Die inverse Diskrete Fourier Transformation

- Konvertierung von der Point-value Form in Koeffizientenform.
- Dazu stellen wir die DFT als Matrix-Vektor Produkt dar

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega_n & \omega_n^2 & \dots & \omega_n^{n-1} \\ 1 & \omega_n^2 & \omega_n^4 & \dots & \omega_n^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_n^{n-1} & \omega_n^{2(n-1)} & \dots & \omega_n^{(n-1)(n-1)} \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n-1} \end{pmatrix}.$$

- D.h. die Vandermonde-Matrix besitzt Einträge $v_{ij} = \omega_n^{ij}$ für $i, j \in \mathbb{Z}_n$.
- Man beachte, dass $V = V^T$. D.h. $v_{ij} = v_{ji}$ für alle i, j.
- V ist invertierbar (s. Übung). Damit ist die inverse DFT

$$a = DFT_n^{-1}(y, \omega) = V^{-1}y.$$

Summationslemma

Lemma Summationslemma

Für alle $n, i \in \mathbb{N}$ mit $n \nmid i$ gilt $\sum_{k=0}^{n-1} (\omega_n^i)^k = 0$.

Beweis:

$$\sum_{k=0}^{n-1} (\omega_n^i)^k = \frac{(\omega_n^i)^n - 1}{\omega_n^i - 1} = \frac{(\omega_n^n)^i - 1}{\omega_n^i - 1} = \frac{1^i - 1}{\omega_n^i - 1} = 0.$$

Berechnung der inversen DFT

Lemma Invertieren von V

Sei $V^{-1} = (v'_{i,j})_{1 \le i,j \le n}$. Dann gilt $v'_{i,j} = \frac{1}{n} \cdot \omega_n^{-ij}$.

Beweis:

- Wir zeigen, dass $V \cdot V^{-1} = I_n$, d.h. die $(n \times n)$-Einheitsmatrix.
- Wir betrachten dazu den (i,j)-Eintrag von $V \cdot V^{-1}$ für $i, j \in \mathbb{Z}_n$

$$\sum_{k=0}^{n-1} \omega_n^{ik} \cdot \frac{1}{n} \cdot \omega_n^{-kj} = \frac{1}{n} \sum_{k=0}^{n-1} \omega_n^{k(i-j)}.$$

- **Fall 1:** $i = j$. Dann ist $\omega_n^{k(i-j)} = 1$ und die Summation liefert 1.
- **Fall 2:** $i \neq j$. Es gilt $|i - j| < n$ und damit $n \nmid (i - j)$.
- Summationslemma liefert in diesem Fall $\sum_{k=0}^{n-1} (\omega_n^{(i-j)})^k = 0$.

Korollar Berechnung der inversen DFT

Für die inverse DFT gilt $\mathrm{DFT}_n^{-1}(y, \omega) = \frac{1}{n} \cdot \mathrm{DFT}_n(y, \omega^{-1})$.
D.h. DFT_n und DFT_n^{-1} lassen sich beide in Zeit $\mathcal{O}(n \log n)$ berechnen.

Multiplizieren von Polynomen

Satz FFT Polynom-Multiplikation

Seien $a, b \in R[x]$ vom Grad kleiner n. Dann lässt sich $ab \in R[x]$ in Zeit $\mathcal{O}(n \log n)$ berechnen.

Beweis:

- Seien $a = (a_0, \ldots, a_{n-1})$, $b = (b_0, \ldots, b_{n-1})$ Koeffizientenformen.
- Berechne in Zeit $\mathcal{O}(n \log n)$ die Point-value Formen
  - $(a(\omega_{2n}^0), \ldots, a(\omega_{2n}^{2n-1})) = \mathrm{DFT}_{2n}((a_0, \ldots, a_{n-1}, 0, \ldots, 0), \omega)$ und
  - $(b(\omega_{2n}^0), \ldots, b(\omega_{2n}^{2n-1})) = \mathrm{DFT}_{2n}((b_0, \ldots, b_{n-1}, 0, \ldots, 0), \omega)$
- Multipliziere in Zeit $\mathcal{O}(n)$ punktweise

$$(a(\omega_{2n}^0) \cdot b(\omega_{2n}^0), \ldots, a(\omega_{2n}^{2n-1}) \cdot b(\omega_{2n}^{2n-1})) =: (c(\omega_{2n}^0), \ldots, c(\omega_{2n}^{2n-1})).$$

- Berechne in Zeit $\mathcal{O}(n \log n)$ die inverse DFT als

$$\tfrac{1}{2n} \cdot \mathrm{DFT}_{2n}(c(\omega_{2n}^0), \ldots, c(\omega_{2n}^{2n-1}), \omega^{-1}) := (c_0, \ldots, c_{2n-1}).$$

- $(c_0, \ldots, c_{2n-1})$ ist die Koeffizientenform von ab.

Körper und Ring

Definition Körper und Ring

Sei K eine Menge. Das Tupel $(K, +, \cdot)$ ist ein *Körper* falls

1. $(K, +)$ ist eine additive abelsche Gruppe mit neutralem Element 0.
2. $(K \setminus \{0\}, \cdot)$ ist eine multiplikative abelsche Gruppe.
3. Distributivität: $a \cdot (b + c) = a \cdot b + a \cdot c$ für alle $a, b, c \in K$.

Wir bezeichnen $(K, +, \cdot)$ als *Ring*, falls unter Punkt 2 *nicht* die Existenz von multiplikativen Inversen gefordert wird.

Notation: Wir schreiben abkürzend K statt $(K, +, \cdot)$.

Beispiele:

- $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ sind Körper.
- $\mathbb{Z}$ ist kein Körper, aber ein Ring.
- $\mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x], \mathbb{Z}[x]$ sind ebenfalls Ringe.

Endlicher Körper

Satz Primkörper

Sei p prim. Dann ist $(\mathbb{Z}_p, +, \cdot)$ ein Körper mit p Elementen. Wir bezeichnen diesen Körper als *Primkörper* $\mathbb{F}_p$.

Beweis:

1. $(\mathbb{Z}_p, +)$ ist eine additive abelsche Gruppe.
2. $(\mathbb{Z}_p \setminus \{0\}, \cdot) = (\mathbb{Z}_p^*, \cdot)$ ist eine multiplikative Gruppe.
3. Die Distributivität folgt aus der Distributivität über $\mathbb{Z}$.

Nullteilerfreiheit in Körpern

Lemma Multiplikation mit Null

Sei K ein Körper. Dann gilt für alle $a \in K$, dass $a \cdot 0 = 0 \cdot a = 0$.

Beweis:

- Es gilt $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$.
- Subtraktion von $a \cdot 0$ auf beiden Seiten liefert $a \cdot 0 = 0$.
- $0 \cdot a = 0$ folgt aus der Kommutativität.

Satz Nullteilerfreiheit

Sei K ein Körper. Dann gilt für alle $a, b \in K$, dass $ab = 0$ gdw $a = 0$ oder $b = 0$.

Beweis:

- $\Leftarrow$: Folgt aus obigem Lemma.
- $\Rightarrow$: Sei $ab = 0$ und $a \neq 0$. Dann gilt

$$b = 1 \cdot b = a^{-1} \cdot a \cdot b = a^{-1} \cdot 0 = 0.$$

Polynome über Körpern

Definition Polynome über Körpern

Sei K ein Körper. Dann bezeichnen wir ein Polynom $a(x) \in K[x]$ mit Koeffizienten aus K als *Polynom über K*.

Anmerkungen:

- Arithmetik $+, -, \cdot, \mathrm{eval}$ ist für $a(x) \in K[x]$ kanonisch definiert.
- Erinnerung: Für $a, b \in \mathbb{Q}[x]$ mit $b \neq 0$ gibt es $q, r \in \mathbb{Q}[x]$ mit
$$a = q \cdot b + r \quad \text{und } \mathrm{grad}(r) < \mathrm{grad}(b).$$
- Gilt analog, falls $\mathbb{Q}$ durch einen anderen Körper K ersetzt wird.

Fundamentalsatz der Algebra

Satz Fundamentalsatz der Algebra

Sei K ein Körper. Sei $p(x) \in K[x]$ mit $\text{grad}(p) = n \geq 0$. Dann besitzt $p(x)$ höchstens n Nullstellen.

Beweis: per Induktion über n.

- **IV** für $n = 0$: Es gilt $p(x) \neq 0$, d.h. $p(x)$ besitzt keine Nullstelle.
- **IS** für $n - 1 \rightarrow n$.
- **Fall 1:** $p(x)$ besitzt keine Nullstelle und damit höchstens n.
- **Fall 2:** Sei $p(x)$ vom Grad $n \geq 1$ mit Nullstelle x_0.
- Euklidische Division liefert q, r mit
$$p = q \cdot (x - x_0) + r \text{ mit } \text{grad}(r) < 1.$$
- Wir werten $p(x)$ an der Nullstelle x_0 aus
$$0 = p(x_0) = q(x_0) \cdot (x_0 - x_0) + r(x_0) = r(x_0).$$
- Damit folgt $r(x) = 0$ und $p(x) = q(x) \cdot (x - x_0)$ mit $\text{grad}(q) = n - 1$.
- Nach IA besitzt q höchstens $n - 1$ Nullstellen.
- Damit besitzt p höchstens n Nullstellen.

Ordnungen und Teilbarkeit

Ziel: Wir wollen zeigen, dass $(K^*, \cdot)$ für jeden Körper K zyklisch ist.

Lemma Teilbarkeit der Ordnung

Sei G eine abelsche (multiplikative) Gruppe. Dann gilt für alle $a \in G$ und $k \in N$, dass $a^k = 1$ gdw $\mathrm{ord}(a)|k$.

Beweis:

- $\Leftarrow$: Sei $k = \mathrm{ord}(a)q$ für ein $q \in \mathbb{N}$. Dann ist $a^k = (a^{\mathrm{ord}(a)})^q = 1$.
- $\Rightarrow$: Falls $a^k = 1$, dann gilt $k \geq \mathrm{ord}(a)$.
- Euklidische Division: q, r mit $k = q \cdot \mathrm{ord}(a) + r$ und $r < \mathrm{ord}(a)$.
- Es gilt $1 = a^k = a^{q \cdot \mathrm{ord}(a)+r} = 1^q \cdot a^r = a^r$ mit $r < \mathrm{ord}(a)$. (Widerspruch zur Minimalität von $\mathrm{ord}(a)$)

Multiplikativität der Ordnung

Lemma Multiplikativität der Ordnung

Sei G eine abelsche Gruppe. Seien a, b in G mit $\mathrm{ggT}(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$. Dann gilt $\mathrm{ord}(ab) = \mathrm{ord}(a) \cdot \mathrm{ord}(b)$.

Beweis:

- Es gilt $\mathrm{ord}(ab) | \mathrm{ord}(a) \cdot \mathrm{ord}(b)$ wegen
$$(ab)^{\mathrm{ord}(a)\cdot\mathrm{ord}(b)} = (a^{\mathrm{ord}(a)})^{\mathrm{ord}(b)} \cdot (b^{\mathrm{ord}(b)})^{\mathrm{ord}(a)} = 1.$$
- Ann: $\mathrm{ord}(ab) \cdot k = \mathrm{ord}(a) \cdot \mathrm{ord}(b)$ mit $k > 1$.
- OBdA $k' = \mathrm{ggT}(\mathrm{ord}(a), k) > 1$ mit $k' | k$. Dann gilt
$$1 = (ab)^{\frac{\mathrm{ord}(a)\mathrm{ord}(b)}{k'}} = a^{\frac{ord(a)\mathrm{ord}(b)}{k'}} \cdot (b^{\mathrm{ord}(b)})^{\frac{\mathrm{ord}(a)}{k}'} = a^{\frac{ord(a)\mathrm{ord}(b)}{k'}}.$$
- D.h. $\mathrm{ord}(a) | \frac{ord(a)\mathrm{ord}(b)}{k'}$ und $\mathrm{ggT}(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$.
- Damit folgt $\mathrm{ord}(a) | \frac{ord(a)}{k'}$. (Widerspruch wegen $k' > 1$)

Elementordnung teilt maximale Ordnung

Lemma Ordnung teilt maximale Ordnung

Sei G eine endliche abelsche Gruppe. Sei $a \in G$ mit maximaler Ordnung. Dann gilt für alle $b \in G$, dass $\mathrm{ord}(b) | ord(a)$.

Beweis:

- Annahme: $\mathrm{ord}(b) \nmid \mathrm{ord}(a)$
- D.h. es existiert eine Primzahlpotenz p^i mit
$$p^{i+1} \mid \mathrm{ord}(b) \text{ und } p^i \mid \mathrm{ord}(a) \text{ aber } p^{i+1} \nmid \mathrm{ord}(a).$$
- Wir definieren $a' = a^{p^i}$ und $b' = b^{\frac{\mathrm{ord}(b)}{p^{i+1}}}$.
- Damit gilt $\mathrm{ord}(a') = \frac{\mathrm{ord}(a)}{p^i}$ und $\mathrm{ord}(b') = p^{i+1}$.
- Wegen $p \nmid \mathrm{ord}(a')$ folgt $\mathrm{ggT}(\mathrm{ord}(a'), ord(b')) = 1$.
- Lemma zur Multiplikativität: $\mathrm{ord}(a'b') = \mathrm{ord}(a) \cdot p > \mathrm{ord}(a)$. (Widerspruch zur Maximalität von $\mathrm{ord}(a)$)

K^* ist zyklisch

Satz K^* ist zyklisch

Sei K ein endlicher Körper. Dann ist die multiplikative Gruppe $(K^*, \cdot) = (K \setminus \{0\}, \cdot)$ zyklisch.

- Sei $a \in K^*$ ein Element maximaler Ordnung.
- Die Elementordnung teilt die Gruppenordnung, d.h. $\mathrm{ord}(a) || K^* |$.
- Wir betrachten das Polynom $p(x) = x^{\mathrm{ord}(a)} - 1$.
- Für alle $b \in K^*$ gilt $\mathrm{ord}(b) \mid \mathrm{ord}(a)$.
- Damit ist $p(b) = b^{\mathrm{ord}(a)} - 1 = 0$, d.h. jedes b ist eine Nullstelle.
- D.h. $p(x)$ besitzt mindestens $|K^*|$ viele Nullstellen.
- Fundamentalsatz: Jedes Polynom vom Grad $\mathrm{ord}(a)$ besitzt höchstens $\mathrm{ord}(a)$ viele Nullstellen über einem Körper K.
- Es folgt $|K^*| \leq \mathrm{ord}(a)$. Mit $\mathrm{ord}(a) \mid |K^*|$ gilt daher $\mathrm{ord}(a) = |K^*|$.
- D.h. das Element a ist ein Generator für K^*.