

Randomisierte Algorithmen

Ein sehr weites Gebiet.

- Las Vegas– und Monte Carlo–Algorithmen
- Universales Hashing, Bloom-Filter
- Symmetry Breaking
- Routing-Algorithmen
- Derandomisierung
- ...

Einfaches Beispiel

Eingabe: Zwei Polynome

Frage: Sind sie gleich?

$$(x - 13)(x - 5)(x - 3)(x + 7)(x^2 + 12)$$
$$\stackrel{?}{=} x^6 - 14x^5 - 16x^4 + 472x^3 - 1701x^2 + 7656x - 16380$$

Ausmultiplizieren: $\Theta(d^2)$ Multiplikationen

Geht es schneller?

Bloom-Filter

Wir wollen einmal ein Wörterbuch erstellen.

Dann schlagen wir sehr oft darin nach, ob es gegebene Wörter enthält.

Das Wörterbuch enthalte w_1, \dots, w_n .

Wieviel Platz benötigen wir dafür?