dots, a_{n-1}$ are pairwise different.
Hint: Show first that the following equation holds:

$$\det V(a_0, \dots, a_{n-1}) = \prod_{0 \le i < j < n} (a_j - a_i)$$

Solution
First we show the hint. Add $(-a_0)$ times the i-th column to the $(i+1)$-st column $(1 \le i \le n-1)$ and then factorize into 2 matrices. This yields:

$$\begin{aligned}
&\det V(a_0, \dots, a_{n-1}) \\
=&\det \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & a_1 - a_0 & a_1^2 - a_0 a_1 & \dots & a_1^{n-1} - a_0 a_1^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_{n-1} - a_0 & a_{n-1}^2 - a_0 a_{n-1} & \dots & a_{n-1}^{n-1} - a_0 a_{n-1}^{n-2} \end{pmatrix} \\
=&\det \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & a_1 - a_0 & a_1(a_1 - a_0) & \dots & a_1^{n-2}(a_1 - a_0) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_{n-1} - a_0 & a_{n-1}^2(a_{n-1} - a_0) & \dots & a_{n-1}^{n-2}(a_{n-1} - a_0) \end{pmatrix} \\
=&1 \cdot \det(\operatorname{diag}(a_1 - a_0, \dots, a_{n-1} - a_0) \cdot V(a_1, \dots, a_{n-1})) \\
=&\det \operatorname{diag}(a_1 - a_0, \dots, a_{n-1} - a_0) \cdot \det V(a_1, \dots, a_{n-1}) \\
=&\prod_{i=1}^{n-1} (a_i - a_0) \cdot \det V(a_1, \dots, a_{n-1})
\end{aligned}$$

With induction we obtain $\det V(a_0, \dots, a_{n-1}) = \prod_{0 \le i < j < n} (a_j - a_i)$ as desired.
Now we prove the main statement. If there is any nontrivial pair (i, j) with $a_i = a_j$, then the product $\prod (a_j - a_i)$ has one factor which is 0. Conversely, if all of the a_i are pairwise different, then this product has only nonzero factors. Linear Algebra tells us that a matrix is invertible if and only if its determinant is not 0.

Task 2 (Fast Fourier Transform)

(a) Use the FFT to compute the discrete Fourier transform of the polynomial $f(x) = x + 2x^2 + 3x^3$ over $\mathbb{C}$.

(b) Compute $(x+2)\cdot(2x-1)$ with the FFT.

Solution

(a) $f(x) = x+2x^2+3x^3$ yields the vector $f = (0,1,2,3)^\top$. Let furthermore ω be a primitive 4-th root of unity. We use devide and conquer to obtain

$$F_4(\omega)\begin{pmatrix}0\\1\\2\\3\end{pmatrix} = \begin{pmatrix}F_2(\omega^2)\begin{pmatrix}0\\2\end{pmatrix}\\ F_2(\omega^2)\begin{pmatrix}0\\2\end{pmatrix}\end{pmatrix} + \begin{pmatrix}1\\\omega\\\omega^2\\\omega^3\end{pmatrix}\circ\begin{pmatrix}F_2(\omega^2)\begin{pmatrix}1\\3\end{pmatrix}\\ F_2(\omega^2)\begin{pmatrix}1\\3\end{pmatrix}\end{pmatrix},$$

$$F_2(\omega^2)\begin{pmatrix}0\\2\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix} + \begin{pmatrix}1\\\omega^2\end{pmatrix}\circ\begin{pmatrix}2\\2\end{pmatrix} = \begin{pmatrix}2\\2\omega^2\end{pmatrix},$$

$$F_2(\omega^2)\begin{pmatrix}1\\3\end{pmatrix} = \begin{pmatrix}1\\1\end{pmatrix} + \begin{pmatrix}1\\\omega^2\end{pmatrix}\circ\begin{pmatrix}3\\3\end{pmatrix} = \begin{pmatrix}4\\1+3\omega^2\end{pmatrix}.$$

Hence

$$F_4(\omega)\begin{pmatrix}0\\1\\2\\3\end{pmatrix} = \begin{pmatrix}2\\2\omega^2\\2\\2\omega^2\end{pmatrix} + \begin{pmatrix}1\\\omega\\\omega^2\\\omega^3\end{pmatrix}\circ\begin{pmatrix}4\\1+3\omega^2\\4\\1+3\omega^2\end{pmatrix} = \begin{pmatrix}6\\\omega+2\omega^2+3\omega^3\\2+4\omega^2\\3\omega+2\omega^2+\omega^3\end{pmatrix}.$$

In particular, for $\mathbb{F} = \mathbb{C}$ we can choose $\omega = e^{2\pi i/4} = i$. Thus,

$$F_4(\omega)\begin{pmatrix}0\\1\\2\\3\end{pmatrix} = \begin{pmatrix}6\\-2-2i\\-2\\-2+2i\end{pmatrix}.$$

For this small example we could have also directly computed the DFT of $f(x)$ by multiplying a 4×4 matrix with a 4×1 vector.

(b) Let $f(x) = 2+x$ and $g(x) = -1+2x$. Hence we get the vectors $f = (2,1,0,0)^\top$ and $g = (-1,2,0,0)^\top$. Also, we immediately use $\omega^2 = -1$ in every step. We use the same approach as in (a) to compute the DFTs of f and g to obtain

$$F_4(\omega)\begin{pmatrix}2\\1\\0\\0\end{pmatrix} = \begin{pmatrix}F_2(\omega^2)\begin{pmatrix}2\\0\end{pmatrix}\\ F_2(\omega^2)\begin{pmatrix}2\\0\end{pmatrix}\end{pmatrix} + \begin{pmatrix}1\\\omega\\\omega^2\\\omega^3\end{pmatrix} \circ \begin{pmatrix}F_2(\omega^2)\begin{pmatrix}1\\0\end{pmatrix}\\ F_2(\omega^2)\begin{pmatrix}1\\0\end{pmatrix}\end{pmatrix} = \begin{pmatrix}3\\2+\omega\\1\\2-\omega\end{pmatrix},$$

$$F_4(\omega)\begin{pmatrix}-1\\2\\0\\0\end{pmatrix} = \begin{pmatrix}F_2(\omega^2)\begin{pmatrix}-1\\0\end{pmatrix}\\ F_2(\omega^2)\begin{pmatrix}-1\\0\end{pmatrix}\end{pmatrix} + \begin{pmatrix}1\\\omega\\\omega^2\\\omega^3\end{pmatrix} \circ \begin{pmatrix}F_2(\omega^2)\begin{pmatrix}2\\0\end{pmatrix}\\ F_2(\omega^2)\begin{pmatrix}2\\0\end{pmatrix}\end{pmatrix} = \begin{pmatrix}1\\-1+2\omega\\-3\\-1-2\omega\end{pmatrix}.$$

The product of the 2 polynomials, which would be a convolution of the coefficients, can now be obtained by simply multiplying the coefficients of their DFTs and then performing the inverse FFT.

$$F_4(\omega)(fg) = \begin{pmatrix}3\\2+\omega\\1\\2-\omega\end{pmatrix} \circ \begin{pmatrix}1\\-1+2\omega\\-3\\-1-2\omega\end{pmatrix} = \begin{pmatrix}3\\-4+3\omega\\-3\\-4-3\omega\end{pmatrix},$$

$$fg = \frac{1}{4}F_4(\omega^{-1})\begin{pmatrix}3\\-4+3\omega\\-3\\-4-3\omega\end{pmatrix}$$

$$= \frac{1}{4}\begin{pmatrix}F_2(\omega^{-2})\begin{pmatrix}3\\-3\end{pmatrix}\\ F_2(\omega^{-2})\begin{pmatrix}3\\-3\end{pmatrix}\end{pmatrix} + \frac{1}{4}\begin{pmatrix}1\\\omega^{-1}\\\omega^{-2}\\\omega^{-3}\end{pmatrix} \circ \begin{pmatrix}F_2(\omega^{-2})\begin{pmatrix}-4+3\omega\\-4-3\omega\end{pmatrix}\\ F_2(\omega^{-2})\begin{pmatrix}-4+3\omega\\-4-3\omega\end{pmatrix}\end{pmatrix}$$

$$= \frac{1}{4}\begin{pmatrix}0\\6\\0\\6\end{pmatrix} + \frac{1}{4}\begin{pmatrix}-8\\6\\8\\-6\end{pmatrix} = \begin{pmatrix}-2\\3\\2\\0\end{pmatrix} \implies (fg)(x) = -2+3x+2x^2$$

Task 3

Let $A, B \subseteq \{1, \dots, 10n\}$ be sets with $|A| = |B| = n$. We want to compute

$$C := \{a + b : a \in A, b \in B\}$$

and the number of possibilities to write $c \in C$ as a sum of elements in A and B. Specify an algorithm that solves the problem in time $\mathcal{O}(n \log n)$.

Solution

We can represent A and B as polynomials of the form $f_A(x) = \sum_{a\in A} x^a$ and $f_B(x) = \sum_{b\in B} x^b$. The coefficient of x^c in $f_A \cdot f_B$ tells us, how often we can write c as a sum of elements in A and B. Using FFT, we can compute $f_A \cdot f_B$ in time $\mathcal{O}(n \log n)$.