Computer Algebra

Sebastian Iwanowski
FH Wedel

4. Polynomarithmetik
Teil 1: Addition und Multiplikation

Referenzen zum Nacharbeiten:

Köpf 6.1-6.3
Seminararbeit 5 (Helge Janetzko)

Computer Algebra 4

Darstellung von Polynomen

- Vektor aus Koeffizienten

  $(a_0,a_1,\ldots,a_{n-1},a_n) \triangleq a_n\, x^n + a_{n-1}\, x^{n-1} + \ldots + a_1\, x + a_0$ Polynom vom Grad n

- Komplexitätsgröße n eines Polynoms

  n ist die Anzahl der Koeffizienten, d.h. der Vektor hat die Länge n.
  Ein Polynom der Größe n hat also Grad n-1.
  Die Größe der Koeffizienten wird in der Regel nicht berücksichtigt.

- Addition und Subtraktion von Polynomen

  gerechnet wird koeffizientenweise ohne Übertrag.
  Größe der Summe/Differenz von Polynomen der Größe n bleibt n.
  Laufzeit: O(n) (trivial)

Computer Algebra 4

Algorithmen zur Multiplikation von Polynomen p und q

Die Polynomgröße beider Operanden sei n => Die Polynomgröße von r = p•q ist 2n-1.

- Schulmethode (Cauchyprodukt)

  $r_k = \sum_{i+j=k} p_i \cdot q_j$ für k=0,…,2n-2

  Gesamtlaufzeit: $O(n^2)$

- Rekursive Bisektionierung

  Algorithmus von Karatsuba: $O(n^{\log_2(3)})$

- über Schnelle Fouriertransformierte (FFT)

  Gesamtlaufzeit: O(n log n)

Computer Algebra 4

Multiplikation über Stützstellenmatrizen für r(x) = p(x) • q(x)

Grundidee: Die Koeffizienten eines Polynoms der Größe n sind durch Angabe von n Funktionswerten eindeutig bestimmt.

für beliebige Stützstellen:

- Berechne die Funktionswerte von p und q für 2n-1 Stützstellen x_i — Laufzeit: $O(n^2)$

  Matrixmultiplikation

- Berechne die Funktionswerte von $r(x_i) = p(x_i) \bullet q(x_i)$ diesen Stützstellen — Laufzeit: $O(n)$

  Einfache Zahlenmultiplikation

- Bestimme die Koeffizienten von r aus diesen Funktionswerten — Laufzeit: $O(n^2)$

  Multiplikation mit der inversen Matrix

Computer Algebra 4

Multiplikation über FFT für r(x) = p(x) • q(x)

Spezialfall: Wähle als Stützstellen eine (2n-1)-te primitive Wurzel von 1
und ihre Potenzen: $\zeta, \zeta^2, \ldots, \zeta^{2n-2}, \zeta^{2n-1} = 1$

für eine (2n-1)-te primitive Einheitswurzel:

- Berechne die Funktionswerte von p und q für diese 2n-1 Stützstellen x_i

  FFT

  Laufzeit: O(n log n)

- Berechne die Funktionswerte von $r(x_i) = p(x_i) \cdot q(x_i)$ diesen Stützstellen

  Einfache Zahlenmultiplikation

  Laufzeit: O(n)

- Bestimme die Koeffizienten von r aus diesen Funktionswerten

  Inverse FFT

  Laufzeit: O(n log n)