

Kódolás hálózatokban

szakdolgozat

Kovács Erika Renáta
matematikus hallgató

Témavezető: *Frank András*, egyetemi tanár
Operációkutatási Tanszék
Eötvös Loránd Tudományegyetem
Természettudományi Kar

Budapest, 2007.

Köszönetnyilvánítás

Hálásan köszönöm témavezetőmnek, Frank Andrásnak a rengeteg segítséget, figyelmet, és hogy megkedveltette velem a kombinatorikus optimalizálást.

Köszönöm továbbá Király Zoltánnak az értékes észrevételeket és kérdésvetéseket.

Tartalomjegyzék

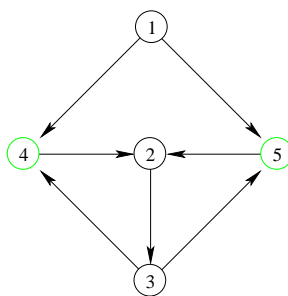
1. Bevezetés	1
1.1. Definíciók	4
2. Aciklikus irányított gráfok	7
2.1. Multicast hálózat	7
2.2. Több forrásos hálózat	13
2.2.1. Skalár lineáris kóddal megoldható problémák	13
2.2.2. Vektorlineáris kódok	15
3. Nem aciklikus irányított gráfok	24
3.1. Dinamikus lineáris kódok	26
3.1.1. Dinamikus folyamatok	26
3.1.2. Kódolási probléma dinamikus gráfja	32
3.2. Időinvariáns lineáris kódok	33
4. Kódolás és fenyőfelbontás	37

4.1. Edmonds fenyőfelbontási tétele	37
4.2. A tétel egy általánosítása	39
5. Független fenyők	45
5.1. Pontfüggetlen feszítő fenyők	45
5.1.1. Kétszeresen pontösszefüggő eset	45
5.1.2. Többszörösen összefüggő eset	47
5.2. Független Steiner fenyők	50
5.2.1. Élfüggetlen úrendszerek	50
5.2.2. Élfüggetlen Steiner fenyők	53
5.2.3. Él- és pontfüggetlenség kapcsolata	57
6. Összefoglalás, további kérdések	59

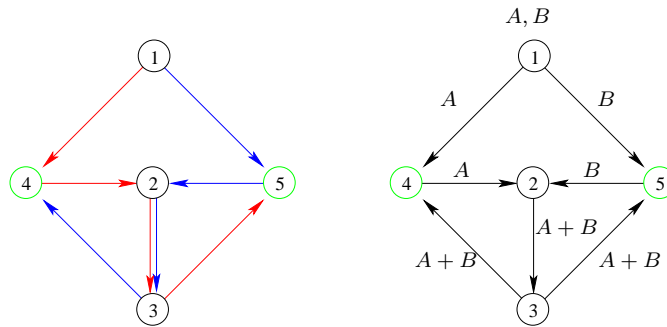
1. fejezet

Bevezetés

Egy s gyökerű $D = (V, A)$ irányított gráf valamely T terminálhalmazát feszítő s gyökerű fenyőt **Steiner fenyő**nek nevezünk. Mi a feltétele k éldiszjunkt Steiner fenyő létezésének? Ha speciálisan $T = V$, a Steiner fenyő feszítő fenyő, s ekkor Edmonds tétele szerint (4.1.) k élidegen feszítő fenyő létezésének szükséges és elégséges feltétele, hogy a gráf minden pontja elérhető legyen s -ből k élidegen úttal. Ez a feltétel szükséges kisebb terminálhalmaz esetén is, Lovász mutatott példát arra, hogy nem mindig elégséges (1.1 ábra). Jelen szakdolgozat az élidegen Steiner fenyők két általánosításával foglalkozik.



1.1. ábra. Lovász ellenpéldája ($T = \{v_4, v_5\}$)



1.2. ábra. Éldiszjunkt fenyők helyett élfüggetlen fenyők vagy lineáris kód

Az egyik a hálózati kódolás (**network coding**), mely napjainkban elméleti és gyakorlati szempontból is sokak által kutatott terület. Azt vizsgálja, milyen feltételek mellett juttathatók el üzenetek egy hálózatban kijelölt forrásokból bizonyos terminálokba oly módon, hogy üzenetküldéskor megengedjük az üzenetek összekódolását is. A módszer kihasználja, hogy az elküldeni kívánt üzenet nem csomag, hanem információ, melyet lehet többszörözni, és másokkal összekódolni. Természetesen, ha elegendő számú éldiszjunkt fenyő megy a források és terminálok között, a feladat kódolás nélkül, fenyőpakolásokkal is megoldható. Ilyen fenyők azonban nem mindig léteznek, amint azt az előbbi ellenpéldában is láttuk. A témában megjelent első jelentős cikk R. Ahlswede, N. Cai, S.-Y.R. Li, és R.W. Yeung munkája, melyben a multicast (egypontú forrás,- többpontú terminálhalmazzal rendelkező) hálózatok megoldhatóságára adnak szükséges és elégséges feltételt. Ők az úgynevezett α -kódokkal dolgoztak, melyek nagyon általánosak, és így igen bonyolultak is lehetnek. Később P. Sanders, S. Egner, és L. Tolhuizen megmutatták, hogy aciklikus gráf esetén a multicast feladatok az úgynevezett **lineáris kódolással** is megoldhatók. Az 1.2 ábra az előbbi ellenpéldán adódó kódolási feladat egy lineáris megoldását mutatja. Az a, b elküldendő információkat egy \mathbb{F} véges test elemeinek tekintjük, melyek összeadhatók. A terminálpontok azért kapják meg a a -t és b -t, mert a beérkező értékekből kiszámolhatók. A lineáris kódoknak több fajtája alkalmazható a hálózat típusától függően. Jelen szakdolgo-

zatban azt vizsgáljuk, a különféle lineáris kódokkal milyen kódolási problémák oldhatók meg.

Ha az éleknek kapacitása is van, a küldött üzenetek szétdarabolására van szükség. Ezt teszi lehetővé a **vektorlineáris kódolás**, mely a lineáris kódolás általánosítása. Azt sejtették, hogy aciklikus esetben minden megoldható probléma megoldható vektorlineáris kóddal is. Erre R. Dougherty, C. Freiling, és K. Zeger adtak ellenpéldát [5]. A 2. fejezetben először a lineáris majd a vektorlineáris kóddal megoldható aciklikus problémákat vesszük sorra, végül bemutatjuk az előbb említett ellenpéldát.

A 3. fejezet a nem aciklikus hálózatok kódolásával foglalkozik. Látni fogjuk, hogy az aciklikus esetben definiált lineáris kódolás nem alkalmazható nem aciklikus gráfokra, ott bonyolultabb kódolásra van szükség. Elsőként az aciklikus esetre visszavezethető **dinamikus lineáris kódokat** mutatjuk be. Ennek hátránya, hogy a kódolás időben változik, előnyösebb az úgynevezett **időinvariáns lineáris kódolás**, mely a fejezet második felében szerepel. Megmutatták, hogy ha egy tetszőleges gráfon adott multicast feladatnak létezik megoldása, időinvariáns lineáris kódolással is létezik, s ez polinomiális algoritmussal kiszámolható (E. Erez és M. Feder [9]).

A 4. fejezetben a hálózati kódolás kapcsolatát vizsgáljuk Edmonds fenyőfelbontási tételével. Két bizonyítást is adunk az utóbbi tételre, az első egy egyszerű, de kevésbé ismert, nem algoritmikus bizonyítás, a második a hálózati kódolás eszközeit használja, és egyúttal egy másik hálózati kódolásról szóló tételt is általánosít.

Az 5. fejezetben a Steiner fenyőket egy másik megközelítést mutatjuk be. Itt olyan fenyőket keresünk, melyek ugyan nem éldiszjunktak, de az általuk meghatározott st utak minden $t \in T$ -re azok. Az ilyen fenyőket **élfüggetlen fenyőknek** nevezzük. Hasonlóan lehet definiálni két fenyő **pontfüggetlenségét**. Az 1.2 ábra az ellenpélda gráfján mutat két élfüggetlen Steiner fenyőt. Király Zol-

tán vetette fel a kérdést: létezik-e mindig k élfüggetlen Steiner fenyő, ha minden terminálpontba vezet k élidegen st út? Ha az állítás igaz valamilyen k -ra, abból következne a pontfüggetlen feszítő fenyők létezése is. Ez utóbbira A. Huck mutatott ellenpéldát a $k \geq 3$ esetben [13], így a kérdésre csak $k = 2$ esetén lehet igen a válasz. Ebben az esetben sikerült belátni az állítást, felhasználva Whitty tételét a $k = 2$, $T = V$ pontfüggetlen esetről [12] (később derült ki, hogy ezt L. Georgiadis és R. E. Tarjan [15]-ban már bebizonyították). Szintén A. Huck látta be, hogy aciklikus gráfban már minden k -ra léteznek pontfüggetlen feszítő fenyők [14], így az élfüggetlen kérdés 2-nél nagyobb k -ra aciklikus gráfokon még lehetne igaz, ám erre sikerült ellenpéldát találnom (5.2 ábra).

1.1. Definíciók

Ebben a részben a hálózati kódolás alapvető fogalmait ismertetjük. Elsőként tekintünk a bevezetőben már említett α -kódot [1]. Ez a kód a multicast problémára ad egy nagyon általános megoldáshalmazt. Látni fogjuk, hogy a későbbiekben szereplő lineáris kódok mindegyike e kód speciális esete.

1.1. Definíció. Egy $G = (V, A)$ irányított gráf, s forrás- és $T = \{t_1, \dots, t_{|T|}\} \subseteq V$ terminálhalmaz valamint K pozitív egész esetén α -**kódnak** nevezzük egy

$$[\{u_i\}, \{v_i\}, \{f_i\}, \{A_i\}_{1 \leq i \leq K}, \{g_j\}_{1 \leq j \leq |T|}, n, k]$$

rendezett halmazt, ha

- 1) $u_i, v_i \in V$ úgy, hogy $(u_i, v_i) \in E$ minden $1 \leq i \leq K$ -ra.
- 2) $f_i : \Omega \rightarrow A_i$, ha $u_i = s$ és $f_i : \prod_{1 \leq j \leq i: v_j = u_i} A_j \rightarrow A_i$ egyébként, ahol $A_i = \{1, \dots, |A_i|\}$ és $\Omega = \{1, \dots, \lceil 2^{nk} \rceil\}$.

3) $g_l : \prod_{1 \leq j \leq l: v_j = t_l} A_j \rightarrow \Omega$ minden $t_l \in T$ -re úgy, hogy $\forall x \in \Omega g_l'(x) = x$, ahol g_l' a megfelelő f_1, \dots, f_K és g_l függvények kompozíciójából adódó $\Omega \rightarrow \Omega$ függvény.

Ekkor egy $x \in \Omega$ az összes elküldendő **üzenet**, az f_i -k a **kódoló függvények**, melyek által felvett értékek a kód során **küldött üzenetek**, k a kód **nagysága**, n az elküldendő k nagyságú kódok száma.

Az alfa kód tehát tulajdonképpen függvények véges sorozata, melyek mindegyike egy élhez tartozik, és egy függvény által küldött üzenet csak a hozzá tartozó él tövébe korábban beérkező üzenetektől függ. Vegyük észre, hogy nincs megkötés arra, hány függvényt rendelünk egy élhez, így speciálisan $k = 1$, vagyis $\Omega = (x_1, \dots, x_n)$, $x_i \in \{0, 1\}$ $1 \leq i \leq n$ és $A_i = \{0, 1\}$ esetén az is megoldás, ha minden t terminálhoz tekintünk egy s -ből odavezető d_t hosszú utat, ezeket egymás után vesszük, rajtuk pedig élről élre haladunk (ez $d = \sum_{t \in T} d_t$ függvény), s ezt n -szer ismételjük: $f_{(j-1)d+i}(x) = x_j \forall x \in \Omega, 1 \leq i \leq d$, ha $u_i = s$, és $f_{(j-1)d+i} = f_{(j-1)d+i-1}$ egyébként. Ekkor, ha egy e él m_e úton szerepel, azt nm_e -szer használja a kód. Tegyük fel, hogy egy f_i végrehajtása valamint egy x_i s -be juttatása egyaránt Δ időbe telik. Ekkor a kód végrehajtása legalább $nm_e \Delta$ időt vesz igénybe, miközben egy $x \in \Omega$ $n \Delta$ idő alatt jut s -be, azaz n növekedtével x egyre nagyobb késéssel jut el a terminálokba. Az ilyen kódokat szeretnénk kizárni, és csak olyanokat megengedni, melyek lényegében $nc(e)$ -szer használnak minden élt, ahol $c(e) \in \mathbb{R}^+$ az él kapacitása (az előbbi példában $c = 1$).

1.2. Definíció. Legyen $\eta : E \rightarrow \mathbb{N}$, melyre $\eta(e) = \prod_{1 \leq i \leq K: (u_i, v_i) = e} A_i$, c pedig $E \rightarrow \mathbb{R}$ kapacitásfüggvény. Egy α -kód α -**megengedhető** (c, G, k') -re, ahol $k' \in \mathbb{R}^+$, ha minden $\epsilon > 0$ -ra elég nagy n -re létezik α -kód, melynek nagysága k' és $n^{-1} \log_2 \eta(e) \leq c(e) + \epsilon$.

Ahlswede és szerzőtársai bizonyították be a következő tételt, mely a hálózati kódolás alap eredménye [1].

1.3. Tétel. (R. Ahlswede, N. Cai, S.-Y.R. Li és R.W. Yeung) *Egy gráfon adott (c, G, k') α -megengedhető $\Leftrightarrow \lambda_c(s, t) \geq k \forall t \in T$.*

Jelen szakdolgozatban belátjuk, hogy a fenti tétel már a kódok egy sokkal szűkebb osztályán, az időinvariáns lineáris kódok körében is igaz, sőt, aciklikus gráfok esetén még egyszerűbb kód is elég. A c függvényről kezdetben feltesszük, hogy egészértékű, majd a racionális esetet vektorlineáris kódok segítségével vezetjük vissza az egész esetre (a valós eset könnyen láthatóan következik a racionálisból).

2. fejezet

Aciklikus irányított gráfok

2.1. Multicast hálózat

2.1. Definíció. *Multicast kódolási feladatnak nevezünk egy $C = (D, s, T, k)$ halmazt, ahol $D = (V, A)$ irányított gráf, $s \in V$ forrás, $T \subseteq V$ terminálhalmaz, k pedig pozitív egész, az elküldeni kívánt üzenet nagysága. Ha a megadott D gráf aciklikus, a multicast feladatot **aciklikusnak** nevezzük.*

2.2. Definíció. *Egy $D = (V, A)$ aciklikus gráf, s forrás és \mathbb{F} véges test és d pozitív egész esetén **lineáris kódnak** nevezünk egy $f : A \rightarrow \mathbb{F}^d$ leképezést, ha s -en kívül minden csúcstra a kimenő élekhez rendelt vektorok előállnak az él tövébe menők lineáris kombinációjaként, azaz*

$$\forall v \in V \setminus s - re \langle f(vv') | vv' \in A \rangle \subseteq \langle f(v''v) | v''v \in A \rangle.$$

Egy f lineáris kód és (x_1, x_2, \dots, x_k) üzenetek esetén valamely e élen küldött üzenetet az $(x_1, x_2, \dots, x_k) \cdot f$ skalárszorozattal kapjuk meg. A fenti definícióban az s -ből kijövő élekre nem kellett kikötést tenni, mert valódi üzenetküldéskor

s rendelkezik minden elküldendő üzenettel, így a vektortér bármely vektorát elküldheti. Annak érdekében, hogy ez a lineáris kódban is megjelenjen, bevezetünk egy új forrást, melyből s az üzeneteket kapja (annyi élen, ahány üzenet van).

2.3. Definíció. Egy multicast kódolási feladat **bővített gráfja** egy $D' = (V + s', A')$ gráf, melyet D -ből úgy kapunk, hogy s -be egy új s' csúcsból k darab $(s's)_1, \dots, (s's)_k$ élt irányítunk.

2.4. Megjegyzés. Ha D -ben $\lambda(s, t) \geq k$, akkor D' -ben $\lambda(s', t) \geq k$.

Egy lineáris kód természetesen még nem feltétlenül α -kód, csak egy megvalósítható üzenetküldés, hiszen nem feltétlenül juttatja el az üzeneteket a terminálokba. Ahhoz, hogy egy lineáris kód ezt megtegye, egyrészt kell, hogy az elküldendő üzenetek megjelenjenek a gráfban (az $(s's)_i$ éleken egy-egy), illetve, hogy ezek mind meg is érkezenek a terminálokba, vagyis az egyes terminálokba menő élek vektorai kifeszítsék a teljes k dimenziós vektorteret.

2.5. Definíció. (2.1 ábra) Egy aciklikus multicast kódolási feladat bővített gráfján értelmezett lineáris kódról azt mondjuk, **lineáris megoldása** a feladatnak, ha

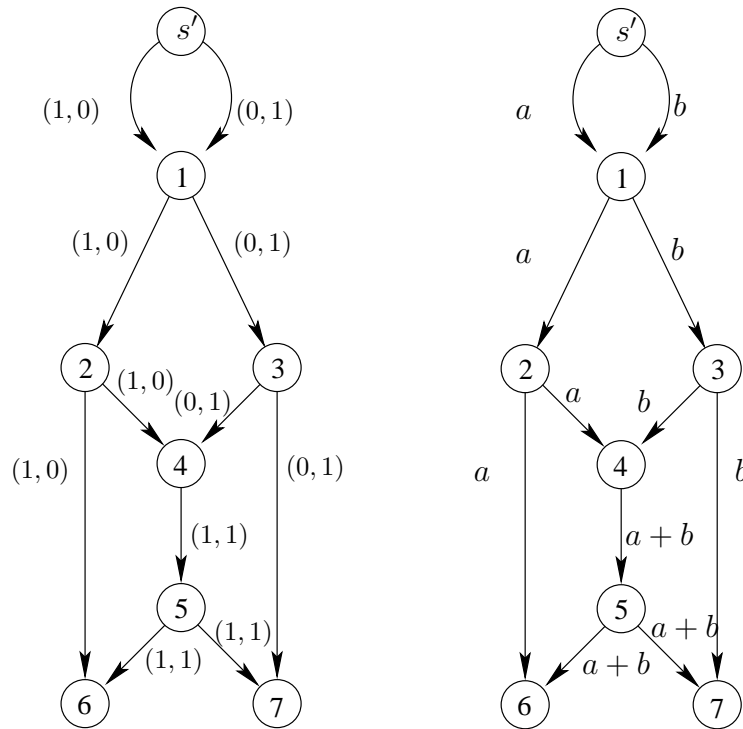
$$(i) \quad d = k$$

$$(ii) \quad f((s's)_i) = e_i, 1 \leq i \leq k, \text{ ahol } e_i \text{ az } \mathbb{F}^k \text{ } i\text{-edik egységvektora}$$

$$(iii) \quad \forall t \in T \dim \langle f(ut) | ut \in A \rangle = k$$

2.6. Megjegyzés. A 2.1 ábrán látható lineáris kód az $s = v_1, T = \{v_6, v_7\}, k = 2$ paraméterű aciklikus kódolási feladat megoldása, így az $f(e)e \in A$ vektorok \mathbb{F}^2 -beliek (\mathbb{F} tetszőleges véges test lehet).

2.7. Megjegyzés. Vegyük észre, hogy egy lineáris megoldás valamely élen felvett értékét $a \in \mathbb{F}$ -fel megszorozva továbbra is lineáris megoldást kapunk, így például feltehető, hogy az egy befokú csúcsok nem kódolnak, azaz f a kimenő éleken a bejövő értékével egyezik meg. Ezt a későbbiekben több bizonyításnál fogjuk használni.

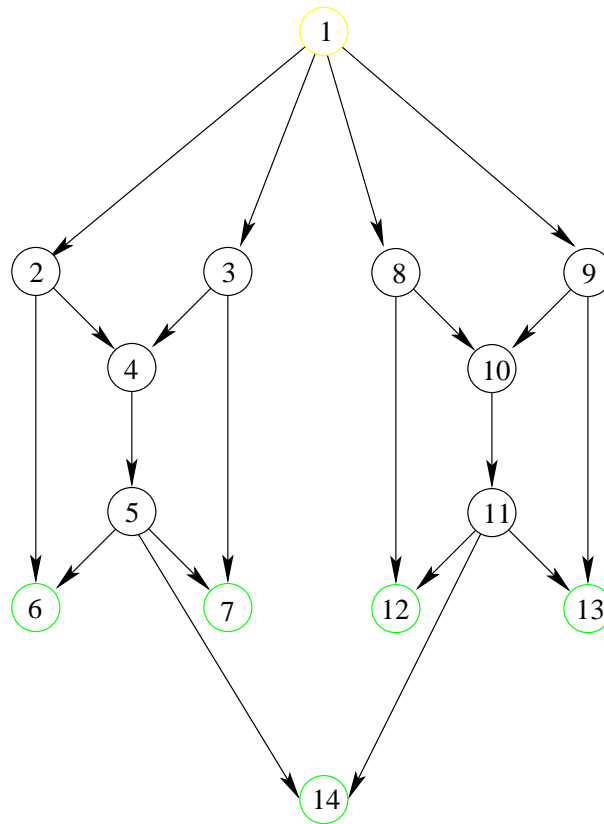


2.1. ábra. Aciklikus (bővített) gráf éleihez rendelt vektorok és a küldött üzenetek a bővített gráfban

2.8. Definíció. Egy aciklikus gráf pontjainak egy $v_1, v_2, \dots, v_{|V|}$ sorrendje **topologikus sorrend**, ha minden csúcs őse a csúcs előtt szerepel. Hasonlóan definiálható az **élek topologikus sorrendje**: $e_1, \dots, e_{|E|}$ sorrend ilyen, ha minden él tövébe menő él előtte szerepel.

2.9. Megjegyzés. A lineáris kód az Ahslwede és szerzőtársai [1] által definiált kódnak is megfelel, hiszen az éleket topologikus sorrendben véve látható, hogy az élfüggvények csak a sorrendben korábbi élektől függenek.

A 2.1 ábra egy kételemű test feletti megoldást mutat be. Ilyen azonban nem mindig létezik. A 2.2 ábrán látható gráfnak például könnyen ellenőrizhetően



2.2. ábra. Példa olyan hálózatra, melyen nincs lineáris megoldás a kételemű test felett (a zöld csúcsok a terminálok, $k=2$)

nincs lineáris megoldása a kételemű test felett, ugyanis a v_4v_5 ill. $v_{10}v_{11}$ élekhez egyaránt csak az $(1, 1)$ vektor tartozhat, különben a $\{v_6, v_7\}$ ill. $\{v_{12}, v_{13}\}$ terminálokba menő élek nem feszítenék ki a kétdimenziós teret. Így viszont v_{14} -be nem megy két különböző vektor. A megoldáshoz szükséges legkisebb test meghatározása NP-teljes[3]. Látni fogjuk, hogy megoldható problémánál az $\mathbb{F} \geq |T|$ feltétel multicast esetben mindig elegendő (2.11. tétel).

2.10. Definíció. Rögzített s, T esetén D **kapacitása** az a maximális χ nemnegatív szám, amelyre létezik $C = (G, s, T, \chi)$ -nek lineáris megoldása.

Nyilván $\chi \leq \min\{\lambda(s, t) \mid t \in T\}$. A P. Sanders, S. Egner, és L. Tolhuizen algoritmikus bizonyítást ad az egyenlőségre [2].

2.11. Tétel. (Sanders és szerzőtársai) *Ha egy aciklikus multicast kódolási feladatban $\lambda(s, t) \geq k \forall t \in T$, $|F| \geq |T|$ akkor a feladatnak létezik lineáris megoldása az F test felett, mely polinomiális időben megtalálható, azaz $\chi \geq k$.*

BIZONYÍTÁS. Az egyes élekhez rendelt vektorokat az élek egy topologikus sorrendjében fogjuk megadni. Egy élre tehát egyszer kerül sor, csak miután tövének minden bemenő éléhez rendeltünk már vektort. Rögzítsünk minden t terminálhoz k éldiszjunkt st utat, jelölje ezek halmazát p_t . Az algoritmus során csak ezen utak éleihez rendelünk vektort, a többi élt elhagyhatjuk, hozzájuk a nulla vektort rendeljük. A topologikus sorrend miatt az algoritmus az egyes utakon is sorrendben halad, azaz amikor egy élhez vektort rendelünk, az úton minden azt megelőző él sorra került már korábban. A legutoljára vett éleket minden terminál minden útján számon tartjuk az algoritmus végéig, egy t terminálra jelölje ezen k él halmazát U_t . Arra ügyelünk, hogy minden lépésben az egyes terminálokhoz tartozó U_t élek vektorai a teljes teret kifestsék. Itt jön elő a kibővített gráf szerepe, így ugyanis minden egyes terminálba menő k út az $(s's)_i$ élekkel kezdődik, melyeken a k egységvektor valóban kifesti az egész teret, kezdetben tehát teljesül a feltétel. Az algoritmus befejeződésével az U_t -k terminálokba menő élekből fognak állni, ami garantálja a (iii) feltétel teljesülését. Tegyük fel, hogy az algoritmusban xy a soron következő él. Jelölje T_{xy} azon terminálok halmazát, melyek p_t halmaza tartalmazza xy -t, $p_t(xy)$ pedig jelölje az xy -t megelőző élt a p_t -beli úton. Az $f(xy)$ vektort úgy kell megválasztani, hogy egyrészt előálljon a $\{p_t(xy) \mid t \in T_{xy}\}$ élek vektorainak lineáris kombinációjaként, másrészt az $U_t \setminus p_t(xy) \cup xy$ élhalmazok vektorai továbbra is k dimenziós teret festszenek. Egy U_t halmaz módosításánál azt kell ellenőrizni, hogy az új él vektora nincs-e benne a régi $k - 1$ él vektorainak alterében. Ezt az alábbi lemma alapján gyorsan el lehet dönteni egy ellenőrző vektor segítségével.

2.12. Lemma. *Legyen B az \mathbb{F}^k egy bázisa, b a bázis eleme, a pedig \mathbb{F}^k -beli vektor, melyre $a \cdot b' = \delta_{b,b'} \forall b' \in B$. Ekkor egy x vektor pontosan akkor van benne a*

$B \setminus b$ vektorok alterében, ha $x \cdot a = 0$.

BIZONYÍTÁS. Nyilvánvaló. \square

A fenti a vektor a B bázis b -hez tartozó **ellenőrző vektora**. Az algoritmus során az U_t halmazok mellett egy-egy $A_t = \{a_t(e) \in \mathbb{F}^k \mid e \in U_t\}$ ellenőrző halmazt is számon fogunk tartani, melyben $a_t(e)$ az $U_t \setminus e$ élek vektoraihoz tartozó ellenőrző vektor. Kezdetben az egységvektorok ellenőrző vektorai önmaguk. Általában, egy xy él $p_t(xy)$ -nal történő cseréje esetén, ha $f(xy) = \sum_{u_i \in U_t} m_i f(u_i)$, $m_i \in \mathbb{F}$ alakban áll elő, az A_t halmaz könnyen ellenőrizhetően az alábbiak szerint módosul: $a_t(xy) = m_{xy}^{-1} a_t(p_t(xy))$, míg $e \neq xy$ -ra $a'_t(e) = a_t(e) - (a_t(e) \cdot f(xy)) a_t(p_t(xy))$.

Ezekkel a jelölésekkel tehát az $\{f(u_i) \mid u_i \in U_t\}$ vektorhoz olyan m_i együttműködőket keresünk, melyekre $f(xy) = \sum_{u_i \in U_t} m_i f(u_i)$ vektorra $f(xy) \cdot a_t(u_i) \neq 0$ egyik i -re sem.

Ilyen együttműködők létezését bizonyítja az következő lemma.

2.13. Lemma. *Az $x_i, y_i \in \mathbb{F}^k$ -beli vektorokra $|\mathbb{F}| \geq k$ és $x_i \cdot y_i \neq 0$ minden $1 \leq i \leq k$ -ra. Ekkor létezik az x_i vektoroknak egy u lineáris kombinációja, melyre $u \cdot y_i \neq 0, 1 \leq i \leq k$.*

BIZONYÍTÁS. Az állítást k szerinti indukcióval bizonyítjuk. $k = 1$ -re az állítás nyilvánvaló. Tegyük fel, hogy $k - 1$ -re igaz az állítás, azaz létezik az x_1, \dots, x_{k-1} vektoroknak egy u_{k-1} lineáris kombinációja, melyre $u_{k-1} \cdot y_i \neq 0, 1 \leq i \leq k - 1$. Ha $u_{k-1} \cdot y_k \neq 0$, az állítás k -ra is igaz. Ha $u_{k-1} \cdot y_k = 0$, bármely $m \in \mathbb{F} \setminus 0$ elemre $(u_{k-1} + mx_k) \cdot y_k \neq 0$. $u_k = u_{k-1} + mx_k$ csak akkor nem jó, ha $u_k \cdot y_i = 0$ valamely $1 \leq i \leq k - 1$ -re. Egy ilyen egyenletnek egyetlen \mathbb{F} -beli megoldása van, így összesen legfeljebb $k - 1$ együttműködő esik ki. Azonban $|\mathbb{F}| \geq k$, így létezik jó m együttműködő. Az állítás tehát igaz. \square

Ezzel beláttuk, hogy folytatható az algoritmus, s ez polinom időben kiszámolható. (Az algoritmus futási ideje $O(|E| \cdot |T| \cdot k \cdot (k + |T|))$.) \square

2.14. Megjegyzés. Vegyük észre, hogy tulajdonképpen azt láttuk be, hogy ha egy megkezdett lineáris kódnál minden terminálhoz tudunk mutatni k utat, melyek utolsó kódolt éleinek vektorai függetlenek, akkor a kód befejezhető (a megkezdett kódon olyan lineáris kódot értünk, mely az élek valamely topologikus sorrendjét tekintve egy élig értelmezett). Ezt a megjegyzést a többpontú forráshalmaz eseténél fogjuk használni.

2.2. Több forrásos hálózat

2.2.1. Skalár lineáris kóddal megoldható problémák

A fentiekben a multicast kódolási feladat megoldásával foglalkoztunk, vagyis amikor egyetlen forrás van, de több terminál, melyek ugyanazt az üzenetet kérik. Ennél általánosabb probléma, amikor forrásból is lehet több, s az egyes forrás- és terminálpontokhoz tartozó üzenetek is eltérhetnek. Látni fogjuk, hogy a feladat több alete is visszavezethető a multicast problémára.

2.15. Definíció. *Általános kódolási feladatnak* hívunk egy $C = (D, S, T, M, g)$ halmazt, ahol $D = (V, A)$ irányított gráf, $S \subseteq V$ forráshalmaz, $T \subseteq V$ terminálhalmaz, $M = (m_1, \dots, m_k)$ az üzenetek halmaza, g pedig egy igényfüggvény, mely az egyes forrásokból elérhető illetve az egyes terminálokba elküldendő üzeneteket adja meg, vagyis M részhalmazait S -hez illetve T -hez rendelő leképezés. A multicast esethez hasonlóan, ha a megadott D gráf aciklikus, a kódolási feladatot **aciklikusnak** nevezzük.

2.16. Megjegyzés. A multicast esetben $S = s$ egyetlen pontból állt, melyre $g(s) = g(t) = M$ minden t terminálra.

A multicast esethez hasonlóan lehet értelmezni a lineáris kódot, csak itt egy forrás helyett több is lehet.

2.17. Definíció. Egy kódolási feladat **bővített gráfja** egy $D' = (V + M', A')$ gráf, melyben egy új m'_i csúcsból akkor megy él s_j -be, ha $m_i \in g(s_j) \forall 1 \leq i \leq k, 1 \leq j \leq |S|$.

2.18. Definíció. Egy aciklikus kódolási feladat bővített gráján értelmezett lineáris kód **lineáris megoldása** a feladatnak, ha

$$(i) \quad d = k$$

$$(ii) \quad f(m_i s_j) = e_i, 1 \leq i \leq k, \text{ ahol } e_i \text{ az } \mathbb{F}^k \text{ } i\text{-edik egységvektora és } m_i \in g(s_j)$$

$$(iii) \quad \forall t \in T \dim \langle f(ut) | ut \in A \rangle = k$$

Az általános probléma néhány alapesetének klasszifikációját A.R. Lehman és E. Lehman végezte [3]-ben. Megmutatták, hogy a multicast feladat mellett szintén polinom időben megoldható a terminálokon egyforma igényfüggvényű ($g(t) = M \forall t \in T$) feladat, tetszőleges forráshalmaz és $g(S)$ esetén.

2.19. Tétel. (A.R. Lehman és E. Lehman) Egy $C = (D, S, T, M, g)$ aciklikus kódolási feladat $g \equiv M$ esetén polinomiális.

BIZONYÍTÁS. A gráf bővített grájához vegyünk fel egy új s' forrásponot, és vezessünk belőle egy-egy élt minden $m'_i, 1 \leq i \leq k$ csúcsba. Tekintsük ezen a gráfon azt a multicast problémát, melyben $S = s', g(s') = M$. Könnyen látható, hogy a két problémának egyszerre van megoldása: egyrészt nyilvánvaló, hogy az eredeti probléma egy lineáris megoldása kiegészíthető az új egy megoldásával (legyen $f(s' m_i) = e_i$). Másrészt, ha az új, multicast probléma megoldható, azaz $\lambda(s', t) \geq k \forall t \in T$, a 2.14. megjegyzés szerint megoldható úgy is, hogy $f(s' m_i) = e_i, f(m_i s_j) = e_i, 1 \leq i \leq k, m_i \in g(s_j)$, hiszen minden terminálra az utolsó kódolt k él éppen e_1, \dots, e_k , vagyis lineárisan független. Tehát a kérdés eldöntése a multicast esethez hasonlóan polinomiális. \square

2.2.2. Vektorlineáris kódok

[3]-ben megmutatták, hogy ha nem ugyanaz a terminálok igényfüggvénye, már nem feltétlenül adható polinomiális algoritmus, sőt még lineáris megoldás sem mindig létezik. Számos ilyen probléma megoldható ún. vektorlineáris kóddal, amely a lineáris kód fogalmát általánosítja. Ez a kód annyiban tér el az eredeti (skalár) lineáris kódtól, hogy az éleken küldött üzeneteket egy véges test feletti véges dimenziós vektortér elemeinek tekintjük. Alkalmazása azért indokolt, mert a gyakorlatban az éleken küldött üzenetek általában adott hosszúságú $0-1$ sorozatok, melyeket a skalár lineáris kód egyetlen számként kezel. A vektorlineáris ezzel szemben külön-külön tekinti őket, növelve ezzel a lehetőségek számát. Tegyük fel, hogy az elküldendő x_1, x_2, \dots, x_k üzenetek \mathbb{F}^r véges test elemei (például a fent említett r hosszú $0-1$ sorozatok). Ekkor úgy is tekinthetünk rájuk, mint rk darab \mathbb{F} -beli üzenetre r kapacitású éleken.

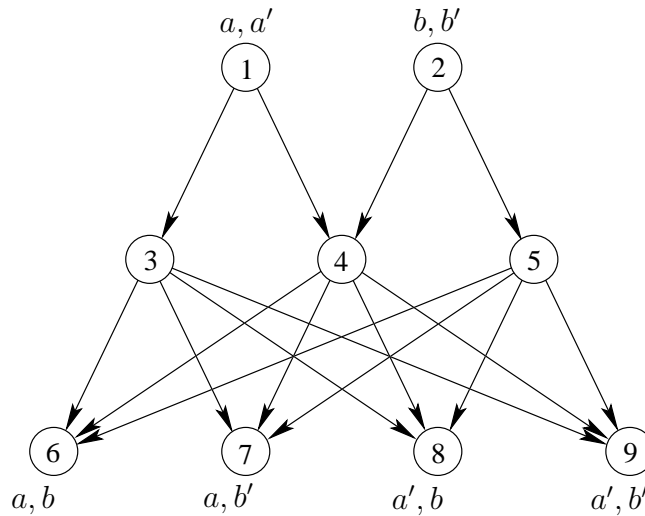
2.20. Definíció. Egy $D = (V, A)$ aciklikus gráf, S forráshalmaz, k, r pozitív egészek és \mathbb{F} véges test esetén **vektorlineáris kódnak** nevezünk egy $m : A \rightarrow \mathbb{F}^{kr \times r}$ leképezést, ha $\forall v \in V \setminus S$ -re $m(vv') = \sum_{u_i v \in A} m(u_i v) M_i$, ahol $M_i \in \mathbb{F}^{r \times r}$

2.21. Megjegyzés. Az r adja meg, hogy az eredeti x_1, x_2, \dots, x_k üzeneteket hány kisebb részre bontjuk, az eredeti lineáris kód az $r = 1$ speciális esetnek felel meg. Az éleken küldött üzeneteket most az $(x_{1,1} \dots x_{1,r}, x_{2,1}, \dots, x_{k,r}) \cdot m$ skalárszorzat adja meg, ahol $x_{i,j}$ az x_i elküldendő üzenet j -edik darabja $1 \leq j \leq r$.

Az alábbi, [4]-ből vett gráf R. Koettertől származik, s példa olyan aciklikus gráfra, mely nem oldható meg skalár lineáris kóddal, de létezik vektorlineáris megoldása.

2.22. Állítás. A 2.3 ábrán látható gráfban nem létezik (skalár) lineáris megoldása a megadott kódolási feladatnak.

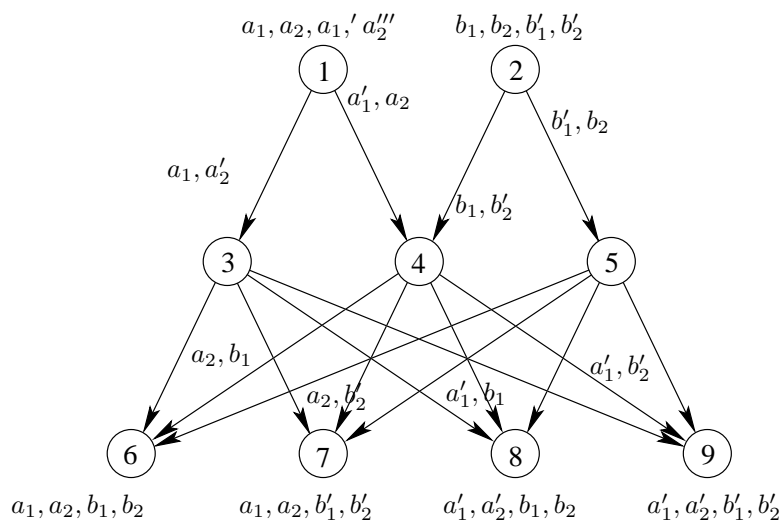
BIZONYÍTÁS. (Az alábbi indoklás kissé eltér a [4]-belitől.) Tegyük fel, hogy létezik $f : E \rightarrow \mathbb{F}^4$ lineáris megoldás. A 2.7. megjegyzés szerint feltehető, hogy f a



2.3. ábra. Példa skalár lineáris kóddal nem megoldható feladatra

v_3 -ból ill. v_5 -ből induló éleken megegyezik az v_1v_3 ill. v_2v_5 éleken felvett értékkel, a terminálokba érkező három él közül tehát kettő mindenhol azonos értéket vesz fel. Ha bennük az A, A', B, B' üzenetek együtthatói közül egy sem nulla, és a terminálok valóban ki tudják számolni a kívánt értékeket, akkor egyúttal a másik két érték is kiszámolható lenne. Azonban csak három egyenlet áll rendelkezésre a négy ismeretlen meghatározásához, ez tehát nem lehetséges, így valamelyik együttható nulla. Feltehető, hogy $f(v_1v_3) = (1, 0, 0, 0)$, azaz a küldött üzenet A . Ekkor a v_8 -as terminál ismeri A -t és A' -t, így az előző indokláshoz hasonlóan nem ismerheti B' -t, ami csak úgy lehet, ha $f(v_2v_5) = (0, 0, 1, 0)$. Ám ugyanezt a gondolatmenetet a v_9 -es terminárra megismételve $f(v_2v_5) = (0, 0, 0, 1)$ adódik, ami lehetetlen. \square

Az alábbi ábrán látható, hogyan oldható meg az előző feladat vektorlineáris kóddal $r = 2$ választással. Vegyük észre, hogy valójában igazi kódolás nem történik, csak egy egész helyett két "fél üzenetet" visz egy-egy él. Ebből látszik, hogy a vektorlineáris kód további előnye, hogy az üzeneteket szét lehet darabolni. Így



2.4. ábra. Megoldás vektorlineáris kóddal

akár tört kapacitású éleken is értelmezhető a kódolási probléma.

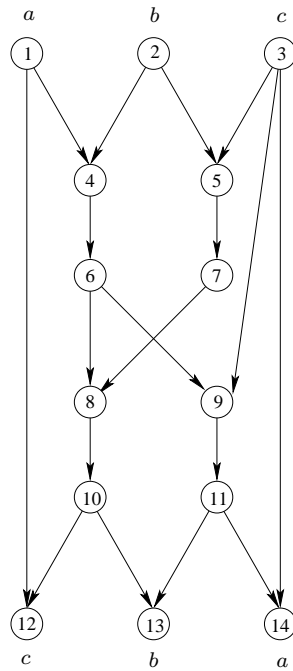
2.23. Definíció. Egy $D = (V, A)$ irányított gráfon adott egy $c : A \rightarrow \mathbb{Q}^+$ kapacitásfüggvény. Legyen l az élkapacitások nevezőinek egy többszöröse. Vegyünk minden $e \in A$ élt $c(e) \cdot l$ -szer, a kapott gráf legyen D_l . Egy D_l -en értelmezett vektorlineáris kód megoldása az eredeti gráfon adott $C = (D, s, T, k)$ feladatnak, ha megoldása D_l -en a $C' = (D, s, T, k \cdot l)$ feladatnak.

Könnyen láthatóan igaz az egész kapacitásoknál bizonyított tétel:

2.24. Tétel. Racionális kapacitású irányított gráfon pontosan akkor létezik egy kódolási problémának vektorlineáris megoldása, ha $\lambda(s, t) \geq k \forall t \in T$.

Médard és szerzőtársai [4]-ben azt a sejtették, hogy vektorlineáris kóddal már minden aciklikus probléma megoldható. A sejtést R. Dougherty, C. Freiling, és K. Zeger cáfolta meg [5]-ban.

2.25. Lemma. Az 2.5 ábrán látható kódolási feladatnak semmilyen dimenzióra sem létezik vektorlineáris megoldása páratlan elemszámú test felett.

2.5. ábra. Az N_1 hálózat

BIZONYÍTÁS (R. DOUGHERTY ÉS SZERZŐTÁRSAI). Indirekten tegyük fel, hogy N_1 -nek mégis létezik m megoldása valamilyen $GF(q)$ páratlan elemszámú test és k dimenzió mellett. Az refmj:ebefkod megjegyzés alapján feltehető, hogy m a v_1, v_2, v_3 -ból induló éleken csupa egy Jelölje I a $k \times k$ -s $GF(q)$ feletti egységmátrixot, $e_{i,j}$ pedig a $v_i v_j$ élen küldött üzenetvektort (azaz $e_{i,j} = m(v_i v_j \cdot (a, b, c))$). Ekkor léteznek olyan m_1, \dots, m_{14} $k \times k$ -s mátrixok, melyekre a következő egyenlőségek teljesülnek:

$$e_{4,6} = M_1 a + M_2 b$$

$$e_{5,7} = M_3 b + M_4 c$$

$$e_{8,10} = M_5 e_{4,6} + M_6 e_{5,7}$$

$$e_{9,11} = M_7 e_{4,6} + M_8 c$$

(1) $c = M_9a + m_{10}e_{8,10}$

(2) $b = M_{11}e_{8,10} + m_{12}e_{9,11}$

(3) $a = M_{113}e_{9,11} + m_{14}e_{5,7}$

Belátjuk, hogy minden M_i mátrix invertálható. Az utolsó három egyenletben az M_i -k együtthatóiba a korábbi egyenleteket helyettesítve kapjuk:

(4) $M_9 +_{10} M_5M_1 = 0$

(5) $M_{10}(M_5M_2 + M_6M_3) = 0$

(6) $M_{10}M_6M_4 = I$

(7) $M_{11}M_5M_1 + M_{12}M_7M_1 = 0$

(8) $M_{11}M_5M_2 + M_{11}M_6M_3 + M_{12}M_7M_2 = I$

(9) $M_{11}M_6M_4 + M_{12}M_8 = 0$

(10) $M_{13}M_7M_1 = I$

(11) $M_{13}M_7M_2 + M_{14}M_3 = 0$

(12) $M_{13}M_8 + M_{14}M_4 = 0$.

A (6)-os és (10)-es egyenletek miatt $M_1, M_4, M_6, M_7, M_{10}, M_{13}$ invertálható, ezért (5) miatt $M_5M_2 + M_6M_3 = 0$, s így (8)-ből

(13) $M_{12}M_7M_2 = I$ adódik, tehát M_2 és M_{12} is invertálható.

(7) miatt $M_{11}M_5 = -M_{12}M_7$, így M_5 és M_{11} is az. Hasonlóan (11)-ből kapjuk, hogy $M_{14}M_3 = -M_{13}M_7M_2$, amiből M_3 és m_{14} invertálhatósága következik. Mivel (4) miatt $M_9 = -M_{10}M_5M_1$, M_9 is invertálható, s végül (12)-ből $M_8 = -M_{13}^{-1}M_{14}M_4$ következik, ami M_8 invertálhatóságát igazolja.

Innen (7)-ből

$$0 = M_{11}M_5 + M_{12}M_7 = M_{11}M_5 + (M_{12}M_7M_2)M_2^{-1} = M_{11}M_5 + M_2^{-1},$$

vagyis $-I = M_{11}M_5M_2$.

Másrészt (9) miatt

$$\begin{aligned} 0 &= M_{11}M_6M_4 + M_{12}M_8 = M_{11}(M_6M_3)M_3^{-1}M_4 - M_{12}M_{13}^{-1}M_{14}M_4 = \\ &= (-M_{11}M_5M_2 + I)M_3^{-1}M_4, \end{aligned}$$

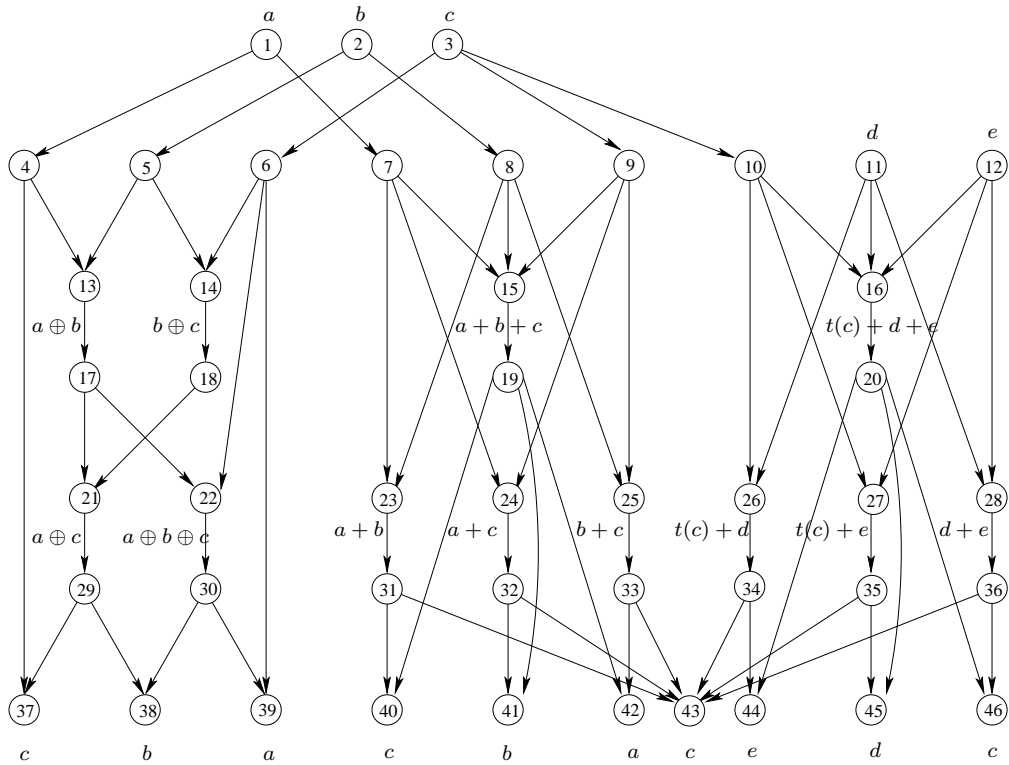
amiből $I = M_{11}M_5M_2$ adódik, amiből $I = -I$ következne, de ez ellentmondás. \square

2.26. Tétel. *Létezik (nemlineáris kóddal) megoldható kódolási feladat, melynek nem létezik vektorlineáris megoldása.*

BIZONYÍTÁS. Tekintsük a 2.6 ábrán látható kódolási feladatot. Először belátjuk, hogy megoldható 4 elemű ábécé felett. Feleltessük meg az ábécé betűit Z_4 ill. $Z_2 \times Z_2$ gyűrűkkel oly módon, hogy a mod 4 maradékosztályok a kettes számrendszerbeli megfelelőjükkel legyenek párban. A kódolás során 4-féle műveletet fogunk használni: a $+/-$ jelek az összeadást ill. szorzást jelentik a modulo Z_4 felett, \times az összeadást jelöli a $Z_2 \times Z_2$ -ben, végül $t(x)$ az x fordítottját jelöli szintén $Z_2 \times Z_2$ -ben. A v_{43} -as terminál kivételével könnyen látható az üzenetek megérkezése. Tekintsük v_{43} -t.

2.27. Állítás. $c = t(e_{32,43} + e_{33,43} - e_{31,43}) + (e_{34,43} + e_{35,43} - e_{36,43})$

BIZONYÍTÁS. $t(e_{32,43} + e_{33,43} - e_{31,43}) + (e_{34,43} + e_{35,43} - e_{36,43}) = t((a + c) + (b + c) - (a + b)) + (t(c) + d) + (t(c) + d) - (d + e) = t(2c) + 2t(c)$ ($2c$ a Z_4 -beli szorzást jelöli). Legyen c kettes számrendszerbeli alakja (x, y) . Ekkor $2c = (y, 0)$, $t(c) = (y, x)$, $t(2c) = (0, y)$, $(2t(c)) = (x, 0)$, tehát $t(2c) + 2t(c) = c$ valóban teljesül. \square



2.6. ábra. Az N_2 hálózat és egy nemlineáris megoldás

Most megmutatjuk, hogy nem létezik N_2 -n vektorlineáris megoldás. A bizonyítás az előző lemmájéhoz hasonlóan történik. Tegyük fel, hogy mégis létezik ilyen valamilyen $GF(q)$ felett k dimenzióra. Mivel N_2 tartalmazza N_1 -et, az előző lemma miatt q csak páros lehet. Ekkor léteznének M_1, \dots, M_{15} $k \times k$ -s $GF(q)$ feletti mátrixok, melyekre

- (1) $e_{23,31} = M_1 a + M_2 b$
- (2) $e_{24,32} = M_3 a + M_4 c$
- (3) $e_{25,33} = M_5 b + M_6 c$

$$(4) e_{15,19} = M_7a + M_8b + M_9c$$

Ezeket a v_{40}, v_{41}, v_{42} terminálokra alkalmazva

$$(5) c = M_{10}(M_1a + M_2b) + M_{11}(M_7a + M_8b + M_9c)$$

$$(6) b = M_{12}(M_3a + M_4c) + M_{13}(M_7a + M_8b + M_9c)$$

$$(7) a = M_{14}(M_5b + M_6c) + M_{15}(M_7a + M_8b + M_9c)$$

Az utolsó három egyenletben csak a bal oldalon szereplő üzenet együtthatója a jobb oldalon is 1, a másik kettőjé 0. Innen, használva, hogy a test karakterisztikája 2, s így a $-$ jelek elhagyhatók:

$$(8) I = M_{11}M_9 = M_{13}M_8 = M_{15}M_7, \text{ valamint}$$

$$(9) M_{10}M_1 = M_{11}M_7$$

$$(10) M_{10}M_2 = M_{11}M_8$$

$$(11) M_{12}M_3 = M_{13}M_7$$

$$(12) M_{12}M_4 = M_{13}M_9$$

$$(13) M_{14}M_5 = M_{15}M_8$$

(14) $M_{14}M_6 = M_{15}M_9$ Ismét belátjuk, hogy a M_i -k invertálhatók minden i -re. A (23)-as egyenlet miatt $M_7, M_8, M_9, M_{11}, M_{13}, M_{15}$ invertálható, emiatt a (24) – (29)-es egyenletek jobb oldalai is azok, így a bal oldalon szereplő többi mátrix is valóban invertálható. Így

$$(15) M_2 = M_1M_7^{-1}M_8$$

$$(16) M_4 = M_3M_7^{-1}M_9$$

$$(17) M_6 = M_5M_8^{-1}M_9, \text{ s ezekből}$$

$$(18) M_1a + M_2b = M_1(a + M_7^{-1}M_8b)$$

$$(19) M_3a + M_4c = M_3(a + M_7^{-1}M_9c)$$

$$(20) M_5b + M_6c = M_5(b + M_8^{-1}M_9c).$$

Végül

$$\begin{aligned} & M_1^{-1}e_{23,31} + M_3^{-1} + M_1^{-1}M_2M_5^{-1}e_{25,33} = \\ & = M_1^{-1}(M_1a + M_2b) + M_3^{-1}(M_3a + M_4c) + M_1^{-1}M_2M_5^{-1}(M_5b + M_6c) = \\ & = (a + M_7^{-1}M_8b) + (a + M_7^{-1}M_9c) + M_1^{-1}(M_1^{-1}M_7^{-1}M_8)(b + M_8^{-1}M_9c) = 0. \end{aligned}$$

Innen

$$e_{23,31} = M_1M_3^{-1}e_{24,32} + M_2M_5^{-1}e_{25,33}.$$

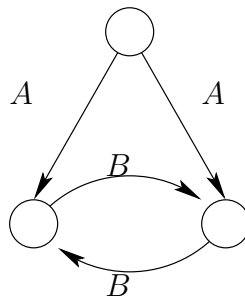
Tetszőleges c üzenet mellett $a = M_3^{-1}M_4c$ és $b = M_5^{-1}M_6c$ választással (18) és (19) miatt $e_{24,32} = e_{25,33} = 0$, s ezért az utolsó sor alapján $e_{23,31}$ is 0. Hasonóan választható d és e úgy, hogy $e_{26,34} = e_{27,35} = e_{28,36} = 0$ teljesüljön. Ekkor v_{43} -ba minden c esetén csupa 0 üzenet érkezik minden élen, ami ellentmondás. \square

2.28. Megjegyzés. A fenti ellenpélda nem véletlenül adódott. Dougherty és szerzőtársai kidolgoztak egy eljárást, amely minden matroidhoz hozzárendel egy kódolási feladatot [6]. Megfigyelték, hogy a reprezentálható matroidokhoz lineáris kóddal megoldható probléma tartozik. Az N_1 példát a Fano matroidból kapták, amely csak páros karakterisztikájú test felett reprezentálható. Az N_2 ellenpélda másik két szárnya az úgynevezett Anti Fano matroidból származik, amely pedig csak páratlan karakterisztikájú test felett reprezentálható.

3. fejezet

Nem aciklikus irányított gráfok

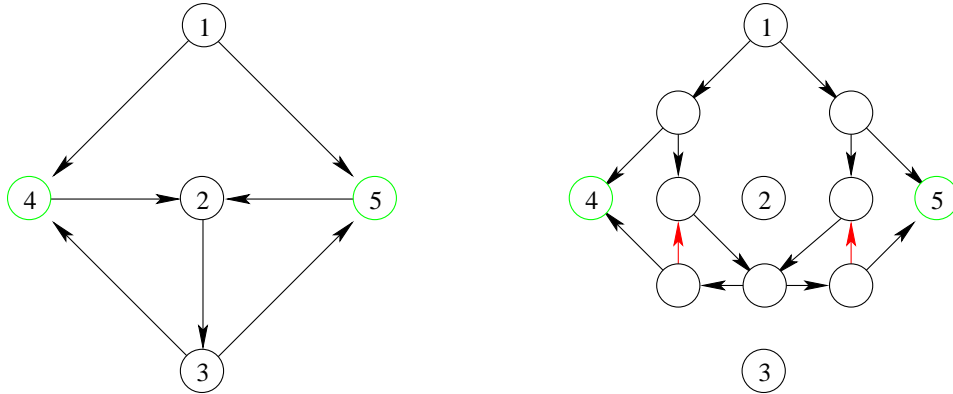
Ha a kódolási feladatban adott D gráf nem aciklikus, a lineáris megoldás feltételeit teljesítő lineáris kód nem feltétlenül ad megvalósítható kódolást (3.1 ábra).



3.1. ábra. Példa olyan lineáris kódra, melyen minden kimenő üzenet előáll a bemenők lineáris kombinációjaként, mégsem valósítható meg.

A korábban vizsgált példák között volt olyan, amely ugyan nem volt aciklikus, mégis létezett hozzá lineáris megoldás (1.2 ábra). A példa valójában egy aciklikus gráf összehúzott változata (5.1 ábra), és így az $L(D) + V$ kiegészített élgráfja

aciklikussá tehető.



3.2. ábra. Példa nem aciklikus gráfra, melynek élgráfja aciklikussá tehető (a piros élek törlésével) úgy, hogy a terminálokba továbbra is vezessen két-két út.

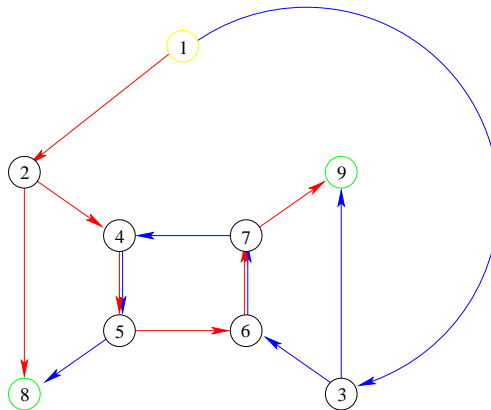
Felvetődik a kérdés, létezik-e mindig ilyen részgráfja az élgráfnak? A válasz nem, már $|S| = 1$, $|T| = 2$, $k = 2$ esetén is adható példa olyan gráfra, melyben mindkét terminálba megy két élidegen út, de az élgráfját nem lehet aciklikussá tenni úgy, hogy ez továbbra is fennálljon. A 3.3 ábrán látható gráf például ilyen, ugyanis a kör bármely két egymást követő éle része valamelyik útnak. Erre a gráfra nem is terjeszthető ki az aciklikus definíció.

3.1. Megjegyzés. A 3.3 ábrán mutatott ellenpélda az élfüggetlen gráfokról szóló fejezetben is felbukkan (5.1 ábra második gráfja).

A ciklikus gráfok kezeléséhez tehát más lineáris kód definícióra van szükség. Ebben a fejezetben két ilyen definíciót mutatunk be.

Az egyik visszavezeti a problémát az aciklikus esetre oly módon, hogy a gráf csúcsaihoz időpontot is rendel. Az eljárás hátránya, hogy az egyes éleken küldött üzenet összetétele időben változhat.

A másik megközelítés a lineáris kód fogalmát általánosítja. Véges test helyett a



3.3. ábra. Példa olyan gráfra, melynek élgráfja nem tehető aciklikussá az összefüggőség megőrzésével.

test feletti polinomok állnak a vektorokban, a polinom kitevőivel jelezve az időbeli késés mértékét. Megmutatták, hogy multicast esetben, ha valamilyen kódolással létezik megoldása egy feladatnak, akkor időinvariáns lineáris megoldás is létezik, és polinom időben megadható ([9]).

3.1. Dinamikus lineáris kódok

3.1.1. Dinamikus folyamatok

Kapacitásos irányított gráfokkal sokféle szállítási probléma modellezhető és könnyen kezelhető. Előfordul azonban, hogy az élek kapacitása mellett jelentős szerepe van az élek hosszának (az élen eltöltött időnek). Ha például az a kérdés, hogy adott idő alatt mennyi áru szállítható el egy raktárba, nem elég csupán az élek kapacitásait figyelembe venni. A feladat visszavezethető a MFMC tételre, azonban ehhez meg kell tudni különböztetni az egy csúcsból eltérő időpontban kiinduló

szállítmányokat, így a csúcsoknak több, időponttal is rendelkező példányára van szükség. Ez lesz a dinamikus gráf (Ford, Fulkerson [7]).

Tekintsünk egy $D = (V, A)$ irányított gráfot s, t forrással és nyelővel, valamint $c : A \rightarrow \mathbb{N}^+$ kapacitás- és $d : A \rightarrow \mathbb{N}^+$ élhosszfüggvénnyel.

3.2. Definíció. Legyen T pozitív egész. A D gráf és s és t közötti T hosszú **dinamikus folyam**nak nevezzük egy $f : V \times V \times [0, T] \rightarrow \mathbb{N}$ leképezést, amelyre az alábbiak teljesülnek:

(i) Minden s, t -től különböző csúcs a τ időpontban beérkezőt tovább is küldi vagy elraktározza:

$$\begin{aligned} & \sum_{uv \in A} f(u, v, \tau - d(uv)) + f(v, v, \tau - 1) = \\ & = \sum_{vu \in A} f(v, u, \tau) + f(v, v, \tau) \forall v \in V \setminus \{s, t\}, 0 \leq \tau \leq T. \end{aligned}$$

(ii) $\forall (uv) \in A, 0 \leq \tau \leq T$ -re $f(u, v, \tau) \leq c(uv)$

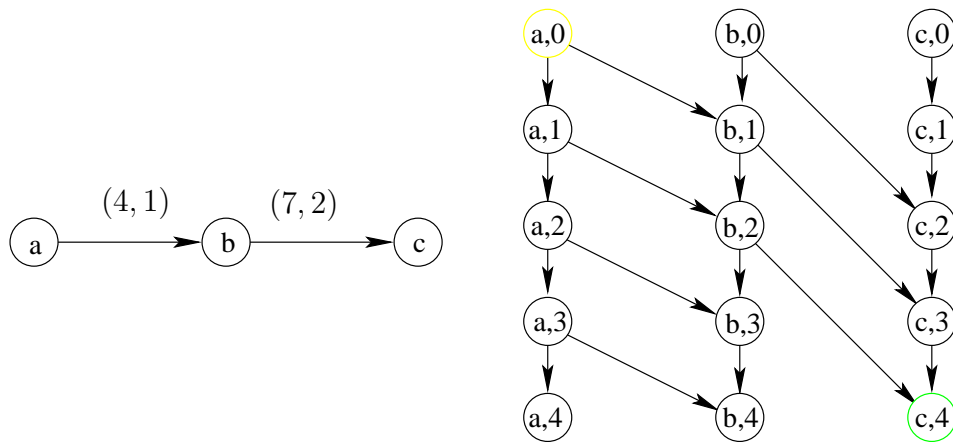
Az első feltétel következménye, hogy az s -ből kiinduló mennyiség megegyezik a t -be beérkezővel, azaz

$$\sum_{0 \leq \tau \leq T} \sum_{su \in A} f(su, \tau) = \sum_{0 \leq \tau \leq T} \sum_{ut \in A} f(ut, \tau) = v.$$

Ezt a v értéket a folyam **nagyságának** nevezzük.

Felmerül a kérdés, hogyan adható meg egy maximális nagyságú dinamikus folyam rögzített T esetén. A feladatot a MFMC tételre vezetjük vissza, ehhez azonban szükségünk lesz egy segédgráfra.

3.3. Definíció. A D gráf T hosszú **dinamikus gráfjának** nevezzük azt a $D_T = (V_T, A_T)$ gráfot, melyre $V_T = V \times [0, 1, \dots, T]$ és $v_1, v_2 \in V, 0 \leq \tau_1, \tau_2 \leq T$ -re $e = (v_1, \tau_1)(v_2, \tau_2) \in A_T$, ha



3.4. ábra. A bal oldalon szereplő gráf dinamikus gráfja (az éleken $c(e), d(e)$ szerepel).

(1) $v_1 v_2 \in A$ és $\tau_2 - \tau_1 = d(v_1 v_2)$, ekkor $c(e) = c(v_1 v_2)$

(2) $v_1 = v_2, \tau_1 = \tau_2 - 1$, ekkor $c(e) = \infty$, ezek a **raktározó élek**

(3.4 ábra)

3.4. Megjegyzés. A dinamikus gráf aciklikus.

3.5. Megjegyzés. Az eredeti gráfon értelmezett T hosszú dinamikus folyam ekvivalens a dinamikus gráfon értelmezett szokásos (statikus) $(s, 0) - (t, T)$ folyammal .

Az utóbbi megjegyzés értelmében elég D_T -ben meghatározni egy maximális folyamot. Látni fogjuk, hogy ilyen a folyamok egy szűkebb osztályában, az úgynevezett ismétlődő folyamok között is találunk. Tekintsünk egy f, v nagyságú statikus $s - t$ folyamot D -n. Ehhez rendelhető egy F dinamikus folyam a következő módon: bontsuk fel f -t $f_1 \dots f_v$ egységnyi útfolyamok összegére. Legyen az f_i -n szereplő élek összhossza d_i . Az f_i útfolyamhoz rendeljük azt az F_i dinamikus folyamot, amely a 0 időpillanattól kezdve annyiszor indul el f_i mentén,

ahányszor csak lehet. Mivel f_i megtételéhez d_i idő szükséges, ez $v_{F_i} = T - d_i + 1$ indítást jelent, vagyis ekkora nagyságú dinamikus folyamot ad. Ezen dinamikus folyamok összege, $F = \sum_{i=1}^k F_i$ is dinamikus folyam, ehhez elég a (ii) feltételt ellenőrizni: a D_T dinamikus gráf egy élén csak akkor nem nulla F_i , ha az élnek megfelelő D -beli élen sem nulla f_i . Az ilyenek összege csak úgy haladhatná meg a kapacitást, ha már f is meghaladta volna az eredetiben. Ám f megengedett volt, így F is az. Az ilyen módon előállítható dinamikus folyamokat nevezzük **ismétlődő folyamoknak**.

3.6. Megjegyzés. A fenti jelöléseket használva a dinamikus folyam nagysága az alábbi módon alakítható:

$$\begin{aligned} v_F &= \sum_{i=1}^k v_{F_i} = \sum_{i=1}^k (T - d_i + 1) = v(T + 1) - \sum_{i=1}^k \sum_{uv \in f_i} d(uv) = \\ &= v(T + 1) - \sum_{uv \in A} d(uv) f(uv) \end{aligned} \quad (3.1)$$

Vegyük észre, hogy az utolsó kifejezés az f_i útfelbontástól független.

A maximális dinamikus folyamot egy speciális statikus folyamból fogjuk előállítani, melyet a fenti 3.6. kifejezés segítségével nyerünk. Valamely rögzített T egészre tekintsünk egy f statikus, v nagyságú folyamot D -n, amely maximalizálja az alábbi lineáris függvényt:

$$(T + 1)v - \sum_{xy \in A} d(xy) f(xy) \quad (3.2)$$

Jelölje ennek optimumát v_T .

3.7. Tétel. v_T éppen a T idejű maximális folyam nagysága.

BIZONYÍTÁS. 3.2 egy lineáris program, melynek duálisában a $\pi : V \rightarrow \mathbb{N}$ potenciálra $\gamma(uv) = \max(0, \pi(v) - \pi(u) - d(uv))$ esetén

$$\sum_{xy \in A} c(xy) \gamma(xy) = (T + 1)v - \sum_{xy \in A} d(xy) f(xy)$$

teljesül. Vegyük az f egy $f_1 \dots f_v$ egységnyi útfelbontását. Mivel f maximalizálja 3.2-et, feltehető, hogy $d_i < T$, különben f_i elhagyható lenne. Tekintsük a felbontáshoz tartozó F ismétlődő dinamikus folyamatot. A fentiek alapján

$$v_F = \sum_{i=1}^v (T + 1 - d_i) = (T + 1)v - \sum_{xy \in A} d(xy)f(xy) = v_T.$$

Belátjuk, hogy F maximális. Ehhez elég egy v_F nagyságú vágást mutatni D_T -ben. Legyen ez a C vágás az alábbi:

$$C = \{[(u, \tau), (v, \tau + d(uv))] | \pi(u) \leq \tau < \pi(v) - d(uv)\}$$

Azaz olyan élek halmaza, melyek töve az

$$U = \{(u, \tau) | \pi(u) \leq \tau\}$$

halmazban, feje pedig ennek \bar{U} komplementerében van. Már csak azt kell belátni, hogy C éppen v_F nagyságú vágás. Ehhez a duálisról fentebb tett megjegyzéseket és az alábbi állítást fogjuk használni.

3.8. Állítás. *Egy (uv) élnek éppen $\gamma(uv)$ darab D_T -beli megfelelője szerepel a vágásban.*

BIZONYÍTÁS. Az (u, i) csúcsok közül a $\{(u, \pi(u)), \dots, (u, T)\}$ csúcsok vannak U -ban, a (v, j) -k közül a $\{(v, 0), \dots, (v, \pi(v) - 1)\}$ -k \bar{U} -ban. Ha $\pi(u) + d(uv) \geq \pi(v)$, egy ilyen él sincs a vágásban, de pontosan ekkor $\gamma(uv)$ is nulla. Egyéb esetben könnyen láthatóan $(\pi(v) - 1) - \pi(u) + d(uv) + 1 = \gamma(uv)$ él van C -ben. □

A vágás nagysága tehát $\sum_{xy \in A} c(xy)\gamma(xy) = (T + 1)v - \sum_{xy \in A} d(xy)f(xy) = v_F$, ahogy állítottuk. □

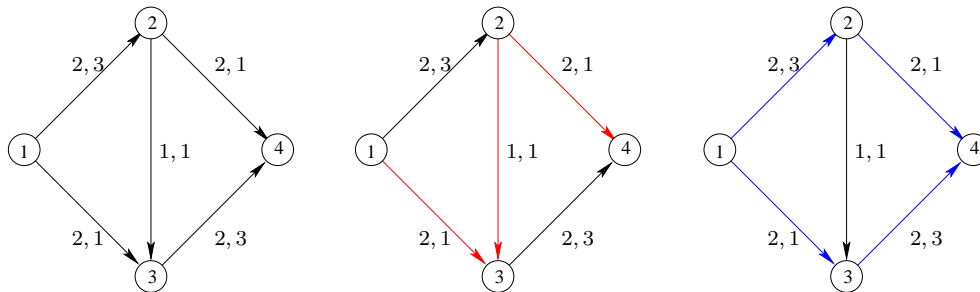
3.9. Következmény. Vegyük észre, hogy az ismétlődő folyamból kapott megoldások nem használják a raktározó éleket, a bizonyításból tehát az is látszik, hogy ezek az élek nem növelik v_T -t.

Felvetődik a kérdés, hogy van-e mindig olyan dinamikus folyam, amely minden $0 \leq \tau \leq T$ -ra v_τ -t szállít v -be, azaz

$$\sum_{0 \leq \tau \leq T} \sum_{ut \in A} f(ut, \tau) = v_\tau$$

Ez az úgynevezett **menekülési probléma** egy forrás és egy nyelő esetén. Az állítás könnyen láthatóan igaz, bizonyításához módosítsuk a D_T dinamikus gráfot oly módon, hogy kivesszük a $(t, i) - (t, i + 1)$ típusú éleket, helyettük $v_i - v_{i-1}$ kapacitású éleket vezetünk a (t, i) csúcsokból egy új t^* csúcsba. Könnyen ellenőrizhető, hogy a kapott gráfban is van v_τ nagyságú $(s, 0) - t^*$ folyam, ami éppen a keresett dinamikus folyamot adja.

Az már nem igaz, hogy a menekülési probléma is mindig megoldható ismétlődő dinamikus folyammal, erre könnyű ellenpéldát mutatni: a 3.5 ábrán látható gráfon $v_3 = 1$, s ezt csak a piros útvonalon lehet teljesíteni. Ha mégis létezne ismétlődő optimum a menekülési problémára, az ezt az útvonalat használná. $T = 5$ esetén azonban $v_5 = 8$, ez elérhető a két utak kétszeri indításával. Ha a piros utat háromszor elindítjuk, a kékeken már csak egy-egy kapacitásnyi folyam mehet, a mi összesen csak 7.



3.5. ábra. Példa gráfra, melyben nem lehet ismétlődő folyamokkal a menekülési probléma optimumát elérni (az éleken c(e),d(e) szerepel).

3.10. Megjegyzés. Megmutattuk, hogy egy gráfbeli dinamikus folyam ekvivalens a gráf dinamikus gráfjának egy statikus folyamával. Ennek mintájára definiál-

hatjuk a **dinamikus vágást**, mint a dinamikus gráf egy (statikus) vágását. A dinamikus folyam értéke a dinamikus gráf egy élén a rajta átmenő folyam nagyságát jelzi egy adott időpontban. Ehhez hasonlóan egy dinamikus vágásbeli él azt jelzi, hogy az adott élt mely időpontokban nem használhatja egy folyam. A MFMC tétel szerint létezik v_T nagyságú (minimális) dinamikus vágás, fentebb éppen egy ilyet mutatunk. A bizonyításból még az a kicsit erősebb állítás is kiolvasható, hogy olyan minimális vágás is van, amely minden élt egyetlen időintervallumra "zár le".

3.1.2. Kódolási probléma dinamikus gráfja

3.11. Definíció. Tekintsünk egy $C = (D, s, T, k)$ multicast kódolási feladatot, s a D gráf τ hosszú dinamikus gráfját ($\tau \in \mathbb{N}$, $c \equiv 1$, $d \equiv 1$). A kapott gráf a kódolási probléma **memóriával rendelkező dinamikus gráfja**.

A dinamikus gráf aciklikus, így azon a $C' = D_{\tau, (s, 0), (T, \tau), k'}$ feladatnak található lineáris megoldása, ahol k' a minimális $(s, 0) - (T, \tau)$ vágás. A kapott kód az eredeti gráfban is lineáris kódot ad. A gyakorlatban előforduló hálózatok egy részében a csomópontoknak nincs memóriája, így szükséges lehet a dinamikus gráf alábbi módosítása.

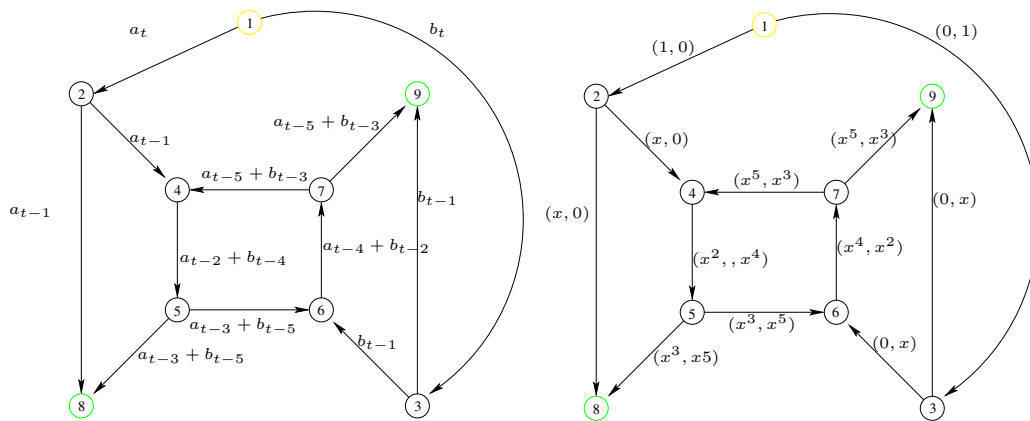
3.12. Definíció. Egy kódolási feladat τ hosszú **memóriával nem rendelkező dinamikus gráfja** az a gráf, melyet d_τ -ból kapunk a $v_i v_{i+1}$ alakú élek törlésével ($v \in V \setminus \{s, T\}$).

3.13. Megjegyzés. A 3.9. következmény miatt a C' probléma ez utóbbi gráfban is megoldható.

3.14. Megjegyzés. Mivel az egyes D -beli éleknek több D_τ -beli megfelelője is van, előfordulhat, hogy az élekhez rendelt vektorok nem állandók. A dinamikus kód tehát (ahogy a neve is mutatja) nem időinvariáns, így sok szempontból nem optimális.

3.2. Időinvariáns lineáris kódok

A dinamikus modell hátránya, hogy nem időinvariáns, azaz az egyes élekhez rendelt vektorok változhatnak. Gyakorlati szempontból ez nem mindig megvalósítható, ezért van szükség az időinvariáns kód definiálására. Ez a kódolás lehetővé teszi eltérő időpontban keletkezett üzenetek összekódolását. Emlékezzünk vissza, hogy egy üzenet valamilyen ábécé betűiből alkotott n hosszú sorozat, például az eddig csak a -val jelölt üzenethez valójában minden t időpontra tartozik egy a_t betű, azaz összesen: $a_1, a_2, a_3, \dots, a_n$. Ezek külön jelölésére eddig nem volt szükség, mivel az összekódolás egy t időpontban keletkezett a_t üzenetet mindig szintén t -beliekkel kódolt.



3.6. ábra. Példa lineáris időinvariáns megoldásra, és a hozzá tartozó polinomvektorokra $E = A$ esetén. Az első ábrán a t időpontban küldött üzenetek szerepelnek, a másodikon az $f(e)$ polinomvektorok.

Tekintsük a fejezet elején bemutatott 3.3 gráfot. Láttuk, hogy a kódolási feladatnak nincs lineáris megoldása. A 3.6 ábrán a probléma egy megoldását láthatjuk. Az egyes éleken szereplő értékek a t időpillanatban küldött üzeneteket jelzik ($1 \leq t \in \mathbb{N}$). Ez a megoldás ugyan lineáris, ám eltérő időpontban keletkezett

üzeneteket kódol össze. Az azonos helyről jövő, de különböző idejű üzeneteket a polinomokban szereplő különböző kitevőjű tagok jelzik, például az x^3 együtthatói a $t - 3$ -ban keletkezett üzenetek együtthatóit mutatják [16], [8].

Jelölje $\langle \mathbb{F}(x) \rangle^d$ az \mathbb{F} véges test feletti polinomokat.

3.15. Definíció. Tetszőleges $D = (V, A)$ gráf, s forrás és \mathbb{F} véges test és $E \subseteq A$ késleltető élhalmaz esetén **időinvariáns lineáris kódnak** nevezzük egy $f : A \rightarrow \langle \mathbb{F}(x) \rangle^d$ leképezést, ha $\forall vw \in E$ -re $\langle f(vw) \rangle \subseteq x \cdot \langle f(v''v) \mid v''v \in A \rangle$, azaz az E -beli élhez rendelt polinomvektor előáll a bemenők x -szel szorzott lineáris kombinációjaként (3.6), és $\forall vw \in (A \setminus E)$ -re $\langle f(vw) \rangle \subseteq x \cdot \langle f(v''v) \mid v''v \in A \rangle$, azaz a többi élen f az aciklikus esetben ismert módon viselkedik.

3.16. Megjegyzés. Eredetileg csak az $E = A$ esetben definiálták a fenti kódot, ám az nem általánosítása az aciklikus esetbeli lineáris kódnak. A fenti definíció tartalmazza az aciklikus esetbeli kódot is, $E = \emptyset$ esetén.

3.17. Megjegyzés. A 3.6 ábrán például a v_4v_5 élre:

$$f(v_4v_5) = (x^2, x^4) = (x - x^5)(x, 0) + x(x^5, x^3) = x[(1 - x^4)f(v_2v_4) + f(v_7v_4)].$$

A v_5 csúcsba menő élek polinomvektorai az $(x, 0)$ és $(0, x^5)$ által meghatározott modulust feszítik ki. Egy kódolási feladat megoldásához tehát nem szükséges $\mathbb{F}(x)^k$ -t feszítenie a polinomvektoroknak, lehet benne x^d késés (következő definíció (iii) pontja).

Az időinvariáns lineáris kód a lineáriséhoz hasonlóan sem feltétlenül α -kód, ehhez az alábbi feltételekre van szükség.

3.18. Definíció. Egy bővített gráfon értelmezett időinvariáns lineáris kód **megoldása** egy kódolási feladatnak, ha

(i) $A \setminus E$ aciklikus

(ii) $f(s'_i) = e_i$, ahol e_i az i -edik egységvektor $\langle \mathbb{F}(x) \rangle^d$ -ben

(iii) minden terminálba a bemenő élek polinomvektorai által feszített modulus $\mathbb{F}(x)^k \cdot (x^{d_1}, \dots, x^{d_k})$ alakban írható.

3.19. Tétel. (E.Erez, M.Feder) Egy $C = (d, s, T, k)$, irányított gráfon adott multicast kódolási feladatnak pontosan akkor létezik időinvariáns lineáris megoldása, ha $\forall t \in T$ -re $\lambda(s, t) \geq k$, s ekkor a kód polinomiális időben megtalálható.

BIZONYÍTÁS. (vázlat) Csak az algoritmust mutatjuk be, a helyességét igazoló teljes bizonyítás megtalálható [9]-ben. A módszer az aciklikus algoritmushoz hasonló: rögzítsünk k élidegen st utat minden t terminálra, ezen utak halmaza ugyanúgy p_t (ez feltehető, hogy aciklikus). Vegyünk továbbá egy E élhalmazt, melyet kivéve a gráfból aciklikus gráfot kapunk. Egy $e \in p_t$ élre jelölje $p_t(e)$ az e -t megelőző élt p_t -ben. Az algoritmus olyan $m(e, p_t(e)) \in \langle \mathbb{F}(x) \rangle$ együtthatókat határoz meg, melyekre f időinvariáns lineáris kódot ad, ahol $f(e) = x \cdot \sum_{p_t|e \in p_t} m(e, p_t(e)) f(p_t(e))$, ha $e \in E$ és $f(e) = \sum_{p_t|e \in p_t} m(e, p_t(e)) f(p_t(e))$ egyébként, ahol E az élek olyan részhalmaza, melyet kivéve aciklikus gráfot kapunk. Mivel itt nem tudunk egyszerre topologikus sorrendben haladni, minden p_t élhalmazban külön-külön sorra vesszük az éleket, és ha kell, módosítunk m -en. Minden terminálhoz hozzunk létre egy k élből álló U_t halmazt, melyek kezdetben $\{s'_i\}$ -vel egyenlők minden terminálra. Amikor az algoritmus p_t élein halad végig, jelölje U_t az egyes p_t -beli st utakon legutóbb sorra került élek k elemű halmazát (feltettük, hogy p_t aciklikus, így abban már tudunk topologikus sorrendben haladni). A p_t éleit elhagyva U_t k darab t -be menő élből fog állni, és többé nem változik. Az algoritmus során arra ügyelünk, hogy az egyes U_t -khez rendelt polinomvektorok ($f(U_t)$) minden t -re teljesítsék a 3.18. (iii) pontját, így az algoritmus végén időinvariáns lineáris kódot kapunk. Az aciklikus esetben megismert módon végigmehetünk p_t -n, hogy U_t teljesítse a feltételeket. Már csak a többi terminálhoz tartozó $U_{t'}$ élhalmazokra kell figyelni. Előfordulhat ugyanis, hogy egy korábban tekintett t terminálba menő U_t élek a későbbiek folyamán elrom-

lanak. Meglepő módon a probléma kiküszöbölhető azzal, ha egy további, $f'(U_t)$ polinomvektor halmazról is megkövetljük 3.18. (iii)-t, ahol a f' lineáris kódot úgy kapjuk, hogy nullára változtatunk minden $m(e', e)$ -t, mely olyan e, e' élekhez tartozik, melyekre $e \in p_t$, de e még nem szerepelt U_t -ben, e' pedig $\notin p_t$. \square

4. fejezet

Kódolás és fenyőfelbontás

Ebben a fejezetben Edmonds jólismert fenyőfelbontási tétele és a hálózati kódolás közötti kapcsolatot vizsgáljuk. Az első részben egy egyszerű, de nem algoritmikus bizonyítást adunk a tételre, a második részben pedig az időinvariáns lineáris kódok létezéséről szóló tétellel közös általánosítását mutatjuk be.

4.1. Edmonds fenyőfelbontási tétele

4.1. Tétel. (Edmonds) *Egy $D = (s + V, A)$ irányított gráf az s gyökérpontból k -szorosán élösszefüggő, azaz minden pontjába vezet k élidegen út s -ből. Ekkor létezik D -ben k éldiszjunkt s gyökerű feszítő fenyő.*

Az eredeti tétel helyett annak egy erősebb alakját látjuk be. Előtte bevezetünk néhány definíciót.

4.2. Definíció. *Egy $D = (s + V, A)$ irányított gráf és az $G_1 \dots G_k$ s -re gyökeresen élösszefüggő éldiszjunkt részgráfok teljesítik a **felbontási feltételt**, ha a gráf*

minden pontjába vezet k élidegen út s -ből, és minden s -et nem tartalmazó halmazba belépő részgráfok és fedetlen élek száma összesen legalább k . A H halaz pontos, ha a belépő részfenyők és fedetlen élek száma éppen k .

4.3. Állítás. (Edmonds erős alak) Egy $D = (s + V, A)$ irányított gráfban adottak az $F_1 \dots F_k$ éldiszjunkt s gyökerű részfenyők, melyek teljesítik a felbontási feltételt. Ekkor a részfenyők kiegészíthetők éldiszjunkt feszítő fenyökké.

BIZONYÍTÁS. Legyen H egy s -et nem tartalmazó csúcshalmaz. Jelölje G_H a H egy h ponttá összehúzásával keletkező gráfot, H' pedig a H -n kívüli pontok összehúzásával keletkezőt. Belátjuk, hogy G_H majd H' is feszítő fenyőkre bontható, s pontos H esetén a két felbontás együtt G -ben is jót ad.

4.4. Állítás. G_H -ban teljesül a felbontási feltétel.

BIZONYÍTÁS. (Nyilvánvaló) Könnyen látható, hogy a részfenyők az összehúzás után is éldiszjunkt, gyökeresen összefüggő részgráfok lesznek, így csak a halmazokba belépő éleket kell ellenőrizni. Tekintsünk az G_H -ban egy s -en kívüli T halmazt! Ha T nem tartalmazza h -t, az összehúzás nem változtat a bemenő éleken, ha pedig tartalmazza, bemenő élei az eredeti gráf $T \setminus h \cup H$ halmazának bemenő éleivel egyeznek meg, amelyek szintén teljesítették a feltételt. \square

A fentiek miatt az F_i részfenyők G_H -beli megfelelői kiegészíthetők G_H -t feszítő éldiszjunkt fenyökké. (Az előfordulhat, hogy valamely F_i összehúzva már nem fenyő, mert H -ba többször is belépett, ekkor tekintsük egy feszítő részhalmozatot.)

4.5. Állítás. A G_H egy felbontásának H' -beli élei kiegészíthetők H' felbontásává.

BIZONYÍTÁS. Azt kell belátni, hogy H' a G_H felbontása után is teljesíti a feltételeket. Vegyünk egy $I \subseteq H$ halmazt, és tegyük fel, hogy nem teljesül rá a felbontási feltétel. Ez csak úgy lehetséges, ha valamely G_H -ban h -ba, G -ben I -be menő élt olyan részgráfhoz adtunk, amely már belépett I -be. A részgráfok gyökeres összefüggősége miatt azonban ha egy részgráf belép I -be, akkor belép H -ba is, s így G_H -ban h -ba is belépett, de akkor G_H felbontása során nem adódhatott ahhoz a fenyőhöz több él. \square

4.6. Állítás. *Tekintsünk egy pontos H halmazt (ilyen van, hiszen feltethető, hogy minden csúcs befoka k). A G_H majd H' felbontását összetéve jó felbontást kapunk G -ben.*

BIZONYÍTÁS. Jelölje a kapott k halmazt L_1, \dots, L_k . Könnyen látható, hogy minden él színe egyértelmű, és minden csúcsba belép mind a k halmaz, ezért csak azt kell belátni, hogy az egyes halmazok körmentesek. Tegyük fel, hogy L_1 tartalmaz egy C kört. Vegyük C -nek azt az e élét, melyet utoljára adtunk L_1 -hez. G_H felbontása részfenyőket ad G -ben, ezért e csak H' -beli lehet, s mivel H pontos volt, csak H -n belül mehet, hiszen a kintről jövő éleket már G_H szétosztotta. Így egyrészt e -t csak H -ból kilépő f él követheti C -ben, másrészt C a G_H -ban is kör, ami csak úgy lehetséges, hogy f már eredetileg is F_1 része volt, vagyis e fejét már e F_1 -hez vétele előtt is elérte F_1 . \square

Ha tehát találunk olyan H pontos halmazt, melyre H és komplementere is legalább két pontból áll, indukcióval készen vagyunk. Ha nincs ilyen halmaz, az két okból lehet: vagy nincs pontos halmaz, s ekkor tetszőleges fedetlen élt hozzávehetünk tetszőleges F_i -hez, vagy minden pontos vágás valamelyik fele egypontú. Az utóbbi esetben vegyük észre, hogy ha egy F_i csúcshalmazából kilépő f_i élt nem vehetünk F_i -hez, akkor létezik egy olyan H_i , mely pontos, tartalmazza f_i fejét, és belelép F_i , azaz H_i legalább kétpontú, így a komplementerének kell egypontúnak lenni, vagyis $H_i = V$, s komplementere s . Ekkor azonban f_i egy H_i -be még nem metsző fenyőhöz illeszthető. \square

4.2. A tétel egy általánosítása

A következő tétel Y. Wu, K. Jain és S.-Y. Kung eredménye [10], melyben Edmonds tételének és az időinvariáns lineáris kód létezéséről szóló 3.19. tételnek adják közös általánosítását. Tételük lényegében a valódi kódolás élhalmazát szűkíti. Ennek precíz megfogalmazásához szükségünk lesz néhány definícióra.

4.7. Definíció. Egy kódolási probléma időinvariáns lineáris megoldásában egy $uv \in A$ élt **kódoló élnek** nevezünk, ha ősei üzenetének valódi lineáris kombinációját küldi tovább, azaz $\exists wu \in A : f(uv) = xf(wu)$ vagy $f(wu)$.

4.8. Definíció. Egy $D = (s+V, A)$ s gyökerű irányított gráfban adott egy $T \subseteq V$ terminálhalmaz. A $V \setminus T$ -beli csúcsokat **Steiner pontoknak** nevezzük, az ezekbe menő éleket **Steiner éleknek**.

4.9. Tétel. [Wu és szerzőtársai] Ha egy C kódolási feladatban $\lambda(s, t) \geq k$ minden $t \in T$ -re, akkor létezik időinvariáns lineáris megoldás, mely csak a Steiner éleken kódol, azaz a többi élen a küldött üzenet megegyezik valamely megelőző él üzenetével.

BIZONYÍTÁS. Belátjuk, hogy minden terminálba menő élhez hozzárendelhető valamelyik őt megelőző él úgy, hogy a többi őstől elvágva a gráf összefüggősége ne változzon. A precízebb megfogalmazás érdekében D minden $e \in A$ élére helyezzünk egy (ugyancsak) e csúcsot, a kapott gráf legyen $D' = (s + V + A, A)$. Valamely $e = uv$ él hozzárendelése egy őt megelőző $f = tu$ -hoz azt jelenti, hogy D' -ben kitöröljük az ue élt, és helyette behúzzuk fe -t. Ezt a műveletet az e él f -hez történő **hegesztésének** nevezzük. A következőkben megadunk egy polinomiális algoritmust, amely minden nem Steiner élt hozzáhegeszt egy azt megelőző élhez. Az algoritmus során két dologra kell ügyelni. Egyrészt minden egyes hegesztés után szükséges, hogy $\lambda(s, t) \geq k$ továbbra is fennálljon T minden t elemére, másrészt biztosítani kell, hogy az algoritmus során minden él sorra kerüljön. Belátjuk, hogy mindezeket már két feltétel is biztosítja:

- (i) Egy élt hegeszteni csak Steiner élhez vagy már korábban hegesztett nem Steiner élhez lehet.
- (ii) A hegesztett él fejébe (egy terminálpontba) továbbra is vezessen k élidegen út.

A következő lemma segítségével bizonyítható $\lambda(s, t) \geq k$ fennmaradása minden t terminálra.

4.10. Lemma. *Egy irányított gráfban az s, v, v' csúcsokra teljesül, hogy léteznek P_1, P_2, \dots, P_k élidegen $s - v$ utak, illetve P'_1, P'_2, \dots, P'_k élidegen utak, melyek közül P'_1 v -ből v' -be, a többi s -ből v' -be megy. Ekkor s -ből v' -be is megy k élidegen út.*

BIZONYÍTÁS. Tegyük fel, hogy nem igaz az állítás, és tekintsünk egy $s - v$ vágást, mely k -nál kevesebb élből áll. Tekintve, hogy $\lambda(s, v) \geq k$, v csak az s -t tartalmazó komponensben lehet. Ekkor viszont a P'_i utak mindegyike metszi a vágást, ami ellentmondás. Az állítás tehát igaz. \square

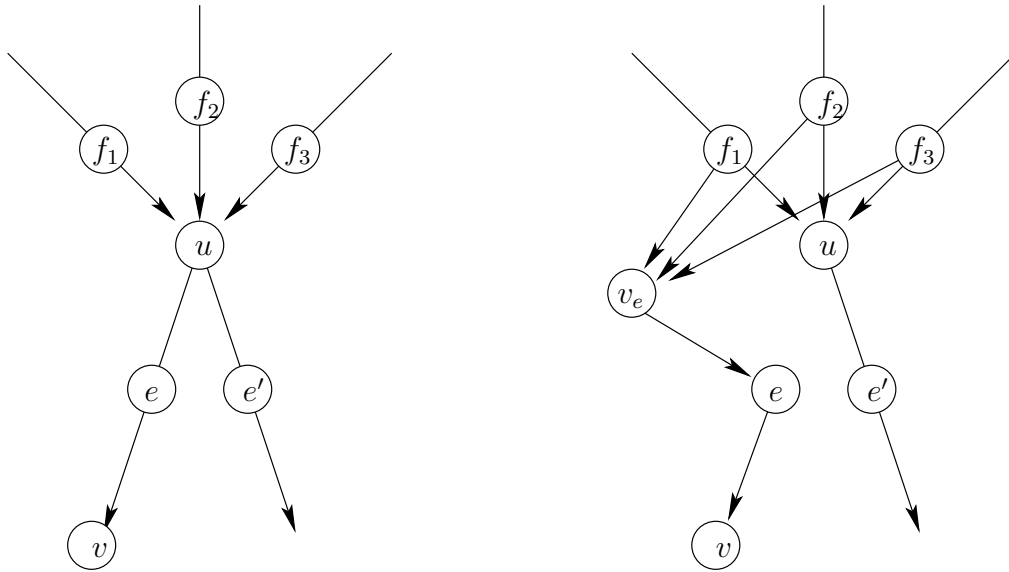
Vegyünk egy t' terminált egy t -be menő e él hegesztése után. Ha $t = t'$, tudjuk, hogy oda továbbra is megy k élidegen út s -ből. Ha t más terminál, nézzük meg mi történhetett a korábban odavezető k úttal. Ha ezek nem használták e -t, továbbra is léteznek. Ha használták, alkalmazhatjuk az előző lemmát $v = t$ és $v' = t'$ választással.

Már csak annak a bizonyítása van hátra, hogy minden nem Steiner él sorra kerül. Ehhez bevezetünk egy új, a hegesztésnél finomabb műveletet. Előtte azonban a gráfon is módosítani kell egy kicsit.

4.11. Definíció. *Tekintsünk az eredeti gráfban egy $e = uv$ élt (melyet most az e csúcs feloszt). Vegyünk fel egy új, v_e csúcsot, melynek ősei u ősei, de egyetlen kimenő éle $v_e e$, majd töröljük ki az $u - e$ élt. Ezt a transzformációt az e él u -ból történő **kiemelésének** nevezzük (4.1 ábra).*

4.12. Megjegyzés. Könnyen látható, hogy egy él kiemelése nem változtat a terminálok összefüggőségén: $\lambda(s, v_e) = \lambda(s, u)$.

Indirekten tegyük fel, hogy a fenti hegesztő algoritmus nem hegesztett minden nem Steiner élt. Jelöljük ezen kimaradt élek halmazát E_R -rel. Emeljük ki E_R

4.1. ábra. Az e él kiemelése az u csúcsból

elemeit, az új $\{v_{e_i} | e_i \in E_R\}$ csúcshalmazt jelölje C . Tekintsük az alábbi (U, \bar{U}) vágást: $\bar{U} = E_R \cup C$. Belátjuk, hogy a $\delta(U)$ élek elhagyása mégis megőrzi az összefüggőséget, ami ellentmondás, mert ezzel újabb csúcsokat lehetne hegeszteni. Indukcióval bizonyítjuk, hogy $\delta(U)$ éleinek bármely k elemű részhalmaza elhagyható. Ez $k = 0$ -ra nyilvánvaló. Tegyük fel, hogy k -ig igaz az állítás, és vegyünk egy $W \subseteq \delta(U)$ $k + 1$ elemű részhalmazt. Vegyük észre, hogy E_R ősei a C -beli csúcsok, így $\delta(U)$ fv_e típusú élekből áll, ahol $e \in E_R$.

Először az olyan terminálokra látjuk be az állítást, melyekbe megy él W fejeiből, azaz a $T_D = \{t \in T | \exists (f, v_e) \in W, e = ut\}$ terminálhalmazra. Tekintsünk egy $t \in T_D$ terminált és egy $(fv_e) \in W$ élt. Az indukciós állítás szerint létezik k éldiszjunkt $s - t$ út a $W \setminus (fv_e)$ élek elhagyásával. Ha ezen utak nem használják fv_e -t, azt is elhagyva is megmarad t összefüggősége. Ha valamely út használja, e az f -hez hegeszthető lenne, tehát T_D -re igaz az állítás.

Most tekintsünk egy $t \in T \setminus T_D$ terminált. Az előző esethez hasonlóan elég

azt vizsgálni, amikor $f v_e$ -t tartalmazza valamely p_i $s - t$ út. A 4.10. lemma segítségével szeretnénk bizonyítani az állítást. Ehhez elég találni a p_i út $f v_e$ -t követő szakaszán egy csúcsot, melybe vezet k út. Ha ez az útrész tartalmaz T_D -beli terminált, az a csúcs megfelel. Ha nem (tehát speciálisan az f, v_e, e csúcsokat sem e feje, hanem egy abból kiemelt $v_{e'}$ csúcs követi) vegyük az utolsó e^* (él)csúcsot, melynek feje T_D -beli (ilyen van, hiszen $f v_e \in W$, így e feje $\in T_D$). Ekkor e^* -ot sem a feje követi, hanem egy kiemelt csúcs. Ezen csúcs bemenő élei viszont már diszjunktak W -tól, hiszen e^* -ot pont így választottuk. Tehát ősei megegyeznek e^* T_D -beli fejének őseivel, így a 4.12. megjegyzés miatt vezet bele k élidegen út.

4.13. Megjegyzés. Az algoritmus futási ideje $O(k^3|T| \cdot |E|)$.

4.14. Következmény. Tekintsünk a $T = V$ esetet. Tegyük fel, hogy minden pont befoka pontosan k . A tétel szerint létezik olyan megoldása a kódolási feladatnak, mely csak a nem Steiner éleken kódol. Ebben az esetben azonban nincs ilyen él, ezért nincs valódi kódolás sem, így a kapott megoldásban az azonos üzeneteket küldő élek k éldiszjunkt feszítő fenyőre bontják az élhalmazt, bizonyítva ezzel Edmonds tételét (4.1. tétel).

4.15. Következmény. A tétel bizonyításából valójában az Edmonds tétel erős alakja is adódik (4.3. tétel). Emlékezzünk vissza, hogy egy V gráfon adott megoldás a bővített gráfon van értelmezve (2.3. definíció). Az előző következmény szerint, az algoritmus minden pillanatában a hegesztett élek k diszjunkt élhalmazt alkotnak aszerint, hogy melyik s -be menő él üzenetét továbbítják. Könnyen meggondolható, hogy a feltétel, miszerint hegesztetni csak már korábban hegesztett élhez szabad éppen azt biztosítja, hogy ezen k élhalmaz mindegyike s gyökerű legyen. Az algoritmus során létrejövő élhalmazok tehát teljesítik az erős alak feltételeit, s a bizonyítás szerint az ilyenek be is fejezhetők feszítő fenyőkké.

4.16. Megjegyzés. Aciklikus gráf esetén a 4.9. tétel jóval egyszerűbben igazolható. Feltehető, hogy minden terminálba pontosan k él megy. Tekintsünk egy lineáris kód megoldást, és indirekten tegyük fel, hogy egy e él egyik őséhez sem

hegeszthető. Az, hogy e nem hegeszthető valamely vu élhez azzal ekvivalens, hogy $f(vu)$ előáll a t -be menő többi él vektorainak lineáris kombinációjaként. Ha ez minden u -ba menő élre igaz volna, ezek lineáris kombinációja, azaz $f(e)$ maga is ilyen lenne, ami ellentmondás, mert akkor a többi t -be menő éllel nem feszíthetnék ki a k dimenziós teret.

Ez a bizonyítás csak a lineáris kód létezését használta aciklikus gráfokon, az eredmény mégis tisztán gráfelméleti:

4.17. Állítás. *Aciklikus s gyökerű gráfban a $T_k = \{v \in V \mid \lambda(s, v) \geq k\}$ -beli csúcsokba menő élek mind hozzáhegeszthetők valamely ősihöz oly módon, hogy T_k ne csökkenjen.*

5. fejezet

Független fenyők

5.1. Pontfüggetlen feszítő fenyők

5.1.1. Kétszeresen pontösszefüggő eset

5.1. Definíció. Egy $D = (V, A)$ s gyökerű irányított gráfban két feszítő fenyő **pontfüggetlen**, ha minden csúcsra a fenyők által meghatározott két odavezető út belsőleg pontdiszjunkt.

Két pontfüggetlen feszítő fenyő létezésének szükséges feltétele, hogy minden pontba vezessen két pontdiszjunkt út s -ből, azaz a gráf kétszeresen gyökeresen pontösszefüggő legyen. R.W. Whitty mutatta meg [12]-ben, hogy ez a feltétel elégséges is.

5.2. Tétel. (R.W. Whitty) Egy $D = (V, A)$ irányított gráf egy s csúcsra nézve kétszeresen gyökeresen pontösszefüggő. Ekkor létezik benne két pontfüggetlen feszítő fenyő.

BIZONYÍTÁS. A tétel helyett a következő, vele ekvivalens állítást látjuk be. Ehhez megjegyezzük, hogy a pontfüggetlenség különböző gyökerű részfenyőkön is értelmezhető, az előző definícióhoz hasonló módon.

5.3. Tétel. *Adott egy $D = (V + \{s_1, s_2\}, A)$ irányított gráf, melyben s_1 és s_2 gyökerpontok, s melyekre teljesül, hogy a gráf minden további x csúcsába vezet egy-egy pontdiszjunkt s_1x, s_2x út. Ekkor létezik két, s_1 illetve s_2 gyökerű V -t feszítő pontfüggetlen fenyő.*

5.4. Állítás. *A 5.2. tétel és a 5.3. tétel ekvivalens.*

BIZONYÍTÁS. \Rightarrow : Tekintsünk egy gráfot, mely teljesíti az utóbbi tétel feltételeit. Vegyünk fel egy s' gyökerpontot, melyből s_1 -be és s_2 -be megy egy-egy él. Erre teljesülnek a 5.2. tétel feltételei, így létezik két s' gyökerű pontfüggetlen feszítő fenyő, melyekből s' -t törölve s_1 és s_2 gyökerűeket kapunk.

\Leftarrow : Most vegyünk egy olyan gráfot, mely a 5.2. tétel feltételeit teljesíti. Osszuk fel az s -ből kimenő éleket egy-egy csúcscsal, majd egy új s' pontból is vezessünk élt az osztópontokba. Ekkor s és s' teljesítik a másik tétel feltételeit, s a kapott két fenyő s és s' összehúzásával könnyen láthatóan megfelelő fenyőfelbontásba megy át. □

Valóban elég tehát az utóbbi tételt belátni. Ehhez először a pontok egy jó sorrendjét keressük meg, melyből a felbontás már könnyen kiolvasható.

5.5. Lemma. *Van a csúcsoknak egy v_0, v_1, \dots, v_n sorrendje, amelyre $v_0 = s_1, v_n = s_2$ és minden más csúcsba megy él balról és jobbról is.*

BIZONYÍTÁS. Az állítást V csúcsszámára menő indukcióval bizonyítjuk. Az $n = 1$ eset nyilvánvaló. Tegyük fel, hogy igaz az állítás $n - 1$ -ig is, és vegyünk egy n csúcsú gráfot, mely teljesíti a feltételeket. Tekintsünk egy V -t feszítő s_1 gyökerű F fenyőt, és vegyünk az s_2 szomszédainak U halmazából egy olyan u csúcsot, mely nem őse más U -belinek F -ben. Belátjuk, hogy u -t és s_2 -t összehúzva

továbbra is minden V -beli csúcsba vezetnek s_1 -ből és s_2 -ből jövő pontdiszjunkt utak. Ha ugyanis az összehúzás után lenne egy X csúcshalmaz, melyet egyetlen y csúcs elvág mindkét gyökértől, az y csak s_2 lehet, de akkor korábban u csak úgy nem lehetett elvágó pont, ha s_2 -nek volt szomszédja X -ben, ám ez ellentmond u választásának, hiszen X minden csúcsának u őse F -ben. \square

Egy ilyen sorrendben tekinthetjük a balra ill. jobbra menő élek feszítő fenyőit, amelyek könnyen láthatóan megfelelő pontfüggetlenek lesznek. \square

5.1.2. Többszörösen összefüggő eset

2-nél nagyobb pontösszefüggőség esetén már nem igaz az állítás, erre Huck adott példát 3-szor összefüggő gráfban [13]. Ugyancsak tőle származik a következő tétel, mely szerint aciklikus gráfban viszont már léteznek független fenyők tetszőleges pontösszefüggőség esetén [14].

5.6. Tétel. (Huck) *Egy $D = (V, A)$ aciklikus irányított gráfban minden csúcsba vezet k pontdiszjunkt út egy s gyökérből. Ekkor létezik a gráfban k darab pontfüggetlen feszítő fenyő.*

BIZONYÍTÁS. Feltehető, hogy minden pont befoka éppen k . Az állítást teljes indukcióval bizonyítjuk. $k = 1$ a gráf élei feszítő fenyőt adnak. Tegyük fel, hogy $k - 1$ -ig igaz az állítás, és tekintsünk egy fent leírt gráfot. Az állítást úgy fogjuk bizonyítani, hogy mutatunk egy feszítő fenyőt, amely minden tőle éldiszjunkt feszítő fenyőtől pontfüggetlen is. Belátjuk továbbá, hogy ezt a gráfból kivéve $k - 1$ -szer gyökeresen pontösszefüggő gráfot kapunk. Erre a visszamaradó gráfra az indukciós állítást alkalmazva $k - 1$ pontfüggetlen feszítő fenyőt kapunk, amelyek a kivett fenyővel k pontfüggetlen feszítő fenyőt alkotnak. Az első fenyő kiválasztásában segít a következő lemma. \square

5.7. Lemma. *A fenti gráfban létezik a csúcsoknak olyan v_0, v_1, \dots, v_n sorrendje, amelyre $v_0 = v_n = s$, minden köztes csúcsba legalább $k - 1$ él megy a kisebb indexű csúcsokból, és legalább 1 a nagyobb indexűekből (úgy értve, hogy s élei legfeljebb egyszer szerepelhetnek vagy v_0 -ból vagy v_n -ből indulva).*

BIZONYÍTÁS. A lemmát csúcsszámra vonatkozó teljes indukcióval bizonyítjuk. Egyetlen csúcs esetén az állítás triviális. Tekintsünk egy n csúcsú gráfot, és töröljünk belőle egy x nyelőt. A fennmaradó kisebb gráf továbbra is teljesíti a feltételeket, így alkalmazható rá az indukciós állítás. Vegyünk tehát egy ilyen v_0, v_1, \dots, v_{n-1} sorrendet. Mivel x -be is vezet k pontdiszjunkt út, x befoka legalább k . Ha minden bejövő él s -ből indul, x -et tetszőleges két csúcs közé téve és egy $s - x$ élt v_n -ből, a többit v_1 -ből irányítva jó sorrendet kapunk. Ha s -en kívül más csúcsból is megy él x -be, tegyük be x -et v_0 és v_1 közé, majd vigyük egyesével v_n felé. Kezdetben balról legfeljebb $k - 1$ él ment x -be, végül viszont $\rho(x)$. Közben minden lépésben legfeljebb eggyel nőtt ez az érték, így valamely két csúcs között éppen $\rho(x) - 1$ volt, amely azt jelenti, hogy jobbról is volt bejövő él. \square

A fenti fenyő kiválasztásához vegyünk egy ilyen sorrendet. Mivel minden pont befoka pontosan k , ez azt jelenti, hogy a v_1, \dots, v_{n-1} csúcsok mindegyikébe pontosan egy él lép be nagyobb indexű csúcsból. Ezek az élek egy feszítő fenyőt alkotnak, melyben minden csúcsba az s -ből odavezető út nagyobb indexű csúcsokat használ. Ezt a fenyőt kivéve, minden csúcsba csak kisebb indexűekből jön él, így minden út a kivett fenyőtől pontfüggetlen, éppen ahogy szerettük volna. Már csak azt kell belátni, hogy a fennmaradó gráf $k - 1$ -szeresen gyökeresen pontösszefüggő. A következő lemmából látszik, hogy ehhez elég, hogy minden csúcs befoka $k - 1$ lett.

5.8. Lemma. *Egy $D = (V, A)$ aciklikus irányított egyszerű gráf pontosan akkor gyökeresen k pontösszefüggő, ha minden gyökéren kívüli pont befoka legalább k .*

BIZONYÍTÁS. Az \Rightarrow irány triviális. A \Leftarrow irány belátásához többet bizonyítunk. Nemcsak a pontösszefüggőséget látjuk be, hanem azt is, hogy tetszőleges (nem

feltétlenül különböző) k csúcsba egyszerre vezet egy-egy belsőleg pontdiszjunkt út. A gráf csúcsainak számára menő teljes indukcióval bizonyítunk. Egyetlen csúcs esetén az állítás nyilvánvaló. Tegyük fel, hogy $n - 1$ -ig már beláttuk az állítást, és vegyünk egy n csúcsú gráfot, amely teljesíti a feltételeket. Egy x nyelőt kitorólva kisebb gráfot kapunk, amely továbbra is teljesíti a feltételeket, így elég az x -et tartalmazó k -asokat ellenőrizni. Vegyünk egy ilyen $K = v_1, v_2, \dots, v_k$ csúcssorozatot. Tegyük fel, hogy x l -szer szerepel a sorozatban. Vegyünk l darab x -be menő élt, és seréljük ki x -et K -ban ezen élek töveire. Erre az új k -asra alkalmazva az indukciós állítást, majd az új l csúcsot egy-egy x -be menő éllel összekötve k , belsőleg pontdiszjunkt utat kapunk. \square

5.2. Független Steiner fenyők

5.2.1. Élfüggetlen útrendszerek

5.9. Definíció. Egy $D = (V, A)$ s gyökerű irányított gráfban két feszítő fenyő *élfüggetlen*, ha minden csúcsra a fenyők által meghatározott két odavezető út éldiszjunkt.

5.10. Állítás. Egy $D = (V, A)$ irányított gráfban az x és y csúcsokba egyaránt vezet két-két élidegen út az s csúcsból. Ekkor létezik két s gyökerű, x , y -t feszítő élfüggetlen fenyő.

BIZONYÍTÁS. Először a fenyők egy-egy ágát keressük meg.

5.11. Lemma. Léteznek s - x ill. s - y egymástól éldiszjunkt utak.

BIZONYÍTÁS. Vegyünk fel egy új, z , csúcsot, és x -ből és y -ből vezessünk bele egy-egy élt. Könnyen látható, hogy minden s - z vágás legalább két élű, így létezik két élidegen út z -be, ami csak élidegen s - x , s - y utakon keresztül mehet. \square

Jelöljük ezeket az utakat X -szel és Y -nal!

5.12. Lemma. X és Y megválasztható úgy is, hogy D -ben legyen X -től éldiszjunkt s - x , Y -tól pedig éldiszjunkt s - y út.

BIZONYÍTÁS. Vegyünk egy olyan X, Y párt, ahol az X út élei nélkül s -ből elérhető pontok S halmaza nem bővíthető. Tegyük fel, hogy S nem tartalmazza x -et. Ekkor S egy $s - x$ vágás, melynek minden éleit fedi az X út. Vegyünk két, S -ből x -be menő utat. Ezek első éleit is fedi X , így, ha X -et úgy módosítjuk, hogy e két él közül a korábban elért élnél az $S - x$ úton haladjon tovább, olyan új X' $s - x$ sétát kapunk, amely a másik $S - x$ út első éleit nem használja. A bevett élek mind S -en kívüliek, ezért Y -tól is éldiszjunktak. X' -ből élek elhagyásával jó utat kapunk, ugyanakkor S bővebb lett. Mivel közben Y nem változott, ugyanezt rá is elmondva egyszerre kaphatunk megfelelő útpárt. \square

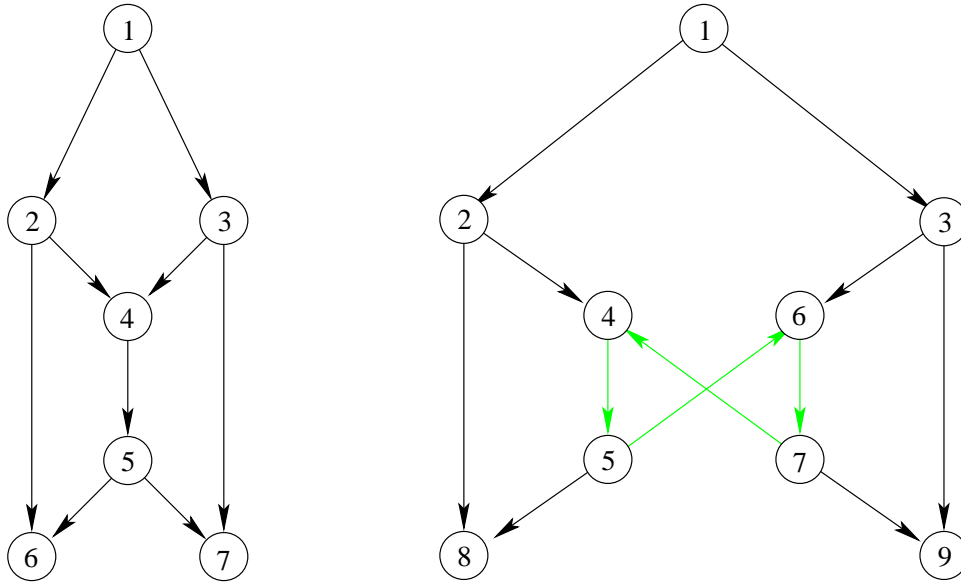
Az állításbeli élfüggetlen feszítőfenyők eléréséhez vegyük az x_1-y_2 ill x_2-y_1 utak egyesítését, és a két befokú csúcsok közül hagyjuk el az y_2 ill. x_2 -beli élt. Az így kapott fenyők könnyen láthatóan jók lesznek (pl. az x csúcsba menő két út közül csak x_2 módosul, és csak y_1 -beli, azaz x_1 -től éldiszjunkt élek kerülhetnek hozzá). Ezzel az állítást beláttuk. \square

5.13. Megjegyzés. A bizonyításban kapott két fenyőnek csak x_2 és y_2 ágakon lehet közös éle. Ha ez nem egyetlen él, feltehető hogy a közös éleket ellentétes sorrendben érinti a két út. Attól függően, hogy hány közös éle van a két útnak kapunk egy-egy "alapgráfot", melyek valamelyikét az állítás feltételeit teljesítő gráfok mindegyike tartalmazza (úgy értve, hogy az élek összehúzhatók). Az egy ill. két közös él esetén kapott gráfokat mutatja a 5.1 ábra. Érdekes, hogy ez a két gráf hálózati kódolásról szóló fejezetekben is többször felbukkant (például 2.2 és 3.3ábra).

5.14. Megjegyzés. A fenti két lemmát összevetve látható, hogy tulajdonképpen olyan x_1, x_2, y_1, y_2 utak létezését bizonyítottuk, ahol $x_1-x_2, y_1-y_2, x_1-y_1$ párok rendre éldiszjunktak. Ennek általánosítása az alábbi állítás.

5.15. Tétel. *Egy $D = (V, A)$ irányított gráfban az x és y csúcsokba vezet két illetve k élidegen út az s csúcsból. Ekkor léteznek x_1, x_2 s -ből x -be és y_1, \dots, y_k s -ből y -ba menő utak oly módon, hogy az egyes csúcsokba menő utak, valamint az x_1, y_1, \dots, y_{k-1} utak éldiszjunktak.*

BIZONYÍTÁS. Az előző bizonyítás 1. lemmájához hasonlóan könnyen látható, hogy léteznek x_1, y_1, \dots, y_{k-1} éldiszjunkt utak. Az x_2 út létezésének bizonyítása is a 2.lemmájéhoz hasonlóan történik. Tegyük fel, hogy a jelenlegi y_1, \dots, y_{k-1} utakhoz nem választható éldiszjunktan egy k . út. Ez azzal ekvivalens, hogy az s -ből ezen utak élei nélkül elérhető pontok S halmaza nem tartalmazza y -t. Ekkor az S egy $s - y$ vágás, melynek minden élét fedi a fenti $k - 1$ út valamelyike. Vegyünk k db $S - y$ utat (jelölje ezeket l_1, \dots, l_k). Ekkor tekinthetjük az l_1, \dots, l_k utak első éleit (jelölje ezeket e_1, \dots, e_k). Az y_1, \dots, y_{k-1} utakat úgy fogjuk módosítani,



5.1. ábra. A két legegyszerűbb alapgráf, x_2 és y_2 egy ill. két közös éle esetén (a zöld élek mutatják, hogy a második gráf nem aciklikus)

hogy csak az l_i utakból veszünk be éleket, ily módon (mivel x_1 nem lép ki S -ből) az utak x_1 -től továbbra is éldiszjunktak lesznek. Minden y_i út minden l_j utat részutakban metsz. Legyen az y_i út **metszési száma** (m_i) az l_j utakkal vett metszeteinek száma. Úgy fogjuk az utakat módosítani, hogy a feltételek megőrzése mellett valamelyik út metszési száma csökkenjen, a többi ne változzon. Tekintsük egy állapotban az egyes l_j utak utolsó metszéseit az y_i utakkal. Feltehető, hogy ezen metszetutak y -ban végződnek, hiszen ha egy l_j -t utoljára metsző y_i utat l_i -n folytatunk, az továbbra is éldiszjunkt lesz a többi úttól. Abban az esetben, ha van egy y_i út, amely két l_j útnak is az utolsó metszése, a korábban folytatva y_i -t az új y_i út metszési száma csökken. Mivel azonban k darab l_j út van, de csak $k - 1$ darab y_i út, a metszési számok mindaddig csökkenthetők, amíg minden l_j út metszi valamelyik y_i -t. Végül kapunk egy olyan l_j -t, amely nem metszi semelyik utat sem, azaz a hozzá tartozó e_j él fedetlen lett, s az S halmaz ezzel az éllel bővült. \square

5.16. Megjegyzés. A fenti állítás a következő formában is írható: Ha $\lambda(s, x) = k$, $\lambda(s, y) = l$, $k \leq l$, akkor minden $0 \leq i \leq k - 1$ -re léteznek olyan x_1, \dots, x_i, x_{i+1} és $y_1, \dots, y_{l-i}, y_{l-i+1}$ x -be és y -ba menő utak, melyekre az azonos csúcsba menő utak mellett az $x_1, \dots, x_i, y_1, \dots, y_{l-i}$ utak is éldiszjunktak.

5.2.2. Élfüggetlen Steiner fenyők

Whitty tételének élfüggetlen megfelelője nem túl érdekes, hiszen az Edmonds éldiszjunkt fenyőfelbontási tételéből következik. Terminálhalmaz esetén viszont értelmes a kérdés, sőt, igaz is. Az állítás bizonyítása után derült ki, hogy ezt már Loukas Georgiadis és Robert E. Tarjan is bebizonyították [15]-ben.

5.17. Definíció. $D = (V + s, A)$ s gyökerű irányított gráf, $T \subseteq V$ terminálhalmaz esetén egy T -t feszítő s gyökerű fenyőt **Steiner fenyőnek** nevezzük.

5.18. Tétel. $D = (V + s, A)$ s gyökerű irányított gráf, $T \subseteq V$ terminálhalmaz, melynek minden t elemére $\lambda(s, t) \geq 2$. Ekkor van a gráfban két élfüggetlen, s gyökerű Steiner fenyő.

BIZONYÍTÁS. Feltehető, hogy T az összes olyan csúcsot tartalmazza, amelybe vezet két élidegen út s -ből. Az állítást a csúcsok számára menő indukcióval fogjuk bizonyítani. Egy csúcsú gráf esetén az állítás semmitmondó. Tegyük fel, hogy $n - 1$ méretű gráfra igaz az állítás, de n -re már nem, és vegyünk egy minimális élszámú n csúcsú ellenpéldát. Így a nem terminálbeli pontok befoka egy, a termináloké kettő. Vegyük észre, hogy a terminálokat feszítő fenyők létezéséből következik az egész V -t feszítő, T -n független fenyők létezése. A továbbiakban ilyen fenyőket keresünk.

5.19. Lemma. Ha van a terminálpontok között olyan, amelybe nem megy két pontdiszjunkt út, az állítás igaz.

BIZONYÍTÁS. Vegyünk egy x csúcsot, amely valamely t terminált elvág s -től. Tekintsük az összes elvágott pont M halmazát, vagyis az összes olyan pontot,

mely x törlésével nem lesz s -ből elérhető (x -et nem vesszük be M -be). Húzzuk össze M -et egyetlen m ponttá, majd hagyjuk el egy kivétellel az összes xm élt. A keletkező gráf legyen D' . Az indukciós állítást alkalmazva külön-külön keresünk $M + x$ -ben és D' -ben feszítő fenyőket, majd ezeket összerakva kapunk D -re jó felbontást.

$M + x$ felbontása: Vegyük észre, hogy mivel t -be megy két élidegen út s -ből, x -be is kell, hogy menjen, vagyis x maga is terminálpont. Így, az $M + x$ gráfot mint x gyökerű gráfot tekintve, $M + x$ termináljainak halmaza (vagyis ahova megy két élidegen út x -ből) éppen $T \cap M$. Mivel s nem szerepel ebben a gráfban, a csúcsok száma kisebb, mint D -ben, vagyis alkalmazható rá az indukciós állítás. A kapott két fenyő függetlenül feszíti $T \cap M$ -et.

D' felbontása: Az összehúzás nem csökkent az M -en kívüli terminálok halmazán, mivel pontok összehúzása nem csökkent az élösszefüggőségen, így legfeljebb az xm élek törlése csökkenthetne, de mivel egy él maradt (amely M definíciója miatt nem lehet elvágó), nem keletkezhetett terminált elvágó él. Ha $|M| > 1$, D' -ben kevesebb csúcs van, mint D -ben, így erre is alkalmazható az indukciós állítás. Ha $|M| = 1$, akkor $M = \{t\}$, és D' -t az egyik xt él törlésével kaptuk. Ebben az esetben csökkent az élek száma, tehát D' nem lehet ellenpélda, így felbontás ebben az esetben is van.

Most vegyük a két gráf két-két élfüggetlen fenyőjét, és tetszőlegesen rakjuk őket két párba. Egy $M + x$ -et és egy D' -t feszítő F_M és $F_{D'}$ fenyőhöz rendeljük azt a D -t feszítő fenyőt, melynek élei $(F_{D'} - xm) \cup F_M$. Ez valóban D -t feszítő fenyő lesz. Már csak azt kell belátni, hogy élfüggetlen a párjától. Ez x -re és így az M -beli terminálokra nyilvánvalóan igaz. Mivel D' -ben minden terminál legfeljebb egyszer használhatta m -et, legfeljebb egy út módosul, s mivel nem D' -beli élekkel bővül, a függetlenség megmarad. \square

Feltehető tehát, hogy a gráfban minden két éldiszjunkt úttal elérhető út pontdisz-

junktakkal is elérhető. Tekintsük a nem terminál (egy befokú) pontok halmazát. Ha két ilyen pont között menne él, azokat összehúzza kisebb ellenpéldát kapnánk. Tehát feltehető, hogy a nem terminálbeli pontok halmaza stabil. Ezen pontok módosításával kétszeresen pontösszefüggő gráffá fogjuk tenni D -t. Azon egy befokú pontokat, melyek őse nem s , töröljük ki a gráfból, és gyerekeinek új őse legyen a pont őse. Az s ősű pontokba egyszerűen vezessünk még egy élt s -ből. A keletkező gráf kétszeresen pontösszefüggő lett, mivel a terminálok útjain csak csökkent a csúcsok száma, a megmaradó nem terminálok pedig terminálok lettek. A kapott gráfra tehát alkalmazható Whitty tétele (5.2.). A két pontfüggetlen feszítő fenyő pedig két élfüggetlen fenyőnek felel meg az eredeti gráfban. \square

5.20. Megjegyzés. A [15]-ben szereplő bizonyítás a mélységi keresés tulajdonságait használva találja meg a két fenyőt.

5.21. Megjegyzés. Whitty eredeti tételéhez hasonlóan itt is megadható a pontok egy sorrendje, melyből a felbontás azonnal kiolvasható. Vegyük észre, hogy 5.2.-ben a bal ill. jobb irányú fenyők létezéséhez csak annyi kellett, hogy ha egy csúcsból indul él tőle jobbra, akkor menjen bele balról és fordítva. Ezt a feltételt fogjuk megtartani.

5.22. Állítás. *A $D = (V + s, A)$ s gyökerű irányított gráfban minden pont befoka az s -ből odavezető éldiszjunkt utak száma, de legfeljebb kettő. Ekkor létezik a pontoknak egy v_0, v_1, \dots, v_m sorrendje, melyben*

(i) $v_0 = v_m = s$

(ii) az elvágó pontok kétszer szerepelnek, minden más pont egyszer

(iii) az egy befokú pontok bemenő élei kétszer szerepelnek, minden más él egyszer

(iv) ha p elvágó pontra $v_i = v_j = p$, ahol $i < j$, akkor v_i -be megy él balról, v_j -be jobbról, és a p által elvágott pontok közöttük vannak a sorban.

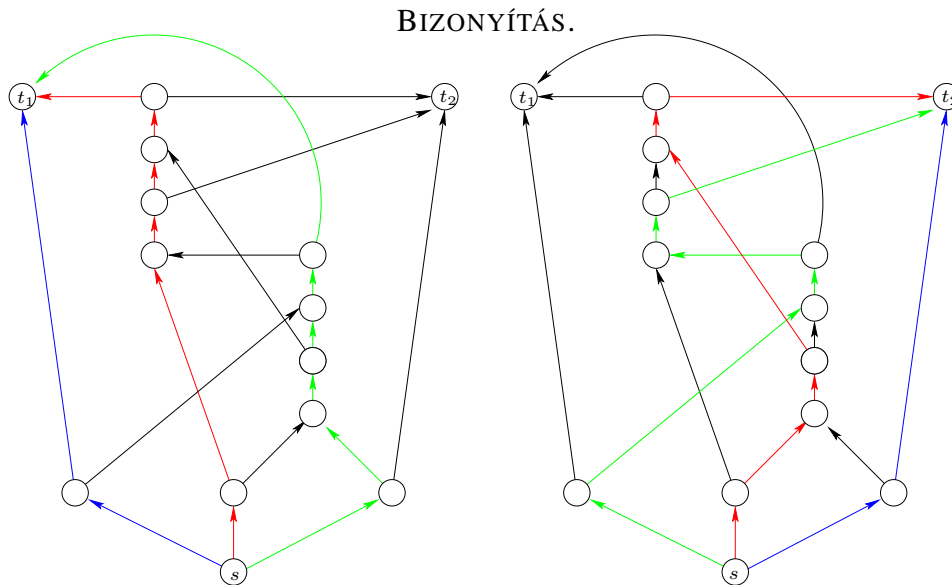
(v) minden más pontba egy él megy jobbról, egy balról. getlen fenyős változattal.

BIZONYÍTÁS. A fenti bizonyítás menetét követve teljes indukcióval bizonyítunk. Feltehető, hogy az egy befokú pontok stabil halmaza alkotnak. Terminált elvágó x pont létezése esetén a bizonyításban kapott két kisebb gráfra alkalmazva az indukciós állítást (a független fenyőkhöz hasonlóan) a sorrendek is összeilleszthetők, hiszen x mindkét gráfban elvágó pont. Ha nincs terminált elvágó pont, a bizonyításban használt transzormációval az egy befokúakat megszüntetve a kapott kétszeresen pontösszefüggő gráfban tekinthető a Whitty tétele során bizonyított pontsorrend, melyből megfelelő sorrend kapható az eredeti gráfban: az egy befokúakat az ősök két példánya közé téve könnyen ellenőrizhetően jó sorrendet kapunk. \square

Egy ilyen sorrendben a jobbra ill. balra menő élek élfüggetlen feszítő fenyőket adnak, ehhez elég a kétszer szereplő élekről belátni, hogy nem szerepelhetnek ugyanazon csúcs két jobb és bal útjában is. Ezek az élek éppen az egy befokú csúcsok bemenő élei. Mivel feltettük, hogy az egy befokúak stabil halmaza alkotnak, elvágó pontok sem lehetnek, ezért a sorban egyszer szerepelnek. Így a bemenő él két példánya akkor szereplhetne egy csúcs két útjában, ha azok kereszteznék egymást. Nem elvágó pontnál ez nyilván nem lehet, elvágó pont esetében pedig a (iv) feltétel miatt nem.

Kettőnél több út esetén nem igaz az állítás. Ez könnyen látszik abból, hogy ha igaz lenne, a 5.25. állításból a pontfüggetlen megfelelője is igaz lenne, de annak speciális esete a $T = V$ független feszítőfenyő keresése, melyre Huck adott ellenpéldát [13]. Aciklikus gráf esetén viszont még lehetne igaz az állítás, ám az alábbi ellenpélda mutatja, hogy ebben az esetben Steiner fenyőknél kevesebb igaz, mint pontfüggetlen feszítőfenyőknél.

5.23. Állítás. *Van olyan aciklikus irányított gráf, melyben egy T terminálhalmaz minden pontjába vezet három élidegen út s -ből, mégsem lehet kiválasztani három élfüggetlen, s gyökerű Steiner fenyőt.*



5.2. ábra. Példa aciklikus gráfra, melyben nem létezik három élfüggetlen Steiner fenyő

Az 5.2 ábrán látható gráfban a terminálhalmaz két csúcsból áll. Könnyen ellenőrizhetően mindkettőbe csak egyféleképpen választható ki három élidegen út s -ből, így, ha létezne három élfüggetlen fenyő, azok ezen utakból tartalmoznának kettőt-kettőt. Egy $s - t_1$ és egy $s - t_2$ út pontosan akkor alkot együtt fenyőt, ha legfeljebb egy, s -ből induló útszakaszban találkoznak. Emiatt a t_2 -be menő piros és zöld út is csak a kék t_1 -be menő úttal lehetne párban. \square

5.2.3. Él- és pontfüggetlenség kapcsolata

Whitty tételének általánosítása az alábbi állítás, melyben az összes csúcs helyett csak egy terminálhalmazt feszítő független fenyőket keresünk.

5.24. Állítás. $D = (V + s, A)$ s gyökerű irányított gráf, $T \subseteq V$ terminálhalmaz, melynek minden pontjába vezet két pontdiszjunkt út s -ből. Ekkor van a gráfban

két pontfüggetlen, T -t feszítő s gyökerű fenyő.

5.25. Állítás. Az 5.18. állításból következik az 5.24. állítás.

BIZONYÍTÁS. Húzzuk szét D minden csúcsát egy-egy éllé, azaz $v \in V$ helyett vegyük a v_1, v_2 csúcsokat, ahol v_1 -ből megy él v_2 -be, v ősei v_1 ősei, v gyerekei v_2 gyerekei. Könnyen látható, hogy ha az eredeti gráfban x -be ment két pontdiszjunkt sx út, az új gráfban x_1 -be megy két éldiszjunkt út, s az új gráf két éldiszjunkt útja pontdiszjunktaknak felel meg az eredetiben. Vegyük az új gráfban a régi T terminálhalmazhoz tartozó új T_1 terminálhalmazt. Az előző megállapítás szerint T_1 teljesíti az 5.18. állítás feltételeit, így létezik két, azt élfüggetlenül feszítő fenyő. Ezek képei az eredeti gráfban pontfüggetlenek lesznek. \square

6. fejezet

Összefoglalás, további kérdések

Az 1-4. fejezetekben beláttuk, hogy multicast kódolási feladat esetén időinvariáns lineáris kód létezésének szükséges és elégséges feltétele, hogy $\lambda(s, t) \geq k$ $\forall t \in T$ -re teljesüljön, s polinomiális algoritmust adtunk a kód megtalálására. Megvizsgáltunk néhány multicastnál általánosabb problémát, és mutattunk példát olyan problémára, mely lineáris kóddal nem megoldható, de általánosabb kódokkal igen. Az ellenpélda szoros kapcsolatban állt a nem reprezentálható matroidokkal. További vizsgálatra érdemes e kapcsolat mélyebb kutatása. A dolgozatban nem érintettünk számos, a hálózati kódolásban fontos területet. A gyakorlati alkalmazások többsége *véletlen lineáris kódokat* használ, mely hasonlóan hatékony, és gyorsan számolható [17]. A kódolást lehet tekinteni *irányítatlan* gráfokban is, az irányított esetben bevezetett definíciók könnyen átvihetők erre az esetre, s az itt felmerülő kérdések sok esetben visszavezethetők irányított problémákra [16]. Vizsgálendő kérdés, hogy irányítatlan esetben létezik-e az élgráf egy aciklikus redukciója (irányított esetben láttuk, hogy nem mindig 3.3. ábra). Egy másik széles körben vizsgált terület a *wireless hálózatok* kódolása. Itt egy irányított hipergráf élein keresendő megfelelő kód. Ez annyival szigorúbb, mint az eredeti közönséges gráfos eset, hogy bizonyos éleken meg kell egyeznie az üzeneteknek. Ez a

kérdés hipergráfok nélkül is vizsgálható: a legutóbbi fejezetben éppen ilyen típusú megkötések mellett bizonyítottuk a lineáris kód létezését. Kérdés, hogy az élfüggvények milyen további szigorításával létezik lineáris kód?

Az 5. fejezetben megmutattuk, hogy kétszeresen gyökeresen pontösszefüggő gráfokban létezik két pontfüggetlen feszítő fenyő. Bebizonyítottuk, hogy kettőnél magasabb összefüggőség esetén aciklikus esetben igaz az állítás (a nem aciklikus esetre van ellenpélda [13]). Bebizonyítottuk továbbá, hogy két élfüggetlen Steiner fenyő létezésének szükséges és elégséges feltétele $\lambda(s, t) \geq 2 \forall t \in T, s$ ellenpéldát adtunk a feltétel elégségeségére a $k \geq 3$ esetben. Megmutattuk, hogy az utóbbi tétel következménye a fenti pontfüggetlen feszítő fenyőkről szóló tétel. A tétel egyszerűbb eseteit útfüggetlen útrendszerek keresésével is megoldottuk, melyből egy további útrendszerekről szóló tétel adódott. Vizsgálandó, hogy az eredeti tétel egésze is bebizonyítható-e ezzel a módszerrel. További kérdés, hogy milyen feltétel mellett léteznek élfüggetlen Steiner fenyők a $k \geq 3$ esetben?

Irodalomjegyzék

- [1] R. Ahlswede, N. Cai, S.-Y.R. Li, and R.W. Yeung, *Network information flow*, IEEE Trans. Inform. Theory, IT-46: 1204-1216, 2000.
- [2] P. Sanders, S. Egnér, and L. Tolhuizen, *Polynomial time algorithms for network information flow* 15th ACM Symposium on Parallelism in Algorithms and Architectures, San Diego, CA, 2003.jún.7-9.
- [3] A.R. Lehman, and E. Lehman, *Complexity Classification of Network Information Flow Problems*, Proceedings of the 15th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA), 2004. jan.
- [4] M. Médard, M. Effros, T. Ho, and D. Karger, *On coding for non-multicast networks*, 41st Annual Allerton Conference on Communication Control and Computing, Monticello, Illinois, 2003.okt.
- [5] R. Dougherty, C. Freiling, and K. Zeger, *Insufficiency of linear coding in network information flow*, IEEE Transactions on Information Theory, vol. 51, no. 8, pp. 2745-2759, 2005. aug.
- [6] Randall Dougherty, Chris Freiling, and Kenneth Zeger, *Networks, Matroids, and Non-Shannon Information Inequalities ..* IEEE Transactions on Information Theory 2006.dec.

- [7] L.R. Ford, and D. R. Fulkerson, *Flows in Networks* (Rand Corporation Research Studies Series)
- [8] R. Koetter and M. Medard, *An algebraic approach to network coding and robust networks*, 2001 IEEE International Symposium on Information Theory, Washington, DC, 2001.jún.24-29.
- [9] E. Erez, and M. Feder, *Convolutional Network Codes for Cyclic Networks* Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on Volume , Issue , 27 June-2 July 2004 Page(s): 146 - Digital Object Identifier 10.1109/ISIT.2004.1365183
- [10] Y. Wu , K. Jain, and S.-Y. Kung, *A unification of Edmonds' graph theorem and Ahlswede et al's network coding theorem* 42nd Annual Allerton Conference on Communication, Control, and Computing, 2004. szept.29-okt.1.
- [11] Zongpeng Li, Baochun Li, Dan Jiang, és Lap Chi Lau, *On achieving throughput with network coding* In Proceedings of INFOCOM 2005, 2005. márc.
- [12] R.W. Whitty., *Vertex-disjoint paths and edge-disjoint branchings in directed graphs* Journal of Graph Theory, 11:349-358, 1987.
- [13] A. Huck, *Disproof of a conjecture about independent branchings in k-connected directed graphs* J. Graph Theory 20 (1995) 235-239 05C38 (05C20 05C40)
- [14] A.Huck, *Independent branchings in acyclic digraphs* Discrete Math. 199 (1999) 245-249 05C05 (05C20)
- [15] Loukas Georgiadis, and Robert E. Tarjan, *Dominator Tree Verification and Vertex-Disjoint Paths* In Proc. 16th ACM-SIAM Symp. on Discrete Algorithms, 433-442. old., 2005.

- [16] S.-Y. R. Li, R.W. Yeung, and N. Cai, *Linear network coding*, IEEE Trans.Inform. Theory, IT-49: 371-381, 2003.
- [17] Kamal Jain, Laszlo Lovasz, and Philip Chou, *Building scalable and robust peer-to-peer overlay networks for broadcasting using network coding*, Tech. Rep., Microsoft Research, 2004,