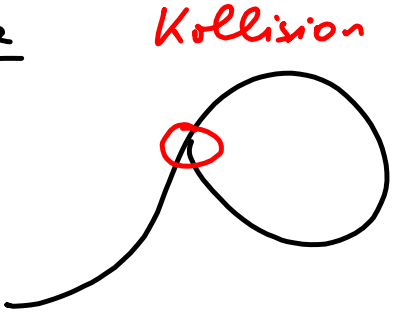
Pollard-ϱ-Analyse



Wann ist eine Kollision zu erwarten, wenn es n mögliche Werte für y gibt?

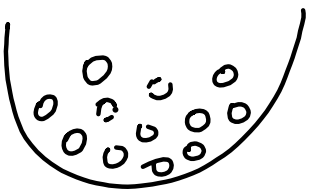
Erwartung gerechtfertigt, wenn Wahrscheinlichkeit dafür $> 50\,\%$, d.h. $> \frac{1}{2}$

Wir berechnen die Wahrscheinlichkeit, dass eine Kollision nach k Versuchen noch nicht erreicht ist.

Urnenmodell:

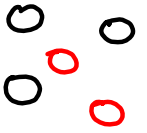
n Kugeln,

Ziehen mit Zurücklegen



1. Zug ✓ $\left[\frac{n-0}{n}=1\right]$
2. Zug $\frac{n-1}{n}$
3. Zug $\frac{n-2}{n}$
⋮
k. Zug $\frac{n-(k-1)}{n}$

} gleichzeitig erfüllt



$$P(k) = \underbrace{\frac{n-1}{n}\cdot\frac{n-2}{n}\cdot\ldots\cdot\frac{n-(k-1)}{n}}_{\prod_{j=1}^{k-1}\frac{n-j}{n}} \overset{!}{\leq} \frac{1}{2}$$

$$= \prod_{j=1}^{k-1}\left(1-\frac{j}{n}\right)$$

Idee: $1+x_j < e^x = 1+\frac{1}{1!}x+\frac{1}{2!}x^2+\frac{1}{3!}x^3+\ldots$

$$\square < \prod_{j=1}^{k-1} e^{-\frac{j}{n}} = e^{\sum_{j=1}^{k-1}-\frac{j}{n}}$$

$e^{x_1}\cdot e^{x_2} = e^{x_1+x_2}$

$$= e^{-\frac{1}{n}\sum_{j=1}^{k-1} j} = e^{-\frac{1}{n}\cdot(k-1)\cdot k/2} \overset{!}{\leq} \frac{1}{2}$$

$$+\frac{1}{2n}\cdot(k-1)\cdot k \leq -\ln\left(\frac{1}{2}\right) = +\ln 2$$

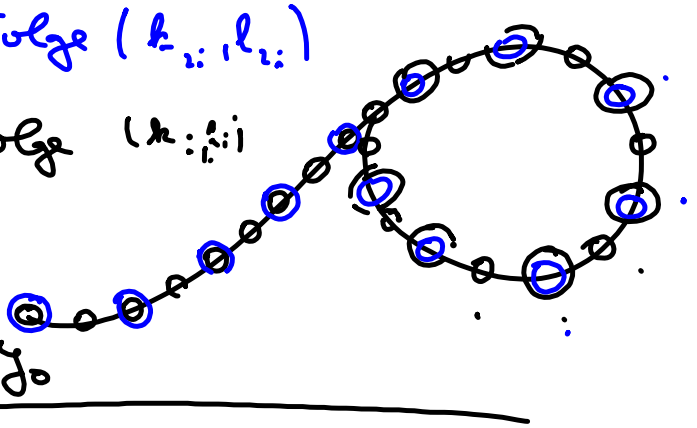
$$k^2 \geqslant (k-1)\cdot k \geqslant 2n\cdot\ln(2)$$

$$k \geqslant \sqrt{2\ln 2\cdot n} \qquad k \sim \mathcal{O}(\sqrt{n})$$

Kollisionserkennung (ohne Hauptspeicherbedarf)

y_{2i} schnelle Folge (k_{2i}, l_{2i})

y_i langsame Folge (k_i, l_i)

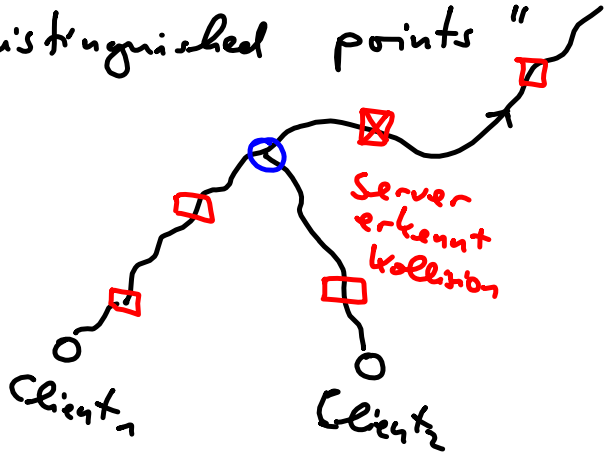


Im Kreis wird die schnelle Folge die langsame Folge einholen, der Abstand vermindert sich jedesmal um 1.

Parallelisierung

1996 v. Oorschot / Wiener Pollard-λ

"distinguished points"



Server sammelt

(y, k, ℓ)

mit "unterste m Bits von y sind $= 0$"

$m > 20$ experimentell setzen