Mathematisches Institut
der Universität München
Pascal Reisert

Wintersemester 2015/2016
Übungsblatt 2
4. November 2015

Übungen zur Algorithmischen Zahlentheorie
Lösung

Aufgabe 6

c) Der folgende Beweis wurde von *Ludwig Fürst* in der Zentralübung vorgerechnet:

Sei α_n der minimale Eintrag von $\vec{p}^{\,n}$ und β_n der maximale Eintrag von $\vec{p}^{\,n}$. Wir erkennen sofort, dass

$$\vec{p}_k^{\,n+1} = \sum_{i\in\mathbb{Z}_m} p_i \vec{p}_{k-i}^{\,n} \leqslant \beta^n \sum_{i\in\mathbb{Z}_m} p_i = \beta_n$$

und somit $\beta_{n+1} \leqslant \beta_n$. Sei i_n ein Index mit $\vec{p}_{i_n}^{\,n} = \beta_n$ und j_0 ein Index mit $p_{j_0} > 0$ minimal. Dann gilt

$$\begin{aligned}\vec{p}_k^{\,n+1} &= \sum_{i\in\mathbb{Z}_m} \vec{p}_i^{\,n} p_{k-i} = \beta_n p_{k-i_n} + \sum_{i_n\neq i\in\mathbb{Z}_m} \vec{p}_i^{\,n} p_{k-i} \\ &\geqslant \beta_n p_{k-i_n} + \alpha_n(1-p_{k-i_n}) \geqslant \alpha_n + (\beta_n-\alpha_n)p_{j_0}.\end{aligned}$$

Wir erhalten für die Differenz $\varepsilon_{n+1} = \beta_{n+1} - \alpha_{n+1} \leqslant \beta_n - \alpha_n - (\beta_n-\alpha_n)p_{j_0} = \varepsilon_n(1-p_{j_0}) = \varepsilon_1(1-p_{j_0})^n \xrightarrow{n\to\infty} 0$. Es folgt, dass für alle $k \in \mathbb{Z}_m : \vec{p}_k^{\,n} \to \frac{1}{m}$, da offensichtlich $\alpha_n \leqslant \frac{1}{m} \leqslant \beta_n$ für alle $n \geqslant 1$ gilt.

Variante:

Man beachte, dass wir die n-fache Faltung als erste Spalte von $P^n,\ n \geqslant 1$ mit

$$P = \begin{pmatrix} p_0 & p_{m-1} & \cdots & p_1 \\ p_1 & p_0 & & p_2 \\ \vdots & & & \vdots \\ p_{m-1} & p_{m-2} & \cdots & p_0 \end{pmatrix}$$

auffassen können. Die Gleichverteilung entspricht der Matrix $U = (1/m)_{i,j\in\mathbb{Z}_m}$. P is offensichtlich normal, da

$$(P^tP - PP^t)_{ij} = \sum_{k\in\mathbb{Z}_m} p_{-i+k}p_{-j+k} - p_{i-k}p_{j-k} = \sum_{k\in\mathbb{Z}_m} p_{-i+(i+j-k)}p_{-j+(i+j-k)} - p_{i-k}p_{j-k} = 0.$$

Da P^n und U kommutieren, sind sie simultan diagonalisierbar (über $\mathbb{C}$). Es bleibt zu zeigen, dass die Eigenwerte von P gegen die Eigenwerte von U konvergieren. Man erkennt sofort, dass U und P den gemeinsamen Eigenvektor $u := (1)_{i\in\mathbb{Z}_m}$ zum Eigenwert 1 haben. Die weiteren Eigenwerte von U sind 0 zu den Eigenvektoren $e_i - e_{i-1}, 1 \leqslant i \leqslant m-1$ wobei e_i die Standardeinheitsvektoren bezeichnen. Sei λ ein Eigenwert von P zum Eigenvektor

$v = (v_i)_{i\in\mathbb{Z}_m} \notin \langle u\rangle$ und $v_{i_0} = \max_{i\in\mathbb{Z}_m} |v_i| \neq 0$. Man beachte, dass es $m-1$ Eigenvektoren $\notin \langle u\rangle$ gibt. Jetzt gilt

$$Pv = \lambda v \Rightarrow \sum_{i\neq i_0} p_{i_0 i} v_i = (\lambda - p_{i_0 i_0}) v_{i_0}$$

$$\Rightarrow |\lambda - p_0| = \left| \sum_{i\neq i_0} p_{i_0 i} \frac{v_i}{v_{i_0}} \right| < \sum_{i\neq i_0} p_{i_0 i} = 1 - p_0,$$

wobei wir in der letzten Ungleichung verwendet haben, dass mindestens ein $v_i \neq v_{i_0}$ ist.[1] Somit sind alle Eigenwerte $\lambda_i, 1 \leqslant i \leqslant m-1$ von P vom Betrag kleiner 1 mit der Ausnahme des einfachen Eigenwertes $\lambda_0 = 1$. P^n hat dann Eigenwerte $\lambda_i^n, 0 \leqslant i \leqslant m-1$, d.h., P konvergiert gegen U und $\vec{p}^{\,n} \to u$.

Aufgabe 8

Man identifiziere

```
A B C D E F G H I J K  L  M  N  O  P  Q  R  S  T  U  V  W  X  Y  Z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25.
```

a) Wir berechnen z.B. für $d = 5$, $\sigma_5(0+3) = 3+5 = \mathtt{I} \Rightarrow \sigma_5(0+8) = 8+5 = \mathtt{N} \Rightarrow \sigma_5(0+13) = 13+5 = \mathtt{S}$, usw.

```
d=5   INSXCHMRWBGLQVAFKPUZEJOTYD
```

Analog erhalten wir

```
d=6   JPVBHNTZFLRXDJPVBHNTZFLRXD
d=13  QDQDQDQDQDQDQDQDQDQDQDQDQD
```

Diese Verschlüsselung hängt jedoch stark von der Assoziation $\mathfrak{A} \simeq \mathbb{Z}_{26}$ ab. Es ist z.B. für

```
A B C D E F G H I J  K  L  M  N  O  P  Q  R  S  T  U  V  W  X  Y  Z
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26.
```

```
d=5   IOUAGMSYEKQWCIOUAGMSYEKQWC
d=6   JQXELSZGNUBIPWDKRYFMTAHOVC
d=13  QESGUIWKYMAOCQESGUIWKYMAOC
```

Wir erkennen, dass dies gerade der ersten Formulierung mit $y_0 = 2$ und $d = 6, 7, 14$ entspricht.

b) Formal gilt

$$y_1 = \sigma_d(x_1 + y_0) = x_1 + y_0 + d, \quad y_2 = \sigma_d(x_2 + y_1) = x_2 + x_1 + y_0 + 2\cdot d,$$

$$y_3 = \sigma_d(x_3 + y_2) = x_3 + x_2 + x_1 + y_0 + 3\cdot d, \text{usw.}$$

Gegeben einen verschlüsselten Text $(y_1, \ldots, y_N)$ bestimme man $y'_1 = y_1$ und $y'_i = y_i - y_{i-1} = x_i + d$, $1 \leqslant i \leqslant N$. Jetzt kann $(y'_2, \ldots, y'_N)$ entschlüsselt werden und anschließend erhält man normalerweise leicht x_1.

[1] Für $\varphi_j \neq \varphi_k$ gilt bereits $\left|p_j e^{i\varphi_j} + p_k e^{i\varphi_k}\right|^2 = p_j^2 + p_k^2 + 2p_j p_k \cos(\varphi_j - \varphi_k) < (p_j + p_k)^2$.

c) Es ist

$$\begin{aligned}&\texttt{NWIREVTPYISBTQXJOXWCSBMRXTGPFKBYDURPUF}\\ &= (14, 23, 9, 18, 5, 22, 20, 16, 25, 9, 19, 2, 20,\\ &\quad 17, 24, 10, 15, 24, 23, 3, 19, 2, 13, 18, 24,\\ &\quad 20, 7, 16, 6, 11, 2, 25, 4, 21, 18, 16, 21, 6).\end{aligned}$$

Wie in b) erhalten wir daraus

$$\begin{aligned}&(y'_2, \ldots, y'_N)\\ &= (9, 12, 9, 13, 17, 24, 22, 9, 10, 10, 9, 18, 23,\\ &\quad 7, 12, 5, 9, 25, 6, 16, 9, 11, 5, 6, 22, 13, 9,\\ &\quad 16, 5, 17, 23, 5, 17, 23, 24, 5, 11).\end{aligned}$$

Wir bestimmen die Häufigkeit der auftretenden Zahlen zu

Buchstabe	Anzahl	Buchstabe	Anzahl	Buchstabe	Anzahl
9	7	12	2	13	2
17	3	24	2	22	2
10	2	18	1	23	3
7	1	5	5	25	1
6	2	16	2	11	2

Wir vermuten, dass $9 = \texttt{e}$, also $d = 4$ und somit

`eheimtreffenschaeublegabrielamsamstag`

Der fehlende Buchstaben ist leicht zu erkennen $x_1 = \texttt{g}$ und $y_0 = 2$. Wie erhalten

Geheimtreffen Schäuble Gabriel am Samstag.