Om Josefus' permutation

Anders Thorup

Institut for Matematiske Fag
Københavns Universitet
København
thorup@math.ku.dk

1 Introduktion

På et indledende algebrakursus i København lærer man, at enhver permutation af tallene $1, 2, \ldots, n$ entydigt kan fremstilles som et produkt (sammensætning) af disjunkte cykler. Ved undervisningen i kurset stilles blandt andet følgende to opgaver:

Opgave 1. Bestem cykelfremstillingen af følgende permutation:

$$\omega = (1\,2\,3\,4\,\ldots\,n)\cdots(1\,2\,3\,4)\;(1\,2\,3)\;(1\,2). \tag{1}$$

Opgave 2.* Samme spørgsmål for permutationen,

$$\sigma = (1\,2)\;(1\,2\,3)\;(1\,2\,3\,4)\cdots(1\,2\,3\,4\,\ldots\,n). \tag{2}$$

Opgaverne er gode øvelser i at arbejde med permutationer og cykler. De to permutationer er angivet som produkter af cykler, der ikke er disjunkte. Det er ikke så svært at vise for ω, at cykelfremstillingen er et produkt af disjunkte 2-cykler (transpositioner),

$$\omega = (1\;\;n)\;(2\;\;n{-}1)\;(3\;\;n{-}2)\;\cdots; \tag{3}$$

hvis n er lige, $n = 2i$, ender fremstillingen med transpositionen $(i\;\;i{+}1)$, og hvis n er ulige, $n = 2i + 1$, er tallet $i + 1$ fixpunkt, og fremstillingen ender med $(i\;\;i{+}2)$. Ækvivalent betyder det, at ω er permutationen, der ombytter rækkefølgen af tallene $1, 2, \ldots, n$, og ω er eksplicit givet ved udtrykket,

$$\omega(x) = n + 1 - x. \tag{4}$$

Opgave 2 ligner overfladisk den første, det er de samme faktorer, der indgår, blot i omvendt rækkefølge. I kurset er opgaven markeret som svær. Faktisk er den i hvert fald så svær, at jeg ikke selv kan løse den! Det er selvfølgelig nemt nok for et givet, ikke for stort, n at bestemme fremstillingen, men problemet er, at det er svært at se et mønster i hvordan fremstillingerne varierer med n. Man kan nøjes med at spørge efter *cykeltypen* af σ, dvs en angivelse af det antal p-cykler for $p = 1, 2, \ldots$, der indgår i fremstillingen af σ (her svarer 1-cykler til fixpunkter og 2-cykler til transpositioner).

Opgaven har gennem årene udfordret nogle af deltagerne i kurset, både studerende og lærere. Et par stykker er blevet lidt sure over at have prøvet kræfter med en opgave, der "ikke kan regnes", men gennem årene er der faktisk blevet opdaget et par overraskende egenskaber ved permutationen σ. De fleste er er fundet ved at lade en computer udskrive cykelfremstillingen af σ for forskellige værdier af n. Det følgende er en beretning om disse opdagelser. Det vil fremgå af afsnit 2, hvorfor permutationen σ kunne kaldes Josefus' permutation. Spørgsmålet om cykeltypen af σ besvares i tilfældet, hvor n er af formen 2^{m-1} eller $2^{m-1} - 1$. Svaret er ganske kompliceret. For n i almindelighed er opgave 2 stadig en udfordring.

2 En færdig formel

Som nævnt er cykelfremstillingen af σ ikke kendt i almindelighed, og når man kigger på fremstillingen for små værdier af n er det svært at finde et mønster. Det var derfor ret overraskende, da Niels Peter Jørgensen i 1997 opdagede en færdig "formel" for σ, nemlig følgende udtryk:

$$\sigma(x) = \frac{\mathrm{odd}(x+n)+1}{2}, \quad \text{for } x = 1, \ldots, n. \tag{5}$$

Her betegner $\mathrm{odd}(a)$ den *ulige del* af det naturlige tal a, opnået ved at dividere a med den størst mulige potens af 2. For eksempel finder man, for $n = 100$, at $\mathrm{odd}(n + 26) = \mathrm{odd}(126) = 63 \quad \sigma(26) = 64/2 = 32$. Den inverse til σ er bestemt ved $\sigma^{-1}(u) = 2^{\nu}(2u - 1) - n$ hvor ν er det mindste tal, så at resultatet er strikt positivt.

Bevis. Permutationen i (2) afhænger af n. I beviset betegner vi den mere præcist σ_n. Lad f_n være funktionen defineret ved højresiden i (5). Vi viser ved induktion efter n, at $\sigma_n(x) = f_n(x)$ for $x = 1, \ldots, n$.

For $n = 1$ og $n = 2$ er påstanden triviel. Antag, at $n > 2$ og at påstanden gælder for $n - 1$. Af fremstillingen (2) ses klart, at

$$\sigma_n = \sigma_{n-1}\gamma, \quad \text{hvor } \gamma := (1\,2\,3\,4\,\ldots\,n).$$

Heraf følger:

for $1 \le x \le n-2$ af induktionsantagelsen: $\sigma_n(x) = \sigma_{n-1}(x+1) = f_{n-1}(x+1) = f_n(x)$,

for $x = n-1$ ved en triviel omskrivning: $\sigma_n(n-1) = n = (\mathrm{odd}(2n-1)+1)/2 = f_n(n)$,

og for $x = n$ igen af induktionsantagelsen: $\sigma_n(n) = \sigma_{n-1}(1) = f_{n-1}(1) = \frac{1}{2}\big(\mathrm{odd}(n)+1\big) = \frac{1}{2}\big(\mathrm{odd}(2n)+1\big) = f_n(n)$.

Hermed er ligheden vist for $x = 1, \ldots, n$. □

3 Josefus' permutation.

Gunnar Forst opdagede i 1998, at permutationen σ hænger tæt sammen med Josefus-problemet: For et givet n bestemmes *Josefus' permutation* J på følgende måde: Sæt tallene $1, \ldots, n$ ordnet i en ring. Spring over 1 og skub 2 ud af ringen, spring over 3 og skub 4 ud, og gentag: springer over et tal og skub det næste ud af ringen. Fortsæt indtil alle er skubbet ud. Sæt

$$J(y) := \text{det } y\text{'te tal, der skubbes ud.} \tag{6}$$

Josefus-*problemet* er så at bestemme $J(n)$, altså det tal, der bliver skubbet sidst ud af ringen. I det rigtige Josefus-problem er det hvert tredje tal, der skubbes ud, men det er en anden historie, se fx Graham–Knuth–Patashnik [1, s. 8–16], eller i Afsnit 10 herunder.

Det er ikke så svært at vise, for givet n, at Josefus-permutationen J er bestemt som følgende produkt:

$$J = (1\,2\,3\,\ldots\,n)\,(2\,3\,\ldots\,n)\,(3\,\ldots\,n)\;\ldots\;(n{-}1\;\;n). \tag{7}$$

Bevis. Lad $J = J_n$ være permutationen defineret i (7). Øjensynlig er er

$$J = (1\,2\,3\,\ldots\,n)J', \text{ hvor } J' = (2\,3\,\ldots\,n)\,(3\,\ldots\,n)\;\ldots\;(n{-}1\;\;n)$$

Permutationen J' har 1 som fixpunkt, $J'(1) = 1$, men har i øvrigt samme form som J, bortset fra at det kun er de $n-1$ tal $2, 3, \ldots, n$, der permuteres.

Vi viser ved induktion efter n, at J er Josefus-permutationen bestemt ved legen ovenfor. Den originale leg begynder med, at man springer over 1 og skubber 2 ud, og så fortsætter: springer over et tal i cirklen og skubber det efterfølgende ud. Leg nu i stedet en ny leg, hvor man begynder med at springe over n, således at 1 er det første, der skubbes ud, og fortsæt. Efter det første trin svarer den nye leg til, at det er de $n-1$ tal $2, \ldots, n$, der er anbragt i cirklen og at man begynder med at springe over 2. Heraf følger, ved induktion efter n, at permutationen bestemt ved den nye leg netop er permutationen J'. Derfor er J permutationen bestemt ved den originale leg. □

Idet ω er rækkefølgeombytningen fra (1), altså $\omega(x) = n+1-x$, følger det, at

$$J^{-1} = \omega\sigma\omega^{-1}. \tag{8}$$

Med formlen (5) for σ får vi derfor et eksplicit udtryk for den inverse Josefus-permutation:

$$J^{-1}(y) = n+1-\tfrac{1}{2}\big(\mathrm{odd}(2n+1-y)+1\big), \tag{9}$$

og heraf fås videre:

(10) $$J(x) = 2n + 1 - 2^{\nu}(2n + 1 - 2x), \text{ med } \nu \geq 1 \text{ størst mulig og } J(x) \geq 1.$$

Specielt, for $x = n$, fås formlen for det tal, der bliver skubbet ud til sidst:

(11) $$J(n) = 2n + 1 - 2^{\nu}, \quad \text{med } \nu \geq 1 \text{ størst mulig.}$$

Eksempel, for $n = 10$:

$$J(10) = 21 - 16 \cdot 1 = 5, \quad J(9) = 21 - 4 \cdot 3 = 9, \quad J(8) = 21 - 4 \cdot 5 = 1,$$
$$J(7) = 21 - 2 \cdot 7 = 7, \text{ osv.}$$

4 Fixpunkter

Det er let at bestemme fixpunkter for σ (svarende til "1-cykler" i cykelfremstillingen) ud fra formlen (5). Funktionen på højresiden er defineret for alle naturlige tal x. Skriv $x + n = u2^{\nu}$, hvor u er ulige. Så er x et fixpunkt for funktionen på højresiden, hvis og kun hvis $(u + 1)/2 = 2^{\nu}u - n$, eller:

(12) $$\big(2^{\nu+1} - 1\big)u = 2n + 1.$$

Fixpunkterne svarer altså til divisorer i $2n + 1$ af formen $2^{\nu+1} - 1$. Med $\nu = 0$ fås løsningen $u = 2n + 1$, altså $x = n + 1$, som ligger uden for definitionsmængden for σ. For de øvrige løsninger til (12) er $x = 2^{\nu}u$ et fixpunkt for σ. Altså gælder det følgende resultat.

Observation 1. *Fixpunkter x for σ svarer til divisorer i $2n+1$ af formen $2^{\nu+1}-1$ med $\nu \geq 1$, idet x ud fra ligning* (12) *er bestemt ved $x = 2^{\nu}u - n$.*

For eksempel, med $2n + 1 = 3^2 \cdot 5 \cdot 7 = 315$, altså $n = 157$, er der 4 fixpunkter svarende til divisorerne $d = 3$, 7, 15 og 63.

d	u	v	x
3	105	1	53
7	45	2	23
15	21	3	11
63	5	5	3

5 Et specialtilfælde: $n = 2^{m-1}$

Troels Windfeldt Hansen opdagede i 2003 på udskrifter fra en computer, at cykeltypen for σ ikke var helt tilfældig, når n er en potens af 2. Fx kunne det "ses", at når $n = 2^{m-1}$ med et primtal m, så er der ét fixpunkt og ellers lutter m-cykler i fremstillingen af σ.

Troels' resultater var udgangspunkt for overvejelserne om fixpunkter, og for de efterfølgende resultater.

Observation 2. *Antag, at $n = 2^{m-1}$. Så har σ præcis 1 fixpunkt når m er ulige, og ingen fixpunkter, når m er lige.*

Bevis. Fixpunkter for σ svarer til divisorer i $2n+1$ af formen $2^{\nu+1}-1$ med $\nu \geq 1$. Betragt et tal $d = 2^{\nu+1}-1$ af denne form, og regn modulo d. Så er $2^{\nu+1} \equiv 1$. Skriv $m = q(\nu+1)+r$ med $0 \leq r < \nu+1$. Da er $2n+1 = 2^m+1 \equiv 2^r+1$. Da $r < \nu+1$ følger det, at d er divisor i $2n+1$, hvis og kun hvis $\nu = r = 1$, og da r desuden var den principale rest af m ved division med $\nu+1$, indtræffer det, hvis og kun hvis m er ulige. □

Observation 3. *Hvis $n = 2^{m-1}$, så er $\sigma^m = \mathrm{id}$.*

Afbildningen $x \mapsto n-x$ afbilder mængden $\{0,\ldots,n-1\}$ bijektivt på mængden $\{1,\ldots,n\}$. Det er bekvemt i beviset at konjugere σ med denne afbildning. Herved erstattes σ med permutationen $\overline{\sigma}$ af $\{0,\ldots,n-1\}$ bestemt ved $\overline{\sigma}(x) = n-\sigma(n-x)$. Udtrykket (5) for σ giver $\overline{\sigma}(x) = n - \frac{1}{2}\big(\mathrm{odd}(2n-x)+1\big)$, som vi omskriver til følgende:

$$\overline{\sigma}(n) = 2n-1-\frac{\mathrm{odd}(2n-1-x+1)-1}{2}-n, \quad 0 \leq x < n. \tag{13}$$

Afbildningen $\overline{\sigma}$ er sammensat af afbildninger, som det er let at beskrive ud fra den *binære* fremstilling af tallene: Tallene x med $0 \leq x \leq 2n-1 = 2^m-1$ kan fremstilles binært, $x = x_0 + x_1 2 + \cdots + x_{m-1}2^{m-1}$ med m bits (cifre), der alle er enten 0 eller 1. Vi identificerer i det følgende tallene med deres bitfølge,

$$x = x_0 x_1 \ldots x_{m-1},$$

idet vi altid medtager *alle* m bits, også når det *ledende bit* x_{m-1} er 0. Fx har tallene med $0 \leq x < n-1$ alle 0 som det ledende bit. Operationerne, der indgår i udtrykket for $\overline{\sigma}$ kan let udføres på de tilsvarende bitfølger. Specielt er operationen $x \mapsto 2n-1-x$ simpel: den fører bitfølgen x over i komplementære bitfølge $\overline{x}$ fremkommet fra x ved at erstatte 0 med 1 og 1 med 0.

Betragt nu et tal x med $0 \leq x \leq n-1$. Det ledende bit er da 0. Antag først, at $x > 0$. Læst fra venstre består bitfølgen x så af et antal, lad os sige ν, af 0-bits efterfulgt at et 1-bit, efterfulgt af en bitfølge z med $m-\nu-1$ bits (det er ikke udelukket, at $\nu = 0$; det indtræffer præcis når x er ulige). Bitfølgen for x har altså formen $00\ldots01z$ med ν 0-bits. I denne beskrivelse er det let at se, hvordan bitfølgen ændres af operationerne, der indgår i $\overline{\sigma}(x)$:

$$x = \overbrace{00\ldots0}^{\nu}1z, \qquad \overline{x} = 2n-1-x = \overbrace{11\ldots1}^{\nu}0\overline{z},$$

$$\overline{x}+1 = \overbrace{00\ldots0}^{\nu}1\overline{z}, \qquad \mathrm{odd}(\overline{x}+1) = 1\overline{z}\overbrace{00\ldots0}^{\nu},$$

$$\mathrm{odd}(\overline{x}+1)-1 = 0\overline{z}\overbrace{00\ldots0}^{\nu}, \qquad u = \tfrac{1}{2}\big(\mathrm{odd}(\overline{x}+1)-1\big) = \overline{z}\overbrace{00\ldots0}^{\nu}0,$$

$$\overline{u} = z\overbrace{11\ldots1}^{\nu}1, \qquad \overline{\sigma}(x) = \overline{u}-n = z\overbrace{11\ldots1}^{\nu}0,$$

altså

$$x = \overbrace{00\ldots0}^{\nu}1z, \qquad \overline{\sigma}(x) = z\overbrace{11\ldots1}^{\nu}0. \tag{14}$$

Ændringen i bitfølgen fra x til $\overline{\sigma}(x)$ kan beskrives dynamisk: Betragt en uendelig følge af bits med en "pointer",

$$\underset{\uparrow}{y_1 y_2 \cdots y_i y_{i+1} \cdots}$$

Lad os vedtage, at pointeren, placeret umiddelbart til venstre for et bit, *udpeger* det tal, hvis bitfølge består af de m bits, der står umiddelbart til højre for pointeren. Med pointeren som ovenfor udpeges altså tallet $y = y_{i+1} \ldots y_{i+m}$. Betragt nu den uendelige bitfølge,

$$x\overline{x}x\overline{x}\cdots = \underset{\uparrow}{\overbrace{00\ldots0}^{\nu}}1z\underset{\uparrow}{\overbrace{11\ldots1}^{\nu}}0\overline{z}\ldots$$

bestående af de m bits i x efterfulgt af de m bits i $\overline{x}$, efterfulgt af .... Den første pointer, til venstre for det første bit i følgen, udpeger øjensynlig x. Placeringen af den anden pointer er opnået ved at flytte den første pointer til højre indtil den passerer det første 1-bit. Af udregningen 14 fremgår, *at den anden pointer udpeger* $\overline{\sigma}(x)$. Det var antaget, at $x > 0$, men det er let at se, at påstanden også gælder for $x = 0$, hvor følgen $x\overline{x}x\ldots$ er $00\ldots011\ldots100\ldots0\ldots$. For $0 \le x < 2^m - 1$ gælder altså den følgende opskrift.

Opskrift A. *Hvis pointeren i følgen* $x\overline{x}x\overline{x}\ldots$ *udpeger* x*, så bestemmes* $\overline{\sigma}(x)$ *ved et flytte pointerne til højre forbi det førstkommende* 1*-bit.*

Følgen $x\overline{x}x\overline{x}\ldots$ har perioden $2m$, endda med $y_{i+m} = 1 - y_i$ (hvor y_i er det i'te led). Heraf ses, at når pointeren i følgen udpeger tallet y, så er bitfølgen efter pointeren bestemt ved $y\overline{y}y\overline{y}\ldots$. Opskriften er derfor gyldig for enhver placering af pointeren: Hvis pointeren udpeger y, så bestemmes $\overline{\sigma}(y)$ ved at flytte pointeren til højre hen forbi det førstkommende 1-bit. Specielt kan opskriften itereres:

Opskrift B. *Hvis pointeren i følgen* $x\overline{x}x\overline{x}\ldots$ *udpeger* x*, så udpeges* $\overline{\sigma}^k(x)$ *ved at flytte pointeren til højre forbi de* k *førstkommende* 1*-bits*

Af det sidste fremgår, at for at vise Observation 3 skal følgende vises.

Observation 4. *Antag, at* $0 \le x < 2^{m-1} - 1$*, Hvis pointeren i følgen* $x\overline{x}x\overline{x}\ldots$ *udpeger* x*, og den flyttes til højre forbi de* m *førstkommende* 1*-bits, så udpeger den igen* x*.*

Bevis. Det kan indses således: I $x\overline{x}$ indgår $2m$ bits. Der er et antal 1-bits i x og det komplementære antal 1-bits i $\overline{x}$. I $x\overline{x}$ er antallet af 1 bits derfor præcis m. Yderligere er $x < 2^{m-1}$, så det ledende bit i x er et 0-bit. Derfor er det ledende bit (det sidste bit) i $\overline{x}$ et 1-bit. Når pointeren har passeret alle 1-bits i $x\overline{x}$ har den derfor passeret samtlige bits i $x\overline{x}$; derfor peger den igen x. □

Observation 5. *Hvis* $n = 2^{m-1}$*, hvor* m *er et ulige primtal, så har* σ *cykeltypen* $1^1 m^k$*, hvor* $k = (2^{m-1} - 1)/m$*.*

Bevis. Det er Troels' opdagelse, og det følger umiddelbart: Da $\sigma^m = \mathrm{id}$, er hver cykels længde divisor i m, og dermed 1 eller m. Ifølge Observation 2 er der kun 1 fixpunkt. Derfor må de øvrige cykler have længde m. □

6 Cykeltypen, for $n = 2^{m-1}$.

Opskrift A i beviset for Observation 3 kan bruges til at bestemme cykeltypen helt, stadig i tilfældet $n = 2^{m-1}$. Permutationerne σ og $\overline{\sigma}$ har samme cykeltype, og vi holder os til $\overline{\sigma}$. Af Observation 3 følger, at hvis x bestemmer en p-cykel for $\overline{\sigma}$, så er p divisor i m (og naturligvis er $\overline{\sigma}^p(x) = x$).

Lad nu p være en sådan divisor, $m = pd$. Betragt for en bitfølge x, med $0 \le x < n = 2^{m-1}$, ligningen $\overline{\sigma}^p(x) = x$. Den betyder, at når pointeren i følgen $x\overline{x}x\overline{x}\ldots$ udpeger x, og så flyttes p gange (hver flytning er til højre forbi det førstkommende 1-bit), så udpeger den igen x. Lad h være det samlede antal bits, som overspringes ved de p flytninger. Når de p flytninger er gentaget d gange, er der flyttet m gange; ifølge lemmaet er der så præcis oversprunget samtlige $2m$ bits i $x\overline{x}$. Altså er $dh = 2m$, og derfor er $h = 2p$. Lad z være bitfølgen bestående af de første p af de oversprungne bits, og lad w være bitfølgen bestående af de næste p bits. Da er

$$x\overline{x} = zw\ldots zwzw,$$

med d gentagelser af de $2p$ bits i zw. Af denne ligning følger først, at d må være ulige, $d = 2e - 1$ (ellers var $x = \overline{x}$), og dernæst, at $w = \overline{z}$. Altså har x har formen,

$$x = z\overline{z}z\overline{z}\ldots z\overline{z}z, \tag{15}$$

hvor z har længde p, og z forekommer e gange og $\overline{z}$ forekommer $e-1$ gange. Omvendt, hvis z er følge med p bits, så ender følgen 15 med det ledende bit i z, dvs $0 \le x < n$. hvis og kun hvis det ledende bit i z er 0. Med andre ord gælder følgende resultat.

Observation 6. *For hver divisor p i m, med $m = dp$, er $\overline{\sigma}^p(x) = x$, hvis og kun hvis d er ulige og x har formen 15, hvor z er en følge af p bits med ledende bit lig med* 0.

Der er 2^{p-1} muligheder for en sådan bitfølge z. Derfor er der præcis 2^{p-1} muligheder for et tal $x < n$ med $\overline{\sigma}^p(x) = x$.

Lad nu $\alpha(p)$ betegner antallet af tal $x < n$ for hvilke cyklen bestemt ved x har længde p. Antallet af muligheder bestemt oven for er antallet at tal $x < n$ for hvilke cyklen bestemt ved x har en længde, der er divisor i p. Der gælder altså:

$$\sum_{q|p} \alpha(q) = \begin{cases} 2^{p-1} & \text{hvis } p \mid m \text{ og } m/p \text{ er ulige,} \\ 0 & \text{ellers.} \end{cases}$$

Herefter bestemmes $\alpha(p)$ ved Möbius-inversion: Med Möbius funktionen $\mu(d)$ er

$$\alpha(p) = \sum_{q|p}{}' \mu(p/q)2^{q-1}, \tag{16}$$

hvor summen er over de divisorer q i m for hvilke m/q er ulige.

Ækvivalent, hvis $m = 2^\nu u$, hvor u er ulige, så er $\alpha(p) = 0$ med mindre p er en divisor i m af formen $2^\nu v$. I det sidste tilfælde er

$$\alpha(2^\nu v) = \sum_{w|v} \mu(v/w) 2^{2^\nu w - 1}. \tag{17}$$

Observation 7. *Antag, at $n = 2^{m-1}$. Da forekommer der p-cykler i σ, hvis og kun hvis $p \mid m$ og m/p er ulige. Antallet af p-cykler, for $p \mid m$ og m/p ulige, er $\alpha(p)/p$, hvor $\alpha(p)$ er summen i 16 (eller i 17).*

7 Eksempel.

For $n = 2^9 = 512$ er $m = 10 = 2 \cdot 5$, så der er 2-cykler og 10-cykler, nemlig

$$\#(\text{2-cykler}) = \frac{1}{2}\mu(1)2^{2-1} = 1, \qquad \#(\text{10-cykler}) = \frac{1}{10}\big((-1)2^{2-1} + 2^{10-1}\big) = 51.$$

8 Et specialtilfælde: $n = 2^{m-1} - 1$.

Lasse Nielsen opdagede i 2003, at der for vilkårligt n gælder, at tallene $x_k = n - (2^k - 1)$, for $k = 0, 1, \ldots$ og $x_k \geq 1$, ligger i samme cykel, idet $\sigma(x_k) = x_{k-1}$:

$$x_k \mapsto x_{k-1} \mapsto \cdots \mapsto x_2 = n - 3 \mapsto n - 1 \mapsto n = x_0.$$

Det størst mulige k er bestemt ved $2^k - 1 < n$, altså $2^k \leq n$, dvs k er den hele del af $\log_2 n$. Der indgår mindst $k + 1$ elementer i cyklen. Altså gælder følgende resultat.

Observation 8. *Længden af den største cykel, der forekommer i σ, er altid mindst lig med $k + 1$, hvor k er den hele del af tallet $\log_2 n$.*

Lasse opdagede videre, ved udskrifter fra en computer, det efterfølgende resultat.

Observation 9. *Antag, at $n = 2^{m-1} - 1$. I cykelfremstillingen af σ forekommer da p-cykler for alle $p = 1, \ldots, m - 1$, og ikke for andre p.*

For at vise denne påstand konjugerer vi σ med permutationen $\omega(x) = n + 1 - x$ fra 1, og betragter altså permutationen σ_0 bestemt ved $\sigma_0(x) = n + 1 - \sigma(n + 1 - x)$, for $1 \leq x \leq 2^{m-1}$. Indsættes formlen 5 for σ fås, efter en lille omskrivning,

$$\sigma_0(x) = 2n + 1 - \frac{\mathrm{odd}(2n + 1 - x) - 1}{2} - (n + 1). \tag{18}$$

Her er $1 \leq x < n = 2^{m-1}$, og som i Afsnit 4 kan vi identificere disse tal med deres bitfølger med m bits og ledende bit 0, men nu med undtagelse af nulfølgen $00 \ldots 0$. Operationerne, som indgår i udtrykket 18 for σ_0 svarer til simple operationer med

bitfølger. Da $2n+1 = 2^m - 1$, svarer operationen $x \mapsto 2n+1-x$ på bitfølger til $x \mapsto \overline{x}$.

Bitfølgen for et tal x med $1 \le x < n$ har formen $11\ldots10y$ med ν 1-bits inden det først 0-bit (det er ikke udelukket, at $\nu = 0$ eller at y er tom). Med denne beskrivelse er det let at se, som i Afsnit 4, hvordan bitfølgen ændres af σ_0:

$$x = \overbrace{11\ldots1}^{\nu}0y, \qquad \sigma_0(x) = y\overbrace{11\ldots1}^{\nu}0, \tag{19}$$

Beskrivelsen 19, sammenholdt med den uendelige bitfølge $xxx\ldots$,

$$xxxx\cdots = \underset{\uparrow}{\overbrace{11\ldots1}^{\nu}0}y\underset{\uparrow}{\overbrace{11\ldots1}^{\nu}0}y\ldots,$$

leder som i Afsnit 4 til en opskrift.

Opskrift C. *Betragt for $1 \le x \le 2^{m-1}-1$ den uendelige bitfølge $xxxx\ldots$. Hvis en pointer i følgen udpeger x, så udpeges $\sigma_0(x)$ ved et flytte pointeren til højre forbi det førstkommende 0-bit.*

Som i Afsnit 4 kan opskriften itereres. Antag, at k er antallet af 0-bits i x. Hvis pointeren i følgen $xxx\ldots$ udpeger x, og den flyttes k gange efter opskriften, så udpeger den $\sigma_0^k(x)$. Pointeren har så præcis overspunget samtlige 0-bits i x, og da det ledende bit i x er et 0-bit, har den altså præcis overspunget samtlige bits i x; den udpeger derfor igen x. Altså er $\sigma_0^k(x) = x$. Specielt er *perioden* for x, dvs længden af den cykel under σ_0, som bestemmes ved x, divisor i k.

Antallet af 0-bits i x kan højst være $m-1$, da $x > 0$. Derfor har en cykel, der indgår i σ_0, højst længden $m-1$. Desuden ses for $k = 1, \ldots, m-1$, at tallet $x := 1\ldots100\ldots0$, hvor antallet af 0-bits er k, præcis har perioden k.

Hermed er Lasses observation 9 eftervist.

9 Cykeltypen, $n = 2^{m-1} - 1$

Antallet af p-cykler kan bestemmes således: Lad $M_\lambda(d)$ være mængden af de bitfølger af længde d, som ikke er lutter 0-bits, hvor det ledende (højre) bit er et 0-bit, og hvor λd er det samlede antal 0-bits. Hvis mængden ikke er tom, må λd være et helt tal med $1 \le \lambda d < d$. Lad $\beta_\lambda(d)$ være antallet af bitfølger i $M_\lambda(d)$. Øjensynlig gælder, når λd er et helt tal med $1 \le \lambda d < d$, at

$$\beta_\lambda(d) = \binom{d-1}{\lambda d - 1}. \tag{20}$$

Lad nu $\beta_\lambda^{\text{prim}}(d)$ betegne antallet af *primitive* bitfølger i $M_\lambda(d)$, dvs bitfølger i $M_\lambda(d)$ som er *primitive*, dvs følger der ikke er af formen $zz\ldots z$ med en følge z i $M_\lambda(e)$ med en ægte divisor $e \mid d$. Det er klart, at $\beta_\lambda(d) = \sum_{e|d} \beta_\lambda^{\text{prim}}(e)$. Ved Möbius-inversion fås så:

$$\beta_\lambda^{\text{prim}}(e) = \sum_{d|e} \mu(d)\beta_\lambda(e/d). \tag{21}$$

Det følger af beskrivelsen ovenfor, når $1 \le x \le 2^{m-1}-1$, at x har periode p under σ_0, hvis og kun hvis bitfølgen x har formen $x = zz\ldots z$, hvor z er en primitiv bitfølge i $M_{p/e}(e)$ (dvs længde e, antal 0-bits lig med p, ledende bit 0, og $z > 0$. Lad $\alpha(p)$ være antallet af tal x med $1 \le x \le n$ for hvilke perioden for x er lig med p. Antallet er 0 for $p \ge m$. For $1 \le p \le m-1$ gælder i følge det foregående, at

$$\alpha(p) = \sum_{e|m} \beta^{\mathrm{prim}}_{p/e}(e).$$

Der er kun bidrag, når $e > p$. Summen kan omskrives ved 20 og 21:

$$\alpha(p) = \sum_{d|e|m} \mu(d)\beta_{p/e}(e/d) = \sum_{d|e|m}{}' \mu(d)\binom{e/d-1}{p/d-1}, \tag{22}$$

hvor der i den sidste sum kun medtages led, når $e > p$ og $d \mid p$.

Observation 10. *Antag, at $n = 2^{m-1}-1$. Da gælder for $p = 1,\ldots,m-1$, at antallet af p-cykler i σ er lig med $\alpha(p)/p$, hvor $\alpha(p)$ er summen 22. Specielt, hvis m er et primtal, så er antallet af p-cykler lig med*

$$\frac{1}{p}\binom{m-1}{p-1}, \quad p = 1,\ldots,m-1. \tag{23}$$

Bevis. Den almindelige formel blev vis ovenfor. Antag, at m er et primtal. For et led i summen 22 er $e > p$ og $e \mid m$, så $e = m$ og da $d \mid e$ og $d \mid p$, er $d = 1$. Der er altså kun 1 led i summen, og det er binomialkoefficienten i 23. Heraf følger påstanden. □

10 Eksempel

$n = 2^9 - 1 = 511$ giver $m+1 = 10$ med divisorer $e = 10, 5, 2$ idet $e > 1$.

$p = 9$, $(e,d) = (10,1)$: $\binom{9}{8}/9 = 1$.
$p = 8$, $(e,d) = (10,1)$, $(10,2)$: $\left(\binom{9}{7} - \binom{4}{3}\right)/8 = 4$.
$p = 7$, $(e,d) = (10,1)$: $\binom{9}{6}/7 = 12$.
$p = 6$, $(e,d) = (10,1)$, $(10,2)$: $\left(\binom{9}{5} - \binom{4}{2}\right)/6 = 20$.
$p = 5$, $(e,d) = (10,1)$, $(10,5)$: $\left(\binom{9}{4} + \binom{4}{0} + \binom{4}{1}\right)/5 = 25$.
$p = 4$, $(e,d) = (10,1)$, $(10,2)$, $(5,1)$: $\left(\binom{9}{3} - \binom{4}{1} + \binom{4}{3}\right)/4 = 21$.
$p = 3$, $(e,d) = (10,1)$, $(5,1)$: $\left(\binom{9}{2} + \binom{4}{2}\right)/3 = 14$.
$p = 2$, $(e,d) = (10,1)$, $(10,2)$, $(5,1)$: $\left(\binom{9}{1} - \binom{4}{0} + \binom{4}{1}\right)/2 = 6$.
$p = 1$, $(e,d) = (10,1)$, $(5,1)$, $(2,1)$: $\left(\binom{9}{0} + \binom{4}{0} + \binom{1}{0}\right)/1 = 3$.

11 Den generelle Josefus permutation

Den generelle udfordring, se [1, s. 79–81], er følgende: Stil tallene $1, 2, \ldots, n$ i ringen og skub hvert q'te tal ud (tilfældet ovenfor er $q = 2$, Josefus' oprindelige problem svarer til $q = 3$). Lad $J_q = J_{q,n}$ være permutationen i S_n bestemt ved at $J_q(x)$ er lig med det x'te tal, der skubbes ud. Findes der en formel for permutationen J_q?

Som ovenfor ses, at

$$J_q = (1\,2\,3\,\ldots\,n)^{q-1}(2\,3\,\ldots\,n)^{q-1}\cdots(n-1\,n)^{q-1},$$

og heraf:

$$J_q^{-1} = \omega\sigma_q\omega^{-1},$$

hvor

$$\sigma_q = \sigma_{q,n} = (1\,2)^{q-1}(1\,2\,3)^{q-1}\cdots(1\,2\,3\,\ldots\,n)^{q-1}$$

Findes der en formel for σ_q, som tillader at bestemme σ_q^{-1}?

Det er let at bestemme et rekursivt udtryk: Hold q fast, og prøv med et udtryk af formen

$$\sigma_{q,n}(x) = f(x + (q{-}1)n).$$

Induktivt kan antages, for $1 \le x \le n - q$, at

$$\sigma_{q,n}(x) = \sigma_{q,n-1}(x{+}q{-}1)) = f(x{+}q{-}1 + (q{-}1)(n{-}1)) = f(x + (q{-}1)n),$$

så ligningen gælder, når bare den gælder for $n - q < x \le n$. For $x = n - q + 1$ er $\sigma_{q,n}(x) = n$, så kravet her er

$$f(n{-}q{+}1 + (q{-}1)n) = n, \qquad \text{altså } f(qn - q + 1) = n.$$

For $n - q + 1 < x \le n$ er $x = n - a$ med $0 \le a < q - 1$, og her er $\sigma_{q,n}(n - a) = \sigma_{q,n-1}(q - 1 - a) = f(q - 1 - a + (q - 1)(n - 1))$; kravet er

$$f(-a + qn) = f(-a + (q - 1)n), \text{for } 0 \le a < q - 1.$$

Erstattes n med $t + 1$ i det første krav, og n med t i de øvrige, er betingelserne:

$$f(qt - a) = f((q{-}1)t - a) \text{ for } a = 0, \ldots, q - 2,\ f(qt + 1) = t + 1.$$

Eksempel. For $q = 2$ fås $f(2t) = f(t)$, $f(2t + 1) = t$, hvoraf $f(x) = [\mathrm{odd}(x) + 1]/2$.

Og for $q = 3$ fås:

$$f(3t - 1) = f(2t - 1), \quad f(3t) = f(2t), \quad f(3t + 1) = t + 1.$$

Man får altså $f(z)$ ved først at reducere, gentagne gange, argumentet z med de to operationer $3t - 1 \mapsto 2t - 1$ og $3t \mapsto 2t$ indtil der fremkommer et tal $\equiv 1$

(mod 3); denne reduktion kunne betegnes $\mathrm{odd}_3(z)$. Med denne betegnelse er $f(z) = (\mathrm{odd}_3(z) + 2)/3$, og altså

$$\sigma_3(x) = \frac{\mathrm{odd}_3(x + 2n) + 2}{3}.$$

Den omvendte af reduktionen ovenfor, $2t \mapsto 3t$ og $2t - 1 \mapsto 3t - 1$, kan fås ved at multiplicere med 3/2 og runde op; med en ikke-standard notation kan denne afbildning betegnes $\lceil 3/2 \rceil$. Med denne notation bestemmes den inverse sådan:

$$x = \sigma_3^{-1}(y) = \lceil 3/2 \rceil^{\nu}(3y - 2) - 2n,$$

med ν mindst mulig og $x \geq 1$ (eller ν størst og $x \leq n$). For den konjugerede, $J_3 = \omega\sigma_3^{-1}\omega^{-1}$, fås:

$$J_3(y) = 3n + 1 - \lceil 3/2 \rceil^{\nu}(3n + 1 - 3y) \text{ med } \nu \text{ størst mulig.}$$

Specielt, "Josefus-tallet" $J_3(n)$, dvs tallet, der skubbes ud til sidst, er

$$J_3(n) = 3n + 1 - \lceil 3/2 \rceil^{\nu}(1), \qquad \nu \text{ størst mulig.}$$

Generaliseringen til $q > 3$ er umiddelbar.

Litteratur

[1] R. L. Graham, D. E. Knuth, O. Patashnik, *Concrete Mathematics, Second edition*, Addison–Wesley, 1995.

Appendix: *Redaktörens anmärkningar*

För den läsare som händelsevis är obekant med notationen vill jag presentera en liten snabbkurs. Med en permutation av talen $(1, 2, \ldots n)$ menas en omordning av talen. En typisk permutation av talen $(1, 2, 3, 4, 5, 6)$ kan presenteras av $(2, 4, 3, 6, 1, 5)$. En permutation σ är en bijektion av objekten, och notationen ovan är helt enkelt en presentation $(\sigma(1), \sigma(2), \sigma(3), \sigma(4), \ldots \sigma(n))$. Notera att alla sådana presentationer har längden n. I artikeln används istället en cykelpresentation. Varje element x ger upphov till en cykel $(x, \sigma(x), \sigma(\sigma(x)), \sigma(\sigma(\sigma(x))), \ldots, \sigma^{m-1}(x))$ där $\sigma^m(x) = x$. Två cykler som är disjunkta kommuterar, och varje permutation kan skrivas på unikt sätt bortsett från ordningen som en produkt av disjunkta cykler. Vårt exempel ovan inses lätt få representationen (12465)(3) (ofta utesluter man cykler av längd 1, dessa motsvaras av fixpunkter). Till varje permutation associeras en cykelstruktur,detta är ingenting annat än en partition av talet n där varje summand ger längden på en cykel. En mycket viktig operation inom gruppteori är konjugationer. Man säger att elementet $\sigma\tau\sigma^{-1}$ är konjugatet av τ med avseende på σ. Konjugatet av en cykel $(xyz \ldots)$ blir då $(\sigma(x)\sigma(y)\sigma(z) \ldots)$ (jmfr (8) s. 27 nederst på sidan). Vi inser att cykelstrukturen hos ett element inte ändras under konjugering. Omvänt är det lätt att visa att två permutationer med samma cykelstruktur är konjugerade.