Shorin algoritmin matematiikkaa

Edvard Fagerholm

Määritelmiä

Määritelmä 1 Ryhmä G on *syklinen*, jos $\exists a \in G$ s.e. $G = \langle a \rangle$.

Määritelmä 2 Olkoon G ryhmä. Tällöin alkion $a \in G$ *kertaluku* $\text{ord}(a)$ on pienin luku $n \in \mathbb{N} \setminus \{0\}$, jolla $a^n = 1$. Jos lukua ei ole, niin $\text{ord}(a) := \infty$.

Määritelmä 3 Kuvausta $\phi : \mathbb{N} \to \mathbb{N}$, $\phi(1) = 1$, $\phi(n) = \#\{k \in \mathbb{N} \mid k < n,\ \gcd(k, n) = 1\}$, $n > 1$, sanotaan Eulerin ϕ-funktioksi.

Algebran perusteita

Lause 4 *Olkoon G ryhmä, $a \in G$ ja $a^k = 1$. Tällöin $ord(a) \mid k$.*

Todistus. Kirjoitetaan $k = n\text{ord}(a) + r$, missä $0 \leq r < \text{ord}(a)$. Tällöin $a^r = a^{k-n\text{ord}(a)} = 1$, joten kertaluvun määritelmän nojalla $r = 0$. ■

Lause 5 *(Lagrangen lause) Jos $H \leq G$ ja G on äärellinen, niin $\#H \mid \#G$.*

Todistus. Ks. diskreetin matematiikan moniste tai C2. ■

Lause 6 *Olkoon* $\gcd(a, n) = 1$. *Tällöin* $a^{\phi(n)} \equiv 1 \,(mod\ n)$.

Todistus. Suoraan määritelmästä $\phi(n) = \#\mathbb{Z}_n^*$. Koska $\langle a \rangle \leq \mathbb{Z}_n^*$, niin Lagrangen lauseen nojalla $\text{ord}(a) = \#\langle a \rangle \mid \phi(n)$. ■

Erään apufunktion periodisuudesta

Lause 7 *Olkoon* $1 < a < M$ *ja* $gcd(a, M) = 1$. *Tällöin kuvaus* $f : \mathbb{Z} \to \mathbb{Z}_M$, $f(x) = a^x \ (mod\ M)$, *on periodinen ja* f*:n pienin periodi on* $ord(a_M)$.

Todistus. Nähdään suoraan, että $f(x + \mathrm{ord}(a_M)) = f(x)$, joten f on periodinen. Edelleen lauseesta 4 seuraa, että tämä on pienin periodi. ■

Shorin algoritmi

Shorin algoritmi perustuu seuraavaan ideaan luvun M faktoroimiseksi.

1. Valitaan jokin $1 < a < M$, jolle $\gcd(a, M) = 1$.
2. Selvitetään kuvauksen $f : \mathbb{Z} \to \mathbb{Z}_M, f(x) = a^x_M$, *pienin* periodi n.
3. Jos n on parillinen, niin $(a^{n/2} - 1)(a^{n/2} + 1) \equiv 0 \pmod{M}$.
4. Lasketaan $d_1 := \gcd(a^{n/2} - 1, M)$ ja $d_2 := \gcd(a^{n/2} + 1, M)$.
5. Katsotaan onko d_1 tai d_2 M:n tekijä.

Huom: Kvanttimekaniikkaa hyödyntää askel 2. Lisäksi algoritmi on *probabilistinen*, joten se ei aina löydä tekijää. Näin käy esim. kun n on pariton.

Algoritmin perustelu

- Oletuksena n on parillinen, joten

$$a^n \equiv 1 \,(\mathrm{mod}\ M) \quad \Leftrightarrow \quad a^n - 1 \equiv 0 \,(\mathrm{mod}\ M)$$
$$\Leftrightarrow \quad (a^{n/2} - 1)(a^{n/2} + 1) \equiv 0 \,(\mathrm{mod}\ M)$$

- Jos $p \mid M$, niin $p \mid a^{n/2} - 1$ tai $p \mid a^{n/2} + 1$.
  $\Longrightarrow d_1 := \gcd(a^{n/2} - 1, M) \neq 1$ tai $d_2 := \gcd(a^{n/2} + 1, M) \neq 1$

- Nyt jos $d_i \neq 1$, niin tämä on joko M:n aito tekijä tai sitten $d_i = M$.
  - Tapaus $d_1 \neq 1$. Jos $d_1 = M$ niin $a^{n/2} \equiv 1 \,(\mathrm{mod}\ M)$.
    Mahdotonta (a:n kertaluku n), joten löydetään aina tekijä.
  - Tapaus $d_2 \neq 1$. Voi olla $d_2 = M$, jolloin $a^{n/2} \equiv -1 \,(\mathrm{mod}\ M)$.

Algoritmin perustelu jatk.

Edellisten nojalla voidaan formuloida seuraava lause:

Lause 8 *Algoritmin iteraatio löytää M:n aidon tekijän, jos n on parillinen ja $a^{n/2} \not\equiv -1 \, (mod \; M)$.*

Algoritmin ideana on ajaa se useita kertoja valitsemalla satunnaisia a kunnes löydetään tekijä. Oleellista on tällöin tapahtuman todennäköisyys

$$\mathbb{P}(\text{"satunnaisella } a \text{ algoritmi ei löydä tekijää"}).$$

Edellisten nojalla on osoitettu, että tämä todennäköisyys on korkeintaan

$$\mathbb{P}(\text{"}n \text{ on pariton tai } a^{n/2} \equiv -1 \, (\text{mod } M)\text{"}).$$

Todennäköisyyden johtaminen

Merkitään:

- $M = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$
- $n = \text{ord}(a_M)$
- $n_i = \text{ord}(a_{p_i^{\alpha_i}})$
- Oletetaan myös, että $2 \nmid M$, jolloin $1 \not\equiv -1 \pmod{p_i^{\alpha_i}}$

Todennäköisyyden johtaminen jatk.

Lemma 9 *Edellisillä merkinnöillä* $n = lcm(n_1, \ldots, n_k)$.

Todistus. Merkitään $m = \text{lcm}(n_1, \ldots, n_k)$. Koska $M \mid a^n - 1$, niin $p_i^{\alpha_i} \mid a^n - 1$ kaikilla i. Lauseesta 4 seuraa, että $n_i \mid n$, joten $m \mid n$. Nyt määritelmän nojalla kaikilla $n_i \mid m$, joten $p_i^{\alpha_i} \mid a^m - 1$. Tästä seuraa, että $M \mid a^m - 1$. Kertaluvun määritelmän nojalla $n \leq m$, joten $m = n$. ■

Todennäköisyyden johtaminen jatk.

Lemma 10 *$a^{n/2} \equiv -1 \,(mod\ M)$ joss $a^{n/2} \equiv -1 \,(mod\ p_i^{\alpha_i})$ kaikilla i.*

Todistus. $\Rightarrow$: Jos $M \mid a^{n/2}+1$, niin $p_i^{\alpha_i} \mid a^{n/2}+1$ kaikilla i.

$\Leftarrow$: Kiinalaisesta jäännöslauseesta seuraa, että yhtälöryhmällä

$$\begin{aligned} x &\equiv -1 \,(\text{mod } p_1^{\alpha_1}) \\ &\vdots \\ x &\equiv -1 \,(\text{mod } p_k^{\alpha_k}) \end{aligned}$$

on ratkaisu ja ratkaisu on yksikäsitteinen modulo M. Selvästi -1 on ratkaisu, joten oletuksen ja ratkaisun yksikäsitteisyyden nojalla $a^{n/2} \equiv -1 \,(\text{mod } M)$. ■

Todennäköisyyden johtaminen jatk.

Lemma 11 *Kirjoitetaan* $n_i = s_i 2^{t_i}$, *missä* $2 \nmid s_i$ *ja olkoon* $s = lcm(s_1, \ldots, s_k)$, $t = \max(t_1, \ldots, t_k)$. *Tällöin seuraavat pätevät:*

(i) $n = s2^t$

(ii) $a^{n/2} \equiv -1 \,(mod\ M) \Rightarrow t_i = t_j,\ i, j = 1, \ldots, k.$

Todistus. Kohta (i) seuraa suoraan lemmasta 9. Kohdan (ii) osoittamiseksi oletetaan, että $\exists i, j$, jolla $t_i \neq t_j$. Tällöin löydetään $t_i < t$, joten $n_i \mid n/2$. Tästä seuraa, että $a^{n/2} \equiv 1 \,(\mathrm{mod}\ p_i^{\alpha_i})$, joten lemman 10 nojalla $a^{n/2} \not\equiv -1 \,(\mathrm{mod}\ M)$. ■

Lemma 12 *Ryhmä* $\mathbb{Z}_{p^n}^*$ *on syklinen.*

Todistus. Sivuutetaan. ■

Todennäköisyyden johtaminen jatk.

Propositio 13 $P(t_i = j) \leq 1/2$.

Todistus. Edellisen lauseen nojalla $\mathbb{Z}^*_{p_i^{\alpha_i}}$ on syklinen, joten olkoon g tämän virittäjä. Nyt ryhmän satunnaisen alkion valinta on sama kuin valitsisi luvun $b \in \{1, \ldots, \phi(p_i^{\alpha_i})\}$. Olkoon sitten $\mathrm{ord}(g) = u2^v$, missä $2 \nmid u$. Jos $a = g^b$, niin $\mathrm{ord}(a) = \mathrm{ord}(g^b) = s_i 2^{t_i}$. Edelleen nähdään, että $(g^b)^{s_i 2^{t_i}} = g^{b s_i 2^{t_i}} = 1$, joten $u2^v = b s_i 2^{t_i}$ ja saadaan kaksi tapausta:

1. b on parillinen
2. b on pariton

Ensimmäisessä tapauksessa $b = 2b'$, joten $u2^v = b' s_i 2^{t_i+1}$ ja jälkimmäisessä tapauksessa on oltava $v = t_i$. Nähdään erityisesti, että puolissa tapauksista $t_i \neq j$, josta seuraa väite. ■

Todennäköisyyden johtaminen jatk.

Lause 14 *Todennäköisyys, että Shorin algoritmi ei löydä luvun* $M = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ *tekijää yhdellä iteraatiolla on korkeintaan* $\frac{1}{2^{k-1}}$.

Todistus. Lauseen 8 nojalla algoritmi ei välttämättä löydä tekijää, jos n on pariton tai $a^{n/2} \equiv -1 \pmod{M}$. Lemman 11 nojalla saadaan ensimmäinen tapaus, jos $t = 0$, ts. $t_i = 0$ kaikilla i, kun jälkimmäinen tapaus seuraa, jos $t_i = j > 0$ kaikilla i. Tapahtumalle $A =$"algoritmi ei löydä tekijää" saadaan siis

$$\begin{aligned} \mathbb{P}(A) &\leq \sum_j \mathbb{P}(t_i = j \ \forall i) = \sum_j \prod_{i=1}^{k} \mathbb{P}(t_i = j) \\ &\leq \frac{1}{2^{k-1}} \sum_j \mathbb{P}(t_1 = j) = \frac{1}{2^{k-1}}. \end{aligned}$$

■