MS-A0409 Grundkurs i diskret matematik
Appendix, del II

G. Gripenberg

Aalto-universitetet

17 oktober 2013

Hur många räkenoperationer behövs i Euklides algoritm för att räkna ut $\operatorname{sgd}(m, n)$

Antag att $m > n$. I Euklides algoritm väljer vi $r_0 = m$, $r_1 = n$ och räknar sedan ut r_i och q_i så att $r_{i-2} = q_i r_{i-1} + r_i$ för $i \geq 2$ tills vi fått $r_M = 0$ och då är $r_{M-1} = \operatorname{sgd}(m, n)$. För detta behövs alltså $M - 1$ "divisioner med rest".
Nu skall vi alltså uppskatta hur stort M kan vara och för det låter vi $x_1 = 1$, $x_2 = 2$ och

$$x_{j+2} = x_{j+1} + x_j, \quad j \geq 1. \tag{$\star$}$$

Nu vet vi att $r_{M-1} \geq x_1$ och $r_{M-2} \geq x_2$ eftersom $r_{M-1} > r_{M-1}$. Om vi nu antar att $r_{M-j} \geq x_j$ för $1 \leq j \leq k$ så får vi, eftersom $q \geq 1$ att

$$r_{M-(k+1)} = q_{M-k+1} r_{M-k} + r_{M-k+1} \geq r_{M-k} + r_{M-k+1} \geq x_k + x_{k-1} = x_{k+1}.$$

Av induktionsprincipen följer nu att $r_{M-j} \geq x_j$ för alla $j = 1, \ldots, M$.
Om man löser ekvation ($\star$) så får man

Hur många räkenoperationer behövs i Euklides algoritm för att räkna ut $\operatorname{sgd}(m, n)$, forts.

$$x_j = \left(1 + \frac{2}{\sqrt{5}}\right)\left(\frac{1+\sqrt{5}}{2}\right)^{j-2} + \left(1 - \frac{2}{\sqrt{5}}\right)\left(\frac{1-\sqrt{5}}{2}\right)^{j-2}.$$

Nu kan man visa att $x_j \geq \left(\frac{1-\sqrt{5}}{2}\right)^{j-2} \geq \left(\frac{1+\sqrt{5}}{2}\right)^{j-1}$, vilket innebär att

$$m = r_0 \geq x_M \geq \left(\frac{1+\sqrt{5}}{2}\right)^{M-1},$$

av vilket följer att

$$M - 1 \leq \frac{\log m}{\log\left(\frac{1+\sqrt{5}}{2}\right)},$$

eller, antalet räkningar för att bestämma $\operatorname{sgd}(m, n)$ är av storleksordningen $O(\log(\max(m, n)))$.

Eulers teorem, bevis

Antag att $[x_1]_n, \ldots, [x_{\phi(n)}]$ *är de invertibla elementen i* $\mathbb{Z}_n$. *Eftersom* $\gcd(a, n) = 1$ *har också* $[a]_n$ *en invers och eftersom* $[\alpha]_n \cdot [\beta]_n$ *är invertibelt om* $[\alpha]_n$ *och* $[\beta]_n$ *är det, är också* $[a]_n \cdot [x_j]$ *invertibelt för alla* j. *Om nu* $[a]_n \cdot [x_j]_n = [a]_n \cdot [x_k]_n$ *så är* $[x_j]_n = [a]_n^{-1} \cdot [a]_n \cdot [x_j]_n = [a]_n^{-1} \cdot [a]_n \cdot [x_k]_n = [x_k]_n$ *vilket innebär att elementen* $[a]_n \cdot [x_1]_n, \ldots [a]_n \cdot [x_{\varphi(n)}]_n$ *är elementen* $[x_1]_n, \ldots, [x_{\phi(n)}]$ *eventuellt i en annan ordning. Men produkterna är de samma, dvs.*

$$[a]_n^{\varphi(n)} \Pi_{i=1}^{\varphi(n)} [x_i]_n = \Pi_{i=1}^{\varphi(n)} ([a]_n \cdot [x_i]_n) = \Pi_{i=1}^{\varphi(n)} [x_i]_n.$$

Eftersom varje element $[x_i]_n$ *är inverterbart, kan vi dividera bort alla* $[x_i]_n$ *och slutresultatet är att* $[a]_n^{\varphi(n)} = [1]_n$ *dvs.* $\mod(a^{\varphi(n)}, n) = 1$.

Vad händer i RSA-algortimen om $\gcd(a, n) \neq 1$?

- *Eftersom man antar att* $0 < a < n$ *så är* $\gcd(a, n) \neq 1$ *endast då* $p|a$ *eller* $q|a$. *Anta att* $p|a$ *så att* $a = p^j \cdot c$ *där* $\gcd(c, n) = 1$
- *Nu är* $[b^d]_n = [((p^j \cdot c)^k)^d]_n = [(p^k)^d]_n^j \cdot [(c^k)^d]_n$ *och eftersom* $\gcd(c, n) = 1$ *så är* $[(c^k)^d]_n = [c]_n$ *och det återstår att visa att* $[(p^k)^d]_n = [p]_n$ *för då är* $[b^d]_n = [p]_n^j \cdot [c]_n = [p^j \cdot c]_n = [a]_n$.
- *Eftersom* q *är ett primtal och* $p \neq q$ *så är* $\gcd(p, q) = 1$ *och därför följer det av enligt Fermats teorem att* $p^{q-1} \equiv 1 \pmod{q}$.
- *Då är också* $p^{(q-1)(p-1)r} \equiv 1 \pmod{q}$ *dvs.* $p^{(q-1)(p-1)r} = 1 + sq$ *och därför också* $p^{1+(q-1)(p-1)r} = p + spq$ *dvs.* $[p^{1+m \cdot r}]_n = [p]_n$ *vilket visar att* $[(p^k)^d]_n = [p]_n = [a]_n$.

Algoritmen fungerar alltså också i detta fall!

En rät linje som en sidoklass

$[\mathbb{R}^2, +]$ *är en grupp med origo som identitetselement och inversen av* $\mathbf{v}$ *är* $-\mathbf{v}$. *Antag att* $\mathbf{u} \in \mathbb{R}^2 \setminus \{\mathbf{0}\}$. *Då är* $H = \{ t\mathbf{u} : t \in \mathbb{R} \}$ *en delgrupp i* $(\mathbb{R}^n, +)$ *och sidoklassen* $\mathbf{w} + H$ *är mängden av alla (eller ortsvektorer till) punkter på linjen genom* $\mathbf{w}$ *med riktning* $\mathbf{u}$.

Kongruensklasser som kvotgrupper

Antag att $n \geq 1$. *Nu är* $[\mathbb{Z}, +]$ *en grupp och* $n\mathbb{Z} = \{ n \cdot j : j \in \mathbb{Z} \}$ *är en delgrupp i* $[\mathbb{Z}, +]$ *och eftersom addition är kommutativ* $(a+b=b+a)$ *så är den en normal delgrupp. Sidoklasserna till* $n\mathbb{Z}$ *är kongruensklasserna modulo* n *och de bildar kvotgruppen* $Z/n\mathbb{Z}$ *med addition som operation.*

Normala delgrupper och kvotgrupper

Antag att G *är en grupp och att* H *är en delgrupp av* G.

- $aH = Ha$ *för alla* $a \in G$ *om och endast om* $axa^{-1} \in H$ *för alla* $a \in G$ *och* $x \in H$.
  Varför? Antag att $a \in G$ *och* $x \in H$. *Nu gäller* $ax \in aH$ *så att om* $aH = Ha$ *så finns det ett* $y \in H$ *så att* $ax = ya$. *Men då är* $axa^{-1} = y \in H$. *Ifall, å andra sidan,* $axa^{-1} = y \in H$ *så då är* $ax = ya$ *så att* $aH \subset Ha$. *Men om vi tar* a^{-1} *istället för a så får vi* $a^{-1}H \subset Ha^{-1}$ *från vilket det följer att* $Ha = aa^{-1}Ha \subset aHa^{-1}a = aH$ *också gäller.*
- *Om* $aH = Ha$ *för alla* $a \in G$ *så följer det att om* $a_1H = a_2H$ *och* $b_1H = b_2H$ *så gäller* $a_1b_1H = a_2b_2H$ *vilket betyder att man definiera produkten av sidoklasserna* aH *och* bH *med* $(aH)(bH) = abH$.
  Varför? Genom att använda antagandet $aH = Ha$ *flera gånger får vi*

$$a_1b_1H = a_1Hb_1 = a_2Hb_1 = a_2b_1H = a_2b_2H.$$

Varför är $|Gx| \cdot |G_x| = |G|$?

Antag att G är en ändlig grupp. Om H är en delgrupp av G så är $|H| \cdot m = |G|$ där m är antalet (tex. vänstra) sidoklasser till H. Eftersom G_x är en delgrupp av G så räcker det att konstruera en bijektion ψ från mängden av sidoklasser till G_x till banan Gx.
Definiera $\psi(gG_x) = gx$. Om $g_1G_x = g_2G_x$ så gäller $g_2^{-1}g_1 \in G_x$ så att $g_2^{-1}g_1x = x$ och därför gäller $g_1x = g_2x$ så att ψ är väl definierad.
Om $g_1x = g_2x$ s gäller $g_2^{-1}g_1x = x$ så att $g_2^{-1}g_1 \in G_x$ och därför $g_1G_x = g_2G_x$ vilket betyder att ψ är en injektion. Om $y \in Gx$ så finns dett ett $g \in G$ så att $y = gx$ och därför gäller $y = \psi(gG_x)$ vilket betyder att ψ är en surjektion.

Varför är antalet banor i gruppverkan på en mängd $\frac{1}{|G|}\sum_{g\in G}|X_g|$?

Låt $E = \{\,[g,x] \in G \times X : gx = x\,\}$. Genom att byta summeringsordning får vi

$$|E| = \sum_{g\in G}|\{\,x \in X : gx = x\,\}| = \sum_{x\in X}|\{\,g \in G : gx = x\,\}|,$$

så att $\sum_{g\in G}|X_g| = \sum_{x\in X}|G_x|$.
Mängden banor betecknar vi med X/G och de är ekvivalensklasser när ekvivalensrelationen $\sim$ definieras med $x \sim y$ om moch endast om $x = gy$ för något $g \in G$. Olika banor har inga gemensamma element och deras union är X. Eftersom $|G_x| = \frac{|G|}{|Gx|}$ och Gx är banan som innehåller x så får vi påståendet med följande räkning:

$$\sum_{g\in G}|X_g| = \sum_{x\in X}|G_x| = \sum_{A\in X/G}\sum_{x\in A}\frac{|G|}{|Gx|} = |G|\sum_{A\in X/G}\sum_{x\in A}\frac{1}{|A|}$$
$$= |G|\sum_{A\in X/G}\frac{1}{|A|}\sum_{x\in A}1 = |G|\sum_{A\in X/G}1 = |G||X/G|.$$

Rotationers cykelindex

Permutationen $p = (1\ 2\ \ldots\ n)$ av mängden $X = \{0, 1, 2, \ldots, n-1\}$ genererar den cykliska gruppen (kallad C_n) med element $e, p, p^2, \ldots, p^{n-1}$ där e är identitetselementet. Denna permutation p motsvarar rotation med vinkeln $\frac{2\pi}{n}$ av en reguljär n-hörning.
Låt $k \in \{0, 1, 2 \ldots, n-1\}$. För varje $j \in \mathbb{Z}$ och $x \in X$ är

$$(p^k)^j(x) = p^{k\cdot j}(x) = \operatorname{mod}(x + k \cdot j, n) = \operatorname{mod}(x + \operatorname{mod}(k \cdot j, n), n).$$

Nu väljer vi d som minsta möjliga positiva heltal så att $\operatorname{mod}(k \cdot d, n) = 0$. Detta innebär att för varje $x \in X$ gäller $(p^k)^j(x) \neq x$ då $1 \le j < d$ men $(p^k)^d(x) = x$. Detta innebär att varje bana för permutationen har längden d och eftersom unionen av banorna är X så delar d talet n och p^k har $\frac{n}{d}$. Nästa steg är att bestämma för hur många värden på k längden av banorna är d för varje d som delar n. Eftersom $\operatorname{mod}(k \cdot d, n) = 0$ så är $k \cdot d = j \cdot n$ och $\operatorname{sgd}(j, d) = 1$ eftersom vi annars kunde dividera bort en gemensamma delaren och få ett mindre tal d. Eftersom $k < n$ måste vi ha $j < d$ så att $k = j \cdot \frac{n}{d}$ där $0 \le j < d$ och $\operatorname{sgd}(j, d) = 1$. Men om vi väljer j

Rotationers cykelindex, forts.

på detta sätt får vi ett tal k mellan 0 och $n-1$ vilket betyder att antalet element p^k som är sådana att banornas längd är d är antalet element i mängden $\{\,j : 0 \le j - 1,\ \operatorname{sgd}(j, d) = 1\,\}$ och detta antal är den sk. eulers funktion $\varphi(d)$.
Cykelindexet blir därför

$$\zeta_{C_n,\mathbb{N}_n}(t_1, t_2, \ldots, t_n) = \frac{1}{n}\sum_{d\,|\,n}\varphi(d)t_d^{\frac{n}{d}}.$$

Bevis för Pólyas teorem om antalet färgningar

Antag att Ω är en mängd färgningar av X som är invarianta då G verkar på X. Då är antalet banor i G:s gruppverkan på Ω enligt tidigare resultat $\frac{1}{|G|}\sum_{g\in G}|\Omega_g|$ där $\Omega_g = \{\,\omega \in \Omega : g\omega = \omega\,\}$ är mängden av färgningar som är fixpunkter under verkan av g och dessa är i sin tur de färgningar som är konstanta på varje bana då g verkar på X. Således kan vi räkna ut detta antal banor skilt för varje $g \in G$ och sedan addera och till sist dividera med $|G|$.

Antag att $A_{g,1}, A_{g,2}, \ldots A_{g,m_g}$ är banorna under verkan av g och låt $s_j = |A_{g,j}|$. Nu finns det förstås exakt ett sätt att använda färgen a_j exakt s_1 gånger för att färga elementen i $A_{g,1}$ med färgen a_j. Detta kan beskrivas med (den genererande) funktionen $a_1^{s_1} + \ldots + a_r^{s_1}$ så att koefficienten $a_j^{s_1}$ är antalet (som här är 1). Antag nu att $p(a_1, \ldots, a_r)$ är en (genererande) funktion så att koefficienten av monomet $a_1^{i_1} \cdot a_2^{i_2} \cdot \ldots \cdot a_r^{i_r}$ är antalet sätt på vilket mängderna $A_{g,1}, \ldots A_{g,k}$ kan färgas så att man använder färgen a_j exakt i_j gånger. Elementen i $A_{g,k+1}$ kan färgas så att man använder en av färgerna s_k gånger och alla olika val ger upphov till olika färgningar.

Bevis för Pólyas teorem om antalet färgningar, forts.

Om vi använder färgen a_q i banan $A_{g,k+1}$ och vill använda färgen a_j exakt i_j gånger för att färga alla mängderna $A_{g,1}, \ldots A_{g,k}, A_{g,k+1}$ då måste vi använda färgen a_j exakt i_j gånger $j \neq q$ och färgen a_q exakt $i_q - s_q$ gånger när vi färgar de första banorna $A_{g,1}, \ldots A_{g,k}$. Eftersom banan $A_{g,k+1}$ kan färgas med a_q på bara ett sätt men q kan väljas bland $1, \ldots, r$ så blir antalet sätt på vilka färgningen kan göras enlit induktionsantagandet

$$\sum_{q=1}^{r} \text{coeff}(p(a_1, \ldots, a_r), a_1^{j_1} \cdot \ldots \cdot a_{q-1}^{j_{q-1}} \cdot a_q^{j_q - s_q} \cdot a_{q+1}^{j_{q+1}} \cdot \ldots \cdot a_r^{j}).$$

Men detta tal är detsamma som

$$\text{coeff}(p(a_1, \ldots, a_r) \cdot (a_1^{s_1} + \ldots + a_r^{s_r}), a_1^{j_1} \cdot \ldots \cdot a_r^{j}),$$

vilket betyder att induktionssteget fungerar och det första delen följer av induktionsprincipen.

Bevis för Pólyas teorem om antalet färgningar, forts.

För fallet när man använder r färger, dvs. man har inga andra begränsningar på färgningarna än att mängden färger har r element kan man gå tillväga på samma sätt som ovan och först konstatera att det räcker att räkna ut hur många färgningar det finns som är konstanta på varje bana som uppstår då ett viss k banor och varje bana skall färgas med en färg så blir det sammanlagt r^k olika möjligheter. Om nu g har k banor så blir $\zeta_{g,X}(r, \ldots r) = r^k$ och vi visat att påståendet gäller.

Hur besvärligt är det att hitta "minimiavståndet" mellan två noder i en graf

Antag att $G = [V, E]$ är en sammanhängande graf så att varje båge $e \in E$ har getts en vikt $w(e) \geq 0$ (och $w(\{v_j, v_k\}) = \infty$ ifall $\{v_j, v_k\} \notin E$) och det gäller att hitta en väg $[v_0, v_1, \ldots, v_k]$ mellan två givna noder v_* och v_{**} så att $\sum_{j=1}^{k} w(\{v_{j-1}, v_j\})$ är så liten som möjligt.

Ett sätt är att gå genom alla alternativ och välja det minsta. Om nu $|V| = n$ och det finns bågar mellan alla alternativ så finns det åtminstone $\sum_{j=2}^{n} \frac{(n-2)!}{(n-j)!} \geq (n-2)!$ olika vägar. Det finns naturligtvis många situationer där antalet alternativ är mycket mindre.

Om man använder dynamisk optimering och man har räknat ut optimivärdet för j punkter så skall man räkna nya testvärden för högst $n - j$ punkter med högst $n - j$ additioner och lika många jämförelser och sedan välja det minsta av testvärdena vilket kräver högst $n - j - 1$ jämförelser. Detta innebär att man måste göra högst $\sum_{j=1}^{n-1} n - j = \frac{1}{2}n(n-1)$ additioner och $\sum_{j=1}^{n-1}(n - j + n - j - 1) = (n-1)^2$ jämförelser. Antalet additioner och jämförelser för en graf med n noder hör alltså till mängden $O(n^2)$.

Den giriga algoritmen för ett minimalt uppspännande träd är optimal

Antag $G = (V, E)$ är en sammanhängande graf så att varje båge $\{v_j, v_k\}$ har getts en vikt $w(\{v_j, v_k\})$ och antag också att $T_* = [V, E_*]$ är ett träd så att $w(T_*) = \sum_{e \in E_*} w(e)$ är så liten som möjligt. Med den giriga algoritmen konstruerar man träden $T_j = (V_j, E_j)$, $j = 1, \ldots, n$ (där n är antalet noder och $E_1 = \emptyset$). Om $E_* = E_n$ så är den giriga algoritmen optimal och om $E_* \neq E_n$ så finns det i alla fall ett tal m, $1 \leq m < n$ så att $E_m \subset E_*$. Låt $e_{m+1} = \{\hat{v}_m, v_{m+1}\}$ vara bågen i $E_{m+1} \setminus E_m$ där $v_{m+1} \in V_{m+1} \setminus V_m$ och $\hat{v}_m \in V_m$. Om nu $e_{m+1} \notin E_*$ så finns det, eftersom T_* är ett träd, en väg i T_* från $\hat{v}_m$ till v_{m+1}. En båge $\{a, b\}$ i denna väg är sådan att $a \in V_m$ och $b \in V_{m+1}$. Om vi nu byter ut $\{a, b\}$ i E_* mot e_{m+1} så är T_* fortfarande ett träd eftersom varje väg som innehåller $\{a, b\}$ kan bytas ut mot exakt en väg som innehåller e_{m+1}. Dessutom gör valet av e_{m+1} i den giriga algoritmen att $w(T_*)$ åtminstone inte växer på grund av bytet.
Därför kan vi anta att vi också har $E_{m+1} \subset E_*$ vilket leder till att $E_n = E_*$.

När finns det en fullständig matchning i en bipartit graf?

Antag att $G = [X \cup Y, E]$ är en bipartit graf med delarna X och Y. Om $A \subset X$ låt $H(X) = \{ y \in Y : \exists x (x \in X \,\&\, \{x, y\} \in E) \}$. Om M är en fullständig matchning i G så är $|A| \leq |H(A)|$ för alla $A \subset X$ eftersom funktionen $x \in A \mapsto y$ där $\{x, y\} \in M$ är en injektion enligt definitionen för en matchning.
Nu skall vi visa att om $|A| \leq |H(A)|$ för alla $A \subset X$ så finns det en fullständig matchning i G. Detta gäller säkert om $|X| = 1$ och antag nu att det gäller då $|X| = k$. Om nu $|X| = k + 1$ så väljer vi en nod $a \in X$. Om möjligt, väljer vi i en delmängd $\hat{X} \subset X \setminus \{a\}$ så att $|H(\hat{X})| = |\hat{X}| > 0$. Om detta inte är möjligt så vet vi att $|H(\hat{X})| \geq |\hat{X}| + 1$ för alla $\hat{X} \subset X \setminus \{a\}$ med $\hat{X} \neq \emptyset$. Nu finns det ett $b \in Y$ så att $\{a, b\} \in E$ och villkoret "$|A| \leq |H(A)|$ för alla $A \subset X$" är uppfyllt för grafen $[(X \setminus \{a\}) \cup (Y \setminus \{b\}), E \setminus (\{ \{a, y\} : y \in Y \} \cup \{ \{x, b\} : x \in X \})]$ eftersom högst en granne tas bort. Genom att tillämpa induktionsantagandet på denna graf och lägga till bågen $\{a, b\}$ får vi en matchning för G.

När finns det en fullständig matchning i en bipartit graf? forts.

Om vi hittar en mängd $\hat{X} \subset X \setminus \{a\}$ så att $|H(\hat{X})| = |\hat{X}| > 0$ så kan vi igen tillämpa induktionsantagandet på grafen $G_1 = [\hat{X} \cup H(\hat{X}), \hat{E}]$ där $\hat{E} = \{ \{x, y\} \in E : x \in \hat{X}, y \in H(\hat{X}) \}$. Men antagandet "$|A| \leq |H(A)|$ för alla $A \subset X$" gäller också för grafen $G_2 = [(X \setminus \hat{X}) \cup (Y \setminus H(\hat{X})), \{ \{x, y\} \in E : x \in X \setminus \hat{X}, y \in Y \setminus H(\hat{X}) \}]$ för om detta antagande inte gäller för G_2 och någon mängd $A \subset X \setminus \hat{X}$ så kan det inte gälla för den ursprungliga grafen G med $A \cup \hat{X}$. Genom att igen använda induktionsantagandet och ta unionen av matcningarna för G_1 och G_2 får vi en matchning för grafen G och eftersom $|X| = k + 1$ så följer påståendet av induktionsprincipen.