Bizánci generálisok

Bizánc, i.sz. 1453

Konstantinápoly, a hajdanán virágzó birodalmi főváros ostrom alatt áll. Megszálló oszmán csapatok táboroznak a falaknál és törnek egyre beljebb véres küzdelmek árán. Habár mindkét fél súlyos veszteségeket szenvedett, a támadók lendülete töretlen, lehengerlő túlerejük ellen a védők tehetetlennek bizonyulnak. Elkeseredett, gigászi erőfeszítéseik ellenére a város sorsa megpecsételődni látszik. Táboraik védelmében az oszmán generálisok végső, mindent eldöntő rohamra készülnek. Hírnökeik táborról táborra járnak titkos üzeneteket hordozván. A siker kulcsa a megfelelő időzítésben rejlik, a túlerő érvényre juttatásához valamennyi generálisnak egyszerre kell rohamra vezetni katonáit.

A rég várt diadal óráit azonban ármány és cselszövés árnyékolja be. Úgy hírlik, némely generálisok lojalitása a birodalom felé meggyengült és más hatalmakkal paktáltak le. Álhírekkel, zavart keltő üzenetekkel próbálják meggátolni a végső ostromot. A birodalom hűséges generálisai embert próbáló kihívás elé néznek: hogyan jussanak egyezségre, ha nem tudják, kiben bízhatnak?

Ötszáz évvel később, a megosztott számítások és szinkronizálás folklórjaként a feladat visszatért a köztudatba. Manapság összekötött, eltérő idő pontokban működésbe lépő számítógépeknek kell egyeztetniük belső óráikat, észlelvén az esetlegesen hibásan működő (vagy szándékosan hibásan beállított) egységeket. Csillagászati méretű számítási problémák oldódnak meg megfelelő részfeladatokra bontással, melyek elvégzésére a világ különböző részein fekvő gépparkokat fognak munkára. A részfeladatok kiosztása, a gépek közötti kommunikáció és adatmegosztás kérdése újraélesztette a bizánci generálisok problémáját.

Bizánc reneszánsza

A felvázolt feladatokban szereplő kommunikációs hálózatot egy n csúcsú teljes gráffal modellezzük. A protokoll során minden résztvevő (modellünkben a gráf csúcsai) minden egyes körben egy bit értékű információt („0”-t vagy „1”-et tartalmazó üzenetet) küld a többieknek és fogad tőlük egyesével. A bejövő üzenetek ismeretében (ideértvén az esetleges korábbi körökben megosztott információt) minden egyes generális döntést hoz a következő körben szomszédainak küldendő üzenetekről[1]. Bár az elküldött adatok sérülés elleni védelme, titkosítása, a küldő személyének hiteles azonosítása számottevő kérdések, az említett témák külön-külön könyvtárnyi méretű szakirodalommal bírnak és kriptográfiai kutatások szerves részét képezik, jelen cikkben ezen kérdések vizsgálatára nem térhetünk ki. Modellünkben valamennyi üzenet sérülés nélkül eljut a címzetthez még az adott körön belül és senki sem képes üzenetet küldeni más nevében.

Feladatunk olyan kommunikációs séma tervezése, mely valamennyi generálisnak előírja, milyen szempontok szerint hozza meg döntéseit a következő körök, majdan pedig a támadás kérdését illetően. A kiosztott, körökre lebontott utasítások halmazát „protokollnak” nevezzük. Jelen problémában az érdeklődésre számot tartó protokollok felé a következő elvárásokat támasztjuk:

1. véges sok kör elteltével valamennyi csúcs döntésre jut (1 bit értékű „igen–nem” kimenetet szolgáltat),
2. a protokoll parancsait végig tiszteletben tartó és azt követő csúcsok (a lojális generálisok) ugyanarra a döntésre jutnak,
3. ha az összes lojális generális támadni akar, az eljárás végén a támadás mellett döntenek, míg ha valamennyien kivárnának, senki se határozza el magát újabb ostromra.

Amennyiben a generálisok véleménye megoszlik, döntésüket – a második pont figyelembe vétele mellett – szabadon hozhatják meg; harmadik pontban feltüntetett feltételünk mindössze azt a triviális megoldást célzott kizárni, melyben a kiosztott utasítások egyetlen bitet, a generálisok által meghozandó döntést tartalmazzák. Támaszthatnánk a leírtnál szigorúbb, természetesnek tűnő elvárásokat (pl. ha a generálisok többsége támadni akar, döntsenek a támadás mellett), jelen cikkben azonban – részben terjedelmi okok miatt, részben az olvasót a kevéssé izgalmas ám hosszadalmas technikai felépítésektől megkímélendő – kizárólag a fent vázolt klasszikus feladattal foglalkozunk.

Szót kell ejtenünk röviden protokollok úgynevezett „uniformitási” tulajdonságáról. Egyes eljárások, alkalmazások során megengedett, hogy a koordinálók a különböző résztvevőknek személyre szabottan osszanak feladatokat; a labdarúgás Európa-bajnokság döntőjén nyilvánvalóan nem a spanyol csapat kapusától várjuk a gólokat. Más környezetben azonban, kiváltképpen, ha a protokollok kiosztására szűkös időkeret áll rendelkezésre (gyári számítógépek szoftverinstallációja), megkövetelt a feladatlisták egységesítése. Uniformnak nevezünk egy protokollt, ha valamennyi részvevő szóról szóra ugyanazt az utasítássorozatot kapja kézhez. A résztvevők tényleges viselkedése – függvénye lévén számos más tényezőnek – természetesen eltérhet az eljárás során. Jelen cikkben – a könnyebb tárgyalhatóság kedvéért – kizárólag uniform protokollokkal foglalkozunk, a közölt eredmények azonban (a bizonyítások megfelelő módosításával) a nem uniform esetre is kiterjeszthetőek.

A demokrácia bukása

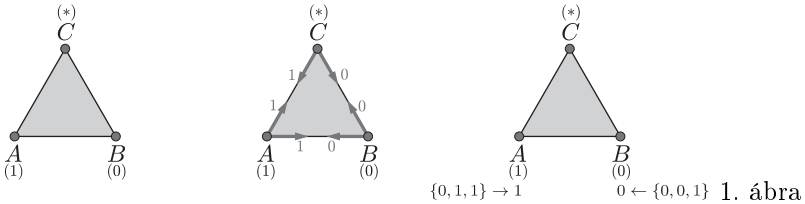
[1] A generálisok precízen Turing-gépekkel modellezhetőek. Turing-gépekről bővebben a KöMaL 2003/1. számában olvashatunk.

Lássunk példát arra, miként képesek az árulók szabotálni az ideális esetben működőképes protokollokat. Példánkban A és B mindketten lojális generálisok, az ostrom állásáról azonban eltérően vélekednek: A azonnali támadást javasol, B kivárna. Harmadik generálisunk, C áruló, célja az A és B közötti megállapodás megakadályozása. Többségi szavazásra bocsájtják a kérdést, elküldvén egymásnak saját meggyőződésüket (egyetlen bitbe kódolva). A „többségi szavazás" uniform protokollja két körből áll és a következőképpen néz ki:

1. kör: Küldd el saját meggyőződésedet mindenkinek.

2. kör: A kapott bejövő adatok közül (sajátodat hozzáadva) válaszd ki a gyakoribbat (egyenlőség esetén az „1"-est) és ezt add vissza kimenetként.

Ha a közölt protokoll mellett C mindkét társát saját elhatározásában erősíti meg (*1. ábra*), a két lojális generális eltérő képet kap a szavazatok halmazáról és ezáltal eltérő döntésre jut. A demokratikus megközelítés tehát már kevés áruló esetén sem garantál egyetértést.



1. ábra

Lehetséges és lehetetlen határa

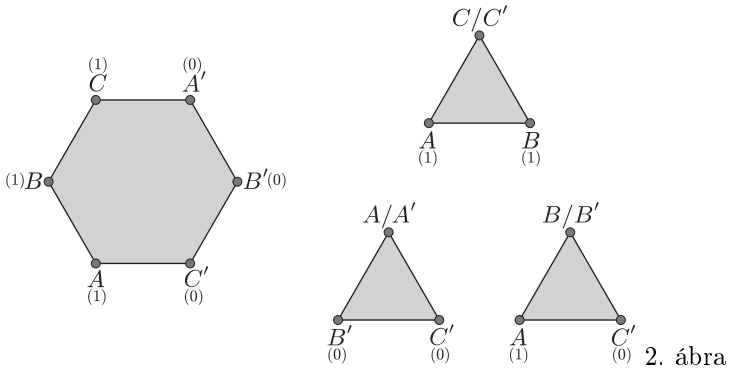
A '80-as éves első felében Lamport, Shostak és Pease [1] eredménye megválaszolta a bizánci generálisok kérdését.

1. tétel [1]. *Ha a generálisok száma n és közülük t áruló, úgy pontosan akkor létezik megfelelő protokoll, ha $t < \frac{n}{3}$.*

A közölt tétel bizonyításának magja annak speciális, $n = 3$ esete:

1. lemma. *Három generális esetén nem létezik olyan protokoll, mely áruló jelenlétében egyetértést garantál a két lojális fél között.*

Bizonyítás: Indirekt módon tegyük fel egy, a fentiekben leírt (uniform) protokoll létezését. Ültessünk le egy szabályos hatszög csúcsaiba lojális generálisokat a *2. ábra* szerint. Mivel valamennyi generális két szomszéddal bír és kizárólag a szomszédokkal képes kommunikálni, az eredetileg 3 főre tervezett protokoll a hatszögön elindítható, véges sok lépésben véget ér és valamennyi generális döntésre jut.



2. ábra

Vizsgáljuk meg közelebbről a született döntéseket: a hatszögön való futás során, annak mintegy melléktermékeként több alkalommal is szimuláltuk három generális – két lojális és egy, általunk előírt módon viselkedő áruló – üzenetváltásait. Első példánkban A és B mindketten támadni szándékozó lojális generálisok. A feltételezett eljárás kezdetén A és B ugyanazokat az üzeneteket küldik egymásnak és harmadik társuknak, mint amely üzenetek a hatszögben történt futás során elküldésre kerültek (egymás között, illetve a C és C' csúcsokhoz). Amennyiben az áruló tartja magát ezen szabályhoz és valamennyi válaszát a BC és AC' éleken történő adatokat másolva küldi, úgy A és B az eljárás során a hatszögben hozottal egyező döntésre jutnak; számukra a kétféle „valóság" között nincs különbség. Mivel az utóbbi esetben A és B egyaránt támadni akartak (és a feltételezett protokoll ezen egyetértést áruló jelenlétében is garantálja), mindketten a támadás mellett kellett, hogy döntsenek (a háromszögben és a hatszögben is).

Két másik szimulációt is felfedezhetünk ugyanezen hatszög esetén. Második példánkon B' és C' generálisok az előzőekhez hasonlóan jutnak „megnemtámadás" döntésre (az áruló előző esettel megegyező tényekedése mellett). Harmadik szimulációnk azonban ellentmondásra vezet: A és C' generálisok nem juthatnak megegyezésre, hiszen a protokoll futását követően döntésük a hatszögben hozottal megegyező lesz (rendre „támadás" és „megnemtámadás", mint azt előző példáinkban felfedeztük). Ezzel állításunkat igazoltuk.

A lehetetlenségi bizonyítás általános esete ügyes redukcióval igazolja, hogy ha létezne adott n-re $t \geq \frac{n}{3}$ feltétel mellett működő protokoll, azt megfelelően módosítva meg tudnánk oldani az előbb elemzett $n = 3$, $t = 1$ esetet is.

Habár a fentiek értelmében három résztvevő esetén a korábban elemzett többségi protokoll semmivel sem rosszabb bármely más megoldási kísérletnél, a résztvevők számát eggyel növelve képessé válunk „elbánni” a (feltételezetten egyetlen) árulóval. Az általános problémára $t < \frac{n}{3}$ feltétel mellett számtalan megoldás ismert, ezek részletes bemutatására nem térünk ki. Az algoritmuselmélet iránt érdeklődő olvasó elegáns, részletesen ismertetett megoldásokat találhat a következő webhelyen: `http://www.nada.kth.se/kurser/kth/2D5340/wwwbook/wwwbook.html`. Megjegyzendő, az ismert (jelen cikk szerzője által ismert) protokollok egyike sem törekszik az árulók leleplezésére és semlegesítésére, nem lehetetlen elképzelés azonban olyan eljárás tervezése, melyben a többek által helytelenül viselkedő résztvevő kiszavazhatóvá válik. Az árulók vadászata helyett a továbbiak azonban más, pacifista kihívások elé nézünk.

Hiányzó láncszemek

A klasszikus feladatban bármelyik generális bármelyik társának küldhetett üzenetet. A probléma természetes általánosításához jutunk ezen feltétel gyengítésével: a generálisok kapcsolati gráfja nem feltétlen teljes, egyes párok nem képesek (természeti akadály, távolság vagy a táborok között állomásozó ellenséges csapatok miatt) közvetlen kommunikációra, kapcsolatot csak más társak bevonásával tarthatnak. Megegyezést garantáló protokoll létezésének továbbra is szükséges feltétele az árulók számára vonatkozó $t < \frac{n}{3}$ felső korlát, elégségességről azonban általánosságban nem beszélhetünk. Amennyiben a generálisok kommunikációs gráfja fagráf, egyetlen, nem levélen elhelyezkedő áruló tönkretehet tetszőleges protokollt. Általánosságban elmondható, hogy ha az árulók elfoglalják a kommunikációs gráf valamely vágását, semmilyen protokoll sem garantálhat sikert. Egy adott hálózat által tolerált árulók maximális száma szükségképpen függ a gráf összefüggőségi számától is.

2. tétel [2]. *$G = (V, E)$ k-összefüggő kommunikációs gráf mellett pontosan akkor érhető el megegyezés t áruló esetén, ha:*

1. $t < \frac{n}{3}$ *és*
2. $t < \frac{k}{2}$.

Bizonyítás: $\Leftarrow$: *„teremtsünk éleket”.* Legyen P az eredeti feladatot $t < \frac{n}{3}$ feltétel mellett megoldó protokoll. Megoldásunkban felhasználjuk Menger-tételét:

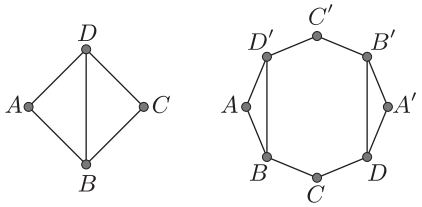
3. tétel [Menger]. *$G = (V, E)$ gráf k-összefüggő $\Leftrightarrow$ minden $s, t \in V$ párra léteznek $P_1, \ldots, P_k$ belül pontdiszjunkt $s - t$ utak.*

Rögzítsünk valamennyi össze nem kötött (s, t) párra $P_1^{(s,t)}, \ldots, P_1^{(s,t)}$ belül pontdiszjunkt utakat. Alkalmazzuk P protokollt és valahányszor s-ből t-be közvetlen információt kell küldenünk, küldjük el azokat $P_1^{(s,t)}, \ldots, P_1^{(s,t)}$ utak mindegyikén. A tétel második feltételében az utak többségén nincs áruló és ezáltal t a küldött üzenetet vissza tudja nyerni. Ezzel visszavezettük a feladatot annak korábban megoldott variánsára (a továbbítások ütemezése könnyű, jórészt technikai részfeladat, melyek részletes ismertetését mellőzzük).

A fordított irány igazolása történhet első tételünk bizonyításához hasonlatos módon.

2. lemma. *Négy generális esetén bármelyik közvetlen kommunikációs csatorna (él) törlésével a kapott gráf mellett nem létezik akár egyetlen árulót is toleráló protokoll.*

Lemmánk igazolásához a korábban látott hatszög helyett módosított nyolcszögön futtatjuk eljárásunkat, és a már látott szimulációs technikával juthatunk ellentmondásra. A részletek végiggondolását az olvasóra bízzuk.



3. ábra

Hiperélen táncolva

Az utóbbi évtizedben népszerűvé vált a feladat hipergráfokra átfogalmazott változatának vizsgálata. Adott $H = (V, E)$ kommunikációs hipergráf esetén egy hiperél bármely részvevője párhuzamosan oszthat meg információt az él többi tagjával. A hiperélre küldött adat mindenkihez egyazon pillanatban érkezik meg. Egyazon hiperélen egyetlen áruló sem képes eltérő biteket küldeni.

Hiperélek bevezetésével a hálózat által tolerált árulók száma megnő. A kapcsolódó általános eredmények ismertetése hosszas technikai bevezetést igényelne, melyek tartalmi okok miatt jelen cikkben nem vállalhatunk, figyelmünket ezért kizárólag 3-uniform hipergráfok felé fordítjuk. Egy hipergráfot h-uniformnak nevezünk, ha valamennyi éle h csúcsot tartalmaz; egy h-uniform hipergráf teljes, ha bármely $v_1, \ldots, v_h$ pontokra illeszkedik hiperél.

4. tétel [3]. *$H = (V, E)$ 3-uniform teljes hipergráfon t áruló jelenlétében pontosan akkor érhető el megegyezés, ha* $t \leq \frac{n-1}{2}$.

A tétel értelmében mindaddig, amíg a generálisok többsége hű a kitűzött célhoz és közülük bármely három összegyűlhet személyes (bár meglehetősen rövid, személyenként 1 bites) eszmecserére, a probléma megoldható. A közölt korlát mellett néhány speciális esetben [4] a fent megkövetelt teljességi feltétel nélkül is elérhető egyetértés. Három uniform hipergráfok esetén a kérdés lényegében – teljes hálózatok esetén teljesen – megoldottnak tekinthető. Korántsem ismert azonban, milyen szükséges és elégséges feltételek szabják meg az egyetértést garantáló protokollok létezését általános hipergráfok esetén. A hiperélekkel felfegyverkezett oszmán csapattestek tanácstalanul állnak az ostromlott város falai előtt és várják a fejleményeket...

Hivatkozások

[1] L. Lamport, R. Shostak, M. Pease, The Byzantine Generals Problem, *ACM Transaction on Programming Languages and Systems,* **4(3)** (July, 1982), 382–401.

[2] D. Dolev, The Byzantine Generals Strike Again, *Journal of Algorithms,* **3** (1982), 14–30.

[3] M. Fitzi, U. Maurer From Partial Consistency to Global Broadcast, *32nd ACM STOC* (2000), pages 494–503.

[4] D. V. S. Ravikant, V. Muthuramakrishnan, V. Srikanth, K. Srinathan, C. Pandu Rangan, *On Byzantine Agreement over* $(2, 3)$*-Uniform Hypergraphs,* Distributed Computing: 18th International Conference, DISC 2004.

Mészáros Gábor