Osme vaje APS2: Hitra Fourierova transformacija

1 Ideja

Naš cilj je izračunati vrednost polinoma $a(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1}$ v točkah ω_n^0, ω_n^1, $\ldots$, ω_n^{n-1}, kjer je ω_n n-ti primitivni koren enote. Direktni pristop (množenje Vandermondove matrike z vektorjem koeficientov ali n izvedb Hornerjevega algoritma) potrebuje $O(n^2)$ časa, izkaže pa se, da lahko s pristopom *deli in vladaj* ta čas zmanjšamo na $O(n \log n)$.

V nadaljevanju bomo predpostavili, da velja $n = 2^m$ za nek $m \geq 0$, poleg tega si bomo pomagali z dvema lastnostma n-tega PKA:

- $\omega_{ac}^{bc} = \omega_a^b$,
- $\omega_n^{n/2} = -1$.

Polinom $a(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$ lahko zapišemo kot

$$a(x) = s(x^2) + xl(x^2),$$

kjer je

$$\begin{aligned} s(x) &= a_0 + a_2x + a_4x^2 + \ldots + a_{n-2}x^{n/2-1}, \\ \ell(x) &= a_1 + a_3x + a_5x^2 + \ldots + a_{n-1}x^{n/2-1}. \end{aligned}$$

Izračunati moramo torej $a(\omega_n^k)$ za $k = 0, 1, \ldots, n-1$:

$$a(\omega_n^k) = s(\omega_n^{2k}) + \omega_n^k \ell(\omega_n^{2k}) \quad [k = 0, 1, \ldots, n-1].$$

Ker je $\omega_n^{2k} = \omega_{n/2}^k$, lahko gornjo enačbo prepišemo takole:

$$a(\omega_n^k) = s(\omega_{n/2}^k) + \omega_n^k \ell(\omega_{n/2}^k) \quad [k = 0, 1, \ldots, n-1].$$

Izkaže se, da zadošča, če $a(\omega_n^k)$ izračunamo za $k = 0, 1, \ldots, n/2-1$. Naj bo $k \in \{0, 1, \ldots, n/2-1\}$ in izračunajmo

$$\begin{aligned} a(\omega_n^{k+n/2}) &= s(\omega_{n/2}^{k+n/2}) + \omega_n^{k+n/2} \ell(\omega_{n/2}^{k+n/2}) \\ &= s(\omega_{n/2}^k \omega_{n/2}^{n/2}) + \omega_n^k \omega_n^{n/2} \ell(\omega_{n/2}^k \omega_{n/2}^{n/2}) \\ &= s(\omega_{n/2}^k) - \omega_n^k \ell(\omega_{n/2}^k) \end{aligned}$$

Če povzamemo:

$$\begin{aligned} a(\omega_n^k) &= s(\omega_{n/2}^k) + \omega_n^k \ell(\omega_{n/2}^k) \quad [k = 0, 1, \ldots, n/2-1] \\ a(\omega_n^{k+n/2}) &= s(\omega_{n/2}^k) - \omega_n^k \ell(\omega_{n/2}^k) \quad [k = 0, 1, \ldots, n/2-1] \end{aligned}$$

Nalogo velikosti n (izračun vrednosti polinoma z n koeficienti v n potencah n-tega PKE) smo torej prevedli na dve nalogi velikosti $n/2$ (izračun vrednosti polinoma z $n/2$ koeficienti v $n/2$ potencah $(n/2)$-tega PKE), za razbijanje naloge na podnaloge in združevanje rešitev podnalog v rešitev izhodiščne naloge pa potrebujemo čas $\Theta(n)$. V formulo za krovni izrek vstavimo torej $a = 2$, $b = 2$ in $d = 1$. Ker je $a = b^d$, je časovna zahtevnost algoritma enaka $\Theta(n^d \log n) = \Theta(n \log n)$.

2 Prvi primer

Izračunajmo DFT polinoma $a(x) = 2 + 3x + 5x^2 + 7x^3$ v obsegu kompleksnih števil. V našem primeru imamo $n = 4$, kar je že potenca števila 2. Zapišimo $a(x) = s(x) + x\ell(x)$, kjer je $s(x) = 2 + 5x$ in $\ell(x) = 3 + 7x$. Izračunati moramo sledeče vrednosti:

$$\begin{aligned}
a(\omega_4^0) &= s(\omega_2^0) + \omega_4^0 \ell(\omega_2^0),\\
a(\omega_4^1) &= s(\omega_2^1) + \omega_4^1 \ell(\omega_2^1),\\
a(\omega_4^2) &= s(\omega_2^0) - \omega_4^0 \ell(\omega_2^0),\\
a(\omega_4^3) &= s(\omega_2^1) - \omega_4^1 \ell(\omega_2^1).
\end{aligned}$$

Izračunajmo vrednosti $s(.)$ in $\ell(.)$ v točkah ω_2^0 in ω_2^1. Polinoma $s(x)$ in $\ell(x)$ lahko zapišemo kot $s(x) = s_1(x) + x\ell_1(x)$ in $\ell(x) = s_2(x) + x\ell_2(x)$, kjer je $s_1(x) = 2$, $\ell_1(x) = 5$, $s_2(x) = 3$ in $\ell_2(x) = 7$:

$$\begin{aligned}
s(\omega_2^0) &= s_1(\omega_1^0) + \omega_2^0 \ell_1(\omega_1^0) = 2 + 5 = 7\\
s(\omega_2^1) &= s_1(\omega_1^0) - \omega_2^0 \ell_1(\omega_1^0) = 2 - 5 = -3\\
\ell(\omega_2^0) &= s_2(\omega_1^0) + \omega_2^0 \ell_2(\omega_1^0) = 3 + 7 = 10\\
\ell(\omega_2^1) &= s_2(\omega_1^0) - \omega_2^0 \ell_2(\omega_1^0) = 3 - 7 = -4
\end{aligned}$$

Torej je

$$\begin{aligned}
a(\omega_4^0) &= s(\omega_2^0) + \omega_4^0 \ell(\omega_2^0) = 7 + 10 = 17\\
a(\omega_4^1) &= s(\omega_2^1) + \omega_4^1 \ell(\omega_2^1) = -3 + i(-4) = -3 - 4i\\
a(\omega_4^2) &= s(\omega_2^0) - \omega_4^0 \ell(\omega_2^0) = 7 - 10 = -3\\
a(\omega_4^3) &= s(\omega_2^1) - \omega_4^1 \ell(\omega_2^1) = -3 - i(-4) = -3 + 4i
\end{aligned}$$

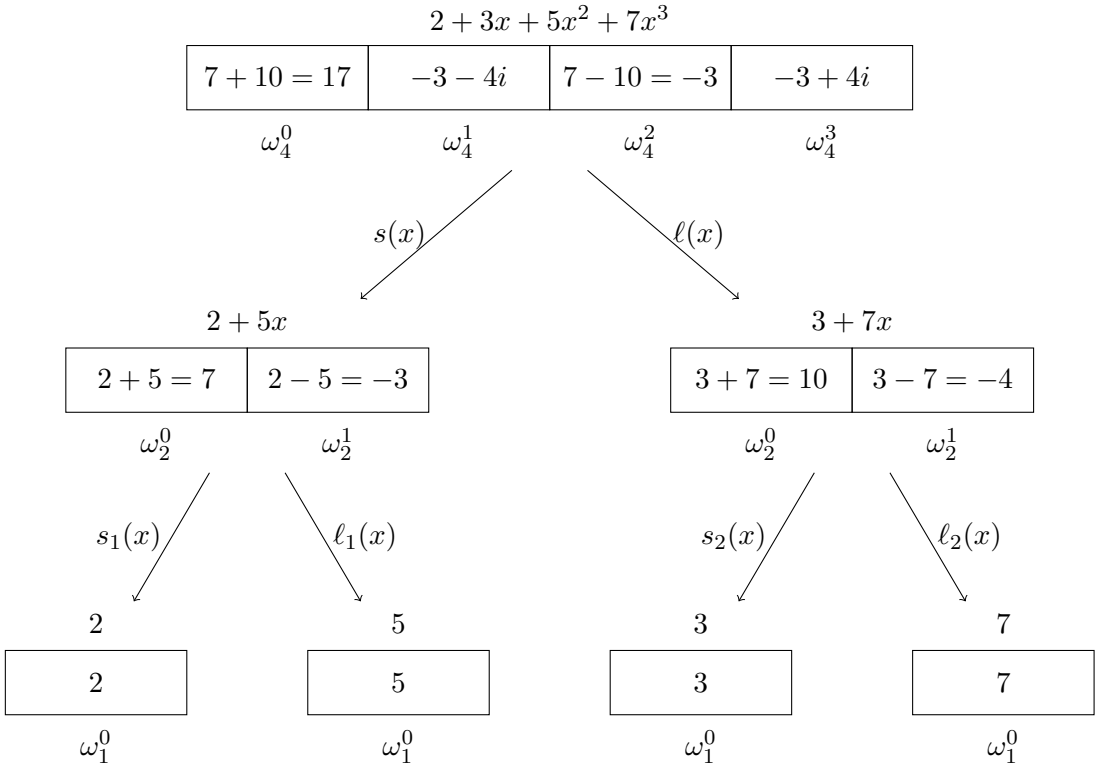
Celoten postopek lahko predstavimo z drevesom na sliki 1.

3 Drugi primer

Zmnožimo polinoma $a(x) = 3+x+2x^2$ in $b(x) = 1+4x+5x^2+3x^3$ v modulskem kolobarju. Produktni polinom ima 6 koeficientov, zato potrebujemo $n = 8$. Kolobar $\mathbb{Z}_{17}$ je najmanjši kolobar z 8. PKE (to je število 2). Ker je $\omega_8 = 2$, je $\omega_4 = 4$, $\omega_2 = 16$ in $\omega_1 = 1$.

Postopek izvršimo v štirih korakih:

1. Izračunamo vrednosti $a(x)$ v točkah $\omega_8^0, \ldots, \omega_8^7$ in dobimo vektor $Fa = [6, 13, 5, 3, 4, 9, 14, 4]^T$ (slika 2).



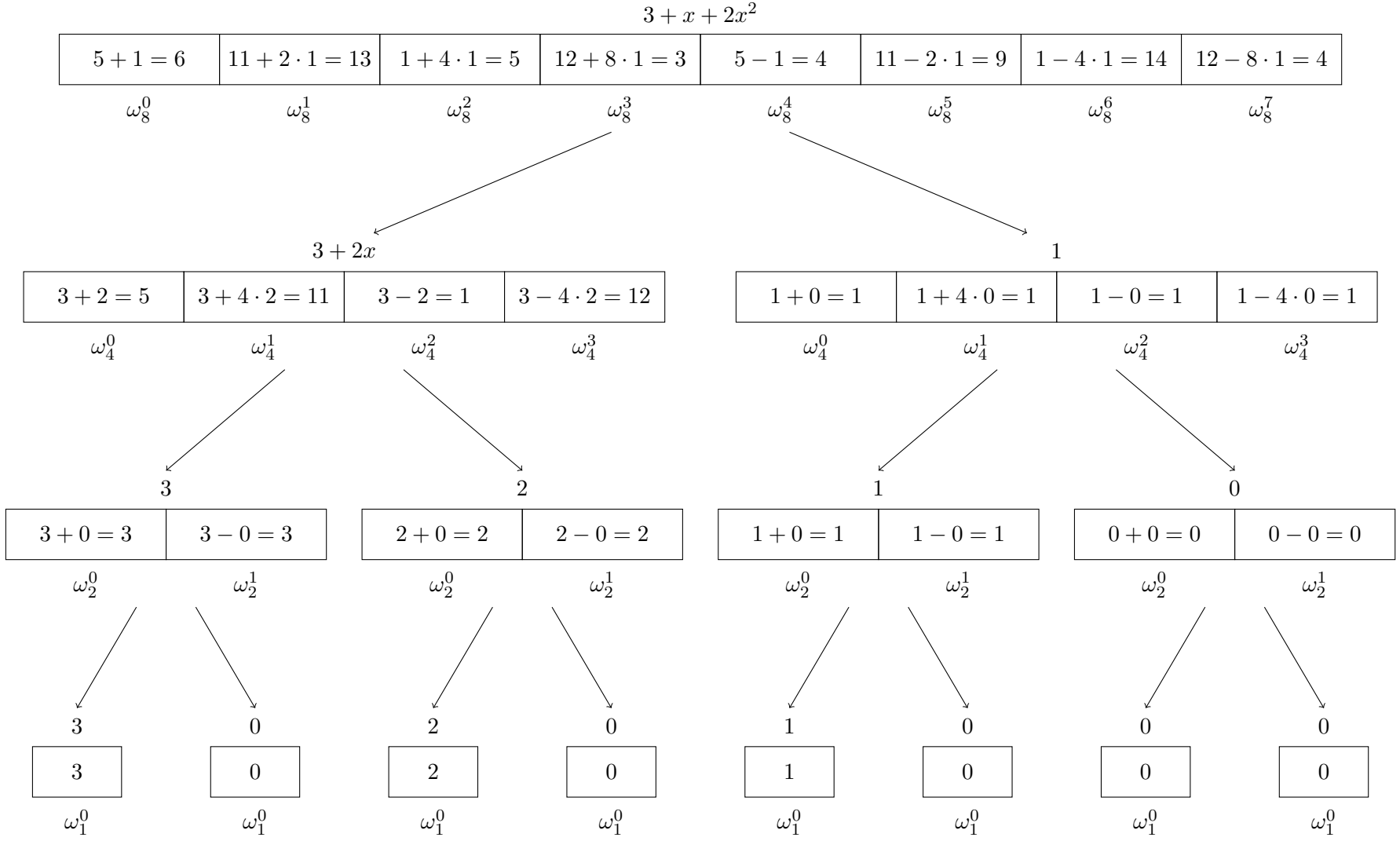
Slika 1: Izračun vrednosti polinoma v točkah ω_4^0, ω_4^1, ω_4^2 in ω_4^3.

2. Izračunamo vrednosti $b(x)$ v točkah $\omega_8^0, \ldots, \omega_8^7$ in dobimo vektor $Fb = [13, 2, 0, 2, 16, 6, 9, 11]^T$ (slika 3).

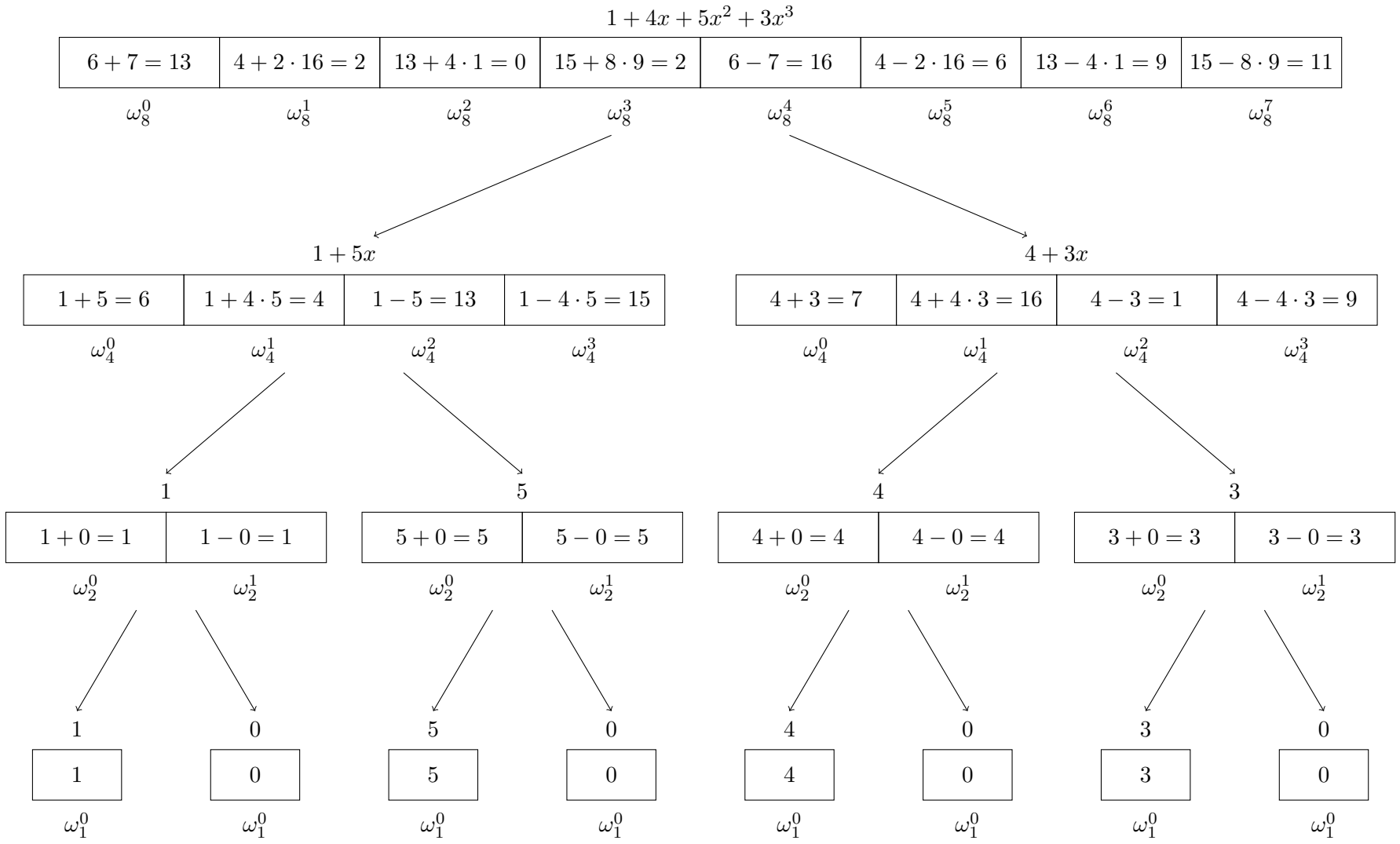
3. Zmnožimo izračunana vektorja po komponentah in dobimo vektor $Fc = [10, 9, 0, 6, 13, 3, 7, 10]^T$.

4. Izračunamo vrednosti $(Fc)(x)$ v točkah $(\omega_8^{-1})^0$, $\ldots$, $(\omega_8^{-1})^7$. Ker je $\omega_8 = 2$, je $\omega_8^{-1} = 9$, $\omega_4^{-1} = 13$, $\omega_2^{-1} = 16$ in $\omega_1^{-1} = 1$. Dobimo vektor $[7, 2, 15, 6, 2, 14, 0, 0]^T$.

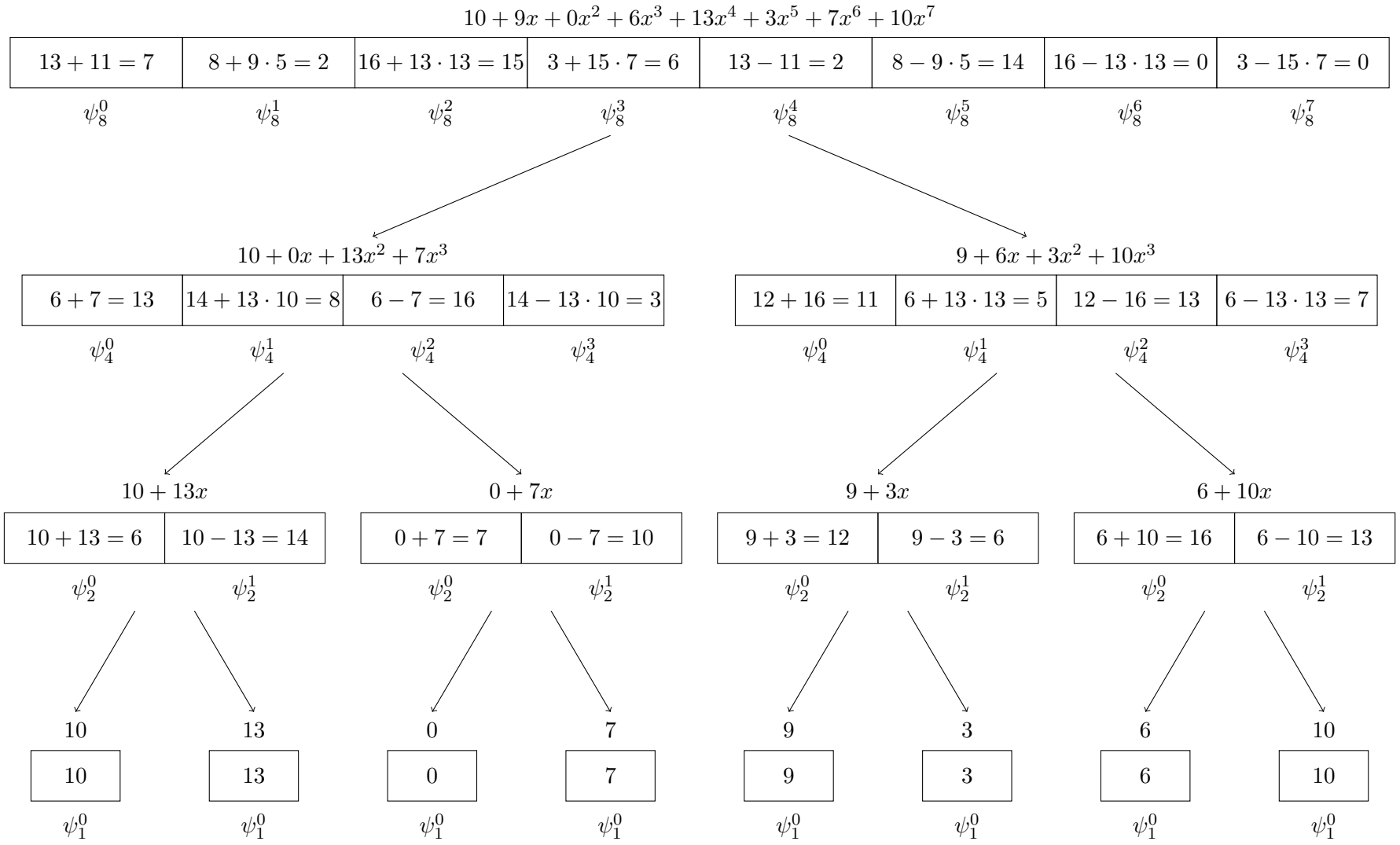
5. Dobljeni vektor pomnožimo še z $n^{-1} = 8^{-1} = 15$. Rezultat je vektor $[3, 13, 4, 5, 13, 6, 0, 0]^T$, ki podaja koeficiente polinoma $c(x) = a(x)b(x) = 3 + 13x + 21x^2 + 22x^3 + 13x^4 + 6x^5$ po modulu 17.



Slika 2: Izračun vrednosti $a(x)$ v točkah ω_8^k.



Slika 3: Izračun vrednosti $b(x)$ v točkah ω_8^k.



Slika 4: Izračun vrednosti $(Fc)(x)$ v točkah ψ_8^k, kjer je $\psi_m = \omega_m^{-1}$.