Diszkréció diszkrét logaritmussal

Professzor dr. **Czédli Gábor** *

SZTE, Bolyai Intézet

2012. április 28.

*http://www.math.u-szeged.hu/∼czedli/

Alapok: **számolás modulo** p ("óraaritmetika")

Modulo 12: $6 + 8$

Alapok: **számolás modulo** p ("óraaritmetika")

Modulo 12: $6+8=2$, $3\cdot 5=$

Alapok: **számolás modulo** p ("óraaritmetika")

Modulo 12: $6+8=2$, $3\cdot 5=5+5+5=3$.

Modulo p (ahol p prímszám): hasonló. Legyen $\mathbf{Z}_5^*=\{1,2,3,4\}$ és $g=2$. Ekkor (modulo 5)

$g^0=1$, $g^1=2$, $g^2=$

Alapok: **számolás modulo** p ("óraaritmetika")

Modulo 12: $6+8=2$, $3\cdot 5=5+5+5=3$.

Modulo p (ahol p prímszám): hasonló. Legyen $\mathbf{Z}_5^*=\{1,2,3,4\}$ és $g=2$. Ekkor (modulo 5)

$g^0=1$, $g^1=2$, $g^2=4$, $g^3=$

Alapok: **számolás modulo** p ("óraaritmetika")

Modulo 12: $6+8=2$, $3\cdot 5=5+5+5=3$.

Modulo p (ahol p prímszám): hasonló. Legyen $\mathbf{Z}_5^*=\{1,2,3,4\}$ és $g=2$. Ekkor (modulo 5)

$g^0=1$, $g^1=2$, $g^2=4$, $g^3=4\cdot 2=3$;

Alapok: **számolás modulo** p ("óraaritmetika")

Modulo 12: $6+8=2$, $3\cdot 5=5+5+5=3$.

Modulo p (ahol p prímszám): hasonló. Legyen $\mathbf{Z}_5^*=\{1,2,3,4\}$ és $g=2$. Ekkor (modulo 5)

$g^0=1$, $g^1=2$, $g^2=4$, $g^3=4\cdot 2=3$; {első 4 hatvány} $=\mathbf{Z}_5^*$. Ezért

Alapok: **számolás modulo** p ("óraaritmetika")

Modulo 12: $6+8=2$, $3\cdot 5=5+5+5=3$.

Modulo p (ahol p prímszám): hasonló. Legyen $\mathbf{Z}_5^*=\{1,2,3,4\}$ és $g=2$. Ekkor (modulo 5)

$g^0=1$, $g^1=2$, $g^2=4$, $g^3=4\cdot 2=3$; {első 4 hatvány} $=\mathbf{Z}_5^*$.
Ezért pl. $\log_g 4=2$ és

Alapok: **számolás modulo** p ("óraaritmetika")

Modulo 12: $6+8=2$, $3\cdot 5=5+5+5=3$.

Modulo p (ahol p prímszám): hasonló. Legyen $\mathbf{Z}_5^*=\{1,2,3,4\}$ és $g=2$. Ekkor (modulo 5)

$g^0=1$, $g^1=2$, $g^2=4$, $g^3=4\cdot 2=3$; {első 4 hatvány} $=\mathbf{Z}_5^*$.
Ezért pl. $\log_g 4=2$ és $\log_g 3=3$.

Alapok: **számolás modulo** p ("óraaritmetika")

Modulo 12: $6+8=2$, $3\cdot 5=5+5+5=3$.

Modulo p (ahol p prímszám): hasonló. Legyen $\mathbf{Z}_5^*=\{1,2,3,4\}$ és $g=2$. Ekkor (modulo 5)

$g^0=1$, $g^1=2$, $g^2=4$, $g^3=4\cdot 2=3$; {első 4 hatvány} $=\mathbf{Z}_5^*$. Ezért pl. $\log_g 4=2$ és $\log_g 3=3$. Általában is megy:

$\mathbf{Z}_p^*=\{1,2,\dots,p-1\}$, p prím, $g\in\mathbf{Z}_p^*$ jól választott logaritmus alap, ekkor $x\in\mathbf{Z}_p^*$-re $\log_g x$ értelmes és $\log_g x\in\{0,1,\dots,p-2\}$.

Ha a 15 milliár fényév sugarú (eddig ismert) Univerzumban minden köb-Ångströmbnyi térrészére egy 1 GHz-es számítógépet raktun volna és azokat az Ősrobbanáskor elindítottuk volna, akkor ezek a gépek együttesen is legfeljebb 10^{136} elemi műveletet végeztek volna el! Ezért legyen $p > 10^{300}$. (Legalább 301 jegyű).

Csakugyan, egy év $\approx 365 \cdot 24 \cdot 3600 = 31536000 \approx 3 \cdot 10^7$ sec, ezért

$$\underbrace{\frac{4}{3}\pi \left(\underbrace{\underbrace{1,5 \cdot 10^{10}}_{\text{fényév}} \cdot 3 \cdot 10^7}_{\text{fény-sec}} \cdot \underbrace{3 \cdot 10^{5+13}}_{\text{Å/sec}} \right)^3}_{\text{univerzum köb-Ångströmben}} \cdot \underbrace{10^9}_{\text{GHz}} \cdot \underbrace{1,5 \cdot 10^{10} \cdot 3 \cdot 10^7}_{\text{Ősrobbanás óta}},$$

ami $\approx 0,6 \cdot 10^{136}$.

Tegyük fel, hogy p és a diszkrét logaritmus g alapja adott. Ekkor $y \in \mathbf{Z}_p^*$ esetén a $\log_g y$ **diszkrét logaritmus gyakorlatilag kiszámíthatatlan**!

Próbálgatva keressük azt az $x \in \{0, 1, 2, \ldots, p-2\}$ kitevőt, amelyre $g^x = y$ (modulo p)?

Tegyük fel, hogy p és a diszkrét logaritmus g alapja adott. Ekkor $y \in \mathbf{Z}_p^*$ esetén a $\log_g y$ **diszkrét logaritmus gyakorlatilag kiszámíthatatlan**!

Próbálgatva keressük azt az $x \in \{0, 1, 2, \ldots, p-2\}$ kitevőt, amelyre $g^x = y$ (modulo p)?

Ennyi kitevőt nem tudunk kipróbálni. De még ha 10^{136} kitevőt ki is próbálhatnánk, akkor is több mint 20 egymást követő lottó öttalálathoz szükséges szerencsére lenne szükségünk — ez nem fog bekövetkezni.

Vannak kissé gyorsabb módszerek és $\mathbf{Z}_p^*$ helyett pl. $GF(2^{1200})$-at érdemes venni, de a lényeget ez nem érinti: **a diszkrét logaritmus jól őrzi a titkot, mert gyakorlatilag kiszámíthatatlan.**

Ha Rómeó titka $r \in \{0, 1, \ldots, p-2\}$, akkor $y := g^r$-t közhírré teheti; abból Tybalt az $r = \log_g y$ értéket nem tudja kiszámítani.

Ha Rómeó titka $r \in \{0, 1, \ldots, p-2\}$, akkor $y := g^r$-t közhírré teheti; abból Tybalt az $r = \log_g y$ értéket nem tudja kiszámítani.

Rómeó könnyen kiszámíthatja $y := g^r$-t !! Pl. ha $r = 43$, akkor

$$g = g^1,\ g^2,\ g^4,\ g^8,\ g^{16},\ g^{32};$$

ez eddig 5 ($\leq \log_2 43$) négyzetre emelés (speciális szorzás), majd legfeljebb ugyanennyi szorzással

$$g^1 \cdot g^2 \cdot g^8 \cdot g^{32} = g^{32+8+2+1} = g^{43} = g^r.$$

Ha Rómeó titka $r \in \{0, 1, \ldots, p-2\}$, akkor $y := g^r$-t közhírré teheti; abból Tybalt az $r = \log_g y$ értéket nem tudja kiszámítani.

Rómeó könnyen kiszámíthatja $y := g^r$-t !! Pl. ha $r = 43$, akkor

$$g = g^1,\ g^2,\ g^4,\ g^8,\ g^{16},\ g^{32};$$

ez eddig 5 ($\leq \log_2 43$) négyzetre emelés (speciális szorzás), majd legfeljebb ugyanennyi szorzással

$$g^1 \cdot g^2 \cdot g^8 \cdot g^{32} = g^{32+8+2+1} = g^{43} = g^r.$$

Általában g^k kiszámításához elegendő $2 \cdot \log_2 k$ szorzás. Hasonlóan, ha $r = 10^{500}$, akkor $2 \cdot \log_2 10^{500} = 1000 \cdot \log_2 10 \approx 3322$ szorzás elegendő; számítógépünknek ez semmiség. Ez volt az ún. **gyors hatványozás**.

Borítékolás: Rómeó ismer egy $t \in \{0, 1, \ldots p-2\}$ titkot. Ha közli $y = g^t$ értékét ($\mathbf{Z}_p^*$-ben), akkor ezzel t-t **borítékolta**. Azaz

(1) Ki tudja **nyitni a borítékot** úgy, hogy felfedi t-t; bárki gyorsan ellenőrizheti, hogy vajon $g^t = y$, tehát nem csalhat.

(2) Amíg Rómeó nem nyitja ki a borítékot, addig senki sem tudhatja meg t-t.

(3) Borítékolás (azaz y közlése) után Rómeó nem tudja a boríték tartalmát megváltoztatni, hiszen $t = \log_g y$.

Alkalmazás:

Borítékolás: Rómeó ismer egy $t \in \{0, 1, \ldots p-2\}$ titkot. Ha közli $y = g^t$ értékét ($\mathbf{Z}_p^*$-ben), akkor ezzel t-t **borítékolta**. Azaz

(1) Ki tudja **nyitni a borítékot** úgy, hogy felfedi t-t; bárki gyorsan ellenőrizheti, hogy vajon $g^t = y$, tehát nem csalhat.

(2) Amíg Rómeó nem nyitja ki a borítékot, addig senki sem tudhatja meg t-t.

(3) Borítékolás (azaz y közlése) után Rómeó nem tudja a boríték tartalmát megváltoztatni, hiszen $t = \log_g y$.

Alkalmazás: Fej vagy írás telefonon.

Házi feladat: Igazságos sorsolás n résztvevő között az Interneten.

A borítékolás azon múlt, hogy a hatványozás egy (alkalmas értelemben) **könnyű probléma**, egy úgynevezett **P-beli probléma**.

A borítékolás azon múlt, hogy a hatványozás egy (alkalmas értelemben) **könnyű probléma**, egy úgynevezett **P-beli probléma**. A diszkrét logaritmus kiszámítása viszont egyfajta **nehéz**, szaknyelven szólva **NP-beli probléma**.

A borítékolás azon múlt, hogy a hatványozás egy (alkalmas értelemben) **könnyű probléma**, egy úgynevezett **P-beli probléma**. A diszkrét logaritmus kiszámítása viszont egyfajta **nehéz**, szaknyelven szólva **NP-beli probléma**.

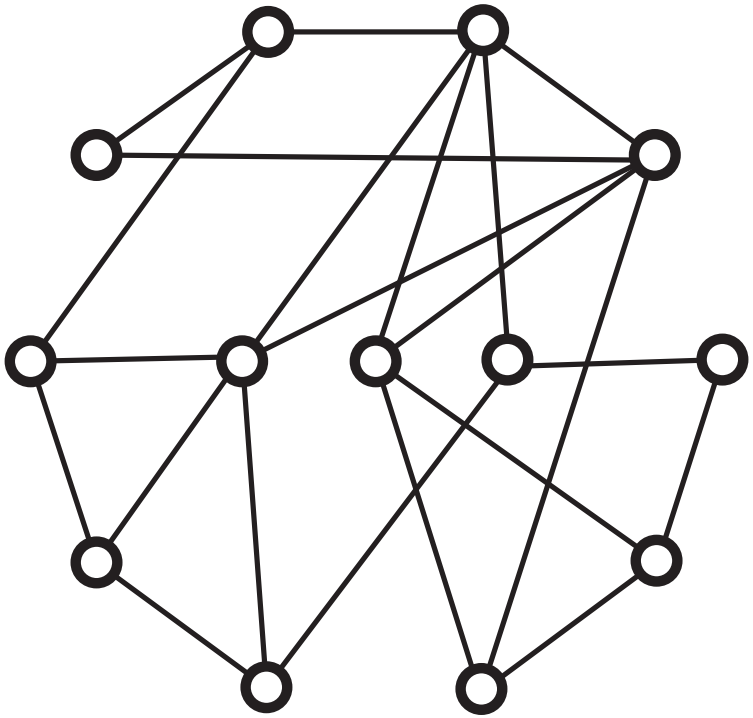
Van olyan NP-beli probléma, amelyre minden más NP-beli probléma *könnyen* visszavezethető. (Azaz a visszavezetés végrehajtása egy P-beli feladat.)

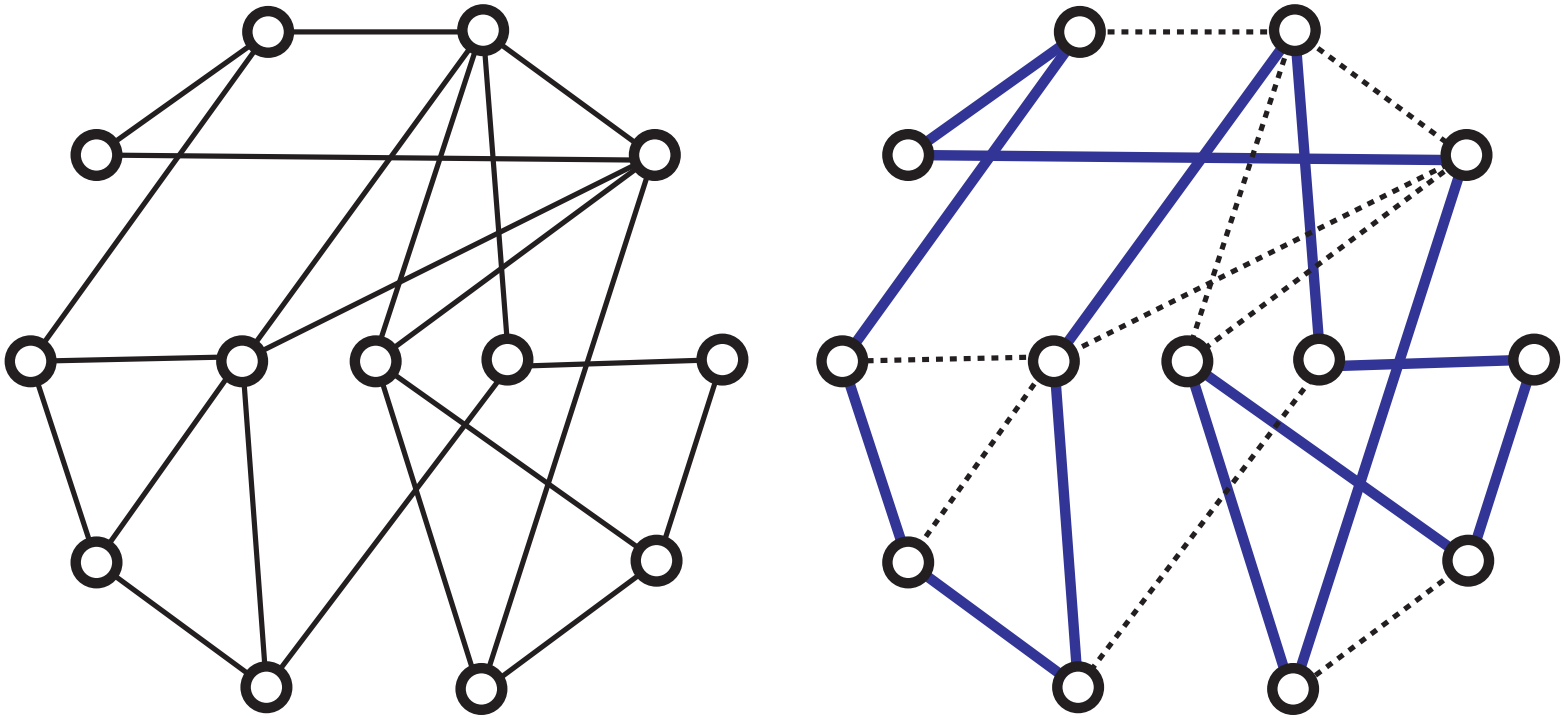
A borítékolás azon múlt, hogy a hatványozás egy (alkalmas értelemben) **könnyű probléma**, egy úgynevezett **P-beli probléma**. A diszkrét logaritmus kiszámítása viszont egyfajta **nehéz**, szaknyelven szólva **NP-beli probléma**.

Van olyan NP-beli probléma, amelyre minden más NP-beli probléma *könnyen* visszavezethető. (Azaz a visszavezetés végrehajtása egy P-beli feladat.)

Pl. ilyen a **Hamilton-kör létezése** probléma. Itt a bemenő adat egy tetszőleges véges gráf, és az a kérdés, hogy tartalmaz-e a gráf olyan kört, amelyik mindegyik szögponton pontosan egyszer megy át.

Hamilton-kör





Nehéz (NP) eldönteni, hogy van-e ilyen kör. De ha valaki talál egyet, akkor azt könnyű (P-beli) ellenőrizni. Ez a "ha már találtunk egyet, akkor már könnyű" tulajdonság minden NP-beli problémára érvényes (definíció szerint).

Tegyük fel, hogy Rómeó megold egy híres problémát, pl. egy 7 MByte-os fájlban bebizonyítja a (ma még megoldatlan!) Ikerprím Sejtést. Adja át Tybaltnak? - ellophatja az elsőbbségét. Csak a tényt közölje? - Tybalt nem hisz neki.

Tegyük fel, hogy Rómeó megold egy híres problémát, pl. egy 7 MByte-os fájlban bebizonyítja a (ma még megoldatlan!) Ikerprím Sejtést. Adja át Tybaltnak? - ellophatja az elsőbbségét. Csak a tényt közölje? - Tybalt nem hisz neki.

Egy matematika bizonyítás ellenőrzése rábízható a számítógépre. Innen ismeretes, hogy az alábbi probléma NP-beli:

Bizonyítható(10) probléma: Bemenő adat: tetszőleges S szöveg. Kérdés: igaz-e, hogy S egy olyan matematikai állítás, amelyet legfeljebb 10 MByte terjedelemben be lehet bizonyítani?

Említettük, hogy a **Hamilton-kör létezése** problémára minden más NP-beli probléma visszavezethető (és az is ismert, hogy hogyan vezethető vissza.) Ezért a **bizonyítható(10)** probléma

Említettük, hogy a **Hamilton-kör létezése** problémára minden más NP-beli probléma visszavezethető (és az is ismert, hogy hogyan vezethető vissza.) Ezért a **bizonyítható(10)** probléma

$$S = \text{"végtelen sok ikerprím létezik"}$$

bemenő adatának megfelel (és mindenki által könnyen kiszámítható) egy

Említettük, hogy a **Hamilton-kör létezése** problémára minden más NP-beli probléma visszavezethető (és az is ismert, hogy hogyan vezethető vissza.) Ezért a **bizonyítható(10)** probléma

$$S = \text{"végtelen sok ikerprím létezik"}$$

bemenő adatának megfelel (és mindenki által könnyen kiszámítható) egy $G = G(S)$ gráf úgy, hogy

Említettük, hogy a **Hamilton-kör létezése** problémára minden más NP-beli probléma visszavezethető (és az is ismert, hogy hogyan vezethető vissza.) Ezért a **bizonyítható(10)** probléma

$$S = \text{"végtelen sok ikerprím létezik"}$$

bemenő adatának megfelel (és mindenki által könnyen kiszámítható) egy $G = G(S)$ gráf úgy, hogy G-ben pontosan akkor van Hamilton-kör, ha az S állításnak van legfeljebb 10 MByte-nyi bizonyítása. T

Említettük, hogy a **Hamilton-kör létezése** problémára minden más NP-beli probléma visszavezethető (és az is ismert, hogy hogyan vezethető vissza.) Ezért a **bizonyítható(10)** probléma

$$S = \text{"végtelen sok ikerprím létezik"}$$

bemenő adatának megfelel (és mindenki által könnyen kiszámítható) egy $G = G(S)$ gráf úgy, hogy G-ben pontosan akkor van Hamilton-kör, ha az S állításnak van legfeljebb 10 MByte-nyi bizonyítása. Továbbá ezen megfeleltetés során a bizonyításából Rómeó (de csak ő) egy Hamilton-kört is kap G-ben.

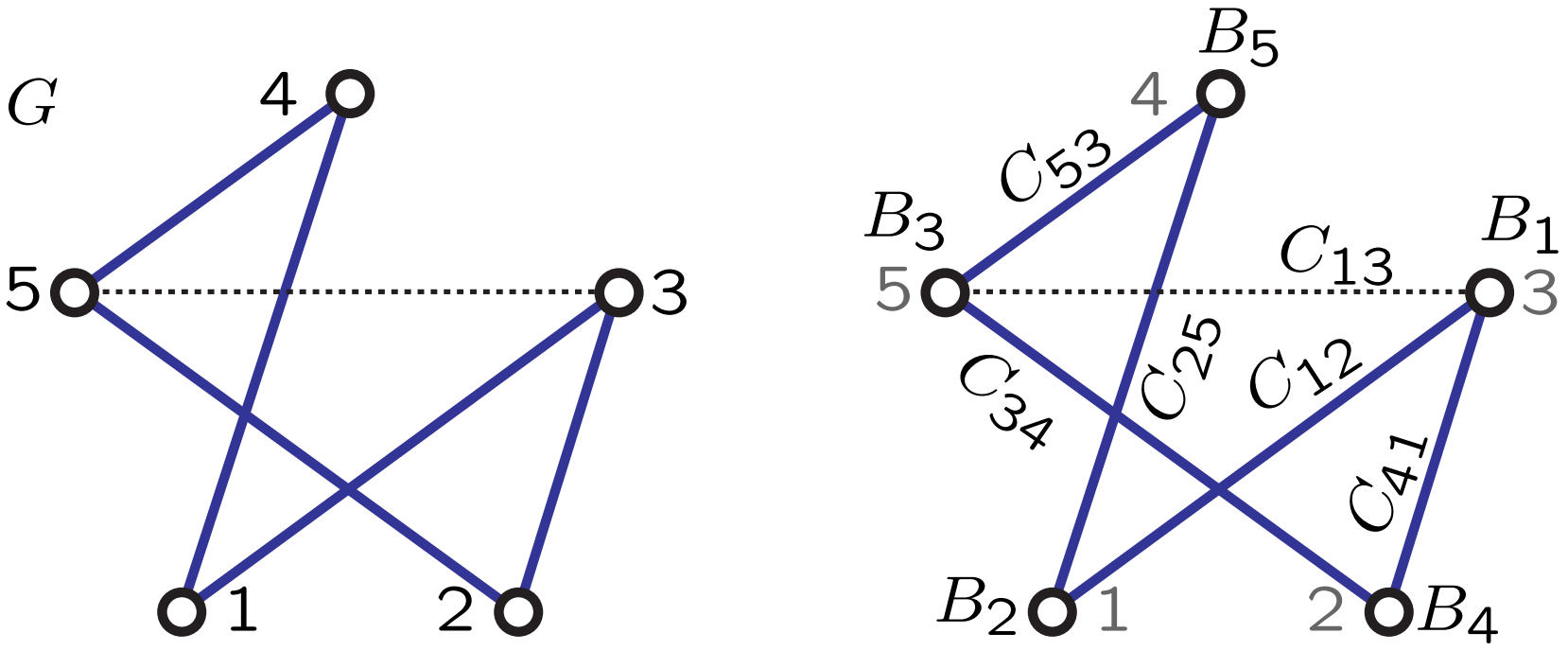
Tehát

Említettük, hogy a **Hamilton-kör létezése** problémára minden más NP-beli probléma visszavezethető (és az is ismert, hogy hogyan vezethető vissza.) Ezért a **bizonyítható(10)** probléma

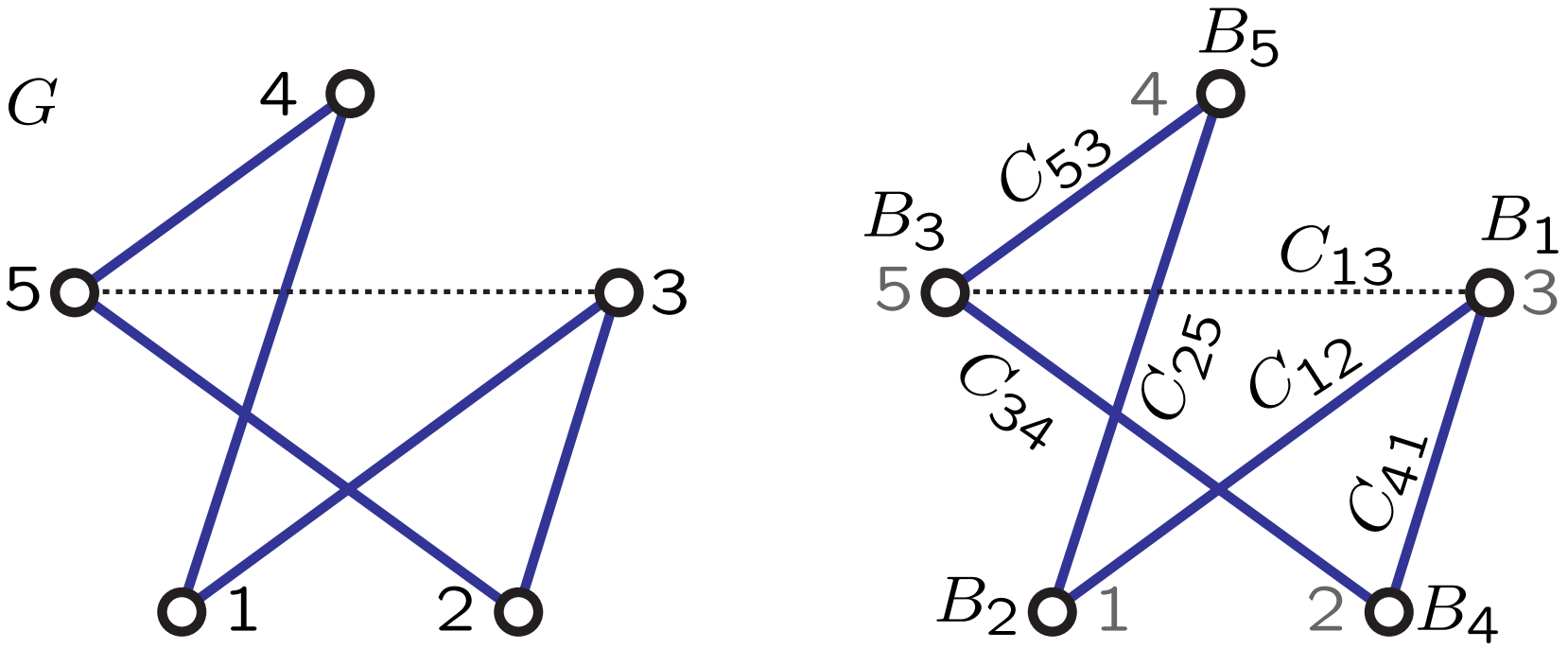
$$S = \text{"végtelen sok ikerprím létezik"}$$

bemenő adatának megfelel (és mindenki által könnyen kiszámítható) egy $G = G(S)$ gráf úgy, hogy G-ben pontosan akkor van Hamilton-kör, ha az S állításnak van legfeljebb 10 MByte-nyi bizonyítása. Továbbá ezen megfeleltetés során a bizonyításából Rómeó (de csak ő) egy Hamilton-kört is kap G-ben.

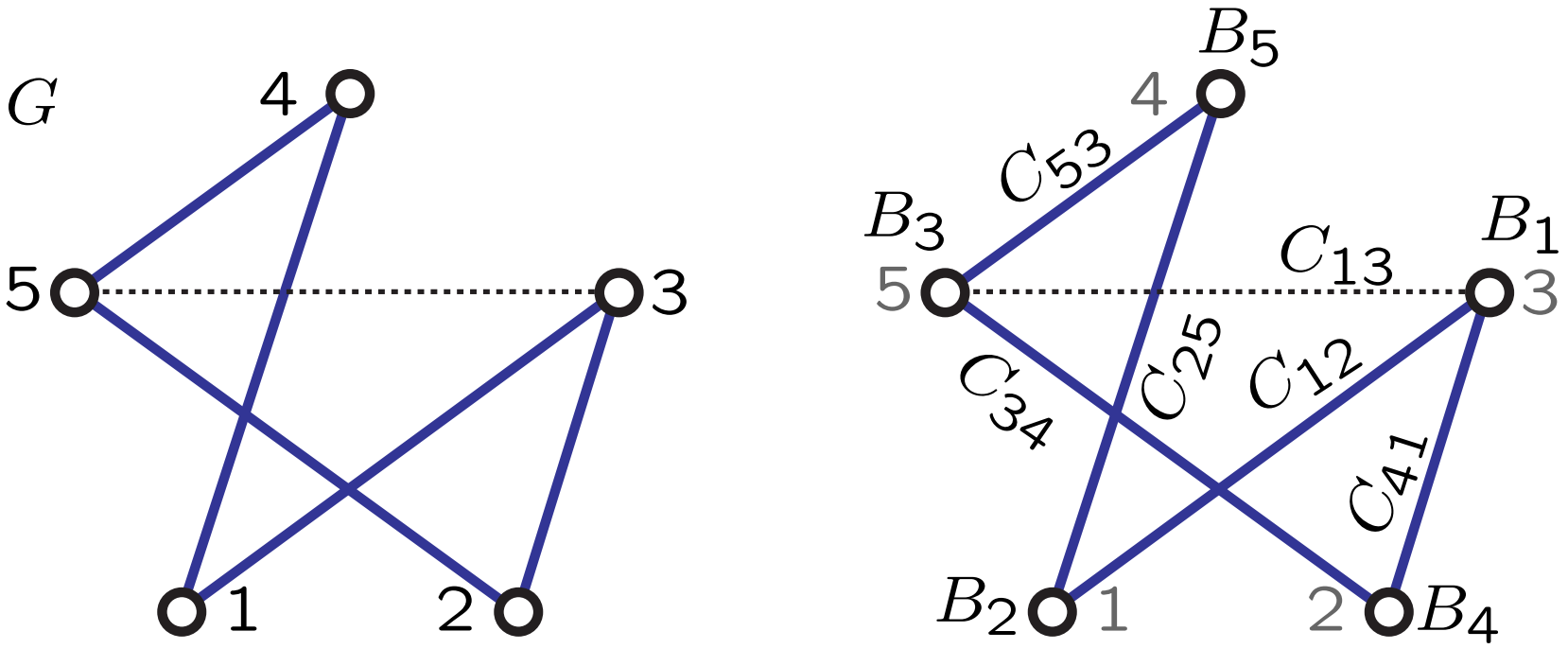
Tehát Rómeónak elegendő azt igazolnia, hogy $G = G(S)$-ben ismer egy Hamilton-kört. Erről az alábbi módon győzheti meg Tybaltot anélkül, hogy bármiféle információt adna a bizonyításról.



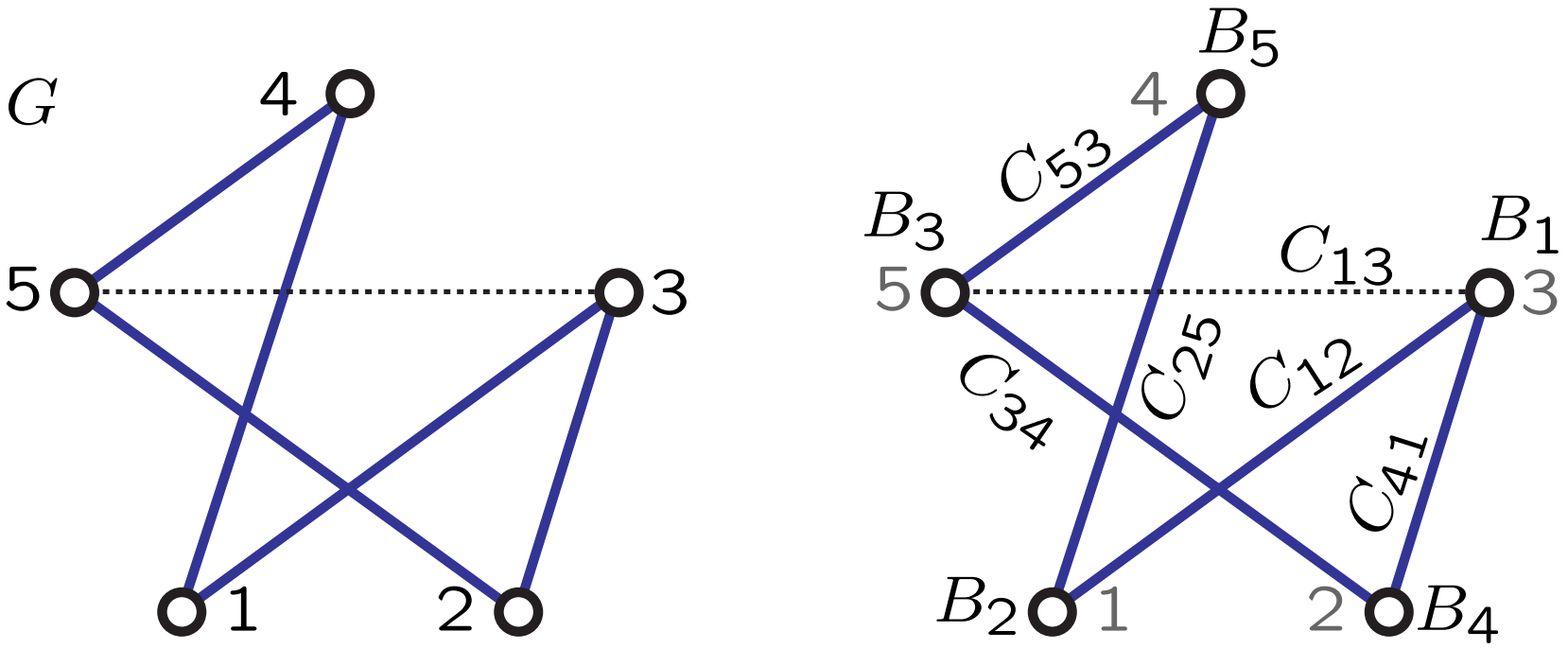
Mondjuk Rómeó a (baloldali) kék Hamilton-kört ismeri.



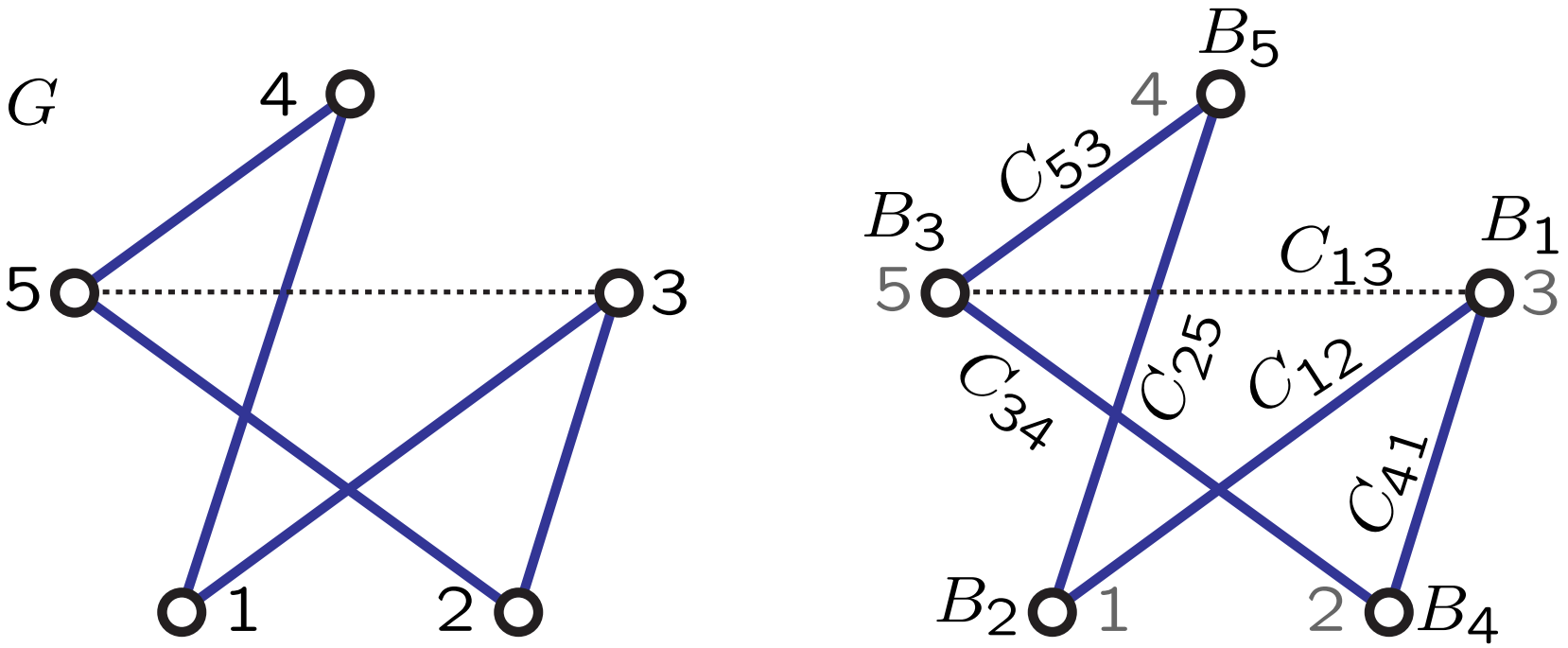
Mondjuk Rómeó a (baloldali) kék Hamilton-kört ismeri. Vesz öt borítékot a csúcsoknak, B_1, ..., B_5, és további húsz borítékot a lehetséges éleknek, C_{12}, C_{13},..., C_{54}.



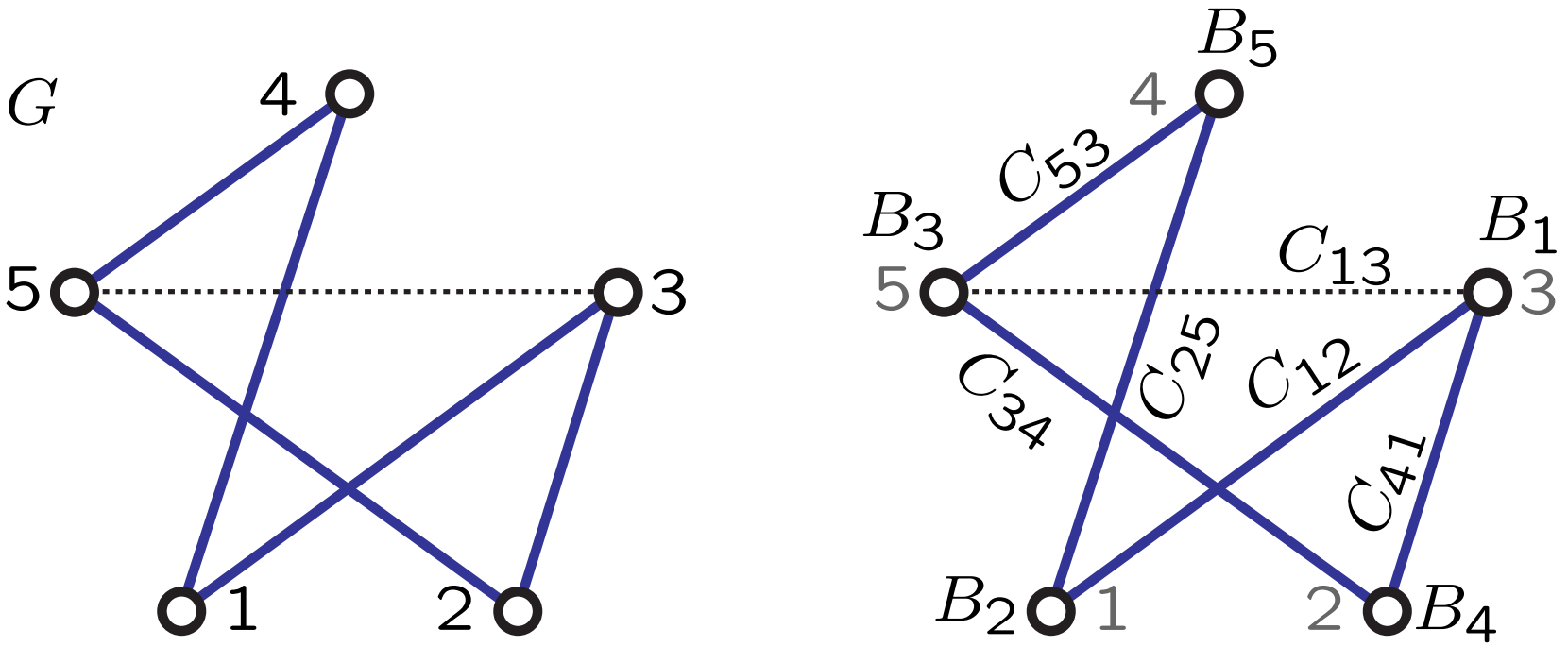
Mondjuk Rómeó a (baloldali) kék Hamilton-kört ismeri. Vesz öt borítékot a csúcsoknak, $B_1, \ldots, B_5$, és további húsz borítékot a lehetséges éleknek, C_{12}, $C_{13}, \ldots, C_{54}$. Véletlen sorrendben a csúcsokat berakja a $B_1, \ldots, B_5$ borítékokba.



Mondjuk Rómeó a (baloldali) kék Hamilton-kört ismeri. Vesz öt borítékot a csúcsoknak, $B_1, \ldots, B_5$, és további húsz borítékot a lehetséges éleknek, C_{12}, $C_{13}, \ldots, C_{54}$. Véletlen sorrendben a csúcsokat berakja a $B_1, \ldots, B_5$ borítékokba. Az éleket a C_{ij}-kbe rakja: ha a B_i és B_j-be rakott két csúcsot él köti össze, akkor $C_{ij} = C_{ji}$-be 1-et rak, ellenkező esetben pedig 0-t.



Ha Tybalt érmével fejet dob, akkor Rómeó kinyitja az összes borítékot, és Tybalt ellenőrzi, hogy G volt-e borítékolva.



Ha Tybalt érmével fejet dob, akkor Rómeó kinyitja az összes borítékot, és Tybalt ellenőrzi, hogy G volt-e borítékolva.

Ha írás, akkor (a kék Hamilton kör mentén haladva) Rómeó rendre kinyitja a C_{12}, C_{25}, C_{53}, C_{34}, C_{41} borítékokat, hogy Tybalt láthatassa: mindegyikben 1 (azaz él) van, tehát a B_1, B_2, B_5, B_3, B_4, B_1 borítékokba rakott csúcsok (ezen sorrendben) egy Hamilton-körön vannak.

Blöffre a lebukás 50 %

Ha Rómeó blöfföl (azaz nem ismer G-ben Hamilton-kört), akkor $\frac{1}{2}$ valószínűséggel lebukik!

Ugyanis ha nem a G gráfot borítékolta,

Ha Rómeó blöfföl (azaz nem ismer G-ben Hamilton-kört), akkor $\frac{1}{2}$ valószínűséggel lebukik!

Ugyanis ha nem a G gráfot borítékolta, akkor fej után Tybalt ezt azonnal észreveszi. Ha

Ha Rómeó blöfföl (azaz nem ismer G-ben Hamilton-kört), akkor $\frac{1}{2}$ valószínűséggel lebukik!

Ugyanis ha nem a G gráfot borítékolta, akkor fej után Tybalt ezt azonnal észreveszi. Ha pedig G-t borítékolta, akkor írásra bukik le, hiszen nem tud G-ben Hamilton-kört felmutatni. (Ha Rómeó előre tudná, hogy mit dob majd Tybalt, akkor persze nem bukna le, de nem tudhatja.)

Ha Rómeó blöfföl (azaz nem ismer G-ben Hamilton-kört), akkor $\frac{1}{2}$ valószínűséggel lebukik!

Ugyanis ha nem a G gráfot borítékolta, akkor fej után Tybalt ezt azonnal észreveszi. Ha pedig G-t borítékolta, akkor írásra bukik le, hiszen nem tud G-ben Hamilton-kört felmutatni. (Ha Rómeó előre tudná, hogy mit dob majd Tybalt, akkor persze nem bukna le, de nem tudhatja.)

Ha Rómeó sorra átmegy 1000 teszten (ez számítógéppel hamar megy); akkor Tybalt $1-(\frac{1}{2})^{1000}$ valószínűséggel biztos lehet abban, hogy Rómeó bebizonyította az ikerprím sejtést; ellenkező esetben ugyanis 1000-szer kellett az érmedobás eredényét eltalálnia, és ennek csak $(\frac{1}{2})^{1000}$ a valószínűsége.

Tybalt semmilyen részletet nem tudott meg Czédli 2012.04.28 $18'/2'$

Tybalt semmilyen részletet nem tudott meg a bizonyításból azon túl, hogy az működik, tehát hogy az ikerprím sejtés igaz!

Milyen információt kap fej után? Az általa is ismert G gráf egy véletlen bedobozolását; nos, ilyet ő is tudna gyártani.

Írás után csak annyit tud meg, hogy van Hamilton kör (azaz az ikerprím sejtés igaz), de ezt Rómeó már előre megmondta.

Félreértés ne essék, az ikerprím sejtés megoldatlan.

Tybalt semmilyen részletet nem tudott meg Czédli 2012.04.28 $18'/2'$

Tybalt semmilyen részletet nem tudott meg a bizonyításból azon túl, hogy az működik, tehát hogy az ikerprím sejtés igaz!

Milyen információt kap fej után? Az általa is ismert G gráf egy véletlen bedobozolását; nos, ilyet ő is tudna gyártani.

Írás után csak annyit tud meg, hogy van Hamilton kör (azaz az ikerprím sejtés igaz), de ezt Rómeó már előre megmondta.

Félreértés ne essék, az ikerprím sejtés megoldatlan. A kivetített fájl a honapom magyar verzióján is olvasható:

http://www.math.u-szeged.hu/∼czedli/

Végül, ha marad rá idő: hogyan vált Rómeó és Júlia titkos üzenetet diszkrét logaritmussal?

Diffie–Hellman-kulcsváltás. Rómeó és Júlia nyílt (Tybalt által lehallgatott) információs csatornán egy közös kulcsban szeretne megállapodni. Íme a protokoll. Az előbbi p és g publikus.

Rómeó választ egy véletlen $r \in \{0, 1, \ldots, p-2\}$, Júlia pedig egy véletlen $j \in \{0, 1, \ldots, p-2\}$ kitevőt.

Rómeó kiszámítja és elküldi Júliának a $g^r \in \mathbf{Z}_p^*$ hatványt. (Tybalt ebből nem tudja meg r-et; igaz, Júlia sem, sebaj.)

Júlia elküldi Rómeónak a $g^j \in \mathbf{Z}_p^*$ hatványt. (Tybalt tehetetlen.)

Rómeó kiszámítja a $(g^j)^r \in \mathbf{Z}_p^*$, Júlia pedig a $(g^r)^j \in \mathbf{Z}_p^*$ hatványt. Mivel mindkettő g^{rj}, ez lesz a közös kulcsuk; csak ők ismerik.

http://www.math.u-szeged.hu/∼czedli/