Algebrai kódelmélet[1]

Először csak a kódelméletet (nem feltétlenül algebrait) vizsgáljuk. Mi az, hogy kód?

Az elmélet a következő, az életben előforduló reális problémából származik. Valamilyen információt szeretnénk valamilyen csatornán továbbítani. Ez lehet egy telefonbeszélgetés, Morse jelek, vagy egy számsorozat, amelyet a számítógépes hálózaton küldünk. Sajnos a csatorna, amelyen továbbítunk, kis $p > 0$ valószínűséggel ugyan, de hibázhat. Képzeljük el, hogy egy nagyon hosszú 0–1 sorozatot küldtünk, ilyenkor előfordul, hogy mi ugyan egy helyen 0-t továbbítottunk, de helyette 1-est vettek. Ez sokszor komoly károkat okoz. A kódelmélet olyan módszereket igyekszik kidolgozni, amellyekkel a hiba csökkenthető.

Egy speciális, de talán fontosabb típusa a kódoknak a következő: a nagyon hosszú üzeneteket felbontjuk egyenlő, mondjuk k hosszúságú részekre

$$\underbrace{0,1,\ldots,1}_{k},\underbrace{0,\ldots\ldots}_{k},\underbrace{\ldots\ldots\ldots}_{k}.$$

A számítógépek speciálisan az ún. ASCII kódokat használják. Ez 8 hosszúságú 0–1 sorozatokat hoz létre, és ez összesen $2^8 = 256$ lehetőséget ad. Közülük az első a 0, 0, ..., 0, az utolsó a csupa 1-esből álló 2-es számrendszerbeli szám. Ez a felosztás 0-tól 255-ig minden természetes számot előállít. Tekintsünk egy ilyen természetes számot, és rendeljünk hozzá egy jelet a számítógépen, ezek között szerepelni fognak az ábécé kis- és nagy betűi és sok minden más. Az ASCII kód a hozzárendelésnek amerikai szabvány szerinti, az egész világon elterjedt módja. Az ASCII kód használata a következőt jelenti: pl. írunk egy hosszú, mondjuk 5 oldalas levelet,majd azt a hosszú 0–1 sorozatot, ami a mi információnkat tartalmazza, $k = 8$ hosszúságú részekre osztjuk, s így továbbítjuk. A számítógépen az a 8 hosszúságú sorozat érkezik meg általában, amit továbbítottunk, már csak azért is, mert a beírás és kibocsátás helye közel van egymáshoz. Nem biztos, hogy ez így lenne ez akkor is, ha pl. Új-Zélandba küldenénk jeleket.

Ezért a következő ötletet alkalmazzák: Minden k hosszúságú sorozat helyett vesznek egy $n > k$ hosszúságú sorozatot. Összesen van 2^k darab k hosszúságú és 2^n darab n hosszúságú sorozat.

Ez utóbbiból alkalmasan kiválasztunk 2^k darabot. Szeretnénk ezt olyan ügyesen megtenni, hogy észrevegyük, hogyha hiba történt az n hosszúságú sorozatban (egy-két 0-ból 1-es lett, vagy fordítva) és meg tudjuk mondani, hogy melyik sorozatot akarták küldeni a kiválasztott 2^k sorozat közül.

Ezt alkalmazzuk akkor is, amikor sajtóhibát veszünk észre. Könnyen felismerhetjük, hogy milyen hibát követtek el. Hogyan? Veszünk egy szót, ami közel van a hibás szóhoz, és feltételezzük, hogy azt akarták írni. Fogalmazzuk meg pontosan ezt a közel levést:

Legyen Q egy véges ábécé. Tekintsük azokat n hosszúságú α_1, α_2, ..., α_n sorozatokat, amelyeknek minden eleme Q-ból való. Majd vegyük a Q^n halmazt, az összes olyan n hosszúságú sorozatot, amelynek elemei a Q-ból valók.

Definició:

$$Q^n = \{(\alpha_1, \alpha_2, \ldots, \alpha_n) \mid \alpha_i \in Q\}$$

E halmaz elemeit nevezzük *szavaknak.* Összesen q^n szó van, ahol a q a Q elemszáma.

Definiáljuk két szó távolságát. Legyen x, $y \in Q^n$, $x = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $y = (\beta_1, \beta_2, \ldots, \beta_n)$ A távolságuk jelentse azt, hogy hány helyen különböznek.

Definició:

$$d(x,y) = |\{i|\ \alpha_i \neq \beta_i \qquad 1 \leqslant i \leqslant n\}|$$

Ezen halmaz elemszáma lesz az x, y *távolsága.*

Két szó tehát akkor van közel egymáshoz, ha kevés helyen különbözik. Kérdés, hogy ezt milyen jogon hívom távolságnak? Azért, mert olyan tulajdonságai vannak, mint a térbeli távolságnak.

A térbeli távolság (amely mindig egy nem negatív valós szám), a következő 3 alapvető tulajdonsággal rendelkezik:

(1)	$d(x,y) \in \mathbb{R}$, és $d(x,y) \geqslant 0$	$d(x,y) = 0 \iff x = y.$
(2)	$d(x,y) = d(y,x)$	(szimmetrikus).
(3)	$d(x,z) \leqslant d(x,y) + d(y,z)$	(érvényes rá a háromszög-egyenlőtlenség).

Az ilyen tulajdonságú halmazokat *metrikus tér*nek nevezzük. Ilyen a közönséges tér is.

További példa metrikus térre: vegyünk egy összefüggő nem irányított gráfot. Legyen $d(x,y)$ a legrövidebb x-et y-nal összekötő út hossza.

Feladat. Miért metrikus tér ez? (Itt és Q^n-ben is, a távolság mindig nem negatív egész szám volt.)

A szavak közti távolságot *Hamming-távolságnak* nevezik.

Most foglalkozzunk egy kicsit precízebben azzal, hogy milyen kódot akarunk csinálni.

Q^n-nek egy részhalmazát nevezzük *kód*nak.

[1] Az Ifjúsági Matematikai Körön elhangzott előadás alapján

Definició:

$$C \subseteq Q^n.$$

Jelöljük két C-beli különböző elem távolságának minimumát d-vel.

Definició:

$$d = \min d(x,y) \qquad \text{ahol} \qquad x, y \in C \qquad \text{és} \qquad x \neq y.$$

Tegyük fel, hogy d páratlan $d = 2e+1$. Ha veszek egy n hosszúságú C-beli szót, amelynek elemei a Q-ból valók, és elrontom néhány, de legfeljebb e helyen, akkor még rekonstruálni tudom, hogy mi volt az eredeti szó.

Más szóval, definiáljuk ebben a „geometriában", amit most csináltunk, a gömb fogalmát.

Definíció:

$$S(x,e) = \{y,\ y \in Q^n \mid d(x,y) \leqslant e,\ x \in Q^n\}$$

az x körüli e sugarú *gömb*.

(Ha úgy tetszik, ez egy zárt gömb, de ha úgy tetszik nyílt.) Ebben a gömbben persze x is benne van, a távolság definiciója szerint.

Tehát, ha a C kód minimális távolsága $2e+1$, akkor ha az $S(x,e)$ gömbök egyesítését vesszük, ahol az x végig fut a C kód elemein, akkor

$$S(x_1,e) \cap S(x_2,e) = \emptyset, \quad \text{ha} \quad x_1 \neq x_2,$$

azaz a kódszavak körüli e sugarú gömbök páronként diszjunktak.

Ha kapok egy szót, és tudom, hogy valaki valamelyik kódszót akarta küldeni, akkor, ha a hibák száma kisebb vagy egyenlő e-nél, akkor ez a szó valamelyik egyértelműen meghatározott gömbben van, s akkor azt mondom, hogy annak a középpontjában lévő kódszót akarta küldeni. Ha egyik gömbben sincs benne, akkor egyrészt biztos, hogy e-nél több hiba történt, másrészt nem sokat tudok mondani.

Két dolgot szeretnénk elérni:

1) az e minél nagyobb legyen, vagyis d is, azaz minél több hibát javítson ki a kód,

2) minél hatékonyabb legyen, vagyis minél több eleme legyen: $|C|$ nagy legyen.

E két dolog nyilvánvalóan ellentmond egymásnak. Sok pont körüli nagy sugarú gömböknek már biztos van nem üres metszete.

Érdekes feladat hatékony kódokat csinálni, olyanokat, amelyeknek sok eleme van és sok hibát javítanak ki. Ehhez célszerű, ha a Q elemeinek van valamilyen struktúrája. Ha Q csak a 0-ból és az 1-ből áll, értelmezzünk rá egy összeadást és egy szorzást. Írjuk ezt táblázatba:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Van egy kivonás is, ez az összeadásból származik, és van egy osztás is. Ezekre a műveleteknél szokásos szabályok érvényesek, pl. $(a+b)c = (ac+bc)$ stb., azaz úgy viselkednek, mint a valós számok.

Ha egy halmazban értelmezve van egy összeadás és egy szorzás, ezekre ugyanolyan szabályok érvényesek mint a valós számokra, akkor ezt a halmazt *testnek* hívjuk.

Példák testekre

$\mathbb{R}$	$\mathbb{Q}$	$\mathbb{C}$
valós számok	racionális számok	komplex számok

Az egész számok nem alkotnak testet: az osztás nem végezhető el, azaz két egész szám hányadosa nem mindig létezik a halmazban. Ezeknek a testeknek végtelenül sok elemük van. Persze van más test is: $\mathbb{R}$ és $\mathbb{Q}$ között csak úgy hemzsegnek a testek.

Véges sok elemű testek

Tekintsünk egy tetszőleges p prímszámot, és tekintsük a $0,\ 1 \ldots p-1$ számokat. Lehet értelmezni egy összeadást és egy szorzást közöttük. A probléma nemcsak az, hogy az eredmény nem lesz mindig a számok között. Ezen azonban könnyen tudunk segíteni: ha az eredmény nagyobb $(p-1)$-nél, akkor elosztjuk p-vel, és a maradékot tekintjük az összeadás vagy szorzás eredményének.

Írjuk fel a műveletek táblázatát $p = 3$-ra:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Látjuk, hogy az 1-es és a 0 a szorzásra úgy viselkedik, mint a számok körében. Figyeljünk fel arra, hogy az összeadásnál minden szám minden sorban és oszlopban pontosan egyszer fordul elő. A szorzásnál ez már csak akkor igaz, ha az első sort és oszlopot kitöröljük. Mivel a p-t tetszőlegesnek választhatjuk, és végtelen sok prímszám van, így végtelen sok véges test létezik, ezeket jelöljük $\mathbb{F}_p$-vel.

Kérdés, nincs-e más véges test? De van, és ezek könnyen áttekinthetők, mert érvényesek rájuk a következő tételek.

1. Tétel. *Ha F egy véges test, akkor elemszáma egy prímhatvány, azaz*

$$|F| < \infty \Longrightarrow |F| = q = p^f \qquad f \geqslant 1,\ p \text{ prím.}$$

2. Tétel. *Minden prímhatványhoz található egy véges test, amelyiknek ennyi az elemszáma:*

$$\forall q \quad \text{prímhatványra} \quad \exists!\ F \qquad \text{test, hogy} \qquad |F| = q.$$

($\exists$ jelentése: van olyan, a felkiáltó jel pedig azt jelenti, hogy csak egy van.)

3. Tétel. Minden q prímhatványhoz lényegében csak egy véges test létezik.($\mathbb{F}_q$ egy q elemű véges testet jelent.)

A testek elmélete fontos része az algebrának. Most már látjuk, miért hívják algebrai kódelméletnek azt, amiről most beszélünk. A továbbiakban az ábécé legyen valamelyik véges test. Most már csak ilyen kódokat fogunk vizsgálni.

Ha $Q = \mathbb{F}_q$ véges test, C kód, akkor megkövetelhetem, hogy a kódnak bizonyos jó szerkezete legyen, vagyis

1. ha $x, y \in C \Longrightarrow x + y \in C$.

Mit jelent az $x + y$ összeg? Legyen $x = (\alpha_1, \ldots, \alpha_n)$, $y = (\beta_1, \ldots, \beta_n)$ n hosszúságú sorozat, akkor

$$x + y = (\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n).$$

Itt végül is vektorokról van szó, az összeadást is úgy értelmezzük, mint a vektoroknál.

2. ha $x \in C$ és $\gamma \in \mathbb{F}_q$, tehát γ egy skalár, akkor

$\gamma x \in C$, $\gamma x = (\gamma\alpha_1, \ldots \gamma\alpha_n)$.

Az ilyen kódokat *lineáris kódoknak* nevezzük. A lineáris kódok ún. vektorteret alkotnak, ezzel a lineáris algebra foglalkozik.

A lineáris kódok elemszáma szükségképpen $|C| = q^k$ valamilyen k-ra, ahol $0 \leqslant k \leqslant n$. Ha $k = 0$, akkor az elemszám $q^0 = 1$, s ez a csupa 0-ból álló sorozat. Ha $k = 1$ akkor q darab vektorom van, ami azt jelenti, hogy veszem közülük valamelyiket, (de nem a csupa 0-át), és annak összes skalárszorosát. Általános k-ra és $q = 2$-re visszajutottunk a 2^k esethez.

Feladat. 1. Készítsük el a 4, 8, 9 elemű véges $\mathbb{F}_4$, $\mathbb{F}_8$, $\mathbb{F}_9$ testet. (Vigyázat, itt nem alkalmazhatjuk azt a fogást, amit prímszám esetén alkalmaztunk, vagyis, hogy a maradékot vesszük.) 2. Mitől igaz, hogy minden lineáris kód elemszáma q^k?

Egy lineáris kódnak 4 jellemzője van.

1. n a kódszavak hossza
2. k a kódszavak számában a q kitevője $\qquad [n, k]$-kód
3. d a minimális távolság $\qquad [n, k, d]$-kód
4. q ahány elemű véges test felett dolgozunk. (Ezt bizonyos szempontból adottnak tekintjük, azaz előre elhatározzuk, hogy mi lesz az alaptest.)

Állítás. *Lineáris kód esetén $d \leqslant n - k + 1$.*

Ha k nagy, azaz sok eleme van a kódnak, akkor $n - k + 1$ kicsi (n rögzített), azaz kicsi a minimális távolság. Nem tudjuk elérni, hogy a nagy sugarú gömbök diszjunktak legyenek, hiszen a fenti állítás ekvivalens azzal, hogy $k \leqslant n - d + 1$.

Feladat: Gondoljuk ezt meg!

Az olyan kódokat, amelyeknél egyenlőség áll fenn, MDS-kódoknak hívjuk (maximal distance code).

MDS-kódok

Ideje lenne valamilyen értelemben jó kódokat csinálni. Az egyik értelem, ami szerint a kód jó, ha benne a távolság olyan nagy, amilyen nagy csak lehet.

Egy MDS-kód az ún. Reed–Solomon kód. Ezt valószínüleg mindenki ismeri, csak nem tud róla. A compact discben (CD) ilyen hibajavító kód van. Előnye, hogy nagyon gyorsan lehet kódolni és dekódolni, vagyis k hosszúságú sorozatból n hosszúságút csinálni és viszont. Ez azért fontos, hogy a hang elhangzása előtt még idejében ki legyen javítva a hiba.

Vegyünk egy F_q q elemű véges testet, ahol q egy prímhatvány, és legyen $k < q$, az $n = q$ legyen. q^k darab n hosszúságú kódszót kellene csinálnunk. Keresni kellene valamiket, amikből q^k darab van.

Jelentse $\mathbb{F}_q[x]$ az x-nek összes olyan polinomját, amelyben az együtthatók a q elemű véges test elemei. Ezekkel a polinomokkal ugyanúgy végezhetünk műveleteket, mint a valós együtthatós polinomokkal. Ha azon polinomokat tekintjük ezek közül, amelyeknek a foka kisebb k-nál, vagyis ezt a halmazt:

$$\{\alpha_0 + \alpha_1 x + \ldots + \alpha_{k-1} x^{k-1} |\ \alpha_i \in \mathbb{F}_q\},$$

ezekből pontosan q^k darab van, mert minden α pontosan q értéket vehet fel.

Ha az összes ilyen polinomot veszem, akkor máris rendelkezem egy természetes módon definiált q^k elemű halmazzal.

Hogyan csinálunk ezekből q^k darab olyan kódszót, amelyeknek hossza $n = q$? Legyen $\mathbb{F}_q = \{\omega_0, \omega_1, \ldots, \omega_{q-1}\}$, ha tetszik, választhatjuk az ω_0-t 0-nak, ω_1-et 1-nek, a többit meg valamilyen módon számozottnak.

Vegyünk egy rögzített f polinomot és sorban helyettesítsük be a polinomba a véges test elemeit. A következő q hosszúságú sorozatot kapjuk:

$y_f = \{(f(\omega_0), f(\omega_1), \ldots, f(\omega_{q-1}))\}$; ha ezt az összes q^k darab f-re megcsinálom, megkapom a Reed–Solomon kódot.

Igaz-e, hogy ez egy lineáris kód?

Igen, mert ha f_1 és f_2 két polinom, akkor az összegük is egy legfeljebb $(k-1)$-ed fokú polinom lesz, és az összeg helyettesítési értéke a tagok helyettesítési értékének az összege lesz. Az is igaz, hogy egy polinom skalárszorosa is egy ugyanolyan fokú polinom (ha nem 0-val szorzunk), és ennek helyettesítési értéke az eredeti helyettesítési érték skalárszorosa.

Mennyi ebben a kódban a minimális távolság? Azt tudjuk, hogy $d \leqslant n-k+1$. Most bebizonyítjuk, hogy $d \geqslant n-k+1$, s ebből következik az egyenlőség.

Vegyünk két polinomot, és írjuk fel különbségüket. Legyen ennek a foka $l \leqslant k-1$, hiszen f_1 és f_2 mindegyike legfeljebb $(k-1)$-ed fokú. Vizsgáljuk meg a különbségek távolságát; ha $f_1 - f_2$ foka l, akkor $d(y_{f_1}; y_{f_2}) \leqslant n-l$, azaz bármely két különböző f_1 és f_2-höz tartozó sorozat sok helyen tér el.

Ugyanis az $\mathbb{F}_q$-beli együtthatós polinomok körében is igaz, hogy egy polinomnak legfeljebb annyi gyöke van, ahányad fokú. Ez a valós együtthatós polinomok körében abból adódik, hogy minden gyök esetén le lehet választani egy elsőfokú tényezőt, s akkor mindig egy 1-gyel alacsonyabb fokú polinomot kapunk. S mindez csak azon múlik, hogy a polinomok együtthatói testet alkotnak. Itt is igaz az, hogy $f_1 - f_2$ gyökeinek száma $\leqslant l$. Hány olyan hely van, ahol megegyezhet az y_{f_1} és az y_{f_2}? Ahol megegyezik, ott az $f_1 - f_2$-nek egy gyöke van, ez legfeljebb l helyen fordulhat elő, tehát legalább $n-l$ helyen eltérnek, azaz a távolság legalább $n-l$, s ezt állítottuk.

Tekintve, hogy $l \leqslant k-1$, $n-1 \leqslant n-k+1$, s ez az előzőekkel összevetve adja, hogy a minimális távolság egyenlő $(n-k+1)$-gyel.

Bináris Hamming-kód

Most egy másik módszer szerint definiálunk egy kódot. A $q = 2$ esetére válasszunk valamilyen $r \leqslant$ 1-et. Föl szeretnénk sorolni az összes r hosszúságú 0–1 sorozatot, azaz a kettes számrendszerbeli számokat 1-től $(2^r - 1)$-ig. (A 0-t kihagyjuk.) $r = 3$-ra foglaljuk táblázatba.

$$H = \begin{array}{|c|c|c|c|c|c|c|} \hline 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ \hline 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ \hline 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ \hline \end{array}$$

Az oszlopok tartalmazzák a számokat nagyság szerinti sorrendben. A sorok hossza $n = 2^r - 1$, esetünkben $n = 7$. Ezt a táblázatot használva következőképpen definiáljuk a bináris Hamming-kódot: azok a 0–1 sorozatok, amelyeket ha vektoroknak tekintjük, merőlegesek erre a 3 vektorra (a táblázat 3 sorára). Azt már elfogadtuk, hogy ezek a sorozatok vektorok és két vektor merőlegességét a skalárszorzat segítségével definiáljuk. Akkor mondunk 2 vektort merőlegesnek, ha skalárszorzatuk 0-val egyenlő. A skalárszorzat definíciója:

$$(x, y) = \sum_{i=1}^{n} \alpha_i \beta_i.$$

A skalárszorzat itt is rendelkezik a vektoroknál szereplő tulajdonságokkal. Ha egy vektor merőleges mindhárom vektorra, és egy másik vektor is merőleges rá, akkor az összegük is és a skalárszorosuk is az. Jelöljük az előzőhöz hasonló táblázatot H-val. H minden sorára merőleges vektorok alkotják a $\mathcal{H}$ kódot.Ez egy lineáris kód, és könnyen belátható, hogy $k = 2^r - r - 1$. Ugyanis a vektorokból összesen q^{2^r-1}, esetünkben 2^{2^r-1} van. r merőlegességi feltétel van, s ezek „függetlenek”.

Mindegyik feltételnek külön-külön a vektorok fele tesz eleget, így r-szer feleződik, azaz a kód elemszáma: $2^k = \frac{2^{2^r-1}}{2^r} = 2^{2^r-r-1}$, vagyis $k = 2^r - r - 1$.

A $\mathcal{H}$ kódok gyakorlati alkalmazása az űrhajózásban van.

Van egy másik tulajdonsága is a $\mathcal{H}$ kódnak. Mivel $d = 3$ (ez legyen feladat), az 1 sugarú gömbök páronként diszjunktak. Hány gömb van? Ahány kódszó, azaz 2^{2^r-r-1}. Definiáljuk a gömb térfogatát. Egy gömb térfogata annyi, ahány pont van benne. Van egy középpont, $x = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, és ez benne van, és ezen kívül mindazok a pontok, amelyek tőle valamelyik helyen különböznek. Ilyen hely $2^r - 1$ van. Ha ezeket összeszorzom $(2^{2^r-r-1})(2^r - 1 + 1) = 2^{2^r-1}$, de ennyi pont van összesen ebben a térben. Ezek tehát olyan páronként diszjunkt gömbök, amelyek egyesítése az egész tér. Az ilyen kódokat *perfekt kódnak* nevezzük.

Páronként diszjunkt gömbökből minél többet elhelyezni a 3 dimenziós közönséges térben egy eddig megoldatlan probléma. A görögdinnye-árusok tapasztalatból tudják, hogy lehet egy térfogatba a legtöbb dinnyét lerakni. Elöször csinálnak egy négyzetrácsot, majd a következő szinten elkezdik a lyukakat kitölteni. Valószínűleg ez a legsűrűbb gömbelhelyezés, de ez nincs bebizonyítva.

Érdekes megemlíteni, hogy a 24-dimenziós euklidészi térben (tehát a korábbi jelöléssel $\mathbb{R}^{24}$-ben) van egy meglepően sűrű gömbelhelyezés, és ennek megtalálásában is az algebrai kódelmélet segített. A 2 elemű test feletti 24 hosszúságú vektorok terében van $[n, k, d] = [24, 12, 8]$ paraméterekkel rendelkező kód, az ún. Golay-kód: G_{24}. Ennek segítségével lehet a 24-dimenziós euklidészi térben egy sűrű gömbelhelyezést csinálni. A Golay-kód sok tekintetben jelentős. Ha elhagyjuk minden vektor utolsó elemét, egy $[n, k, d] = [23, 12, 7]$ paraméterű kódot kapunk: G_{23}-at (ezt is Golay fedezte fel). $d = 7$ azt jelenti, hogy $d = 2e + 1$, ahol $e = 3$. Tehát ez a kód 3 hibát javít. És ez a kód perfekt! (Ezt mindenki maga ki tudja számolni.)

Van egy másik perfekt Golay-kód is, mégpedig a 3-elemű test feletti. Zárjuk a cikket Tietäväinen és van Lint egy híres eredményével: Ha $|Q| = q$ prímhatvány és C egy nem-triviális perfekt e-hibajavító kód, ahol $e > 1$, akkor C a két perfekt Golay-kód egyike. (kérdés: mik a triviális perfekt kódok $e > 1$-re?)