Capítol 2

Taxa d'informació

La taxa d'informació, com a paràmetre que mesura l'eficiència de l'esquema per a compartir secrets, ha estat àmpliament estudiat en les dues vessants següents:

- caracterització de les estructures ideals
- fitació de la taxa d'informació òptima

La qüestió de caracteritzar les estructures ideals és un problema encara obert. Hem fet un breu resum en el Capítol 1 dels resultats que relacionen les estructures ideals i els matroides. Alguns resultats s'han donat per a famílies particulars d'estructures d'accés.

Pel que fa a la qüestió de fitar la taxa d'informació, s'han trobat resultats per famílies d'estructures, com són les estructures definides per grafs, que ja hem comentat al Capítol 1. També existeixen resultats vàlids per a qualsevol estructura d'accés, com és la fita inferior de la taxa d'informació òptima donada per l'esquema circuital.

Nosaltres hem estudiat famílies d'estructures d'accés que responen a situacions bastant reals, o si més no, són famílies bastant àmplies: les estructures definides amb pesos i llindar, les estructures bipartites, el cas particular d'estructura bipartita definida per dos pesos i llindar, i les estructures homogènies. La nostra anàlisi ha anat dirigida cap el càlcul de fites superiors i inferiors després de fer un estudi de l'estructura d'accés com a estructura combinatòria. També ens hem ocupat de la caracterització de les estructures ideals a la família de les estructures bipartites.

2.1 Estructures definides per pesos i llindar

A l'article fundacional de la teoria dels esquemes per a compartir secrets [83], Shamir proposa com a estructura més complexa que una estructura de llindar els esquemes definits amb pesos i llindar. Curiosament després d'aquesta definició no s'ha fet cap proposta ni estudi al voltant d'aquestes estructures. Aquestes estructures són una generalització de les estructures de llindar. En aquest tipus d'estructures d'accés hi ha una jerarquia entre els participants donada per un pes assignat a cadascun d'ells, de forma que un subconjunt és autoritzat quan la suma dels pesos dels seus participants és almenys el llindar. És en aquest treball on es fa una primera proposta d'esquema per aquest tipus d'estructura: a partir d'un esquema de llindar, s'assigna a cada participant tants fragments com pes tingui. Tot això en la suposició de tenir pesos naturals. Nosaltres hem estudiat les estructures definides amb pesos i llindar en general, trobant que són definibles sempre per pesos i llindar naturals. Pel cas definible mitjançant un graf aconseguim caracteritzar-les trobant els pesos i llindar mínims que la defineixen. Per a aquestes trobem una fita inferior per a la taxa d'informació òptima. També trobem una àmplia família d'estructures definides per pesos i llindar que no són representables per un graf però que el seu dual sí, de forma que determinem els pesos i llindar mínims que la defineixen.

Donat un conjunt de n participants P, un llindar $t > 0$ i una funció $\omega : P \to \mathbb{R}$ que assigna un pes $\omega(p) \geq 0$ per a cada participant, la (t, n, ω)-*estructura d'accés definida per pesos i llindar* consisteix en tots els subconjunts $A \subset P$ tals que $\omega(A) = \sum_{p \in A} \omega(p) \geq t$.

Evidentment hi ha estructures d'accés que no es poden definir mitjançant pesos i llindar. Per exemple, en el conjunt $P = \{A, B, C, D\}$, l'estructura d'accés Γ amb base $\Gamma_m = \{\{A, B\}, \{B, C\}, \{C, D\}\}$ no és definible per pesos i llindar. En efecte, com que $\{A, B\} \in \Gamma$, però $\{D, B\} \notin \Gamma$ obtenim que $\omega(A) > \omega(D)$. De la mateixa manera $\omega(D) > \omega(A)$ ja que $\{C, D\} \in \Gamma$ i $\{A, C\} \notin \Gamma$, afirmació contradictòria amb l'anterior.

Les estructures d'accés definides per pesos i llindar han estat definides amb $t, \omega(p) \in \mathbb{R}$. A la proposició següent, provem que qualsevol estructura d'accés definida per pesos i llindar pot ser definida amb pesos i llindar naturals.

Proposició 2.1.1 *Per a qualsevol (t, n, ω)-estructura d'accés definida per pesos i llindar, existeixen $t' \in \mathbb{N}$ i $\omega' : P \to \mathbb{N}$ tals que l'estructura d'accés definida per t i ω és igual a la definida per t' i ω'.*

Demostració: Sigui $\Gamma = \{A \subset P \,|\, \omega(A) \geq t\}$ l'estructura d'accés definida per t i ω. Considerem $\epsilon = \min\{t - \omega(A) \,|\, A \notin \Gamma\} > 0$. Considerem també $\overline{t} \in \mathbb{Q}$ tal que $t - \epsilon/2 < \overline{t} \leq t$ i per a qualsevol $p \in P$, $\overline{\omega}(p) \in \mathbb{Q}$ tal que $\omega(p) \leq \overline{\omega}(p) < \omega(p) + \epsilon/(2n)$. No és difícil veure que

$$\Gamma = \{A \subset P \,|\, \overline{\omega}(A) \geq \overline{t}\}$$

D'aquesta manera obtenim un llindar t' i pesos $\omega'(p)$ els quals són nombres naturals amb $\Gamma = \{A \subset P \,|\, \omega'(A) \geq t'\}$ multiplicant $\overline{t}$ i $\overline{\omega}(p)$ pel mínim comú multiple dels seus denominadors.□

Les estructures d'accés definides per pesos i llindars van ser considerades per primera vegada per Shamir [83] com a generalització del seu esquema de llindar. El (t, n, ω)-esquema definit per pesos i llindar, amb $t, \omega(p) \in \mathbb{N}$, proposat per Shamir s'obté d'un esquema de llindar (t, m), on $m = \omega(P) = \sum_{p \in P} \omega(p)$. Cada participant $p \in P$ rep $\omega(p)$ fragments diferents corresponent a $\omega(p)$ participants del (t, m)-esquema de llindar. Si hem utilitzat un esquema de llindar (t, m) ideal, la taxa d'informació del (t, n, ω)-esquema de llindar definit per pesos i llindar construït d'aquesta manera té $\rho = 1/W$, on $W = \max\{\omega(p) \,|\, p \in P\}$.

2.1.1 Caracterització de les estructures d'accés definides per pesos i llindar de rang dos

En aquest apartat trobarem la forma de totes les estructures d'accés definides per pesos i llindar de rang dos, és a dir, que es poden expressar mitjançant grafs.

El pes de qualsevol participant d'una estructura d'accés definida per pesos i llindar que individualment forma un subconjunt autoritzat minimal pot ser agafat igual al llindar. D'altra banda, podem posar $\omega(p) = 0$ per a qualsevol participant que no pertany a cap subconjunt autoritzat minimal. Considerarem només estructures d'accés sense aquestes dues classes de participants, perquè el seu paper no és rellevant.

Per tant nosaltres ens hem concentrat en l'estudi de les estructures d'accés de rang dos homogènies i connectades. Com hem dit abans, una estructura d'accés d'aquest tipus pot ser representada per un graf sense vèrtexs aïllats. Recordem que el significat d'estructura connectada és el d'una estructura tal que tots els participants estan en algun minimal, concepte diferent del d'una estructura definida per un graf connectat. El conjunt de vèrtexs d'aquest graf és P i la base Γ_m és el conjunt d'arestes.

Sigui $t > 0$ un llindar i $\omega : P \to \mathbb{N}$ una funció de pesos que defineix una estructura d'accés Γ homogènia i connectada de rang dos. Sigui G el graf que representa Γ. No és difícil veure que un vèrtex de G amb pes màxim és adjacent cap a qualsevol altre vèrtex. Per tant el graf G és un graf connectat. En general, existeix un conjunt $C \subset P$ de vèrtexs adjacents cap a qualsevol altre vèrtex. De fet, C és el *centre* del graf G i els vèrtexs de C són anomenats *centrals*. És clar que el pes d'un vèrtex central és més gran que el pes de qualsevol vèrtex no central. D'altra banda, si $C \neq P$ i eliminem els vèrtexs centrals de G, apareixerà un conjunt de vèrtexs aïllats, $A \subset P$. Aquest conjunt A de vèrtexs aïllats és no buit ja que almenys conté el vèrtex de pes mínim. Això darrer és cert perquè tots els vèrtexs adjacents a un de pes mínim són centrals. Aquests vèrtexs, els quals són adjacents només amb els vèrtexs centrals, els anomenarem *subordinats*. El pes dels vèrtexs de A és més petit que el pes dels altres vèrtexs.

En el subgraf de G induït per $P' = P - (C \cup A)$ no hi ha vèrtexs aïllats. Si $P' \neq \emptyset$, la restricció de l'estructura d'accés Γ a P', $\Gamma' = \{B \subset P' \,|\, \omega(B) \geq t\}$, és connectada. Això és, obtenim una nova estructura d'accés definida per pesos i llindar, connectada, homogènia de rang dos després d'esborrar els vèrtexs centrals i els subordinats.

Teorema 2.1.2 *Sigui G un graf que representa una estructura d'accés Γ definida per pesos i llindar connectada i homogènia de rang dos. Aleshores, existeix una única partició dels vèrtexs de G,*

$$P = C_1 \cup A_1 \cup C_2 \cup A_2 \cdots \cup C_k \cup A_k,$$

on $C_i \neq \emptyset$ per $i = 1, \ldots, k$, $A_i \neq \emptyset$ si $i = 1, \ldots, k-1$ o bé $A_k = \emptyset$ i $|C_k| \geq 2$ o bé $|A_k| \geq 2$, tal que el conjunt d'arestes de G és

$$\Gamma_m = \{\{u, v\} \,|\, u, v \in \bigcup_{i=1}^{k} C_i,\ u \neq v\} \cup \{\{v, p\} \,|\, v \in C_i, p \in A_j,\ 1 \leq i \leq j \leq k\}.$$

Demostració: Els conjunts C_i i A_i es troben amb l'algorisme següent:

1. Posa $i = 1$, $P_1 = P$, $\Gamma_1 = \Gamma$ i $G_1 = G$.

2. Esborra de P_i el conjunt C_i de vèrtexs centrals de Γ_i. Si $P_i - C_i = \emptyset$, posa $k = i$, $A_k = \emptyset$ i acaba.

3. Esborra de $P_i - C_i$ el conjunt A_i de vèrtexs subordinats de Γ_i. Els vèrtexs de A_i són els vèrtexs aïllats en el subgraf de G_i induït per $P_i - C_i$. Si $P_i - (C_i \cup A_i) = \emptyset$, posa $k = i$ i acaba.

4. Posa $P_{i+1} = P_i - (C_i \cup A_i)$, sigui G_{i+1} el subgraf de G_i induït per P_{i+1} i sigui Γ_{i+1} l'estructura d'accés en P_{i+1} definida pel graf G_{i+1}. Posa $i = i + 1$ i anar a 2.

Aquest algorisme funciona perquè en cada pas s'obté una estructura d'accés definida per pesos i llindar connectada homogènia de rang dos. S'observa que si $A_k = \emptyset$, l'algorisme ha acabat perquè $P_k - C_k = \emptyset$ i, llavors, $C_k = P_k$ ha de tenir almenys dos elements, perquè no hi ha vèrtexs aïllats en el graf G_k. D'altra banda, si $A_k \neq \emptyset$, $P_k = C_k \cup A_k$. Si $A_k = \{p\}$, tots els vèrtexs de C_k serien adjacents amb p i, aleshores p seria un vèrtex central de G_k, la qual cosa no és possible. Per tant $|A_k| \geq 2$. A partir de la construcció dels conjunts C_i i A_i, no és difícil comprovar les adjacències del graf G.□

A la Figura 3.1 es pot observar l'estructura general d'aquests grafs.

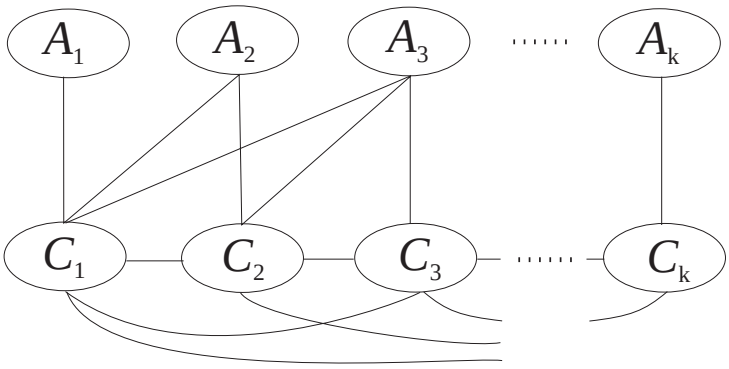

Figura 2.1: Estructura d'accés homogènia de rang 2 definida per pesos i llindar.

El recíproc del Teorema 3.1.2 és també cert, com està provat en el teorema següent. Després d'això, els grafs que representen una estructura d'accés definida per pesos i llindar de rang dos estaràn completament caracteritzats.

Teorema 2.1.3 *Sigui G un graf pel qual hi ha una partició dels seus vèrtexs i un conjunt d'arestes Γ_m com en el Teorema 3.1.2. Llavors, existeix un enter $t > 0$ i una funció pes $\omega : P \to \mathbb{N}$ tal que el graf G representa l'estructura d'accés $\Gamma = \{B \subset P \,|\, \omega(B) \geq t\}$.*

Demostració: Per tal de construir la funció pes $\omega : P \to \mathbb{N}$ que busquem, podem asumir que tots els participants de A_i tenen el mateix pes, això és, $\omega(p) = a_i$ per a tot $p \in A_i$. Igualment, suposem que $\omega(v) = c_i$ per a tot participant $v \in C_i$.

Considerem, per a qualsevol $i = 1, \ldots, k$, $n_i = |A_i|$ i $B_i = \bigcup_{j=1}^{i} A_i$. Els participants de A_1 han de tenir el pes mínim. Per tant posem $a_1 = 1$. Per a qualsevol $i \geq 2$, i per a qualsevol $v \in C_i$, el conjunt $\{v\} \cup B_{i-1}$ no és autoritzat i, aleshores, $c_i + \omega(B_{i-1}) < t$. D'altra banda, com que $\{v, p\} \in \Gamma_m$ per a qualsevol $v \in C_i$, $p \in A_i$, tenim que $c_i + a_i \geq t$. D'aquí deduïm que a_i ha de ser més gran que $\omega(B_{i-1})$. El mínim valor possible per a_i, $1 \leq i \leq k$, ve donat recursivament per $a_1 = 1$ i $a_{i+1} = \omega(B_i) + 1$ si $1 \leq i \leq k-1$ pel cas $A_k \neq \emptyset$ i si $1 \leq i \leq k-2$ pel cas $A_k = \emptyset$. S'observa que

$$a_{i+1} = \omega(B_i) + 1 = \omega(A_i) + \omega(B_{i-1}) + 1 = n_i a_i + a_i = (n_i + 1)a_i.$$

Per tant, $a_{i+1} = \prod_{j=1}^{i}(n_j + 1)$.

Si $A_k \neq \emptyset$, hem de tenir en compte que $B_k \notin \Gamma$. Llavors, el mínim valor possible pel llindar és

$$t = \omega(B_k) + 1 = \prod_{j=1}^{k}(n_j + 1).$$

Finalment, per a qualsevol $i = 1, \ldots, k$, posem $c_i = t - a_i$.

Si $A_k = \emptyset$, utilitzem el fet que per a qualsevol $v \in C_k$, $\{v\} \cup B_{k-1}$ no és un conjunt autoritzat, i llavors $c_k + \omega(B_{k-1}) < t$. Ja que C_k té almenys 2 elements i són adjacents, $2c_k \geq t$. Per tant $c_k > \omega(B_{k-1})$. Prenem els valors mínims per c_k i t:

$$c_k = \omega(B_{k-1}) + 1 = \prod_{j=1}^{k-1}(n_j + 1),$$

$$t = c_k + \omega(B_{k-1}) + 1 = 2c_k.$$

Finalment, per a $1 \leq i \leq k-1$, posem $c_i = t - a_i$.

La demostració s'acaba comprovant que l'estructura d'accés $\Gamma = \{A \subset P \,|\, \omega(A) \geq t\}$, on t i ω són el llindar i la funció pes que hem construït, representa el graf G.□

S'observa que el llindar i els pesos donats a la demostració del Teorema 3.1.3 són, per construcció, mínims. Per tant aquesta demostració ens dóna un algorisme per trobar llindar i pesos mínims per a una estructura d'accés definida per pesos i llindar de rang dos.

Fem un breu resum dels valors que hem trobat per pesos i llindar:

Càlcul de pesos i llindar mínims
Anomenem $n_i = |A_i|$, per a tot $p \in A_i, \omega(p) = a_i$
i per a tot $p \in C_i$, $\omega(p) = c_i$.
• Si $A_k \neq \emptyset$
$t = \prod_{j=1}^{k}(n_j + 1)$, $a_1 = 1$ per $1 \leq i \leq k-1$,
$a_{i+1} = \prod_{j=1}^{i}(n_j + 1)$, i $c_i = t - a_i$ per $1 \leq i \leq k$.
• Si $A_k = \emptyset$
$t = 2\prod_{j=1}^{k-1}(n_j + 1)$, $a_1 = 1$ per $1 \leq i \leq k-2$,
$a_{i+1} = \prod_{j=1}^{i}(n_j + 1)$, $c_i = t - a_i$, per $1 \leq i \leq k-1$,
i $c_k = \prod_{j=1}^{k-1}(n_j + 1)$.

Els grafs que representen estructures d'accés definides per pesos i llindar connectades, homogènies de rang dos, estan completament caracteritzats pels Teoremes 3.1.2 i 3.1.3. Anomenarem aquests tipus de grafs *k-grafs amb pesos*, on k és el paràmetre que apareix en el Teorema 3.1.2. La representació gràfica d'aquests grafs s'ha donat a la Figura 3.1.

La caracterització dels k-grafs està feta amb un algorisme descrit a la demostració del Teorema 3.1.2 que consisteix en determinar a cada pas el conjunt de vèrtexs centrals, el conjunt de vèrtexs subordinats i anar-los eliminant. Per determinar els vèrtexs centrals i subordinats es pot fer servir el grau dels vèrtexs de forma que obtenim una caracterització d'aquests grafs en funció només dels graus dels vèrtexs.

Aquesta nova formulació es basa en el fet que si un vèrtex c és central aleshores el seu grau és $\deg(c) = |P| - 1$. El recíproc també és cert: si c és un vèrtex amb $\deg(c) = |P| - 1$ llavors està connectat amb la resta de participants. Diem C_1 al conjunt de vèrtexs centrals. Els vèrtexs subordinats $v \in P$ són els que només estan connectats amb els vèrtexs centrals, per tant han de tenir $\deg(v) = |C_1|$. Recíprocament si un vèrtexs té grau $\deg(c) = |C_1|$ vol dir que només està connectat amb els vèrtexs de C_1, ja que els de C_1 ho estan amb tots. Així podem determinar el conjunt de centrals i de subordinats com

$$C_1 = \{c \in P | \deg(c) = |P| - 1\},\ A_1 = \{v \in P | \deg(v) = |C_1|\}$$

Podria ser que $A_1 = \emptyset$ i $P = C_1$ amb la qual cosa tindríem que $k = 1$ i ja hauríem trobat que l'estructura és un 1-graf. Si no s'ha acabat el procés hauríem de procedir a eliminar els vèrtexs de $C_1 \cup A_1$ de l'estructura i hauríem de repetir el procés. S'observa que no cal fer cap eliminació i que només cal

consultar els graus. Així doncs, pel segon pas caldria determinar els centrals i subordinats del segon nivell amb

$$C_2 = \{c \in P | \deg(c) = |P| - 1 - |A_1|\},\ A_2 = \{v \in P | \deg(v) = |C_1| + |C_2|\}$$

Aquest procés s'ha d'anar iterant de forma que l'algorisme que determina si un graf és un k-graf i que en cas afirmatiu retorna els paràmetres que el defineixen és

$i := 0$
fer
$\quad i := i + 1$
$\quad C_i := \{c \in P | \deg(c) = |P| - \quad 1 - |A_1| - \ldots - |A_{i-1}|\}$
$\quad A_i := \{c \in P | \deg(c) = |C_1| + \quad \ldots + |C_i|\}$
fins que $C_i = \emptyset$ **o** $A_i = \emptyset$
si $P = C_1 \cup A_1 \cup \ldots, C_i \cup A_i$ **llavors**
$\quad$ **si** $C_i \neq \emptyset$ **llavors** És un k-graf amb $k := i$
$\quad$ **si no** És un k-graf amb $k := i - 1$
$\quad$ **si no** No és un k-graf.

D'aquesta manera hem demostrat que els paràmetres que defineixen un k-graf queden determinats pels graus dels vèrtexs del graf i que es poden obtenir sense fer cap manipulació sobre el graf, només observant els valors del graus. El recíproc també és cert.

2.1.2 Fites en la taxa d'informació òptima

Sigui $\Gamma = \{A \subset P \,|\, \omega(A) \geq t\}$ una estructura d'accés connectada definida per pesos i llindar, representada per un graf G. A partir d'un (t, m)-esquema de llindar ideal, on $m = \omega(P)$, considerem l'esquema amb estructura d'accés Γ obtingut a assignant a cada participant tants fragments com el seu pes. Aquest és l'esquema que Shamir a [83] proposa per una estructura definida per pesos i llindar. La taxa d'informació d'aquest esquema és $\rho = 1/W$, on W és el pes màxim. A partir del Teorema 3.1.3, el pes máxim possible és $W = c_1 = t - 1$, on $t = \prod_{j=1}^{k}(n_j + 1)$ o bé $t = 2\prod_{j=1}^{k-1}(n_j + 1)$. Llavors la taxa d'informació òptima de l'estructura d'accés Γ satisfà $\rho^*(\Gamma) \geq 1/W$, quantitat que és de l'ordre de $1/2^k$ en el millor dels casos. Tot seguit trobarem una fita de l'ordre de $1/\log k$.

L'objectiu d'aquesta secció és trobar millors fites per a la taxa d'informació òptima de les estructures d'accés de rang dos definides per pesos i llindar. Algunes tècniques per fitar la taxa d'informació òptima d'estructures d'accés donades per grafs presentades a [18] es poden trobar a la Secció 2.7. Utilitzarem els *recobriments multipartits complets* pel nostre objectiu.

Denotarem per $K(A)$ el graf complet amb conjunt de vèrtexs A i $K(A, B)$ denotarà el graf bipartit complet amb conjunts de la partició A i B. Més en general denotarem per $K(A_1, \ldots, A_r)$ el graf r-partit complet amb conjunts de la partició $A1, \ldots, A_r$.

Proposició 2.1.4 *Per a qualsevol $q \geq 1$, sigui G_q un k-graf amb pesos amb $k = 2^q - 1$ tal que $A_k \neq \emptyset$. Aleshores, existeix un recobriment multipartit complet Π_q de G_q amb $R(\Pi_q) \leq q$.*

Demostració: La demostració és per inducció sobre q. Si $q = 1$, llavors $k = 1$ i G_1 és un graf multipartit complet com es pot observar a la Figura 3.2. En aquest cas, $\Pi_1 = \{G_1\}$ verificant $R(\Pi_1) \leq 1$.

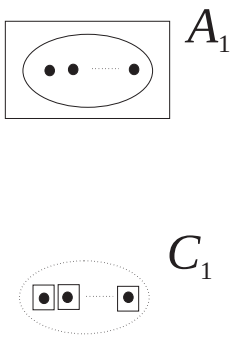

Figura 2.2: El 1-graf és un graf multipartit complet.

Sigui ara $q \geq 2$, i suposem que existeix un recobriment multipartit complet Π_{q-1} de G_{q-1} tal que $R_v \leq q - 1$ per a tot vèrtex v. Sigui $G_q^{(1)}$ el subgraf de G_q induït per

$$\bigcup_{j=1}^{2^{q-1}-1} (C_j \cup A_j)$$

i $G_q^{(2)}$ el subgraf de G_q induït per

$$\bigcup_{j=2^{q-1}+1}^{2^q-1} (C_j \cup A_j).$$

Ambdós $G_q^{(1)}$ i $G_q^{(2)}$ són isomorfs a un G_{q-1}. Considerem

$$\Pi_q = \{H_{q,0}, H_{q,1}\} \cup \Pi_{q-1}^{(1)} \cup \Pi_{q-1}^{(2)},$$

amb (veure Figura 3.3)

$$H_{q,0} = K(\bigcup_{j=1}^{2^{q-1}-1} C_j, C_{2^{q-1}}, \bigcup_{j=2^{q-1}+1}^{2^q-1} C_j \cup \bigcup_{j=2^{q-1}}^{2^q-1} A_j) \text{ i } H_{q,1} = K(C_{2^{q-1}})$$

on $\Pi_{q-1}^{(i)}$, $i = 1, 2$, és la família de subgrafs que són recobriment multipartits

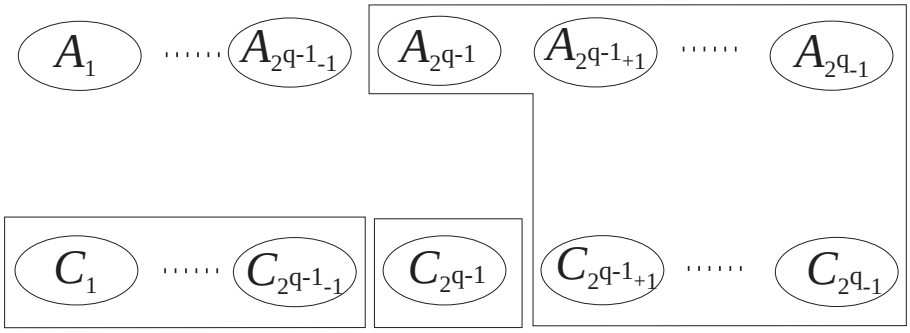

Figura 2.3: Graf multipartit complet $H_{q,0}$.

complets de $G_q^{(i)}$.

No és difícil veure que Π_q és un recobriment multipartit complet de G_q. Qualsevol vèrtex p de G_q, pot aparèixer a $H_{q,0}$, a $H_{q,1}$ i a com a màxim $q-1$ grafs de $\Pi_{q-1}^{(1)} \cup \Pi_{q-1}^{(2)}$. Per la construcció de $H_{q,0}$, $H_{q,1}$, $\Pi_{q-1}^{(1)}$, $\Pi_{q-1}^{(2)}$ tenim que $R(\Pi_q) \leq q$.□

Teorema 2.1.5 *Sigui* $\Gamma = \{A \subset P \,|\, \omega(A) \geq t\}$ *una estructura d'accés representada per un* k*-graf amb pesos,* G*. Llavors,*

$$\rho^*(\Gamma) \geq \frac{1}{\lceil \log_2(k+1) \rceil}.$$

Demostració: Sigui q el mínim enter tal que $k \leq 2^q - 1$, això és, $q = \lceil \log_2(k+1) \rceil$. Aleshores, G és un subgraf induït d'un graf G_q en les condicions de la Proposició 3.1.4. A més, la restricció del recobriment multipartit complet Π_q de G és un recobriment multipartit complet de G amb $R \leq q$. Per tant,

$$\rho^*(\Gamma) \geq \frac{1}{R} = \frac{1}{\lceil \log_2(k+1) \rceil}$$

□

Per $k = 1$ l'estructura és un graf multipartit complet i per tant ideal. Per $k = 2$ aquesta fita pot ser millorada utilitzant més d'un recobriment multipartit complet de la manera descrita a [18]. Amb el resultat d'utilitzar aquesta tècnica i les anteriors fites obtenim la taula resum:

$k = 1$	$\rho^* = 1$
$k = 2$	$\rho^* = 2/3$
$k \geq 2$	$\rho^* \geq \frac{1}{\lceil \log_2(k+1) \rceil}$

L'estudi i implementació dels algorismes per decidir quan una estructura de rang 2 està definida per pesos i llindar, ha estat recollit en el Projecte Final de Carrera [97] realitzat a l'*Escola Tècnica Superior d'Enginyeria de Telecomunicacions de Barcelona*. En aquest s'ha creat tot un entorn amigable per la introducció de les estructures d'accés i el seu estudi, així com per a la repartició i recuperació dels secrets en k-grafs.

2.1.3 Estructura dual d'una estructura definida per pesos i llindar

Veurem ara que l'estructura dual d'una estructura d'accés definida per pesos i llindar és una altra estructura d'accés definida per pesos i llindar.

Proposició 2.1.6 *Sigui Γ una estructura definida per pesos i llindar. Aleshores l'estructura dual Γ^* és una estructura definida per pesos i llindar.*

Demostració: Si Γ és una estructura definida per pesos i llindar podem trobar uns nous pesos naturals $\omega : P \longrightarrow \mathbb{N}$ i un llindar natural $t \in \mathbb{N}$ de forma que defineixen la mateixa estructura, com vam provar a la Proposició 3.1.1. Demostrem que l'estructura dual Γ^* és una estructura definida pels pesos $\omega^*(p) = \omega(p)$ per a tot $p \in P$ i llindar $t^* = \omega(P) - t + 1$. Farem servir la Proposició 2.4.1 que afirma

$$\Gamma^* = \mathrm{cl}(\{P - M | M \text{ és un no autoritzat maximal de } \Gamma\})$$

Per tal de demostrar la proposició anomenem Γ' a l'estructura definida per $\omega^*(p) = \omega(p)$ per a tot $p \in P$ i llindar $t^* = \omega(P) - t + 1$. Volem veure que $\Gamma^* = \Gamma'$, per a la qual cosa provarem les dues inclusions.

Veiem en primer lloc que $\Gamma^* \subset \Gamma'$. Sigui $A \in \Gamma^*$, aleshores existeix un $M \notin \Gamma$ maximal tal que $P - M \subset A$. Tenim que $\omega(M) < t = \omega(P) - t^* + 1$,

per la qual cosa $\omega(P-M) > t^*-1$, per tant $\omega(P-M) \geq t^*$, és a dir, $P-M \in \Gamma'$ i llavors $A \in \Gamma'$.

Veiem ara que $\Gamma' \subset \Gamma^*$. Sigui $A \in \Gamma'$, aleshores $\omega(A) \geq t^* = \omega(P) - t + 1$, per la qual cosa $\omega(P-A) \leq t-1$, per tant $P-A \notin \Gamma$. Llavors per cert $M \notin \Gamma$ maximal es verifica $P-A \subset M$ i d'aquí $P-M \subset A$, per la qual cosa $A \in \Gamma^*$. □

S'observa que si Γ està definida per pesos $\omega : P \longrightarrow \mathbb{N}$ i llindar $t \in N$, aleshores l'estructura dual Γ^* és una estructura definida pels pesos $\omega^*(p) = \omega(p)$ per a tot $p \in P$ i llindar $t^* = \omega(P) - t + 1$.

Les estructures definides per pesos i llindar de rang 2 han quedat caracteritzades a la Subsecció 3.1.1. Fent ús de la proposició anterior l'estructura dual d'una de rang 2 també està definida per pesos i llindar. Però, quina forma tenen aquestes estructures?

Denotem per $\widetilde{S}$, l'expressió com a forma booleana del subconjunt $S \subset P$, això és, $\widetilde{S} = \Pi_{p \in S} p$. També per a una estructura $\Gamma \subset 2^P$ hem convingut denotar per $\widetilde{\Gamma_m} = \sum_{S \in \Gamma_m} \widetilde{S}$, la conjunció de les fórmules determinades per tots els subconjunts autoritzats minimals. Aquestes notacions simplifiquen el càlcul del dual d'una estructura. Abans de calcular el dual d'una estructura de pesos i llindar homogènia de rang 2 justificarem el lema següent que ens ajudarà en els càlculs.

Lema 2.1.7 *Sigui $A \subset P$ amb $|A| = t \geq 2$ i $K(A)$ el graf complet dels vèrtexs A. Aleshores*

$$K(A)^* = \mathcal{P}_{t-1}(A)$$

amb $\mathcal{P}_{t-1}(A)$ la col·lecció de subconjunts de A amb $t-1$ elements.

Demostració: Fem un raonament per inducció sobre t, el cardinal de A.

Per $t = 2$ és cert ja que per $A = \{p_1, p_2\}$ tenim $K(A) = \{\{p_1, p_2\}\}$ i llavors $\widetilde{K(A)} = p_1 p_2$, per la qual cosa $\widetilde{K(A)}^* = p_1 + p_2$, i per tant

$$K(A)^* = \{\{p_1\}, \{p_2\}\}$$

Suposem ara que el lema és cert per t i volem veure que és cert per $t+1$. Per $A = \{p_1, \ldots, p_{t+1}\}$ tenim $K(A) = K(\{p_1, \ldots, p_t\}) \cup \{\{p_i, p_{t+1}\} | i = 1, \ldots, t\}$ i llavors $\widetilde{K(A)} = K(\{\widetilde{p_1, \ldots, p_t}\}) + \sum_{i=1}^{t} p_i p_{t+1}$, i per tant

$$\widetilde{K(A)}^* = \mathcal{P}_{t-1}(\{\widetilde{p_1, \ldots, p_t}\}) \Pi_{i=1}^{t}(p_i + p_{t+1}) = \mathcal{P}_{t-1}(\{\widetilde{p_1, \ldots, p_t}\})(p_1 \ldots p_t + p_{t+1}) =$$

$$p_1 \ldots p_t + \mathcal{P}_{t-1}(\{\widetilde{p_1, \ldots, p_t}\}) p_{t+1} = \mathcal{P}_t(\{\widetilde{p_1, \ldots, p_{t+1}}\}).$$

□

S'observa que en el cas que $A = P$, es pot afirmar que el dual d'un graf complet és una estructura de $(t-1,t)$-llindar, i a l'inrevés, és a dir, el dual d'una estructura de $(t-1,t)$-llindar és un graf complet. Es pot demostrar que el dual d'una estructura de (t,n)-llindar és una estructura de $(n-t+1,n)$-llindar.

La proposició següent, que és una mena de proposició dual del Teorema 3.1.2, ens dóna quina forma tenen les estructures definides per pesos i llindar que són dual d'una definida per pesos i llindar de rang 2.

Proposició 2.1.8 *Sigui Γ una estructura d'accés definida per pesos i llindar tal que Γ^* és homogènia de rang 2. Aleshores, existeix una única partició $P = C_1 \cup A_1 \cup C_2 \cup A_2 \cdots \cup C_k \cup A_k$, amb $C_i \neq \emptyset$ per $i = 1,\ldots,k$, $A_i \neq \emptyset$ si $i = 1,\ldots,k-1$ tal que*

$$\Gamma_m = \{C_1 \cup \ldots \cup C_k\} \cup \{A_i \cup \ldots \cup A_k \cup C_1 \cup \ldots \cup C_k - \{c\} |\ \textit{per } i = 1,\ldots,k,\ c \in C_i\}$$

si $|A_k| \geq 2$ i, o bé

$$\Gamma_m = \{C_1 \cup \ldots \cup C_{k-1} \cup C_k - \{c\} | c \in C_k\} \cup$$

$$\{A_i \cup \ldots \cup A_{k-1} \cup C_1 \cup \ldots \cup C_k - \{c\} |\ \textit{per } i = 1,\ldots,k-1,\ c \in C_i\}$$

si $A_k = \emptyset$ i $|C_k| \geq 2$.

Demostració: Sabem per hipòtesi que Γ^* és una estructura de rang 2 definida per pesos i llindar. Llavors existirà pel Teorema 3.1.2 una partició $P = C_1 \cup A_1 \cup C_2 \cup A_2 \cdots \cup C_k \cup A_k$, amb $C_i \neq \emptyset$ per $i = 1,\ldots,k$, $A_i \neq \emptyset$ si $i = 1,\ldots,k-1$.

De les dues possibilitats considerem ara la primera, és a dir que $|A_k| \geq 2$. En aquest cas podem escriure

$$\widetilde{\Gamma_m}^* = (\sum_{p \in C_1} p)(\sum_{p \in A_1 \cup \ldots A_k} p + \sum_{p \in C_2 \cup \ldots \cup C_k} p) + \widetilde{K(C_1)} +$$

$$(\sum_{p \in C_2} p)(\sum_{p \in A_2 \cup \ldots \cup A_k} p + \sum_{p \in C_3 \cup \ldots \cup C_k} p) + \widetilde{K(C_2)} + \ldots + (\sum_{p \in C_k} p)(\sum_{p \in A_k} p) + \widetilde{K(C_k)}$$

Demostrem que és cert el resultat enunciat per inducció sobre k. Per $k = 1$ tenim

$$\widetilde{\Gamma_m}^* = (\sum_{p \in C_1} p)(\sum_{p \in A_1} p) + \widetilde{K(C_1)}$$

Fent ús del Lema 3.1.7

$$\widetilde{\Gamma_m} = (\widetilde{C_1} + \widetilde{A_1}) \cdot \sum_{c \in C_1} \widetilde{C_1 - \{c\}} = \widetilde{C_1} + \sum_{c \in C_1} \widetilde{A_1 C_1 - \{c\}}$$

quedant provat el primer pas de la inducció. Suposem que és cert pel cas k i veiem que és cert per $k+1$. A partir de

$$\widetilde{\Gamma_m}^* = (\sum_{p \in C_1} p)(\sum_{p \in A_1 \cup \ldots A_{k+1}} p + \sum_{p \in C_2 \cup \ldots \cup C_{k+1}} p) + \widetilde{K(C_1)} +$$

$$(\sum_{p \in C_2} p)(\sum_{p \in A_2 \cup \ldots \cup A_{k+1}} p + \sum_{p \in C_3 \cup \ldots \cup C_{k+1}} p) + \widetilde{K(C_2)} + \ldots + (\sum_{p \in C_{k+1}} p)(\sum_{p \in A_{k+1}} p) + \widetilde{K(C_{k+1})}$$

obtenim pel Lema 3.1.7 i per la hipòtesi d'inducció

$$\widetilde{\Gamma_m} = (\widetilde{C_1} + \widetilde{A_1} \ldots \widetilde{A_{k+1}} \widetilde{C_2} \ldots \widetilde{C_{k+1}}) \cdot (\sum_{c \in C_1} \widetilde{C_1 - \{c\}}) \cdot$$

$$(\widetilde{C_2} \ldots \widetilde{C_{k+1}} + \sum_{i=2; c \in C_i}^{k+1} \widetilde{A_i} \ldots \widetilde{A_{k+1}} \widetilde{C_2} \ldots \widetilde{C_i - \{c\}} \ldots \widetilde{C_{k+1}}) =$$

$$(\widetilde{C_1} + \sum_{c \in C_1} \widetilde{A_1} \ldots \widetilde{A_{k+1} C_1 - \{c\}} \widetilde{C_2} \ldots \widetilde{C_{k+1}}) \cdot$$

$$(\widetilde{C_2} \ldots \widetilde{C_{k+1}} + \sum_{i=2; c \in C_i}^{k+1} \widetilde{A_i} \ldots \widetilde{A_{k+1}} \widetilde{C_2} \ldots \widetilde{C_i - \{c\}} \ldots \widetilde{C_{k+1}}) =$$

$$\widetilde{C_1} \ldots \widetilde{C_{k+1}} + \sum_{i=2; c \in C_i}^{k+1} \widetilde{A_i} \ldots \widetilde{A_{k+1}} \widetilde{C_1} \ldots \widetilde{C_i - \{c\}} \ldots \widetilde{C_{k+1}} +$$

$$\sum_{c \in C_1} \widetilde{A_1} \ldots \widetilde{A_{k+1} C_1 - \{c\}} \widetilde{C_2} \ldots \widetilde{C_{k+1}} =$$

$$\widetilde{C_1} \ldots \widetilde{C_{k+1}} + \sum_{i=1; c \in C_i}^{k+1} \widetilde{A_i} \ldots \widetilde{A_{k+1}} \widetilde{C_1} \ldots \widetilde{C_i - \{c\}} \ldots \widetilde{C_{k+1}}$$

i així queda justificat el resultat pel cas $|A_k| \geq 2$.

Pel cas en el qual $A_k = \emptyset$ i $|C_k| \geq 2$ tenim provat el resultat per $k = 1$ ja que es redueix al Lema 3.1.7. Quan $k \geq 2$ podem expressar

$$\widetilde{\Gamma_m}^* = \widetilde{\Gamma}' + (\sum_{p \in C_k} p)(\sum_{p \in C_1 \cup \ldots \cup C_{k-1}} p) + \widetilde{K(C_k)}$$

amb Γ' un $(k-1)$-graf amb els conjunts de subordinats amb més de dos elements. Fent servir el que tenim ja provat per inducció:

$$\widetilde{\Gamma_m} = (\widetilde{C_1}\dots\widetilde{C_{k-1}} + \sum_{i=1;c\in C_i}^{k-1} \widetilde{A_i}\dots\widetilde{A_{k-1}}\widetilde{C_1}\dots\widetilde{C_i-\{c\}}\dots\widetilde{C_{k-1}})(\widetilde{C_k}+\widetilde{C_1}\dots\widetilde{C_{k-1}})\cdot$$

$$(\sum_{c\in C_k}\widetilde{C_k-\{c\}}) =$$

$$(\widetilde{C_1}\dots\widetilde{C_{k-1}} + \sum_{i=1;c\in C_i}^{k-1} \widetilde{A_i}\dots\widetilde{A_{k-1}}\widetilde{C_1}\dots\widetilde{C_i-\{c\}}\dots\widetilde{C_{k-1}})\cdot$$

$$(\widetilde{C_k} + \sum_{c\in C_k}\widetilde{C_1}\dots\widetilde{C_{k-1}}\widetilde{C_k-\{c\}}) =$$

$$\widetilde{C_1}\dots\widetilde{C_k} + \sum_{c\in C_k}\widetilde{C_1}\dots\widetilde{C_{k-1}}\widetilde{C_k-\{c\}} + \sum_{i=1;c\in C_i}^{k-1}\widetilde{A_i}\dots\widetilde{A_{k-1}}\widetilde{C_1}\dots\widetilde{C_i-\{c\}}\dots\widetilde{C_k} +$$

$$\sum_{c\in C_k}\widetilde{A_{k-1}}\widetilde{C_1}\dots\widetilde{C_{k-1}}\widetilde{C_k-\{c\}} =$$

$$\sum_{c\in C_k}\widetilde{C_1}\dots\widetilde{C_{k-1}}\widetilde{C_k-\{c\}} + \sum_{i=1;c\in C_i}^{k-1}\widetilde{A_i}\dots\widetilde{A_{k-1}}\widetilde{C_1}\dots\widetilde{C_i-\{c\}}\dots\widetilde{C_k}$$

com es volia provar. □

A les Figures 3.4 i 3.5 es poden observar els subconjunts minimals d'aquestes estructures en les seves dues variants.

S'observa que el $\operatorname{rang}\Gamma^* = |P| - 1$. Aquesta proposició l'hem obtingut per dualització de la proposició que ens dóna la forma de totes les estructures homogènies de rang 2. Podríem pensar que tota estructura de rang $|P|-1$ definida per pesos i llindar hagi de ser d'aquesta forma, però desgraciadament no és cert. Un contraexemple de que no tota estructura definida per pesos i llindar de rang $|P|-1$ és dual d'una definida per pesos i llindar homogènia de rang 2 és el següent: Γ definida a $P = \{p_1, p_2, p_3, p_4\}$ pels pesos $\omega(p_1) = \omega(p_2) = 1, \omega(p_3) = 2, \omega(p_4) = 3$ i el llindar $t = 4$ determinen el conjunt de minimals $\Gamma_m = \{\{p_1,p_2,p_3\},\{p_1,p_4\},\{p_2,p_4\},\{p_3,p_4\}\}$, per tant $\operatorname{rang}\Gamma = 3 = |P|-1$. L'estructura dual està definida pels pesos $\omega^*(p) = \omega(p)$ per a tot $p \in P$ i $t^* = 7 - 4 + 1 = 4$, per la qual cosa és una estructura autodual, això és, $\Gamma^* = \Gamma$, però no té rang 2.

Ara podem enunciar el dual del Teorema 3.1.3:

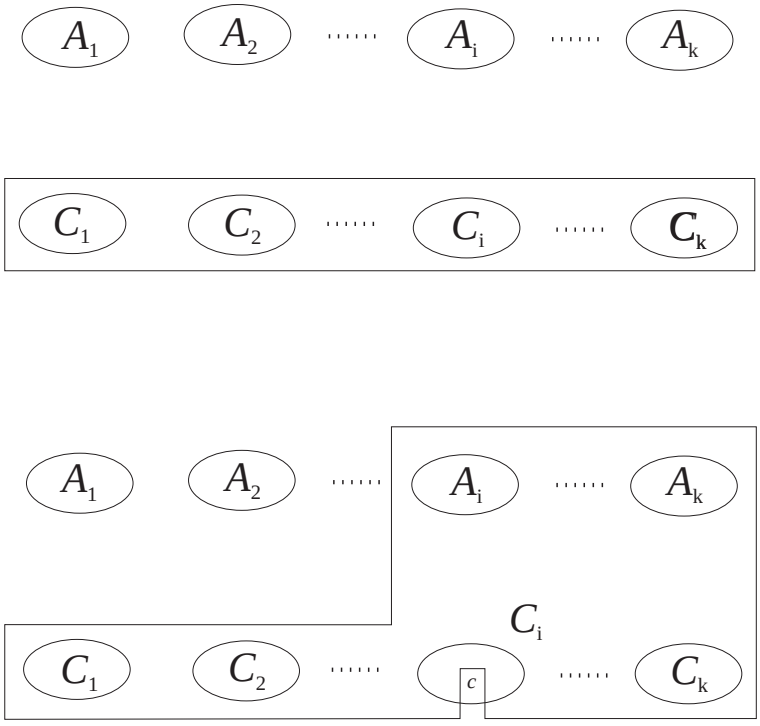

Figura 2.4: Minimals del dual d'una estructura de rang 2 homogènia amb $|A_k| \geq 2$

Proposició 2.1.9 *Sigui* Γ *una estructura d'accés de la forma especificada a la Proposició 3.1.8. Llavors, existeix un enter* $t \in \mathbb{N}$ *i una funció pes* $\omega : P \to \mathbb{N}$ *tal que l'estructura* Γ *coincideix amb* $\Gamma = \{B \subset P \,|\, \omega(B) \geq t\}$. *A més aquesta assignació de pesos i llindar és mínima entre tots els pesos i llindars que defineixen* Γ.

Demostració: Com que Γ^* és de rang 2 definida per pesos i llindar, llavors tenim una assignació de pesos i llindar ω_m i t_m mínims que defineixen Γ^* trobada al Teorema 3.1.3. Per la Proposició 3.1.6 sabem que Γ està definida per $\omega = \omega_m$ i $t = \omega(P) - t_m + 1$.

Veiem que els pesos $\omega = \omega_m$ i llindar $t = \omega(P) - t_m + 1$ són els mínims valors enters amb els quals es pot definir Γ. En efecte, si ω' i t' són pesos i llindar enters que defineixen Γ aleshores ω' i $\omega'(P) - t' + 1$ definirien Γ^*, però sabem que per a tot participant $p \in P$ tenim $\omega_m(p) \leq \omega'(p)$, per tant $\omega(p) \leq \omega'(p)$, és a dir, els pesos ω són mínims. Per justificar que el llindar és mínim observem que pel Teorema 3.1.3, si $a \in A_1,\ c \in C_1$ llavors $\omega(a) + \omega(c) = t_m$ i per tant $\omega(P - \{a, c\}) = \omega(P) - t_m = t - 1$. Però com que $P - \{a, c\} \notin \Gamma$ aleshores

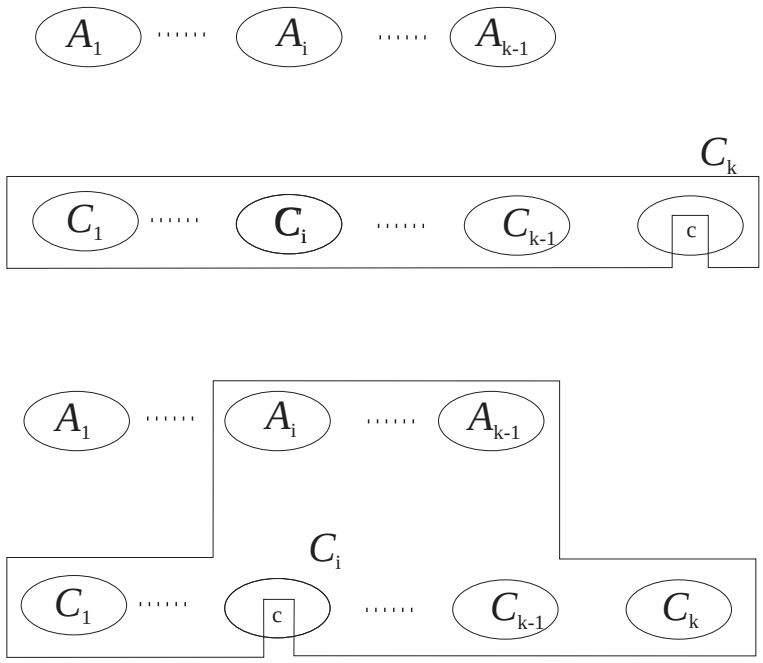

Figura 2.5: Minimals del dual d'una estructura de rang 2 homogènia amb $A_k = \emptyset$ i amb $|C_k| \geq 2$

$t - 1 = \omega(P - \{a, c\}) \leq \omega'(P - \{a, c\}) < t'$, per la qual cosa $t \leq t'$. □

Amb aquests resultats hem caracteritzat una nova família d'estructures d'accés definides per pesos i llindar, i hem trobat el valor mínim de pesos i llindar. Veiem ara que d'aquestes dues famílies d'estructures podem derivar dues famílies més d'estructures, completament caracteritzades i amb pesos i llindar mínims coneguts.

Ja vam comentar a la Subsecció 3.1.1 que la determinació de l'estructura definida per pesos i llindar per estructures de rang 2 no només abarca el cas homogeni. També es poden considerar minimals de cardinal 1 dels quals podem suposar que tenen pes $\omega(p) = t$. Què passa amb els elements que ells sols són autoritzats quan es fa el dual? Veiem-ho per a qualsevol estructura d'accés: sigui Γ_m la base d'una estructura a P de tal manera que $\{p\} \in \Gamma_m$, per a tot $p \in C_0 \subset P$, llavors existeix Γ'_m base d'una estructura en $P - C_0$ de forma que $\Gamma_m = \Gamma'_m \cup \{\{p\} | p \in C_0\}$. Així $\widetilde{\Gamma_m} = \widetilde{\Gamma'_m} + \sum_{p \in C_0} p$, per tant $\widetilde{\Gamma_m}^* = \widetilde{\Gamma'_m}^* \Pi_{p \in C_0} p$, per la qual cosa podem afirmar que els participants que són autoritzats en solitari corresponen a participants que estan a tots els minimals de l'estructura dual. I recíprocament.

Si apliquem aquest fet a una estructura definida per pesos i llindar obtenim el resultat següent:

Proposició 2.1.10 *Sigui* Γ *definida per pesos* $\omega : P \longrightarrow \mathbb{N}$ *i llindar* $t \in \mathbb{N}$. *Sigui* C_0 *un subconjunt de participants disjunt amb* P, *això és* $C_0 \cap P = \emptyset$. *L'estructura* $\Gamma' = \{C_0 \cup A | A \in \Gamma\}$ *definida a* $P' = P \cup C_0$ *està definida per pesos* ω' *i llindar* t' *donats per*

$$\omega'(p) = \begin{cases} \omega(p) & si\ p \in P \\ \omega(P) - t + 1 & si\ p \in C_0 \end{cases}, \ t' = |C_0|(\omega(P) - t + 1) + t$$

Demostració: Com hem comentat $\Gamma'^*_m = \Gamma^*_m \cup \{\{p\} | p \in C_0\}$. Sabem per la Proposició 3.1.6 que si Γ està definida per ω i t, llavors Γ^* ve donada per $\omega^*(p) = \omega(p)$, per $p \in P$ i $t^* = \omega(P) - t + 1$. D'aquí tenim que Γ'^* està definida pels mateixos pesos, llindar i per $\omega^*(p) = t^*$ per $p \in C_0$. Tornant a aplicar la Proposició 3.1.6 obtenim $\omega'(p) = \omega^*(p) = \omega(p)$ per $p \in P$, $\omega'(p) = \omega^*(p) = t^* = \omega(P) - t + 1$ per $p \in C_0$ i el llindar $t' = |C_0|(\omega(P) - t + 1) + \omega(P) - (\omega(P) - t + 1) + 1 = |C_0|(\omega(P) - t + 1) + t$. $\square$

S'observa que si els pesos ω i el llindar t són els mínims que defineixen Γ, llavors ω' i t' són els mínims que defineixen Γ'. També s'observa que d'aquesta manera obtenim una altre família, més extensa encara, d'estructures que tenen rang $|C_0| + 2$, definides per pesos i llindar que corresponen al resultat d'afegir a cada aresta del k-graf el subconjunt C_0. Aquestes estructures les podem identificar i podem calcular els pesos i llindar mínims. El mateix resultat és cert si ara combinem amb les duals de les definides per pesos i llindar de rang 2. Hem representat els minimals d'aquesta nova família d'estructures a la Figura 3.6 i a la Figura 3.7.

Pel que fa a la taxa d'informació podem assegurar que les fites que tenim per les estructures definides per pesos i llindar de rang 2 són també vàlides per les seves duals. Aquestes fites inferiors s'han obtingut amb construccions que són 1-descomposicions formades amb estructures d'espai vectorial clàssiques (grafs multipartits complets). Fent servir el Teorema 3.1.5 i la Proposició 2.4.2 obtenim que pel cas d'estructures definides per pesos i llindar que són duals d'un k-graf es verifica:

Proposició 2.1.11 *Sigui* Γ *una estructura d'accés definida per pesos i llindar tal que* Γ^* *és un* k*-graf. Aleshores si* $k = 1$ *llavors* $\rho^* = 1$, *si* $k = 2$ *tenim* $\rho^* = 2/3$ *i per* $k \geq 2$ *es verifica*

$$\rho^* \geq \frac{1}{\lceil \log_2(k+1) \rceil}$$

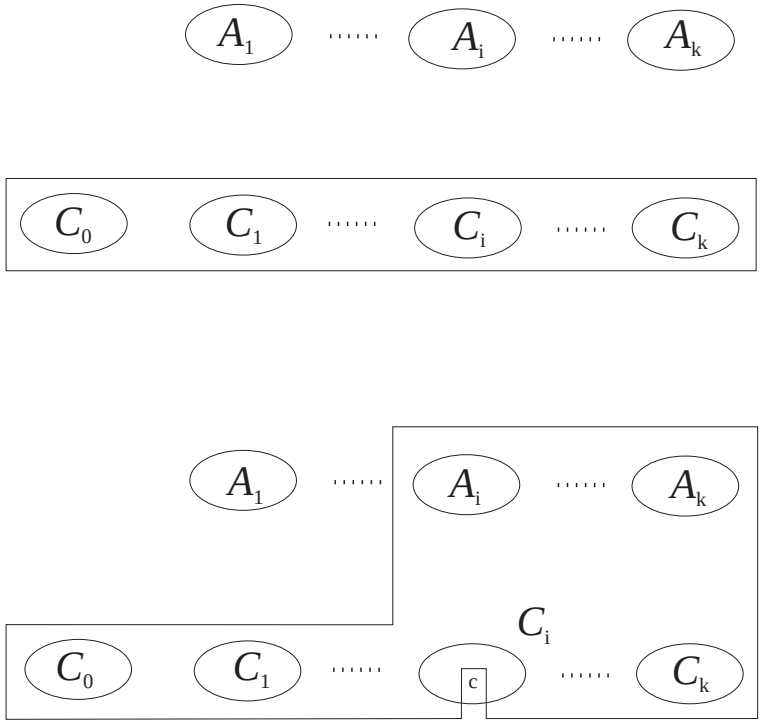

Figura 2.6: Minimals del dual d'una estructura de rang 2 no homogènia amb $|A_k| \geq 2$.

2.2 Estructures d'accés bipartites

Les estructures definides per pesos i llindar proporcionen una simetria al conjunt de participants. Aquesta consisteix en que els participants d'un mateix pes són intercanviables a tot arreu. Aquest fet ens ha portat a plantejar l'estudi d'estructures amb una certa simetria entre els participants, que ara mateix precisem. Considerarem el cas de tenir els participants subdividits en dos subconjunts, de forma que un subconjunt és autoritzat si i només si només depén de quants elements de la primera part i de la segona part conté, però no pas de quins són en concret. Aquest plantejament engloba el cas de les estructures definides per dos pesos i llindar, però és més general. Per a aquests tipus d'estructures, que anomenarem bipartites, determinarem quines són ideals, trobant que són exactament les d'espai vectorial. També veurem que són les que la seva taxa d'informació òptima és més gran que 2/3. Per les estructures que no són ideals determinarem fites inferiors i superiors de la taxa d'informació òptima.

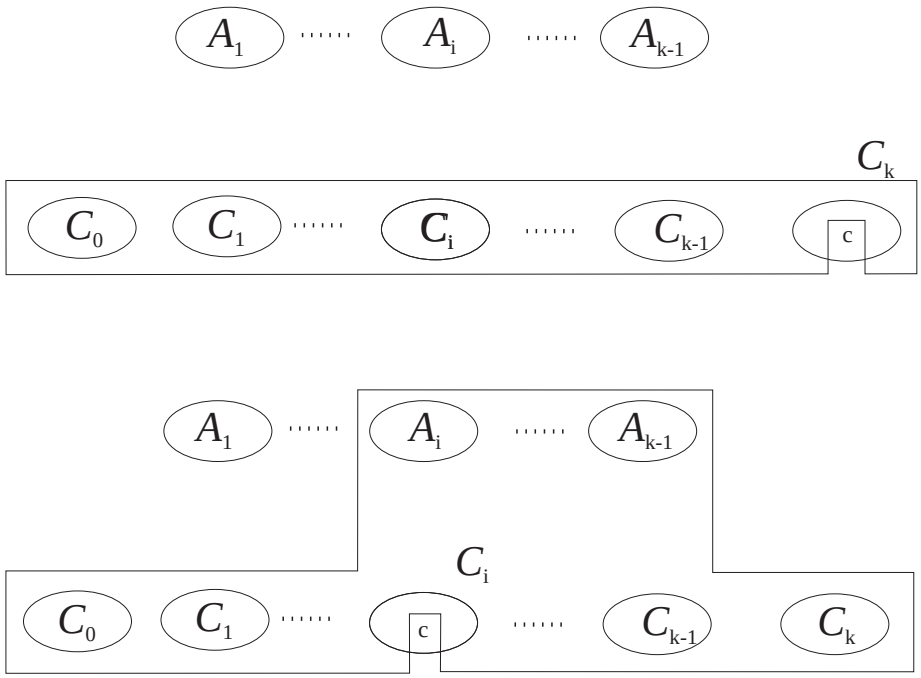

Figura 2.7: Minimals del dual d'una estructura de rang 2 no homogènia amb $A_k = \emptyset$ i $|C_k| \geq 2$.

Sigui Γ una estructura d'accés en un conjunt de participants P dividit en dues parts, $P = X \cup Y$. Direm que Γ és una (X, Y)-*estructura d'accés bipartita* si $\sigma(\Gamma) = \Gamma$ per a qualsevol permutació σ de P amb $\sigma(X) = X$ i $\sigma(Y) = Y$. Una (N_1, N_2)-*estructura d'accés bipartita* és una (X, Y)-estructura d'accés bipartita amb $|\, X \,| = N_1$ i $|\, Y \,| = N_2$.

Donada una partició $P = X \cup Y$ del conjunt P, per a qualsevol subconjunt $A \subset P$, considerem el punt $\pi(A) = (x(A), y(A)) \in \mathbb{Z} \times \mathbb{Z}$, on $x(A) = |\, A \cap X \,|$ i $y(A) = |\, A \cap Y \,|$. Donada una (X, Y)-estructura d'accés bipartita Γ, considerem la regió

$$\pi(\Gamma) = \{\pi(A) \,|\, A \in \Gamma\} \subset \mathbb{Z} \times \mathbb{Z}.$$

És fàcil veure que $A \in \Gamma$ si i només si $\pi(A) \in \pi(\Gamma)$. Per tant, Γ està determinada per la regió $\pi(\Gamma) \subset \mathbb{Z} \times \mathbb{Z}$.

A més, si Γ_0 és la família dels subconjunts minimals autoritzats de Γ, considerem

$$\Pi_0 = \pi(\Gamma_0) = \{(x_1, y_1), (x_2, y_2), \ldots, (x_r, y_r)\}.$$

Evidentment, Γ està determinada pels punts de Π_0, perquè $A \in \Gamma$ si i només si, per a algun $i = 1, \ldots, r$, $x(A) \geq x_i$ i $y(A) \geq y_i$. Els elements de Π_0 els ano-

menarem *punts minimals* de Γ. Podem suposar que $0 \leq x_1 < x_2 < \cdots < x_r$ i, en aquesta situació, no és difícil veure que $y_1 > y_2 > \cdots > y_r \geq 0$. D'ara endavant, ordenarem el conjunt de punts minimals de qualsevol estructura d'accés bipartita d'aquesta manera. Anomenarem *punts consecutius* de Π_0 a un subconjunt de punts de Π_0 de la forma $(x_i, y_i), (x_{i+1}, y_{i+1}), (x_{i+2}, y_{i+2}), \ldots, (x_{i+s}, y_{i+s})$ amb $1 \leq i \leq i+s \leq r$.

2.2.1 Estructures d'accés bipartites ideals

En aquesta secció, caracteritzem les estructures d'accés bipartites que admeten un esquema ideal. Provem que una estructura d'accés bipartita és ideal si i només si és una estructura d'accés d'espai vectorial. A més provem que $\rho^*(\Gamma) \leq 2/3$ per a qualsevol estructura d'accés bipartita no ideal Γ.

Sigui $P = X \cup Y$ una partició del conjunt de participants amb $|\, X \,| = N_1$ i $|\, Y \,| = N_2$. Siguin n, n_1, n_2 enters tal que $0 \leq n_i \leq N_i$ i $n_i \leq n \leq n_1 + n_2$, per $i = 1, 2$. Una estructura d'accés Γ en P s'anomena (X, Y)-*estructura d'accés bipartita de quasi llindar* si $\Gamma = \Omega_j(n, n_1, n_2) \subset 2^P$ per a algun $j = 1, 2, 3, 4$, amb (veure Figura 3.8)

- $A \in \Omega_1(n, n_1, n_2)$ si i només si $|\, A \,| \geq n$, o bé $x(A) \geq n_1$, o bé $y(A) \geq n_2$.
- $A \in \Omega_2(n, n_1, n_2)$ si i només si $|\, A \,| \geq n$ i $y(A) \geq n - n_1$, o bé $y(A) \geq n_2$.
- $A \in \Omega_3(n, n_1, n_2)$ si i només si $|\, A \,| \geq n$ i $x(A) \geq n - n_2$, o bé $x(A) \geq n_1$.
- $A \in \Omega_4(n, n_1, n_2)$ si i només si $|\, A \,| \geq n$, i $x(A) \geq n - n_2$, i $y(A) \geq n - n_1$.

La principal aportació d'aquesta secció és provar que una estructura d'accés bipartita Γ és ideal si i només si és una estructura d'accés bipartita de quasi llindar.

Provarem primer que qualsevol estructura d'accés bipartita de quasi llindar és una estructura d'accés d'espai vectorial.

Teorema 2.2.1 *Sigui $P = X \cup Y$ una partició del conjunt de participants amb $|\, X \,| = N_1$ i $|\, Y \,| = N_2$. Siguin n, n_1, n_2, N_1, N_2 enters tals que $0 \leq n_i \leq N_i$ i $n_i \leq n \leq n_1 + n_2$, per $i = 1, 2$. Llavors, per a tot $j = 1, \ldots, 4$, existeix un enter positiu $M = M(j, n, n_1, n_2, N_1, N_2)$ tal que, si q és una potència de primer amb $q > M$ i E és un espai vectorial n-dimensional sobre el cos finit $GF(q)$, existeix una aplicació $\psi : P \cup \{D\} \to E$ que defineix a P la (X, Y)-estructura d'accés bipartita $\Omega_j(n, n_1, n_2)$ com a estructura d'espai vectorial.*

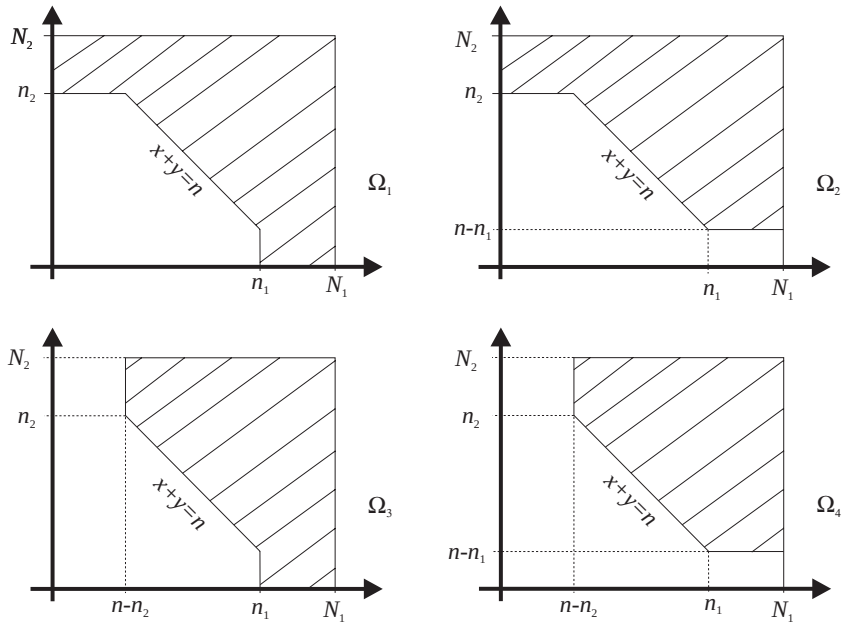

Figura 2.8: (X, Y)-estructures d'accés bipartites de quasi llindar $\Omega_j(n, n_1, n_2)$

La demostració completa es troba després d'introduir alguna notació i provar uns lemes tècnics. La idea de la demostració és la següent: considerem dos subespais $E_1, E_2 \subset E$ amb $\dim(E_1) = n_1$, $\dim(E_2) = n_2$ i $E_1 + E_2 = E$. Per exemple per $\Omega_4(n, n_1, n_2)$ per q suficientment gran, és possible definir-la per una aplicació $\psi : P \cup \{D\} \to E$ amb $\psi(X) \subset E_1$, $\psi(Y) \subset E_2$ i $\psi(D) \in E - (E_1 \cup E_2)$. Per tal de fer-ho hem de trobar N_1 vectors de E_1 i N_2 vectors de E_2 en "posició general". És a dir, de tal manera que qualsevol conjunt de n d'aquests vectors amb almenys $n - n_2$ vectors de E_1 i $n - n_1$ vectors de E_2 és una base de E. A més, el vector $\psi(D)$ no ha d'aparèixer en cap subespai generat per $n-1$ d'aquests vectors. L'estructura d'accés $\Omega_j(n, n_1, n_2)$ per $j = 1, 2, 3$ pot ser definida per una aplicació semblant. L'única diferència és la posició del vector $\psi(D)$:

- si $j = 1$, llavors escollim $\psi(D) \in E_1 \cap E_2$,
- si $j = 2$, llavors escollim $\psi(D) \in E_2 - E_1$,
- si $j = 3$, llavors escollim $\psi(D) \in E_1 - E_2$,

Fem ara la introducció d'alguna notació que ens serà d'utilitat per provar uns lemes tècnics. Donat un cos finit $GF(q)$, un enter positiu n i $\alpha \in GF(q)$,

denotarem $V_n(\alpha) = (1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) \in GF(q)^n$. És ben conegut que, si $\alpha_1, \ldots, \alpha_n$ són n elements diferents de $GF(q)$, aleshores $\{V_n(\alpha_1), \ldots, V_n(\alpha_n)\}$ és una base de $GF(q)^n$.

Sigui n, n_1, n_2 enters amb $0 \leq n_1, n_2 \leq n \leq n_1 + n_2$. Sigui E un espai vectorial n-dimensional sobre un cos finit $GF(q)$ i siguin $E_1, E_2 \subset E$ dos subespais amb $\dim(E_1) = n_1$, $\dim(E_2) = n_2$ i $E_1 + E_2 = E$. S'observa que $r = \dim(E_1 \cap E_2) = n_1 + n_2 - n$. Considerem r elements diferents $\lambda_1, \ldots, \lambda_r$ de $GF(q)$ i dos isomorfismes, $\phi_i : GF(q)^{n_i} \to E_i$, on $i = 1, 2$, tals que $\phi_1(V_{n_1}(\lambda_j)) = \phi_2(V_{n_2}(\lambda_j))$ per a qualsevol $j = 1, \ldots, r$. Així, $\{\phi_1(V_{n_1}(\lambda_j))\}_{1 \leq j \leq r}$ és una base de $E_1 \cap E_2$. Considerem les aplicacions $\mathbf{v} : GF(q) \to E_1$ i $\mathbf{w} : GF(q) \to E_2$ definides per $\mathbf{v}(\alpha) = \phi_1(V_{n_1}(\alpha))$ i $\mathbf{w}(\alpha) = \phi_2(V_{n_2}(\alpha))$. S'observa que $\mathbf{v}(\lambda_j) = \mathbf{w}(\lambda_j) \in E_1 \cap E_2$ per a qualsevol $j = 1, \ldots, r$. Denotarem $\Lambda = \{\lambda_1, \ldots, \lambda_r\}$.

Lema 2.2.2 *Siguin $\mathcal{A}, \mathcal{B}$ dos subconjunts de $GF(q) - \Lambda$ tals que $|\mathcal{A}| = n_1$ i $|\mathcal{B}| = n - n_1$, o bé $|\mathcal{A}| = n - n_2$ i $|\mathcal{B}| = n_2$. Llavors, $\mathbf{v}(\mathcal{A}) \cup \mathbf{w}(\mathcal{B})$ és un base de E.*

Demostració: Suposem que $|\mathcal{A}| = n_1$ i $|\mathcal{B}| = n - n_1$. L'altre cas es prova anàlogament. S'observa que $\mathbf{w}(\Lambda)$, $\mathbf{w}(\Lambda) \cup \mathbf{w}(\mathcal{B})$ i $\mathbf{v}(\mathcal{A})$ són, respectivament, base de $E_1 \cap E_2$, E_2 i de E_1.□

Lema 2.2.3 *Siguin $\mathcal{A}, \mathcal{B}$ dos subconjunts de $GF(q) - \Lambda$ tals que $|\mathcal{A}| = k - 1$ i $|\mathcal{B}| = n - k$, on $n - n_2 + 1 \leq k \leq n_1$, i el subespai $F \subset E$ de dimensió $n - 1$, generat per $\mathbf{v}(\mathcal{A}) \cup \mathbf{w}(\mathcal{B})$. Aleshores, $\dim(F \cap (E_1 \cap E_2)) = r - 1$.*

Demostració: S'observa que $k - 1 \geq n - n_2$ i que $n - k \geq n - n_1$. Prenem $\mathcal{A}' \subset \mathcal{A}$ i $\mathcal{B}' \subset \mathcal{B}$ tals que $|\mathcal{A}'| = n - n_2$ i $|\mathcal{B}'| = n - n_1$. Llavors, $\mathbf{v}(\Lambda) \cup \mathbf{v}(\mathcal{A}')$ és una base de E_1 i $\mathbf{v}(\Lambda) \cup \mathbf{w}(\mathcal{B}')$ és una base de E_2. Per tant, $\mathbf{v}(\Lambda) \cup \mathbf{v}(\mathcal{A}') \cup \mathbf{w}(\mathcal{B}')$ és una base de E. Aleshores, a partir del teorema de Steinitz, hi ha un vector $\mathbf{v}(\lambda_j) \in \mathbf{v}(\Lambda)$ tal que $\{\mathbf{v}(\lambda_j)\} \cup \mathbf{v}(\mathcal{A}) \cup \mathbf{w}(\mathcal{B})$ és una base de E. Com que $\dim(F) = n - 1$ i es verifica que $(E_1 \cap E_2) + F = E$, tenim que $\dim(F \cap (E_1 \cap E_2)) = r - 1$.□

Lema 2.2.4 *Per a qualsevol parell d'enters N_1, N_2 amb $N_1 \geq n - n_2$ i $N_2 \geq n_2$, existeix un enter positiu $L = L(n, n_1, n_2, N_1, N_2)$ tal que, per a qualsevol potència de primer $q > L$, existeixen dos subconjunts $\mathcal{X}, \mathcal{Y} \subset GF(q) - \Lambda$, amb $|\mathcal{X}| = N_1$ i $|\mathcal{Y}| = N_2$, tals que per a qualsevol $k = n - n_2, \ldots, \min\{N_1, n_1\}$ i per a qualsevol $\mathcal{A} \subset \mathcal{X}$ i $\mathcal{B} \subset \mathcal{Y}$ amb $|\mathcal{A}| = k$ i $|\mathcal{B}| = n - k$, el conjunt $\mathbf{v}(\mathcal{A}) \cup \mathbf{w}(\mathcal{B})$ és una base de E.*

Demostració: Utilitzant inducció sobre N_1, provarem que, si q és suficientment gran, per a qualsevol $\mathcal{Y} \subset GF(q) - \Lambda$ amb $|\,\mathcal{Y}\,| = N_2$ existeix $\mathcal{X} \subset GF(q) - \Lambda$ amb $|\,\mathcal{X}\,| = N_1$ verificant les condicions requerides.

Si $N_1 = n - n_2$, podem prendre qualsevol subconjunt $\mathcal{X} \subset GF(q) - \Lambda$ amb $|\,\mathcal{X}\,| = N_1$, perquè, pel Lema 3.2.2, per a qualsevol $\mathcal{B} \subset \mathcal{Y}$ amb $|\,\mathcal{B}\,| = n_2$, el conjunt $\mathbf{v}(\mathcal{X}) \cup \mathbf{w}(\mathcal{B})$ és una base de E. En aquest cas, q ha de ser més gran que $L(n, n_1, n_2, n - n_2, N_2) = \max\{n - n_2, N_2\}$.

Si $N_1 \geq n - n_2 + 1$, per hipòtesi d'inducció, existeix un enter $L_1 = L(n, n_1, n_2, N_1 - 1, N_2)$ tal que, si $q > L_1$, existeix $\mathcal{X}' \subset GF(q) - \Lambda$ amb $|\,\mathcal{X}'\,| = N_1 - 1$ verificant que per a qualsevol $k = n - n_2, \ldots, \min\{N_1 - 1, n_1\}$ i per a qualsevol $\mathcal{A} \subset \mathcal{X}'$ i $\mathcal{B} \subset \mathcal{Y}$ amb $|\,\mathcal{A}\,| = k$ i $|\,\mathcal{B}\,| = n - k$, el conjunt $\mathbf{v}(\mathcal{A}) \cup \mathbf{w}(\mathcal{B})$ és una base de E. Pel Lema 3.2.3, per a qualsevol $k = n - n_2 + 1, \ldots, \min\{N_1, n_1\}$ i per a qualsevol $\mathcal{A} \subset \mathcal{X}'$ i $\mathcal{B} \subset \mathcal{Y}$ amb $|\,\mathcal{A}\,| = k - 1$ i $|\,\mathcal{B}\,| = n - k$, si $F_{\mathcal{A},\mathcal{B}} \subset E$ és el subespai generat per $\mathbf{v}(\mathcal{A}) \cup \mathbf{w}(\mathcal{B})$, llavors, $\dim(F_{\mathcal{A},\mathcal{B}} \cap E_1) = n_1 - 1$. Per tant, existeixen com a màxim $n_1 - k$ elements diferents $\alpha \in GF(q) - (\Lambda \cup \mathcal{X}')$ tals que $\mathbf{v}(\alpha) \in F_{\mathcal{A},\mathcal{B}} \cap E_1$. Aleshores, si

$$q > L_2 = \sum_{k=n-n_2+1}^{\min\{N_1,n_1\}} \left(\begin{array}{c} N_1 - 1 \\ k - 1 \end{array} \right) \left(\begin{array}{c} N_2 \\ n - k \end{array} \right) (n_1 - k) + N_1 - 1$$

existeix $\alpha_{N_1} \in GF(q) - (\Lambda \cup \mathcal{X}')$ tal que $\mathbf{v}(\alpha_{N_1}) \notin F_{\mathcal{A},\mathcal{B}}$ per a qualsevol $\mathcal{A} \subset \mathcal{X}'$, $\mathcal{B} \subset \mathcal{Y}$ amb $|\,\mathcal{A}\,| = k - 1$, $|\,\mathcal{B}\,| = n - k$, on $n - n_2 + 1 \leq k \leq \min\{N - 1, n_1\}$. Per tant, si $q > L(n, n_1, n_2, N_1, N_2) = \max\{L_1, L_2\}$ existeix $\mathcal{X} = \mathcal{X}' \cup \{\alpha_{N_1}\} \subset GF(q) - \Lambda$, amb $|\,\mathcal{X}\,| = N_1$, tal que per a qualsevol $k = n - n_2, \ldots, \min\{N_1, n_1\}$ i per a qualsevol $\mathcal{A} \subset \mathcal{X}$ i $\mathcal{B} \subset \mathcal{Y}$ amb $|\,\mathcal{A}\,| = k$ i $|\,\mathcal{B}\,| = n - k$, el conjunt $\mathbf{v}(\mathcal{A}) \cup \mathbf{w}(\mathcal{B})$ és una base de E.□

Demostració del Teorema 3.2.1: Prenem una potència d'un primer $q > L = L(n, n_1, n_2, N_1, N_2)$ i considerem els subconjunts $\mathcal{X}, \mathcal{Y} \subset GF(q) - \Lambda$, amb $|\,\mathcal{X}\,| = N_1$ i $|\,\mathcal{Y}\,| = N_2$, l'existència dels quals vé donada pel Lema 3.2.4. Considerem dues aplicacions bijectives $\psi_X : X \to \mathbf{v}(\mathcal{X})$ i $\psi_Y : Y \to \mathbf{w}(\mathcal{Y})$.

Prenem un isomorfisme $\phi : GF(q)^r \to E_1 \cap E_2$ i l'aplicació $\mathbf{u} : GF(q) \to E_1 \cap E_2$ definida per $\mathbf{u}(\lambda) = \phi(V_r(\lambda))$. Pel Lema 3.2.3, per a qualsevol $k = n - n_2 + 1, \ldots, n_1$ i per qualsevol $\mathcal{A} \subset \mathcal{X}$ i $\mathcal{B} \subset \mathcal{Y}$ amb $|\,\mathcal{A}\,| = k - 1$ i $|\,\mathcal{B}\,| = n - k$, si $F_{\mathcal{A},\mathcal{B}} \subset E$ és el subespai generat per $\mathbf{v}(\mathcal{A}) \cup \mathbf{w}(\mathcal{B})$, llavors $\dim(F_{\mathcal{A},\mathcal{B}} \cap (E_1 \cap E_2)) = r - 1$. Aleshores, hi ha com a màxim $r - 1$ elements diferents $\lambda \in GF(q)$ tals que $\mathbf{u}(\lambda) \in F_{\mathcal{A},\mathcal{B}}$. Per tant, si

$$q > M_1 = \sum_{k=n-n_2+1}^{n_1} \left(\begin{array}{c} N_1 \\ k - 1 \end{array} \right) \left(\begin{array}{c} N_2 \\ n - k \end{array} \right) (r - 1)$$

existeix $\lambda_0 \in GF(q)$ tal que per a qualsevol $k = n - n_2 + 1, \ldots, n_1$ i per a qualsevol $\mathcal{A} \subset \mathcal{X}$ i $\mathcal{B} \subset \mathcal{Y}$ amb $|\mathcal{A}| = k - 1$ i $|\mathcal{B}| = n - k$, el subespai $F_{\mathcal{A},\mathcal{B}}$ no conté el vector $\mathbf{u}(\lambda_0)$. Per tant, per a qualsevol $q > M(1, n_1, n_2, N_1, N_2) = \max\{L, M_1\}$, l'estructura d'accés $\Omega_1(n, n_1, n_2)$ és estructura d'accés d'espai vectorial donada per l'aplicació $\psi_1 : P \cup \{D\} \to E$, definida per $\psi_1(p) = \psi_X(p) \in E_1$ si $p \in X$, $\psi_1(q) = \psi_Y(q) \in E_2$ si $q \in Y$ i $\psi_1(D) = \mathbf{u}(\lambda_0) \in E_1 \cap E_2$.

Anàlogament, podem veure que si

$$q > M_4 = \sum_{k=n-n_2}^{n_1+1} \begin{pmatrix} N_1 \\ k-1 \end{pmatrix} \begin{pmatrix} N_2 \\ n-k \end{pmatrix} (n-1)$$

existeix un vector $\mathbf{u}_0 \in E$ tal que per a qualsevol $k = n - n_2, \ldots, n_1 + 1$ i per a qualsevol $\mathcal{A} \subset \mathcal{X}$ i $\mathcal{B} \subset \mathcal{Y}$ amb $|\mathcal{A}| = k - 1$ i $|\mathcal{B}| = n - k$, el subespai $F_{\mathcal{A},\mathcal{B}} \subset E$ generat per $\mathbf{v}(\mathcal{A}) \cup \mathbf{w}(\mathcal{B})$ no conté $\mathbf{u}_0$. Per tant, per a qualsevol $q > M(4, n_1, n_2, N_1, N_2) = \max\{L, M_4\}$, l'estructura d'accés $\Omega_4(n, n_1, n_2)$ és l'estructura d'accés d'espai vectorial donada per l'aplicació $\psi_4 : P \cup \{D\} \to E$, definida per $\psi_4(p) = \psi_X(p) \in E_1$ si $p \in X$, $\psi_4(q) = \psi_Y(q) \in E_2$ si $q \in Y$ i $\psi_4(D) = \mathbf{u}_0 \in E - (E_1 \cup E_2)$.

Donada una potència de primer $q > L(n, n_1, n_2, N_1, N_2 + 1)$, considerem els subconjunts $\mathcal{X}, \mathcal{Y} \subset GF(q) - \Lambda$, amb $|\mathcal{X}| = N_1$ i $|\mathcal{Y}| = N_2 + 1$, l'existència dels quals vé donada pel Lema 3.2.4. Considerem l'aplicació $\psi_2 : P \cup \{D\} \to E$ definida a partir de dues aplicacions bijectives $\psi_X : X \to \mathbf{v}(\mathcal{X})$ i $\psi_Y : Y \cup \{D\} \to \mathbf{w}(\mathcal{Y})$. No és difícil veure que ψ_2 defineix l'estructura d'accés $\Omega_2(n, n_1, n_2)$. Per tant, $M(2, n, n_1, n_2, N_1, N_2) = L(n, n_1, n_2, N_1, N_2 + 1)$.

Simètricament, si $q > M(3, n, n_1, n_2, N_1, N_2) = L(n, n_1, n_2, N_1 + 1, N_2)$, podem trobar una aplicació $\psi_3 : P \cup \{D\} \to E$ que determina l'estructura d'accés $\Omega_3(n, n_1, n_2)$. □

El lema següent, el qual no és difícil de comprovar, s'utilitza per provar el recíproc del Teorema 3.2.1.

Lema 2.2.5 *Sigui* Γ *una estructura d'accés bipartita amb conjunt de punts minimals*

$$\Pi_0 = \{(x_1, y_1), (x_2, y_2), \ldots, (x_r, y_r)\}.$$

Si Γ *no és una estructura d'accés bipartita de quasi llindar, aleshores estem en una de les situacions següents:*

1. $x_1 = 0$ *i* $y_2 \neq y_1 - 1, 0$.

2. $y_r = 0$ *i* $x_{r-1} \neq x_r - 1, 0$.

3. *Per a algun* $i = 1, 2, \ldots, r-1$, $x_i \neq 0$, $y_{i+1} \neq 0$ *i* $(x_{i+1}, y_{i+1}) \neq (x_i + 1, y_i - 1)$.

Teorema 2.2.6 *Sigui* Γ *una estructura d'accés bipartita que no és de quasi llindar. Llavors,* $\rho^*(\Gamma) \leq 2/3$.

Demostració: Pel Lema 3.2.5, podem distingir tres casos.
Cas 1: $x_1 = 0$ i $y_2 \neq y_1 - 1, 0$. Si $(x_2, y_2) = (1, 1)$, considerem $B_1, B_2 \subset P$ tal que $B_1 \subset B_2$, $\pi(B_1) = (0, 1)$ i $\pi(B_2) = (0, y_1 - 1)$. Considerem $p \in X$ i $q \in Y$ tal que $q \notin B_2$. Aleshores, si prenem $X_1 = \{p\}$ i $X_2 = \{q\}$, la successió $B_1 \subset B_2$ és independent. Com que $A = \{p, q\} \in \Gamma$ fa $B_1 \subset B_2 \subset B_3$ independent, $\rho^*(\Gamma) \leq |A|/(m+1) = 2/3$. Si $(x_2, y_2) \neq (1, 1)$, considerem la successió $B_1 \subset B_2 \subset B_3$ tal que $\pi(B_1) = (x_2 - 1, y_2 - 1)$, $\pi(B_2) = (x_2 - 1, y_2)$ i $\pi(B_3) = (x_2 - 1, y_1 - 1)$. Considerem $p \in X$ i $q \in Y$ tal que $p, q \notin B_3$ i els subconjunts $X_1 = \{p, q\}$, $X_2 = \{p\}$ i $X_3 = \{q\}$. Llavors, la successió $B_1 \subset B_2 \subset B_3$ és independent. Per tant $A = \{p, q\} \notin \Gamma$ fa $B_1 \subset B_2 \subset B_3$ independent i obtenim $\rho^*(\Gamma) \leq |A|/m = 2/3$.
Cas 2: $y_r = 0$, $x_{r-1} \neq x_r - 1, 0$. Aquest cas és simètric al Cas 1.
Cas 3: per a algun $i = 1, 2, \ldots, r-1$, $x_i \neq 0$, $y_{i+1} \neq 0$ i $(x_{i+1}, y_{i+1}) \neq (x_i + 1, y_i - 1)$. Si $y_{i+1} \neq y_1 - 1$, sigui una successió $B_1 \subset B_2 \subset B_3$ tal que $\pi(B_1) = (x_{i+1} - 1, y_{i+1} - 1)$, $\pi(B_2) = (x_{i+1} - 1, y_{i+1})$ i $\pi(B_3) = (x_{i+1} - 1, y_i - 1)$. Prenem $X_1 = \{p, q\}$, $X_2 = \{p\}$, $X_3 = \{q\}$, on $p \in X$, $q \in Y$ i $p, q \notin B_3$. Aleshores, $A = \{p, q\} \notin \Gamma$ fa independent la successió $B_1 \subset B_2 \subset B_3$. Per tant $\rho^*(\Gamma) \leq |A|/m = 2/3$. Si $x_{i+1} \neq x_i + 1$, podem trobar anàlogament una successió independent que prova que $\rho^*(\Gamma) \leq 2/3$.□

El teorema següent resumeix els resultats d'aquesta secció. Observi's el paral·lelisme d'aquest teorema amb el Teorema 2.6.3. Només cal intercanviar *bipartita* per *representable per un graf* i *bipartita de quasi llindar* per *representable per un graf multipartit complet.*

Teorema 2.2.7 *Sigui* Γ *una estructura d'accés bipartita. Llavors, les afirmacions següents són equivalents:*

1. Γ *és una estructura d'accés bipartita de quasi llindar.*

2. Γ *és una estructura d'accés d'espai vectorial.*

3. Γ *és una estructura d'accés ideal.*

4. $\rho^*(\Gamma) > 2/3$.

Observi's que no existeix cap estructura d'accés bipartita la taxa d'informació òptima de la qual estigui a l'interval $(2/3, 1)$. Presentem a la Secció 3.2.2 una estructura d'accés bipartita que assoleix la màxima taxa d'informació per a una estructura d'accés bipartita no ideal, és a dir, amb $\rho^*(\Gamma) = 2/3$.

2.2.2 Fites de la taxa d'informació òptima

Presentem en aquesta secció dues tècniques per a trobar esquemes per a compartir secrets per estructures d'accés bipartites. Amb aquestes construccions trobarem fites inferiors de la taxa d'informació òptima d'aquest tipus d'estructura d'accés. Provem que aquestes fites són ajustades en el sentit que podem trobar una estructura d'accés bipartita, la taxa d'informació òptima de la qual és arbitràriament propera a la fita inferior. Per tal de fer això, utilitzem fites superiors calculades a partir del Teorema 2.8.6.

La primera tècnica és una tècnica de recobriment: busquem estructures d'accés bipartites ideals que puguin ser combinades per tal d'obtenir l'estructura donada. Per exemple, considerem l'estructura d'accés Γ definida per pesos i llindar amb un llindar $t = 40$ i una funció de pesos $\omega : P \to \mathbf{R}^+$ tal que, per a qualsevol $p \in P$, $\omega(p) = 4$ o bé $\omega(p) = 5$, il·lustrada a la Figura 3.9. Aleshores, $P = X \cup Y$, on $X = \omega^{-1}(4)$ i $Y = \omega^{-1}(5)$ i

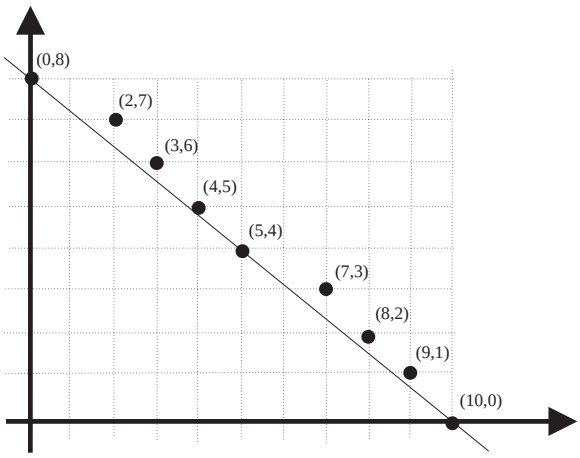

Figura 2.9: Estructura d'accés Γ definida per pesos 4 i 5 i per llindar $t = 40$ amb $|\omega^{-1}(4)| > 10$ i $|\omega^{-1}(5)| > 8$.

Γ és la (X, Y)-estructura d'accés bipartita definida per $\pi(\Gamma) = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \,|\, 4x + 5y \geq 40\}$. El conjunt de punts minimals de Γ és $\Pi_0(\Gamma) = \{(0, 8), (2, 7), (3, 6), (4, 5), (5, 4), (7, 3), (8, 2), (9, 1), (10, 0)\}$. Observem que $\Gamma =$

$\Gamma_1 \cup \Gamma_2$, on Γ_1 és l'estructura d'accés bipartita amb conjunt de punts minimals $\Pi_0(\Gamma_1) = \{(0,8),(2,7),(3,6),(4,5),(5,4)\}$ i Γ_2 és la (t,N)-estructura de llindar amb $t = 10$. Com que ambdues Γ_1 i Γ_2 són estructures d'accés ideals, podem trobar un esquema per a compartir secrets realitzant Γ amb taxa d'informació igual a $1/2$. Per tant, $\rho^*(\Gamma) \geq 1/2$.

En general, com que qualsevol estructura d'accés bipartita amb només un punt minimal pot ser realitzada per un esquema ideal, una estructura d'accés bipartita Γ amb r punts minimals té taxa d'informació òptima $\rho^*(\Gamma) \geq 1/r$, perquè és la unió de r estructures d'accés ideals.

La segona tècnica que farem servir per trobar fites inferiors de la taxa d'informació òptima està basada en la proposició següent.

Proposició 2.2.8 *Siguin a, b enters positius i sigui Γ' una (aN_1, bN_2)-estructura d'accés bipartita ideal. Sigui Γ una (N_1, N_2)-estructura d'accés bipartita tal que $(x,y) \in \pi(\Gamma)$ si i només si $(ax, by) \in \pi(\Gamma')$. Llavors, $\rho^*(\Gamma) \geq \min\{1/a, 1/b\}$.*

Demostració: Siguin $P' = X' \cup Y'$ i $P = X \cup Y$ respectivament el conjunt de participants de l'estructura d'accés Γ' i Γ. Per tal de definir un esquema per a compartir secrets Σ en Γ, identifiquem cada participant $p_i \in X$, on $1 \leq i \leq N_1$, amb un subconjunt $S_i \subset X'$ amb a elements de tal manera que $X' = \cup_{i=1}^{N_1} S_i$. Igualment, cada participant $q_j \in Y$, on $1 \leq j \leq N_2$, és identificat amb un subconjunt $T_j \subset Y'$ de b elements i, com abans, $Y' = \cup_{j=1}^{N_2} T_j$. Sigui Σ' un esquema ideal amb estructura d'accés Γ' i conjunt de secrets $\mathcal{K}$. L'esquema Σ està definit de la manera següent: donat un secret $k \in \mathcal{K}$, el fragment d'un participant $p_i \in X$ està format pels a fragments que corresponen als participants del conjunt $S_i' \subset X'$ per l'esquema ideal Σ' i el fragment d'un participant $q_j \in Y$ consisteix en els b fragments dels participants de $T_j \subset Y'$. No és difícil veure que Σ és un esquema per a compartir secrets per Γ amb taxa d'informació $\rho(\Sigma, \Gamma, \mathcal{K}) = \min\{1/a, 1/b\}$.□

Aquesta proposició pot ser utilitzada, per exemple, per trobar fites inferiors per la taxa d'informació òptima d'una estructura d'accés definida per dos pesos i llindar. Aquestes són estructures d'accés bipartites tal que $(x,y) \in \pi(\Gamma)$ si i només si $ax + by \geq t$, on a, b, t són enters positius. Podem suposar que $a \leq b$. En aquest cas, podem aplicar la Proposició 3.2.8 essent Γ' la $(t, aN_1 + bN_2)$-estructura de llindar. Aleshores, $\rho^*(\Gamma) \geq 1/b$.

Per tal de provar que les fites inferiors obtingudes amb aquestes dues tècniques són en alguns casos ajustades, considerem, per a qualssevol enters positius r, b, l'estructura d'accés de pesos i llindar $\Gamma_{r,b}$ definida per l'equació $x + by \geq rb$.

Per la Proposició 3.2.8, $\rho^*(\Gamma_{r,b}) \geq 1/b$. D'altra banda, el conjunt de punts minimals de $\Gamma_{r,b}$ és $\Pi_0(\Gamma_{r,b}) = \{(kb, r-k) \in \mathbb{Z} \times \mathbb{Z} \,|\, 0 \leq k \leq r\}$. Sigui Γ_0 l'estructura d'accés bipartita, amb conjunt de punts minimals $\{(0,r),(rb,0)\}$. Per a qualsevol $k = 1, \ldots, r-1$, considerem Γ_k tal que $(kb, r-k)$ és el seu únic punt minimal. Observi's que per a qualsevol $k = 0, 1, \ldots, r-1$, Γ_k és una estructura d'accés ideal i, a més, $\Gamma_{r,b} = \cup_{k=0}^{r-1} \Gamma_k$. Per tant, $\rho^*(\Gamma_{r,b}) \geq 1/r$.

Per tal de trobar una fita superior de $\rho^*(\Gamma_{r,b})$, considerem la successió $B_1 \subset B_2 \subset \cdots \subset B_{rb-1}$, on $\pi(B_j) = (j, 0)$. Sigui X_1 tal que $X_1 \cap B_1 = \emptyset$ i $\pi(X_1) = (b-1, r-1)$ i $X_{kb+s} \subset X_1$, on $0 \leq k \leq r-1$ i $0 \leq s \leq b-1$, tal que $X_{kb+s} \cap B_{kb+s} = \emptyset$ i $\pi(X_{kb+s}) = (b-s, r-k-1)$. Llavors $A = X_1 \notin \Gamma$ fa independent la successió $B_1 \subset B_2 \subset \cdots \subset B_{rb-1}$. Per tant,

$$\max\{\frac{1}{r}, \frac{1}{b}\} \leq \rho^*(\Gamma_{r,b}) \leq \frac{b+r-2}{rb-1}$$

Aquesta fita inferior és ajustada perquè per a qualsevol enter positiu r i per a qualsevol $\epsilon > 0$, existeix un enter positiu b tal que

$$\frac{1}{r} \leq \rho^*(\Gamma_{r,b}) \leq \frac{1}{r} + \epsilon.$$

D'altra banda, si fixem b, per a qualsevol $\epsilon > 0$ podem trobar un valor de r tal que

$$\frac{1}{b} \leq \rho^*(\Gamma_{r,b}) \leq \frac{1}{b} + \epsilon.$$

Presentem una estructura d'accés bipartita Γ tal que $\rho^*(\Gamma) = 2/3$. Sigui Γ una (N_1, N_2)-estructura d'accés bipartita amb conjunt de punts minimals $\Pi_0 = \{(0,3),(1,1)\}$ representada a la Figura 3.10. Considerem la $(2N_1, N_2)$-estructura d'accés bipartita ideal $\Gamma' = \Omega_4(3,2,3)$ amb conjunt de punts minimals $\Pi_0' = \{(0,3),(1,2),(2,1)\}$. És clar que $(x,y) \in \pi(\Gamma)$ si i només si $(2x, y) \in \pi(\Gamma')$. Sigui Σ' un esquema ideal per l'estructura d'accés Γ' i conjunt de secrets $\mathcal{K}$. Sigui Σ_1 l'esquema per a compartir secrets per l'estructura d'accés Γ_1 i conjunt de secrets $\mathcal{K}$ construït a partir de Σ' utilitzant la idea de la demostració de la Proposició 3.2.8. Aleshores a l'esquema Σ_1 cada participant $p \in X$ rep com a fragment dos elements de $\mathcal{K}$, que són els fragments corresponents a dos participants a l'esquema Σ', i els fragments pels participants de Y s'agafen a $\mathcal{K}$. D'altra banda, $\Gamma = \Gamma_1 \cup \Gamma_2$, on l'únic punt minimal de Γ_1 és $(0,3)$ i l'únic punt minimal de Γ_2 és $(1,1)$. Considerem l'esquema Σ_2 per Γ amb conjunt de secrets $\mathcal{K}$ definit a partir d'esquemes ideals per Γ_1 i Γ_2. Com que els participants de X no apareixen a Γ_1 els seus fragments s'agafen de $\mathcal{K}$. Els fragments dels participants de Y s'agafen de $\mathcal{K}^2$. Per acabar considerem

l'esquema Σ per Γ definit de la manera següent: donat un secret $(k_1, k_2) \in \mathcal{K}^2$, el distribuïdor reparteix k_1 utilitzant Σ_1 i k_2 utilitzant Σ_2. Cada participant rep un fragment de $\mathcal{K}^3$. Per tant, $\rho^*(\Gamma) \geq 2/3$. A partir del Teorema 3.2.6 tenim $\rho^*(\Gamma) \leq 2/3$. Llavors, $\rho^*(\Gamma) = 2/3$.

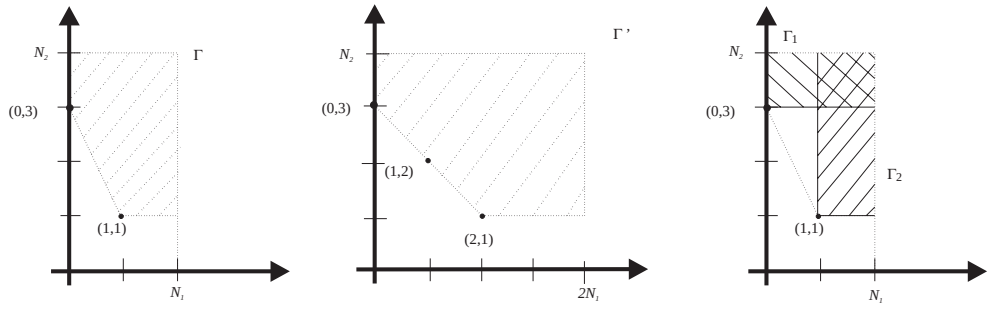

Figura 2.10: Estructures d'accés Γ, Γ', Γ_1 i Γ_2

Presentem un algorisme que, per una estructura d'accés bipartita donada, computa la millor fita superior de la taxa d'informació òptima que pot ser trobada directament a partir del Teorema 2.8.6.

Lema 2.2.9 *Sigui* Γ *una estructura d'accés bipartita amb* Π_0 *la col·lecció dels seus punts minimals. Considerem qualsevol subconjunt* $(x_1, y_1), (x_2, y_2), \ldots (x_s, y_s)$ *de punts consecutius de* Π_0. *Anomenem* $b = y_1 - y_{s-1}$, $a_i = x_i - x_{i-1}$, *per* $2 \leq i \leq s$, *i* $a_1 = x_1 + 1$. *Aleshores, per a qualsevol* $\alpha = 1, \ldots, \max\{a_1, \ldots a_s\}$,

$$\rho^* \leq \frac{\alpha + b}{-1 + \sum_{i=1}^{s} \min\{\alpha, a_i\}}$$

Demostració: Siguin $\alpha_i = \min\{\alpha, a_i\}$ per $1 \leq i \leq s$. Considerem la successió de subconjunts

$$B_{11} \subset \cdots \subset B_{1\alpha_1} \subset B_{21} \subset \cdots \subset B_{2\alpha_2} \subset \cdots \subset B_{s1} \subset \cdots \subset B_{s\alpha_s - 1}$$

on $\pi(B_{ij}) = (x_i - \alpha_i + j, y_{s-1} - 1)$ per $1 \leq j \leq \alpha_i$ si $1 \leq i \leq s-1$ i $1 \leq j \leq \alpha_s - 1$ si $i = s$. Sigui la successió

$$X_{11}, \cdots, X_{1\alpha_1}, X_{21}, \cdots, X_{2\alpha_1}, \cdots, X_{s1}, \cdots, X_{s\alpha_s - 1}$$

amb $\pi(X_{ij}) = (x_i, y_i) - \pi(B_{ij}) = (\alpha_i - j, y_i - y_{s-1} + 1)$ per $1 \leq j \leq \alpha_i$ quan $1 \leq i \leq s-1$ (veure Figura 3.11) i per $i = s$ agafem X_{sj} tal que $\pi(X_{sj}) = (x_s, y_{s-1} - 1) - \pi(B_{sj}) = (\alpha_s - j, 0)$, per $1 \leq j \leq \alpha_s - 1$.

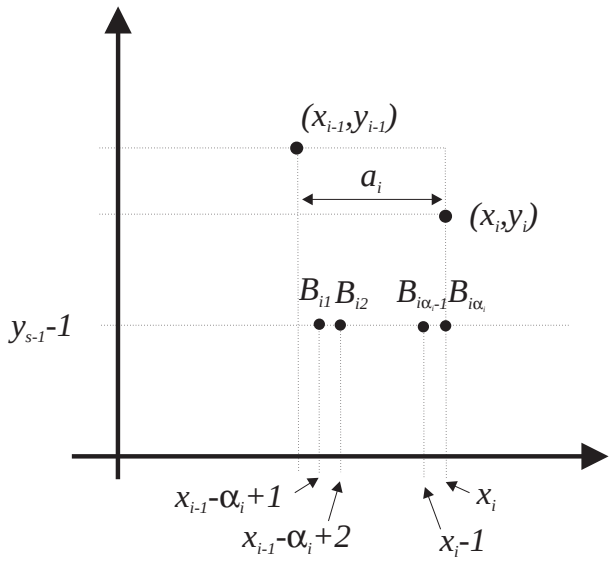

Figura 2.11: Successió $\{B_{ij}\}_{i,j}$ per $i \neq s$.

Podem escollir $B_{ij} \cap X_{ij} = \emptyset$ ja que $|X| \geq x_s$ i $|Y| \geq y_1$. Les dues successions de subconjunts verifiquen $X_{ij} \cup B_{ij} \in \Gamma$ perquè $\pi(X_{ij} \cup B_{ij})$ és, per construcció, el punt associat a un subconjunt autoritzat. Per $j \neq 1$ tenim $\pi(X_{ij} \cup B_{ij-1}) = (x_i - 1, y_i)$, punt d'un subconjunt no autoritzat, per la qual cosa $X_{ij} \cup B_{ij-1} \notin \Gamma$. Per $j = 1$ tenim $\pi(X_{i1} \cup B_{i-1\alpha_{i-1}}) = (x_{i-1} + \alpha_i - 1, y_i - 1)$, punt d'un no autoritzat i per tant $X_{i1} \cup B_{i-1\alpha_{i-1}} \notin \Gamma$. Si diem $A = \bigcup_{i,j} X_{ij}$, tenim $|A| = \max_{i,j}(\alpha_i - j) + \max_i(y_i - y_{s-1}) = \max_i(\alpha_i - 1) + y_1 - y_{s-1} + 1 = \alpha - 1 + b + 1 = \alpha + b$. Utilitzant el fet que la longitud de la successió és $\alpha_1 + \ldots + \alpha_s - 1 = -1 + \sum_{i=1}^{s} \min\{\alpha, a_i\}$, el resultat queda provat. □

Anem a descriure un algorisme per trobar una fita superior de la taxa d'informació òptima que es basa en el lema anterior. Segons aquest resultat cal trobar el mínim d'una funció definida per a uns certs valors. Denotem per $A_1 < \ldots < A_r$ els nombres $a_1, \ldots, a_s$ ordenats de forma que A_i surt γ_i vegades amb $\gamma_i \geq 1$, $\gamma_1 + \ldots + \gamma_r = s$ i també $1 \leq r \leq s$. Hem de trobar el mínim de la funció

$$\varphi(\alpha) = \frac{\alpha + b}{-1 + \sum_{i=1}^{r} \gamma_i \min\{\alpha, A_i\}}$$

Suposem que $A_r \neq 1$. De la funció φ ens interessa només els valors que pren sobre $\mathbb{Z}$, però nosaltres la considerarem sobre l'interval real $[1, \max\{a_1, \ldots, a_s\}] = [1, A_r]$, per facilitar-nos els raonaments. S'observa que $\varphi(\alpha)$ és una funció contínua en aquest interval.

Si $A_1 \neq 1$ tenim que a l'interval $]1, A_1[$ la funció és derivable amb

$$\varphi(\alpha) = \frac{\alpha + b}{-1 + s\alpha},\ \varphi'(\alpha) = \frac{-1 - bs}{(-1 + s\alpha)^2}$$

En el cas que $A_1 = 1$ llavors tenim que a l'interval $]A_1, A_2[$ la funció és derivable amb

$$\varphi(\alpha) = \frac{\alpha + b}{-1 + \gamma_1 A_1 + (\gamma_2 + \ldots + \gamma_r)\alpha},\ \varphi'(\alpha) = \frac{-1 + \gamma_1 A_1 - b(\gamma_2 + \ldots + \gamma_r)}{(-1 + \gamma_1 A_1 + (\gamma_2 + \ldots + \gamma_r)\alpha)^2}$$

A l'interval $[A_i, A_{i+1}]$ amb $i \geq 1$ la funció pren valors

$$\varphi(\alpha) = \frac{\alpha + b}{-1 + \gamma_1 A_1 + \ldots + \gamma_i A_i + (\gamma_{i+1} + \ldots + \gamma_r)\alpha}$$

És derivable a l'interval $]A_i, A_{i+1}[$ amb derivada de signe constant

$$\varphi'(\alpha) = \frac{-1 + \gamma_1 A_1 + \ldots + \gamma_i A_i - b(\gamma_{i+1} + \ldots + \gamma_r)}{(-1 + \gamma_1 A_1 + \ldots + \gamma_i A_i + (\gamma_{i+1} + \ldots + \gamma_r)\alpha)^2}$$

per $i = 1, \ldots, r-1$. El signe de $\beta_i = -1 + \gamma_1 A_1 + \ldots + \gamma_i A_i - b(\gamma_{i+1} + \ldots + \gamma_r)$ per $i = 1, \ldots, r-1$ decideix quin és el valor mínim d'aquesta funció. Aquesta successió és estrictament decreixent. L'algorisme per trobar el mínim consisteix en buscar el primer valor i pel qual $\beta_i \geq 0$ verificant-se llavors que $\rho^* \leq \varphi(A_i)$. S'observa que trobar el primer i pel qual $\beta_i \geq 0$, és equivalent a dir que

$$\gamma_1(A_1 + b) + \ldots + \gamma_i(A_i + b) > bs$$

i que llavors obtenim

$$\rho^* \leq \frac{A_i + b}{-1 + \gamma_1 A_1 + \ldots + \gamma_{i-1} A_{i-1} + (\gamma_i + \ldots + \gamma_r) A_i}$$

Cal assenyalar que aquest algorisme s'ha d'aplicar a qualsevol subconjunt de punt consecutius de Π_0 així com al subconjunt resultat d'intercanviar la primera i la segona coordenada dels punts. Aquest darrer subconjunt de punts correspon a una estratègia consisten en agafar els subconjunt independents amb primera coordenada fixada, simètrica a l'estratègia d'agafar la segona coordenada fixa.

Podem resumir l'algorisme en el quadre:

Algorisme per trobar una fita superior de ρ^* per Γ bipartita
Sigui una estructura d'accés bipartita Γ amb Π_0 la col·lecció dels seus punts minimals. Per un subconjunt de punts $(x_1, y_1), (x_2, y_2), \ldots, (x_s, y_s)$ de Π_0 denotem per:
$b = y_1 - y_{s-1},\ a_i = x_i - x_{i-1}$ per $2 \leq i \leq s$, i $a_1 = x_1 + 1$.
Siguin $A_1 < \ldots < A_r$ els nombres $a_1, \ldots, a_s$ ordenats de forma que A_i surt γ_i vegades.
Es determina el mínim i tal que
$\gamma_1(A_1 + b) + \ldots + \gamma_i(A_i + b) > bs$
i llavors podem afirmar

$$\rho^* \leq \frac{A_i + b}{-1 + \gamma_1 A_1 + \ldots + \gamma_{i-1} A_{i-1} + (\gamma_i + \ldots + \gamma_r) A_i}$$

Repetir sobre tot subconjunt consecutiu de punts de Π_0 i sobre el conjunt de punts resultat d'intercanviar la primera i la segona coordenada.

Aquest algorisme ha estat estudiat i implementat en el Projecte Final de Carrera [86] realitzat a l'*Escola Tècnica Superior d'Enginyeria de Telecomunicacions de Barcelona*.

Un cas particular és quan considerem només dos punts minimals de la forma $(x_1, y_1), (x_1 + a, y_1 - c)$ amb $x_1 > 0,\ y_1 > 1,\ a, c \geq 1$ com queda il·lustrat a la Figura 3.12.

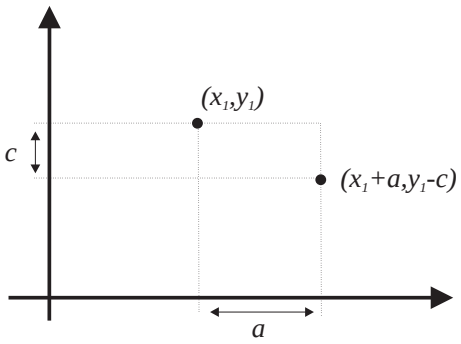

Figura 2.12: Cas de dos minimals en una estructura bipartita.

Llavors $s = 2, b = y_1 - y_1 = 0,\ a_1 = x_1 + 1, a_2 = x_1 + a - x_1 = a$. Ara hem d'ordenar a_1, a_2. Si $a_1 \neq a_2$ llavors obtindrem $A_1 < A_2$, $r = 2$ i $\gamma_1 = \gamma_2 = 1$. La mínima i que verifica la condició és $i = 1$ perquè $1 \cdot (A_1 + 0) > 0 \cdot 2$, per tant

$\rho^* \leq A_1/(-1+2A_1)$. En el cas que $a_1 = a_2$ llavors obtindrem $r = 1$ i $\gamma_1 = 2$. La mínima i que verifica la condició és també $i = 1$ perquè $1 \cdot (A_1 + 0) > 0 \cdot 2$ obtenint la mateixa fitació. Resumint podem dir que

$$\rho^* \leq \frac{A_1}{-1+2A_1}$$

amb $A_1 = \min\{x_1 + 1, a\}$.

2.2.3 Generalització per estructures d'accés multipartites

Les estructures bipartites les hem considerat a la Secció 3.2 com a una generalització de les estructures definides per dos pesos i llindar. Aquestes estructures gaudeixen d'una simetria entre els participants de cadascuna de les parts X, Y en que està subdividit el conjunt de participants. Per aquest tipus d'estructures d'accés hem caracteritzat les estructures ideals i hem donat mètodes per a determinar fites inferiors i superiors per a la taxa d'informació òptima.

Generalitzant aquest estudi considerarem el cas en el qual el conjunt de participants estigui subdividit en ℓ parts de participants intercanviables dins d'una mateixa part. Exemple immediat d'aquest tipus d'estructures són les estructures definides per ℓ pesos diferents i un llindar.

Sigui Γ una estructura d'accés en un conjunt de participants P dividit en ℓ parts, $P = X_1 \cup \ldots \cup X_\ell$ disjuntes dos a dos, això és $X_i \cap X_j = \emptyset$ per $i \neq j$. Direm que Γ és una $(X_1, \ldots, X_\ell)$-*estructura d'accés multipartita* si $\sigma(\Gamma) = \Gamma$ per a qualsevol permutació σ de P amb $\sigma(X_i) = X_i$ per a tota i.

Donada una partició $P = X_1 \cup \ldots \cup X_\ell$ del conjunt P, per a qualsevol subconjunt $A \subset P$, considerem el punt $\pi(A) = (x_1(A), \ldots, x_\ell(A)) \in \mathbb{Z}^\ell$, on $x_i(A) = |\, A \cap X_i \,|$. Donada una $(X_1, \ldots, X_\ell)$-estructura d'accés multipartita Γ, considerem la regió

$$\pi(\Gamma) = \{\pi(A) \,|\, A \in \Gamma\} \subset \mathbb{Z}^\ell.$$

Com en el cas de les bipartites és fàcil veure que $A \in \Gamma$ si i només si $\pi(A) \in \pi(\Gamma)$. Per tant Γ està determinada per la regió $\pi(\Gamma) \subset \mathbb{Z}^\ell$.

Podem considerar el conjunt $\Pi_0 = \pi(\Gamma_0)$, els elements del qual els anomenarem *punts minimals* de Γ. Evidentment, Γ està determinada pels punts de Π_0.

Per tal de determinar una fita inferior de la taxa d'informació òptima utilitzarem una estructura multipartita ideal per a fer recobriments:

Proposició 2.2.10 *Sigui* $P = X_1 \cup \ldots \cup X_\ell$ *amb* $X_i \cap X_j = \emptyset$ *per* $i \neq j$ *i nombres naturals* $n_1, n_2, \ldots, n_\ell$ *tals que* $n_i \leq |X_i|$. *L'estructura d'accés* Ω_1 *definida per*

$$A \in \Omega_1 \text{ si i només si } x_1(A) \geq n_1 \quad i \quad \ldots \quad i \quad x_\ell(A) \geq n_\ell$$

és una estructura ideal.

Demostració: És fàcil comprovar que la funció

$$\begin{array}{rlll} \psi: & P \cup \{D\} & \longrightarrow & GF(q)^{n_1+\ldots+n_\ell} \\ & p_i & \longmapsto & (1, x_i, \ldots, x_i^{n_1-1}, \ldots, 0, 0, \ldots, 0) \text{ si } p_i \in X_1 \\ & \ldots & \ldots & \ldots \\ & p_i & \longmapsto & (0, 0, \ldots, 0, \ldots, 1, x_i, \ldots, x_i^{n_\ell-1}) \text{ si } p_i \in X_\ell \\ & D & \longmapsto & (1, 0, \ldots, 1, 0, \ldots, 0) \end{array}$$

amb $x_1, \ldots, x_n$ elements no nuls de $GF(q)$ defineix l'estructura d'accés Ω_1. Aquesta distribució de fragments correspon a un esquema polinomial de Shamir modificat, en el qual el secret és $k = p_1(0) + \ldots + p_\ell(0)$ repartint fragments amb $p_i(x) = a_{i0} + a_{i1}x + a_{i2}x^2 + \ldots + a_{in_i-1}x^{n_i-1}$ si $p_i \in X_i$. □

De la mateixa manera es demostra que una altra estructura d'accés multipartita ideal és:

Proposició 2.2.11 *Sigui* $P = X_1 \cup \ldots \cup X_\ell$ *amb* $X_i \cap X_j = \emptyset$ *per* $i \neq j$ *i nombres naturals* $n_1, n_2, \ldots, n_\ell$ *tals que* $n_i \leq |X_i|$. *L'estructura d'accés* Ω_2 *definida per*

$$A \in \Omega_2 \text{ si i només si } x_1(A) \geq n_1 \quad o \quad \ldots \quad o \quad x_\ell(A) \geq n_\ell$$

és una estructura ideal.

En aquest cas l'aplicació que s'utilitza és la definida per

$$\psi(p_i) = (1, x_i, \ldots, x_i^{n_1-1}, \ldots, 0, 0, \ldots, 0) \text{ si } p_i \in X_1$$

$$\psi(p_i) = (1, 0, \ldots, 0, \ldots, 0, x_i, \ldots, x_i^{n_\ell-1}) \text{ si } p_i \in X_\ell$$

i $\psi(D) = (1, 0, \ldots, 0)$ que correspon a la distribució amb un esquema polinomial de Shamir modificat en el qual es calcula el fragment amb $p_i(x) = k + a_{i1}x + a_{i2}x^2 + \ldots + a_{in_i-1}^{n_i-1}$ si $p_i \in X_i$.

Trivialment recobrint una estructura multipartita per $|\Pi_0|$ estructures ideals del tipus Ω_1 s'obté el resultat:

Proposició 2.2.12 *Per a una estructura multipartita amb conjunt de punts minimals* Π_0 *es verifica*

$$\rho^* \geq \frac{1}{|\Pi_0|}$$

Per la fita superior es pot trobar un resultat semblant al donat pel Lema 3.2.9 i l'algorisme posterior.

2.3 Fites per les estructures de llindar amb dos pesos

S'han estudiat les estructures d'accés de rang 2 definides per pesos i llindar a la Secció 3.1 trobant fites inferiors per la taxa d'informació òptima. En aquesta Secció estudiarem fonamentalment la taxa d'informació per estructures definides per dos pesos i llindar amb rang arbitrari. També ens hem plantejat l'estudi a la Secció 3.2 d'una família més àmplia que la definida per dos pesos i llindar, la de les estructures bipartites. Per tant particularitzarem els resultats de la Secció 3.2 al nostre cas.

En primer lloc es troben fites inferiors de la taxa d'informació òptima amb les tècniques per a estructures bipartites de la Secció 3.2.2. A continuació es troben fites superiors fent servir els resultats de la Secció 3.2.2 adaptats al cas de dos pesos.

2.3.1 Fites inferiors de la taxa d'informació òptima per dos pesos i llindar

Com que una família particular de les estructures bipartites són les estructures definides per dos pesos i llindar, només caldrà aplicar les tècniques ja estudiades a la secció 3.2.2.

Sigui una estructura Γ definida per dos pesos ω_1, ω_2 i el llindar t amb $0 < \omega_1 < \omega_2 < t$. L'estructura Γ així definida és una (X, Y)-estructura d'accés bipartita pel conjunt $X = \omega^{-1}(\omega_1)$ dels participants de pes ω_1 i pel conjunt $Y = \omega^{-1}(\omega_2)$ dels participants de pes ω_2.

Recordem que per a un conjunt $A \subset P$ denotarem per $x(A) = |A \cap X|$, $y(A) = |A \cap Y|$ i per $\pi(A) = (x(A), y(A)) \in \mathbb{Z} \times \mathbb{Z}$. D'aquesta manera $A \in \Gamma$ si i només si $\pi(A) \in \pi(\Gamma)$ amb $\pi(\Gamma) = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} | \omega_1 x + \omega_2 y \geq t,\ 0 \leq x \leq |X|,\ 0 \leq y \leq |Y|\}$. Anomenarem $\Pi = \pi(\Gamma)$ i $\Pi_0 = \pi(\Gamma_0)$.

La primera fita inferior que podem trobar és la que ens dóna la Proposició 3.2.8: $\rho^*(\Gamma) \geq 1/\omega_2$. Aquesta fita coincideix amb la que s'obté fent servir

l'esquema que Shamir va proposar a [83]. En aquest esquema es lliura a cada participant tants fragments com indiqui el seu pes. El participant que en rep més és el de pes màxim, és a dir de pes ω_2, per la qual cosa la taxa d'informació és més gran que $1/\omega_2$.

La fita següent per a la taxa d'informació òptima la obtindrem recobrint la regió $\pi(\Gamma)$ mitjançant estructures ideals.

Proposició 2.3.1 *Suposem que $\omega(P) = \{\omega_1, \omega_2\}$ amb $\omega_1 < \omega_2 < t$ i $|X| \geq \lceil t/\omega_1 \rceil$, $|Y| \geq \lceil t/\omega_2 \rceil$, llavors la taxa d'informació òptima per l'estructura definida per ω i t verifica*

$$\rho^* \geq \frac{1}{\left\lceil \frac{t}{\omega_2} \right\rceil}$$

Demostració: Podem recobrir la regió $\pi(\Gamma)$ de la manera següent

$$\pi(\Gamma) = \left\{ (x,y) \in \mathbb{Z} \times \mathbb{Z} | x \geq \left\lceil \frac{t}{\omega_1} \right\rceil \text{ o bé } y \geq \left\lceil \frac{t}{\omega_2} \right\rceil \right\} \cup$$

$$\left(\bigcup_{k=1}^{\left\lceil \frac{t}{\omega_2} \right\rceil - 1} \left\{ (x,y) \in \mathbb{Z} \times \mathbb{Z} | x \geq \left\lceil \frac{t - \omega_2 k}{\omega_1} \right\rceil, \ y \geq k \right\} \right)$$

cadascuna d'aquestes subestructures és ideal segons hem provat al Teorema 3.2.1 i per tant $\rho^* \geq 1/\left\lceil \frac{t}{\omega_2} \right\rceil$ fent servir el fet que podem distribuir un fragment per a cadascuna de les estructures ideals. □

Per tal de trobar fites inferiors de la taxa d'informació òptima quan $|X| < \lceil t/\omega_1 \rceil$ o bé quan $|Y| < \lceil t/\omega_2 \rceil$ definim $T_m(x_m, y_m)$ com el punt de $\mathbb{Z} \times \mathbb{Z}$ verificant $\omega_1 x + \omega_2 y \geq t$, $0 \leq x \leq |X|$, $0 \leq y \leq |Y|$ amb suma de coordenades mínima.

Si $|Y| = n_2 \geq \left\lceil \frac{t}{\omega_2} \right\rceil$ aleshores

$$T_m(0, \left\lceil \frac{t}{\omega_2} \right\rceil)$$

i si $|Y| = n_2 < \left\lceil \frac{t}{\omega_2} \right\rceil$ llavors

$$T_m(\left\lceil \frac{t - \omega_2 n_2}{\omega_1} \right\rceil, n_2)$$

Sigui $T_M(x_M, y_M)$ el punt amb suma de coordenades màxima a la mateixa regió. Si $|X| \geq \left\lceil \frac{t}{\omega_1} \right\rceil$ aleshores

$$T_M(\left\lceil \frac{t}{\omega_1} \right\rceil, 0)$$

i si $|X| = n_1 < \left\lceil \frac{t}{\omega_1} \right\rceil$ llavors

$$T_M(\left\lceil \frac{t - \omega_2 \left\lceil \frac{t-\omega_1 n_1}{\omega_2} \right\rceil}{\omega_1} \right\rceil, \left\lceil \frac{t - \omega_1 n_1}{\omega_2} \right\rceil)$$

En termes de T_m i T_M podem expressar, per exemple, $\operatorname{rang} \Gamma = x_M + y_M$ i fent servir la mateixa idea que a la demostració de la Proposició 3.3.1 tenim

Proposició 2.3.2 *Suposem que $\omega(P) = \{\omega_1, \omega_2\}$ amb $\omega_1 < \omega_2 < t$ llavors la taxa d'informació òptima per l'estructura definida per ω i t verifica*

$$\rho^* \geq \frac{1}{y_m - y_M + 1}$$

No és aquesta l'única manera de recobrir tots els punts de Π. Per exemple si $\lceil \omega_2/\omega_1 \rceil = 2$ llavors és millor (o igual) la taxa d'informació que resulta de fer servir les estructures ideals de la forma

$$\{(x, y) | y \geq k,\ x + y \geq k + \ell\}$$

(estructures que són de quasi llindar, en concret Ω_4), perquè en molts casos s'abarquen dos punts minimals en una estructura. El recompte del nombre d'estructures que calen ens porta a $\rho^* \geq 1(\lceil t/\omega_1 \rceil - \lceil t/\omega_2 \rceil)$ quan $|X| \geq \lceil t/\omega_1 \rceil$, $|Y| \geq \lceil t/\omega_2 \rceil$ o més en general:

$$\rho^* \geq \frac{1}{x_M - x_m + y_M - y_m + 1}$$

que coincideix amb $\rho^* \geq 1/(d(T_m, T_M) + 1)$ amb d la *distància del taxista.*

2.3.2 Fites superiors de la taxa d'informació òptima per esquemes per dos pesos i llindar

Per trobar fites superiors de la taxa d'informació òptima a cada cas concret farem servir l'algorisme que s'ha trobat a partir del Lema 3.2.9. De tota manera donarem una fita superior per un cas particular d'aquest tipus d'estructures bipartites:

Proposició 2.3.3 *Suposem que* $\omega(P) = \{\omega_1, \omega_2\}$ *amb* $\omega_1 < \omega_2 < t$ *amb* $|\omega^{-1}(\omega_1)| \geq \left\lceil \frac{t}{\omega_1} \right\rceil$ *i* $|\omega^{-1}(\omega_2)| \geq \left\lceil \frac{t}{\omega_2} \right\rceil$ *aleshores la taxa d'informació òptima per l'estructura definida per* ω *i* t *verifica*

$$\rho^* \leq \frac{\lceil \omega_2/\omega_1 \rceil + \lceil t/\omega_2 \rceil - 2}{(\lceil \omega_2/\omega_1 \rceil - 1)\lceil t/\omega_2 \rceil}$$

Demostració: Apliquem el Lema 3.2.9 i s'obté $s = \lceil t/\omega_2 \rceil + 1$, $b = \lceil t/\omega_2 \rceil - 1$, $a_1 = 1$, $a_i = \lceil \omega_2/\omega_1 \rceil$ o bé $\lceil \omega_2/\omega_1 \rceil - 1$. La funció que cal minimitzar és

$$\varphi(\alpha) = \frac{\alpha + b}{-1 + \min\{\alpha, 1\} + s_1 \min\{\alpha, \left\lceil \frac{\omega_2}{\omega_1} \right\rceil\} + s_2 \min\{\alpha, \left\lceil \frac{\omega_2}{\omega_1} \right\rceil - 1\}} \leq$$

$$\frac{\alpha + b}{-1 + \min\{\alpha, x_m + 1\} + (s-1)\min\{\alpha, \left\lceil \frac{\omega_2}{\omega_1} \right\rceil - 1\}}$$

essent s_1 el número de subíndexos $i \neq 1$ tals que $a_i = \lceil \omega_2/\omega_1 \rceil$ i s_2 el número de subíndexos $i \neq 1$ tals que $a_i = \lceil \omega_2/\omega_1 \rceil - 1$. Per tant el problema de minimització queda reduït a un altre amb $s = \lceil t/\omega_2 \rceil + 1$, $b = \lceil t/\omega_2 \rceil - 1$, $a_1 = 1$, $a_i = \lceil \omega_2/\omega_1 \rceil - 1$. Aplicant ara l'algorisme tenim $r = 2$, $A_1 = 1$, $\gamma_1 = 1$, $A_2 = \lceil \omega_2/\omega_1 \rceil - 1$, $\gamma_2 = s - 1$. El valor mínim de l'índex i no és 1 i per 2 ens dóna la fitació de l'enunciat. □

Per exemple si considerem pes $\omega_1 = k$ i $\omega_2 = n$ un pes molt més gran amb llindar $t = kn$, obtenim que la fita superior és aproximadament $1/k$. Aquesta fitació junt amb la fita inferior que s'obté aplicant la Proposició 3.3.2 a $T_m(0, k)$, $T_M(n, 0)$ ens proporciona

$$\frac{1}{k+1} \leq \rho^* \leq \frac{1}{k} + \frac{k-1}{k\,(\lceil n/k \rceil - 1)}$$

2.3.3 Generalització per fites de la taxa d'informació òptima per més de dos pesos

En les seccions anteriors hem estudiat fites per la taxa d'informació òptima d'estructures definides per pesos i llindar sota certes restriccions. Així les estructures d'accés de rang 2 definides per pesos i llindar han estat tractades a la Secció 3.1 trobant fites inferiors per la taxa d'informació òptima. A la Secció 3.3 s'han estudiat fites superiors i inferiors pel cas de tenir un rang arbitrari però disposar només de dos pesos. Aquest segon cas s'ha plantejat

com a cas particular d'estructura bipartita (Secció 3.2). Ara considerarem estructures definides per pesos i llindar sense cap restricció, com a cas particular d'estructura multipartita, estudiades a la Secció 3.2.3.

Sigui Γ una estructura definida per pesos naturals $\omega : P \longrightarrow \mathbb{N}$ i un llindar $t \in \mathbb{N}$. En primer lloc hem de recordar que tenim com a primera fita de la taxa d'informació òptima la donada per l'esquema proposat per Shamir a [83]. Aquest consisteix en repartir el secret segons un esquema de llindar ideal entre tants participants com pes té el conjunt P. A continuació es reparteix a cada participant tants fragments com indiqui el seu pes. Aquest esquema és un esquema perfecte que realitza l'estructura definida per pesos i llindar amb taxa d'informació $1/W$ amb W el pes màxim d'un participant.

Podem particularitzar els resultats obtinguts per estructures multipartites a estructures definides per pesos i llindar. L'aplicació de la Proposició 3.2.12 ens dóna una fita inferior de la taxa d'informació òptima.

Proposició 2.3.4 *Suposem que* $\omega(P) = \{\omega_1, \omega_2, \ldots, \omega_k\}$ *amb* $\omega_1 < \omega_2 < \ldots < \omega_k < t$ *verificant que* $|\omega^{-1}(\omega_i)| \geq \lceil t/\omega_i \rceil$ *per a tot* $i = 1, \ldots, k$, *aleshores la taxa d'informació òptima per l'estructura definida per* ω *i* t *verifica*

$$\rho^* \geq \frac{1}{N_k(\omega_1, \omega_2, \ldots, \omega_k, t)}$$

on $N_k(\omega_1, \omega_2, \ldots, \omega_k, t) = \sum_{i=0}^{\lceil t/\omega_1 \rceil} N_{k-1}(\omega_1, \omega_2, \ldots, \omega_{k-1}, t - \omega_k i)$ *si* $t > 0, k \geq 3$;$N_k(\omega_1, \omega_2, \ldots, \omega_k, t) = 1$ *si* $t \leq 0$ *i* $N_2(\omega_1, \omega_2, t) = \lceil t/\omega_2 \rceil$ *si* $t \geq 0$.

Demostració: Aplicant la Proposició 3.2.12, només necessitarem calcular el cardinal de Π_0, el conjunt de punts minimals. Una fita del cardinal de Π_0 ve donada per $N_k(\omega_1, \omega_2, \ldots, \omega_k, t)$ definida a l'enunciat del teorema observant que es pot recobrir d'una forma recursiva

$$\{(x_1, \ldots, x_k) | \omega_1 x_1 + \ldots + \omega_k x_k \geq t,\ 0 \leq x_i \leq |\omega^{-1}(\omega_i)|\} =$$

$$\bigcup_{i=0}^{\lceil t/\omega_k \rceil} \{(x_1, \ldots, x_{k-1}) | \omega_1 x_1 + \ldots + \omega_{k-1} x_{k-1} \geq t - \omega_k i,\ 0 \leq x_i \leq |\omega^{-1}(\omega_i)|\} \times \{i\}$$

□

Aquest resultat es pot generalitzar a estructures per les quals no tots els pesos verifiquen $|\omega^{-1}(\omega_i)| \geq \lceil t/\omega_i \rceil$, de forma que la unió s'extén per $i = 0$ fins $m_i = \min\{\lceil t/\omega_k \rceil, |\omega^{-1}(\omega_k)|\}$. Tot això provoca un canvi a l'índex superior del sumatori que defineix N_k que va fins $i = \min\{\lceil t/\omega_k \rceil, |\omega^{-1}(\omega_k)|\}$, així com les diferents possibilitats per N_2 si $t \geq 0$ a partir dels valors de T_m i T_M.

És pot trobar una fita més explícita observant que $N_n(\omega_1, \ldots, \omega_n, t) \leq m_2 \cdot \ldots \cdot m_n$ de forma que $\rho^* \geq 1/(m_2 \cdot \ldots \cdot m_n)$. Pel cas que cada $|\omega^{-1}(\omega_i)| \geq \lceil t/\omega_i \rceil$ llavors podem dir $\rho^* \geq 1/(\lceil t/\omega_2 \rceil \cdot \ldots \cdot \lceil t/\omega_n \rceil)$.

Pel cas de la fita superior es pot aplicar una tècnica semblant a la utilitzada en el cas de les estructures definides per dos pesos i llindar. Aquesta consisteix en observar que la construcció d'una successió d'elements independent es pot fer tenint en compte només elements de pesos ω_i, ω_j amb $1 \leq i < j \leq k$ i prenent 0 elements de pes diferent de ω_i, ω_j. D'aquesta manera es redueix la construcció de la successió d'elements independents a la de dos pesos que es pot fer, com ja hem comentat a la Secció 3.3.2 amb l'algorisme determinat pel Lema 3.2.9. Així doncs, podem afirmar

Proposició 2.3.5 *Suposem que Γ és l'estructura definida pels pesos donats per ω i el llindar t en el conjunt P amb $\omega(P) = \{\omega_1, \omega_2, \ldots, \omega_k\}$ amb $\omega_1 < \omega_2 < \ldots < \omega_k < t$ amb $|\omega^{-1}(\omega_i)| \geq \left\lceil \frac{t}{\omega_i} \right\rceil$ per a tot i. Per a cada $1 \leq i < j \leq k$ anomenem Γ_{ij} l'estructura definida pels pesos ω_i, ω_j i llindar t en el conjunt de participants $P_{ij} = \omega^{-1}(\omega_i) \cup \omega^{-1}(\omega_j)$. En aquestes condicions la taxa d'informació òptima per Γ verifica*

$$\rho^* \leq \min_{1 \leq i < j \leq k} \frac{\lceil \omega_j/\omega_i \rceil + \lceil t/\omega_j \rceil - 2}{(\lceil \omega_j/\omega_i \rceil - 1)\lceil t/\omega_j \rceil}$$

2.4 Fites inferiors per les estructures homogènies

Dins del ventall d'estructures simples que s'han estudiat, cal destacar les definides per grafs i les de llindar. En tots dos casos tenim estructures homogènies, la primera de les quals és una subestructura de l'estructura de $(2, n)$-llindar. Com a generalització d'aquests dos casos, sembla bastant natural plantejar-se l'estudi de les estructures homogènies de rang arbitrari. A més tota estructura d'accés es pot posar com a reunió de subestructures homogènies.

Per totes aquestes raons hem buscat fites inferiors de la taxa d'informació òptima per les estructures homogènies. No ens oblidem que en el fons també busquem esquemes que realitzin l'estructura de la forma més raonable possible. L'estudi de la fita inferior de la taxa d'informació òptima per estructures homogènies ja s'ha plantejat per altres autors i algunes propostes s'han fet. Nosaltres hem proposat dues construccions amb les respectives fites inferiors. Hem fet una comparació de les fites entre elles i amb les que s'han proposat fins ara.

La clau pel càlcul d'aquestes fites és la introducció d'un nou paràmetre associat a un participant en una estructura homogènia. Aquest paràmetre és el *grau d'un participant*. Aquest paràmetre permet fins i tot millorar les fites proposades anteriorment.

2.4.1 Primera construcció

Aquestes fites es calculen en termes d'un paràmetre de l'estructura d'accés. El paràmetre és el *k-grau* d'un participant p, el qual és clarament una generalització del mateix concepte per un graf. Aquest paràmetre, $\deg(k,p)$, és el nombre de diferents k-subconjunts $A \subset P$ tals que $p \notin A$, i $A \cup \{p\} \subset B$ per a algun $B \in \Gamma_0$. En altres paraules, és el nombre de k-subconjunts diferents continguts en un subconjunt minimal autoritzat junt amb p. S'observa que en un graf el grau d'un vertex v és $\deg(1,v)$.

En termes del grau podem expressar, per exemple, el subconjunt de participants apareixent en almenys un subconjunt minimal autoritzat $P_0 = P(\Gamma_0)$ com $P_0 = \{p \in P | \deg(0,p) = 1\}$ perquè $\deg(0,p) = 1$ si i només si p apareix en algun minimal i $\deg(0,p) = 0$ quan no apareix en cap minimal. Una propietat del grau d'un vèrtex en un graf que té la seva generalització en una estructura d'accés homogènia de rang r és

$$\sum_{p \in P} \deg(r-1,p) = r|\Gamma_0|$$

la qual és la generalització del *Lema de les mans encaixades*, que diu que la suma dels graus dels vèrtexs en un graf dóna el doble del número d'arestes.

Trobarem les primeres fites utilitzant la *construcció per descomposició* deguda a D.R. Stinson [95] (veure Secció 2.7). Definirem una λ-descomposició per una estructura d'accés general Γ de rang r. Aquesta λ-descomposició és una col·lecció d'estrelles generalitzades a partir de la idea d'estrella en un graf [18, 92, 95, 27]. En una estructura d'accés homogènia de rang r, per a cada $B \subset P$ amb $|B| = r-1$ tal que existeixi $A \in \Gamma_0$, $B \subset A$, considerem l'*estrella des de un subconjunt* B o *estrella generalitzada* com

$$S_B = \{C \in \Gamma_0 | B \subset C\}$$

Aquesta subestructura de Γ va ser considerada per primera vegada per D.R. Stinson a [92]. És fàcil veure que S_B és ideal. Anomenem

$$\Omega(\Gamma) = \{B \subset P | |B| = r-1 \text{ i } S_B \neq \emptyset\}.$$

Serem capaços de trobar una fita inferior de la taxa d'informació òptima per a una estructura general utilitzant aquesta descomposició, com es pot veure a la proposició següent.

Teorema 2.4.1 *Sigui* Γ *una estructura d'accés homogènia de rang* $r \geq 2$ *definida en un conjunt de* N *participants. Per a cada* $q > |\Omega(\Gamma)|$ *potència d'un primer, existeix un esquema per a compartir secrets que realitza* Γ*, repartint secrets de* $\mathcal{K} = (GF(q))^r$ *amb taxa d'informació*

$$\rho_1 = \frac{r}{\max_{p \in P}(\deg(r-2,p) + \deg(r-1,p))}$$

i taxa mitjana d'informació

$$\tilde{\rho_1} = \frac{rN}{r|\Gamma_0| + \sum_{p \in P} \deg(r-2,p)}$$

Demostració: Per a cada $B \in \Omega(\Gamma)$ considerem l'estrella des del subconjunt B

$$S_B = \{C \in \Gamma_0 | B \subset C\}$$

una subestructura ideal de Γ verificant que $\Gamma_0 = \cup_{B \in \Omega(\Gamma)} S_B$. La col·lecció $\{S_B\}_{B \in \Omega(\Gamma)}$ és una λ-descomposició de Γ_0 amb $\lambda = \min_{A \in \Gamma_0} |\{S_B | A \in S_B\}|$. Sabem que $\lambda = r$ perquè per un $A \in \Gamma_0$ fixat, només pertany a les r estrelles S_B amb $B \subset A$ i $|B| = r-1$. Ara hauríem de calcular en quantes estrelles apareix un participant $p \in P_0$. Hi ha dos tipus d'estrelles diferents des del punt p. En primer lloc les estrelles S_B per a B amb $p \in B$ en un nombre de $\deg(r-2,p)$ per definició de grau. En segon lloc les estrelles S_B amb $p \notin B$ en un nombre de $\deg(r-1,p)$. Aplicant el Corol·lari 3.1 de [95] es troba la taxa d'informació.

Per calcular la taxa mitjana d'informació sabem que cada $\tilde{\rho}_h = 1$ perquè l'estrella és una estructura ideal. Hem de calcular $\sum_{h=1}^{n} |P_h|$. Utilitzarem una funció φ_h definida com $\varphi_h(p) = 1$ si $p \in P_h$ i $\varphi_h(p) = 0$ altrament. El càlcul és com segueix:

$$\sum_{h=1}^{n} |P_h| = \sum_{h=1}^{n} \sum_{p \in P} \varphi_h(p) = \sum_{p \in P} \sum_{h=1}^{n} \varphi_h(p)$$

De fet $\sum_{h=1}^{n} \varphi_h(p) = \deg(r-1,p) + \deg(r-2,p)$, per a un $p \in P$ fixat, perquè és el nombre d'estrelles en les quals p apareix com hem provat anteriorment. Aleshores la taxa mitjana d'informació òptima val

$$\tilde{\rho_1} = \frac{rN}{\sum_{p \in P}(\deg(r-1,p) + \deg(r-2,p))} = \frac{rN}{r|\Gamma_0| + \sum_{p \in P} \deg(r-2,p)}$$

□

Aquesta construcció ens proporciona una fita de la taxa d'informació òptima i una altra per la taxa d'informació mitjana òptima per una estructura homogènia de rang r. Per $r = 2$ recuperem la fita trobada per D.R. Stinson [95], això és, la taxa d'informació òptima està fitada inferiorment per $2/(1 + d)$, on d és el grau màxim del graf. De fet aquesta fita inferior és ajustada com C. Blundo, A. De Santis, R. De Simone i U. Vaccaro van provar a [20]. També en el cas $r = 2$ amb la taxa mitjana recuperem, una altra vegada, el resultat trobat per D.R. Stinson [95], és a dir, la taxa mitjana d'informació òptima està fitada inferiorment per $2N/(2M + N)$, on M és el nombre d'arestes i N el nombre de vèrtexs.

2.4.2 Segona construcció

La segona construccció es tracta d'una millora de la λ-descomposició i està inspirada en el treball [85] de H.M. Sun i S.P. Shieh. Per fer-la demostrem primer un parell de resultats tècnics, el primer dels quals ens indica que un participant aliè a la nostra estructura afegit a tots els subconjunts autoritzats no modifica la taxa d'informació.

Lema 2.4.2 *Sigui Γ una estructura d'accés en el conjunt P per a la qual existeix un esquema per a compartir secrets que per secrets escollits en $(GF(q))^\ell$ reparteix fragments de $(GF(q))^m$ amb $\ell \leq m$. Donat un participant $p \notin P$ existeix un esquema per a compartir secrets per l'estructura $\Gamma' = \{A \cup \{p\} | A \in \Gamma\}$ en el conjunt $P \cup \{p\}$ que reparteix secrets del mateix conjunt de secrets i que manté les taxes d'informació dels participants i pel nou participant $\rho(p) = 1$.*

Demostració: Sigui un secret $k \in (GF(q))^\ell$ per repartir a l'estructura Γ'. A partir de $r \in (GF(q))^\ell$ un vector aleatori, repartim a Γ el secret $k' = k - r$ rebent cada participant un fragment a partir de l'esquema que sabem que existeix. Pel participant $p \notin P$ se li assigna en privat el fragment $s_p = r \in (GF(q))^\ell$.

L'esquema així construït és un esquema per a compartir secrets perfecte que verifica el que hem demanat. En efecte, si una col·lecció de participants autoritzats $A \in \Gamma'$ ajunten els seus fragments podran deduir k' ja que $A - \{p\} \in \Gamma$ però també coneixen $s_p = r$, el fragment de $p \in A$, i a partir d'aquests dos valors podran recuperar el secret fent $k = k' + r$. Sigui una col·lecció de participants no autoritzats $A \in \Gamma'$. Si $p \in A$ llavors $A - \{p\} \notin \Gamma$ i per tant tots els secrets k són igualment probables a partir dels seus fragments, cosa que també passarà amb $k + r$. Pel cas en que $p \notin A$ també tots els secrets

són igualment probables a partir dels fragments dels quals es disposa ja que el vector r s'ha agafat aleatòriament. □

El segon resultat tècnic que farem servir és una propietat important sobre els graus, resumida en el lema següent:

Lema 2.4.3 *Sigui p un participant i Γ_p una estructura homogènia de rang r definida per $\Gamma_p = \{A \in \Gamma_0 | p \in A\}$ en el conjunt $P_p = \bigcup_{A\in\Gamma_p} A$ dels participants que intervenen en algun minimal de Γ_p. Considerem l'estructura $\Gamma'_p = \{A \subset P | p \notin A \text{ i } A \cup \{p\} \in \Gamma_0\}$ homogènia de rang $r-1$ definida a $P'_p = \bigcup_{A\in\Gamma'_p} A$. Llavors es verifica que*

$$\sum_{q\in P'_p} \deg_{\Gamma'_p}(k,q) = (k+1)\deg(k+1,p)$$

i també

$$\sum_{\{q|p\in P'_q\}} \deg_{\Gamma'_q}(k,p) = (k+1)\deg(k+1,p)$$

on $\deg_{\Gamma'_p}(k,q)$ és el k-grau del participant q a l'estructura Γ'_p.

Demostració: Per veure que és certa la primera igualtat diem $d = \deg(k+1,p)$, llavors existirà una col·lecció de d subconjunts diferents $\mathcal{C} = \{S_1,\ldots,S_d\}$ que verifiquen que per a tota $j = 1,\ldots,d$, $|S_j| = k+1$, $p \notin S_j$ i existeix $S'_j \in \Gamma_0$ tal que $S_j \cup \{p\} \subset S'_j$. Trobem aquesta col·lecció $\mathcal{C}$ d'una altra manera. Considerem $q \in P'_p$ i el seu grau $d_q = \deg_{\Gamma'_p}(k,q)$. Per tant existeixen $A_{q1},\ldots,A_{qd_q} \subset P'_p$ amb $|A_{qj}| = k$, $q \notin A_{qj}$ i verificant $A_{qj} \cup \{q\} \subset A'_{qj}$ per cert $A'_{qj} \in \Gamma'_p$ per a tot $j = 1,\ldots,d_q$. Llavors $B_{qj} = A_{qj} \cup \{q\}$ verifica que $|B_{qj}| = k+1$, $p \notin B_{qj}$ i que $B_{qj} \cup \{p\} \subset A'_{qj} \cup \{p\} \in \Gamma_0$. És a dir que aquests d_q subconjunts diferents B_{qj} són de $\mathcal{C}$. D'altra banda cada $\{q_1,\ldots,q_{k+1}\} \in \mathcal{C}$ està en les $k+1$ col·leccions

$$\{B_{q_1 j}\}_{j=1}^{d_{q_1}},\ldots,\{B_{q_{k+1} j}\}_{j=1}^{d_{q_{k+1}}}$$

Per tant $\sum_{q\in P'_p} d_q = (k+1)d$, com es volia demostrar.

Per justificar la segona igualtat procedirem de la mateixa manera: sigui $d = \deg(k+1,p)$, llavors existirà una col·lecció de d subconjunts diferents $\mathcal{C} = \{S_1,\ldots,S_d\}$ que verifiquen que per a tota $j = 1,\ldots,d$, $|S_j| = k+1$, $p \notin S_j$ i existeix $S'_j \in \Gamma_0$ tal que $S_j \cup \{p\} \subset S'_j$. Trobem aquesta col·lecció $\mathcal{C}$ d'una altra manera. Prenem un participant q tal que $p \in P'_q$ i anomenem $d_q = \deg_{\Gamma'_q}(k,p)$. Per tant existeixen $A_{q1},\ldots,A_{qd_q} \subset P'_q$ amb $|A_{qj}| = k$, $p \notin A_{qj}$ i verificant $A_{qj} \cup \{p\} \subset A'_{qj}$ per cert $A'_{qj} \in \Gamma'_q$ per a tot $j = 1,\ldots,d_q$. Aleshores

$B_{qj} = A_{qj} \cup \{q\}$ verifica que $|B_{qj}| = k+1$, $p \notin B_{qj}$ i que $B_{qj} \cup \{p\} \subset A'_{qj} \cup \{q\} \in \Gamma_0$. És a dir que aquests d_q subconjunts diferents B_{qj} són de $\mathcal{C}$. També sabem que cada $\{q_1, \ldots, q_{k+1}\} \in \mathcal{C}$ està en les $k+1$ col·leccions

$$\{B_{q_1 j}\}_{j=1}^{d_{q_1}}, \ldots, \{B_{q_{k+1} j}\}_{j=1}^{d_{q_{k+1}}}$$

Per tant $\sum_{\{q|p \in P'_q\}} d_q = (k+1)d$, com afirma la segona igualtat. □

Ara farem la segona construcció d'un esquema per a compartir secrets per una estructura d'accés homogènia.

Proposició 2.4.4 *Sigui $q > (r-1)!N$ una potència de primer. Per a tota estructura d'accés homogènia de rang r existeix un esquema per a compartir secrets que reparteix secrets de $\mathcal{K} = (GF(q))^{r!}$ assignant fragments de longitud*

$$\log q \sum_{k=0}^{r-1} (r-1-k)! k! \deg(k, p)$$

a cada participant $p \in P$.

Demostració: Fem una demostració per inducció sobre el rang r de l'estructura:

Cas $r = 2$: En aquest cas l'esquema trobat per D.R. Stinson donat per la 2-descomposició en estrelles d'un graf assigna fragments de longitud $\log q(1!0! \deg(0, p) + 0!1! \deg(1, p)) = \log q(1 + \deg(p))$ per secrets escollits en $(GF(q))^2$. Aquest esquema coincideix amb el de la primera construcció.

Cas $r-1$ implica el cas r: Per demostrar aquesta part utilitzarem una construcció semblant a la que es fa servir a la λ-descomposició. Sigui Γ una estructura homogènia de rang r en el conjunt $P = \{p_1, \ldots, p_N\}$ determinada pel conjunt de minimals Γ_0. Considerem per a cada participant $p_i \in P$ la subestructura $\Gamma_i = \{A \in \Gamma_0 | p_i \in A\}$ i a partir d'aquestes el recobriment

$$\Gamma_1, \overset{(r-1)!}{\ldots}, \Gamma_1, \Gamma_2, \overset{(r-1)!}{\ldots}, \Gamma_2, \ldots, \Gamma_N, \overset{(r-1)!}{\ldots}, \Gamma_N$$

que designarem per $\{\Gamma'_i\}_{i=1}^{(r-1)!N}$. Cada $A \in \Gamma_0$ pertany a $\lambda = r(r-1)! = r!$ subestructures de la col·lecció. Escollim $L_1, \ldots, L_{(r-1)!N} \in (GF(q))^{r!}$ tals que agafats de $r!$ en $r!$ siguin linealment independents. Donat un secret $k \in (GF(q))^{r!}$ repartirem a cada subestructura Γ'_i el secret $k \cdot L_i$. Agruparem els secrets a repartir en les $(r-1)!$ còpies de l'estructura Γ_1 de forma que repartirem el secret $(k \cdot L_1, \ldots, \cdot, k \cdot L_{(r-1)!})$ fent ús del Lema 3.4.2 i de la hipòtesi d'inducció. Aquesta manera de procedir l'estendrem a totes les subestructures, rebent cada participant p_i un fragment de $(r-1)! \log q$ bits (de les subestructures

que són còpies de Γ_i) i uns altres fragments de longitud $\log q \sum_{k=0}^{r-2}(r-2-k)!k!\deg_{\Gamma'_j}(k,p_i)$ per a cada subestructura Γ_j per la qual $p_i \in P_j$, per la hipòtesi d'inducció. En total el seu fragment tindrà longitud

$$(r-1)!\log q + \sum_{\{j|p_i\in P_j\}} \log q \sum_{k=0}^{r-2}(r-2-k)!k!\deg_{\Gamma'_j}(k,p_i) =$$

$$\log q((r-1)! + \sum_{k=0}^{r-2}(r-2-k)!k! \sum_{\{j|p_i\in P_j\}} \deg_{\Gamma'_j}(k,p_i)) =$$

fent ús del Lema 3.4.3 obtenim que la longitud és

$$\log q((r-1)! + \sum_{k=0}^{r-2}(r-2-k)!k!(k+1)\deg(k+1,p_i)) =$$

$$\log q((r-1)!0!\deg(0,p_i) + \sum_{k=0}^{r-2}(r-2-k)!(k+1)!\deg(k+1,p_i)) =$$

$$\log q \sum_{k=0}^{r-1}(r-1-k)!k!\deg(k,p)$$

□

Amb aquest resultat tenim construït un esquema per una estructura homogènia de rang r qualsevol que ens proporciona fites per la taxa d'informació òptima i per a la taxa mitjana d'informació òptima .

Teorema 2.4.5 *Sigui $q > (r-1)!N$ una potència de primer i $\mathcal{K} = (GF(q))^{r!}$. Per a tota estructura d'accés homogènia de rang r en un conjunt de N participants, existeix un esquema per a compartir secrets amb taxa d'informació*

$$\rho_2 = \frac{r}{\max_{p\in P}(\sum_{k=0}^{r-1}\frac{\deg(k,p)}{\binom{r-1}{k}})}$$

i taxa mitjana d'informació

$$\tilde{\rho}_2 = \frac{rN}{\sum_{k=0}^{r-2}\left(\frac{1}{\binom{r-1}{k}}\sum_{p\in P}\deg(k,p)\right) + r|\Gamma_0|}$$

Demostració: Per a cada participant $p \in P$ tenim segons l'anterior proposició

$$\rho(p) = \frac{r! \log q}{\log q \sum_{k=0}^{r-1} (r-1-k)!k! \deg(k,p)} = \frac{r}{\sum_{k=0}^{r-1} \frac{(r-1-k)!k!}{(r-1)!} \deg(k,p)}$$

$$= \frac{r}{\sum_{k=0}^{r-1} \frac{\deg(k,p)}{\binom{r-1}{k}}}$$

i d'aquí el resultat enunciat de ρ_2. Per la taxa mitjana tenim que

$$\tilde{\rho}_2 = \frac{N}{\sum_{p \in P} \frac{1}{\rho(p)}} = \frac{N}{\sum_{p \in P} \frac{\sum_{k=0}^{r-1} \frac{\deg(k,p)}{\binom{r-1}{k}}}{r}} =$$

$$\frac{rN}{\sum_{k=0}^{r-1} \frac{1}{\binom{r-1}{k}} \sum_{p \in P} \deg(k,p)} = \frac{rN}{\sum_{k=0}^{r-2} \left(\frac{1}{\binom{r-1}{k}} \sum_{p \in P} \deg(k,p) \right) + r|\Gamma_0|}$$

□

2.4.3 Comparació entre les dues construccions

Per fer la comparació entre els dos parells de fites ρ_1, ρ_2 i $\tilde{\rho}_1, \tilde{\rho}_2$ trobades a la secció anterior, necessitarem un lema tècnic sobre els graus.

Lema 2.4.6 *Sigui Γ una estructura homogènia de rang $r \geq 2$ i sigui $1 \leq k \leq r$ aleshores per a tot $p \in P$ es verifica*

1. $\deg(k,p) \geq \frac{r-k}{k} \deg(k-1,p)$
2. $\deg(k,p) \geq \frac{\binom{r-k+i-1}{i}}{\binom{k}{i}} \deg(k-i,p)$ *per* $k-r+1 \leq i \leq k$
3. $\deg(k,p) \leq \frac{\binom{k+i}{i}}{\binom{r-k-1}{i}} \deg(k+i,p)$ *per* $i \leq r-k$

Demostració: Per la primera desigualtat fem una demostració per inducció sobre el rang r.

Cas $r = 2$: És evident ja que llavors o bé $k = 1$ en el qual cas sempre es verifica $\deg(1,p) \geq (r-1)\deg(0,p)$ i o bé $k = 2$ pel qual també és evident.

Cas $r-1$ implica el cas r: Sigui $q \in P'_p$. Com que $\operatorname{rang} \Gamma'_p = r-1$, per hipòtesi d'inducció tenim

$$\deg_{\Gamma'_p}(k-1,q) \geq \frac{r-1-(k-1)}{k-1} \deg_{\Gamma'_p}(k-2,q)$$

per a tota $2 \leq k \leq r-1$. Ara sumant totes aquestes desigualtats que resulten de fer variar q en P'_p obtenim

$$\sum_{q \in P'_p} \deg_{\Gamma'_p}(k-1,q) \geq \sum_{q \in P'_p} \frac{r-1-(k-1)}{k-1} \deg_{\Gamma'_p}(k-2,q)$$

i fent ús del Lema 3.4.3

$$k \deg(k,p) \geq \frac{r-k}{k-1}(k-1)\deg(k-1,p)$$

i d'aquí s'obté el resultat per $2 \leq k \leq r-1$. Els casos $k=1$ i $k=r$ són trivials.

La segona desigualtat s'obté aplicant la primera i vegades. Per la tercera es fa un canvi de k per $k+i$ a la segona. □

De la comparació entre les taxes òptimes per les dues construccions se'n dedueix que la segona és millor que la primera. Més concretament es verifica el següent:

Proposició 2.4.7 *Les fites per a les taxes d'informació òptima verifiquen* $\rho_1 \leq \rho_2 < \frac{r}{2}\rho_1$ *per* $r > 2$.

Demostració: En primer lloc veiem que és millor la segona que la primera fent ús de l'apartat 3 del Lema 3.4.6:

$$\sum_{k=0}^{r-1} \frac{\deg(k,p)}{\binom{r-1}{k}} = \deg(r-1,p) + \sum_{k=0}^{r-2} \frac{\deg(k,p)}{\binom{r-1}{k}} \leq$$

$$\deg(r-1,p) + \sum_{k=0}^{r-2} \frac{\binom{r-2}{r-2-k}\deg(r-2,p)}{\binom{r-k-1}{r-k-2}\binom{r-1}{k}} =$$

$$\deg(r-1,p) + \deg(r-2,p)\sum_{k=0}^{r-2} \frac{1}{r-1} = \deg(r-1,p) + \deg(r-2,p)$$

Prenent màxims tenim que $\rho_1 \leq \rho_2$. Veiem ara quant millora la segona a la primera. Per fer la comparació entre aquestes dues fites haurem de considerar primer el cas en el qual el màxim es pren sobre el mateix participant i després considerar un segon cas en el qual el màxim es pren sobre participants diferents.

En el cas en el qual els dos màxims s'assoleixen en el mateix participant anomenarem $x_k = \deg(k,p)$ on $p \in P$ és l'esmentat participant. El quocient de ρ_1/ρ_2 val

$$\frac{\rho_1}{\rho_2} = \frac{x_{r-2}+x_{r-1}}{1+\frac{x_1}{\binom{r-1}{1}}+\frac{x_2}{\binom{r-1}{2}}+\ldots+\frac{x_{r-3}}{\binom{r-1}{r-3}}+\frac{x_{r-2}}{r-1}+x_{r-1}}$$

Per l'apartat 2 del Lema 3.4.6 obtenim que $x_k \geq \binom{r-1}{k}$, o sigui $x_k/\binom{r-1}{k} \geq 1$ i per tant

$$\frac{\rho_1}{\rho_2} \leq \frac{x_{r-2}+x_{r-1}}{r-2+\frac{x_{r-2}}{r-1}+x_{r-1}}$$

Sabem pel apartat 1 del Lema 3.4.6 que $x_{r-1} \geq x_{r-2}/(r-1)$ i per tant $x_{r-2} \leq (r-1)x_{r-1}$. És a dir que $x_{r-2} = \alpha x_{r-1}$ amb $\alpha \in [0, r-1]$. Així tenim que:

$$\frac{\rho_1}{\rho_2} \leq \frac{\alpha x_{r-1}+x_{r-1}}{r-2+\frac{\alpha x_{r-1}}{r-1}+x_{r-1}} = \frac{(\alpha+1)x_{r-1}}{r-2+(1+\frac{\alpha}{r-1})x_{r-1}} <$$

$$\frac{\alpha+1}{1+\frac{\alpha}{r-1}} = \frac{(r-1)(\alpha+1)}{r-1+\alpha} < \frac{(r-1)(r-1+1)}{r-1+r-1} = \frac{r}{2}$$

En el cas en el qual els dos màxims s'assoleixen en punts diferents anomenem $x_k = \deg(k,p)$ i $x'_k = \deg(k,p')$ amb p i p' els participants on s'assoleixen els màxims, és a dir:

$$x_{r-2}+x_{r-1} > x'_{r-2}+x'_{r-1}$$

$$1+\frac{x'_1}{\binom{r-1}{1}}+\ldots+\frac{x'_{r-3}}{\binom{r-1}{r-3}}+\frac{x'_{r-2}}{r-1}+x'_{r-1} > 1+\frac{x_1}{\binom{r-1}{1}}+\ldots+\frac{x_{r-3}}{\binom{r-1}{r-3}}+\frac{x_{r-2}}{r-1}+x_{r-1}$$

Aquest cas es redueix al primer observant que

$$\frac{\rho_1}{\rho_2} = \frac{x_{r-2}+x_{r-1}}{1+\frac{x'_1}{\binom{r-1}{1}}+\frac{x'_2}{\binom{r-1}{2}}+\ldots+\frac{x'_{r-3}}{\binom{r-1}{r-3}}+\frac{x'_{r-2}}{r-1}+x'_{r-1}} \leq$$

$$\frac{x_{r-2}+x_{r-1}}{1+\frac{x_1}{\binom{r-1}{1}}+\frac{x_2}{\binom{r-1}{2}}+\ldots+\frac{x_{r-2}}{\binom{r-1}{r-3}}+\frac{x_{r-2}}{r-1}+x_{r-1}} \leq \frac{r}{2}$$

i per tant la desigualtat també és certa en aquest cas. □

La comparació de les dues fites trobades per la taxa mitjana d'informació òptima dóna un resultat semblant:

Proposició 2.4.8 *Les fites per a les taxes mitjanes d'informació òptima d'una estructura d'accés homogènia de rang r en un conjunt de N participants verifiquen $\tilde{\rho}_1 \leq \tilde{\rho}_2 < (r-1)\tilde{\rho}_1$ per $r > 2$.*

Demostració: Al començament de l'anterior proposició hem trobat que

$$\sum_{k=0}^{r-1} \frac{\deg(k,p)}{\binom{r-1}{k}} \leq \deg(r-1,p)+\deg(r-2,p)$$

desigualtats que sumades sobre tots els participants $p \in P$ s'obté:

$$\sum_{p\in P}(\sum_{k=0}^{r-1}\frac{\deg(k,p)}{\binom{r-1}{k}}) \leq \sum_{p\in P}(\deg(r-1,p)+\deg(r-2,p))$$

cosa que és equivalent a dir

$$\sum_{k=0}^{r-2}(\frac{1}{\binom{r-1}{k}}\sum_{p\in P}\deg(k,p))+r|\Gamma_0| \leq \sum_{p\in P}\deg(r-2,p)+r|\Gamma_0|$$

i per tant $\tilde{\rho}_1/\tilde{\rho}_2 \geq 1$. D'altra banda si diem $c=|\Gamma_0|$, $\alpha=\sum_{p\in P}\deg(r-2,p)$ i $M=\sum_{k=0}^{r-3}(\frac{1}{\binom{r-1}{k}}\sum_{p\in P}\deg(k,p))$ llavors ens queda

$$\frac{\tilde{\rho}_1}{\tilde{\rho}_2}=\frac{\alpha+rc}{\frac{1}{r-1}\alpha+rc+M}<\frac{1}{\frac{1}{r-1}}=r-1$$

□

Com que la millora amb la segona tècnica està fitada i en canvi el conjunt de claus per la segona tècnica creix desmesuradament (en funció de $r!$), en algunes aplicacions pràctiques pot ser millor la primera construcció per la seva simplicitat.

2.4.4 Comparació amb les fites per estructures homogènies de rang r

Fem ara la comparació amb les fites conegudes fins ara per les taxes d'informació en el cas d'estructures homogènies de rang r. D.R. Stinson amb un cas particular de la λ-descomposició i fent servir coloracions d'arestes de grafs bipartits obté a [92] la fita

$$\rho=\frac{r}{(2r-1)\binom{N-1}{r-2}+\max_{p\in P}\deg(r-1,p)}$$

per la taxa d'informació òptima d'estructures homogènies de rang r en un conjunt de N participants. Aquesta fita es pot millorar afinant els càlculs fets a [92] amb la introducció del concepte de grau. La fita resultant d'aquesta millora és

$$\rho_S=\frac{r}{\max_{p\in P}((2r-1)\deg(r-2,p)+\deg(r-1,p))}$$

En aquest treball també es dóna una fita per la taxa mitjana d'informació òptima:

$$\tilde{\rho} = \frac{rN}{N(2r-1)\binom{N-1}{r-2} + r|\Gamma_0|}$$

la qual també és fàcil de millorar, obtenint

$$\tilde{\rho}_S = \frac{rN}{(2r-1)\sum_{p\in P}\deg(r-2,p) + r|\Gamma_0|}$$

Aquestes fites van suposar la millora asimptòtica de les fites conegudes fins aquell moment en un factor de r. Aquestes fites anteriors eren les que van trobar Benaloh i Leichter a [8] utilitzant un circuit booleà per a una forma normal disjuntiva (veure Secció 2.2) que també admeten una millora fent servir el concepte de grau. La fita inferior per la taxa d'informació òptima, obtinguda per aquesta construcció és

$$\frac{1}{\binom{N-1}{r-1}}$$

que afinada amb el nostre grau dóna:

$$\frac{1}{\max_{p\in P}\deg(r-1,p)}.$$

Les nostres fites milloren les fites de D.R. Stinson en un factor de $2r-2$ com a màxim.

Proposició 2.4.9 *La fita inferior de la taxa d'informació òptima ρ_1 verifica $\rho_S \leq \rho_1 \leq (2r-2)\rho_S$.*

Demostració:

En el cas en el qual els dos màxims s'assoleixen en el mateix participant anomenarem $x_k = \deg(k,p)$ on $p \in P$ és l'esmentat participant. El quocient de ρ_1/ρ_S val

$$\frac{\rho_1}{\rho_S} = \frac{(2r-1)x_{r-2} + x_{r-1}}{x_{r-2} + x_{r-1}} \geq 1$$

Per l'apartat 1 del Lema 3.4.6 tenim que $x_{r-1} \geq x_{r-2}/(r-1)$, per tant $x_{r-2} \leq (r-1)x_{r-1}$ i d'aquí $x_{r-2} = \alpha x_{r-1}$ amb $\alpha \in [0, r-1]$. Així tenim que:

$$\frac{\rho_1}{\rho_S} = \frac{(2r-1)\alpha x_{r-1} + x_{r-1}}{\alpha x_{r-1} + x_{r-1}} = \frac{(2r-1)\alpha + 1}{\alpha + 1} \leq$$

$$\frac{(2r-1)(r-1)+1}{r-1+1} = 2r-3+\frac{2}{r} \leq 2r-2$$

Quan el màxim no s'assoleixi en el mateix punt, si no que un s'assoleix en $p \in P$ i l'altre en $p' \in P$, llavors dient $x_k = \deg(k,p)$ i $x'_k = \deg(k,p')$ tenim que $x_{r-2}+x_{r-1} \geq x'_{r-2}+x'_{r-1}$ i $(2r-1)x'_{r-2}+x'_{r-1} \geq (2r-1)x_{r-2}+x_{r-1}$. Llavors

$$\frac{\rho_1}{\rho_S} = \frac{(2r-1)x'_{r-2}+x'_{r-1}}{x_{r-2}+x_{r-1}} \geq \frac{(2r-1)x_{r-2}+x_{r-1}}{x_{r-2}+x_{r-1}} \geq 1$$

I també per les desigualtats anteriors tenim:

$$\frac{\rho_1}{\rho_S} = \frac{(2r-1)x'_{r-2}+x'_{r-1}}{x_{r-2}+x_{r-1}} \leq \frac{(2r-1)x'_{r-2}+x'_{r-1}}{x'_{r-2}+x'_{r-1}} \leq 2r-2$$

□

La comparació de les fites per la taxa mitjana d'informació òptima dóna un resultat semblant:

Proposició 2.4.10 *La fita inferior de la taxa mitjana d'informació òptima* $\tilde{\rho}_1$ *verifica* $\tilde{\rho}_S \leq \tilde{\rho}_1 < (2r-1)\tilde{\rho}_S$.

Demostració: De la mateixa manera que abans tenim

$$1 \leq \frac{\tilde{\rho}_1}{\tilde{\rho}_S} = \frac{(2r-1)\sum_{p\in P}\deg(r-2,p)+r|\Gamma_0|}{\sum_{p\in P}\deg(r-2,p)+r|\Gamma_0|} < 2r-1$$

□

La comparació s'ha fet amb les fites de D.R. Stinson millorades. Si s'hagués fet amb les fites originals es veuria que són molt pitjors. Ilustrem-ho amb un exemple: anomenem *cicle generalitzat* de rang r i llargada $N \geq 2r-1$ a l'estructura d'accés definida en el conjunt de participants $P = \mathbb{Z}_N$ que és la clausura de

$$\Gamma_0 = \{\{i, i+1, \ldots, i+r-1\} \subset P | i \in \mathbb{Z}_N\}$$

S'observa que es tracta d'una estructura d'accés homogènia de rang r. Un simple càlcul ens porta a que el $\deg(r-1,p) = r$ i que $\deg(r-2,p) = (r-1)^2$ de forma que $\rho_1 = r/(r^2-r+1)$ i $\rho_S = r/(2r^3-5r^2+5r-1)$. El quocient entre ambdues taxes val $\rho_1/\rho_S = 2r-3+2/(r^2-r+1)$. Si el quocient es fa amb la fita sense millorar el quocient val $((2r-1)\binom{N-1}{r-2}+r)/(r^2-r+1)$ la qual cosa prova que per a tot rang r aquest quocient tendeix a infinit quan N tendeix a infinit.

Més recentment H.M. Sun i S.P. Shieh a [85] han establert fites per estructures d'accés homogènies en general. El primer dels resultats d'aquest article és una fita per a una estructura homogènia de rang r

$$\rho_{S1} = \frac{N-r+1}{\binom{N}{r}}$$

pitjor que la primera de les nostres ja que

$$\max_{p\in P}(\deg(r-2,p)+\deg(r-1,p)) \leq \binom{N-1}{r-2}+\binom{N-1}{r-1} = \binom{N}{r-1}$$

i per tant $\rho_1 \geq r/\binom{N}{r-1} = (N-r+1)/\binom{N}{r} = \rho_{S1}$.

2.4.5 Comparació amb les fites per estructures homogènies de rang 3

En el treball [92] de D.R. Stinson es presenten unes fites per les taxes d'informació fent servir aquesta vegada sistemes de Steiner per construir la descomposició. El principal resultat al qual s'arriba per estructures homogènies amb rang $r = 3$ és:

$$\rho_{STE} = \frac{6}{(N-1)(N-2)}$$

si $N \equiv 2,4 (\mathrm{mod}\, 6)$. Per altres valors de N l'autor indica el camí per derivar fites a partir d'aquesta. D'aquest càlcul surten les fites: $\rho_{STE} = 6/(N(N+1))$ si $N \equiv 0 (\mathrm{mod}\, 6)$, $\rho_{STE} = 6/(N(N-1))$ si $N \equiv 1,3 (\mathrm{mod}\, 6)$ i $\rho_{STE} = 6/((N+1)(N+2))$ si $N \equiv 5 (\mathrm{mod}\, 6)$. Per exemple en el cicle generalitzat de rang $r = 3$ i $N \geq 5$ participants tenim que és millor la nostra fita ρ_1. De fet d'aquesta manera tenim una manera fàcil de generar una família infinita d'estructures que tenen una taxa d'informació ρ_1 molt més gran que la taxa que ens donen els sistemes de Steiner (quocient entre les dues fites tan gran com es vulgui).

La fita ρ_{STE} és pitjor que ρ_1 per $N \not\equiv 2,4 (\mathrm{mod}\, 6)$ com es pot veure trivialment a partir de la fitació grollera de ρ_1

$$\rho_1 \geq \frac{3}{\binom{N-1}{1}+\binom{N-1}{2}} = \frac{6}{N(N-1)}$$

Per tant només cal fer la comparació en el cas que $N \equiv 2,4 (\mathrm{mod}\, 6)$. La conclusió en aquest cas és que és pitjor que ρ_1 per la majoria de les estructures d'accés. Més exactament:

Proposició 2.4.11 *Sigui* Γ *una estructura homogènia de rang* 3 *en un conjunt de* N *participants amb* $N \equiv 2, 4 (\mathrm{mod}\, 6)$ *llavors*

1. *Si per a tot participant* $p \in P$ *tenim que* $\deg(1,p) < N-1$ *llavors* $\rho_1 \geq \rho_{STE}$.
2. *Si per tots els participant* $p \in P$ *pels quals* $\deg(1,p) = N-1$ *es verifica* $\deg(2,p) \leq (N-1)(N-4)/2$ *llavors* $\rho_1 \geq \rho_{STE}$.

Demostració: Pel primer cas només cal observar que si diem $k = \deg(1,p)$ llavors $\deg(2,p) \leq \binom{k}{2} = (k^2-k)/2 \leq ((N-2)^2-(N-2))/2 = (N^2-5N+6)/2$. Llavors comparant amb $\rho_{STE} = \frac{3}{(N-1)(N-2)/2}$,

$$\deg(1,p) + \deg(2,p) - \frac{(N-1)(N-2)}{2} \leq$$

$$N - 2 + \frac{N^2-5N+6}{2} - \frac{(N-1)(N-2)}{2} = 0$$

per tant $\max_{p\in P}(\deg(1,p)+\deg(2,p)) \leq (N-1)(N-2)/2$ i d'aquí $\rho_1 \geq \rho_{STE}$.

En el segon cas si el $\max_{p\in P}(\deg(1,p)+\deg(2,p))$ s'assoleix en un punt amb $\deg(1,p) < N-1$ pel mateix raonament fet al primer apartat tindrem provat el resultat. Si el màxim s'assoleix en un punt en el qual $\deg(1,p) = N-1$ llavors per la hipòtesi

$$\max_{p\in P}(\deg(1,p)+\deg(2,p)) \leq N-1+\frac{(N-1)(N-4)}{2} = \frac{(N-1)(N-2)}{2}$$

□

Observi's que sempre $\deg(1,p) \leq N-1$ i que només en el cas que hi hagi un participant amb grau màxim podrà ser la fita ρ_{STE} millor que ρ_1. Però fins i tot en el cas que hi hagi un participant p amb el 1-grau màxim, només si l'estructura d'accés conté gairebé tots els subconjunts que es poden formar amb el participant p, serà millor ρ_{STE} que ρ_1.

En el cas que el màxim s'assoleixi en un participant amb 1-grau màxim, es pot demostrar (fent servir la mateixa argumentació que a la Proposició 3.4.11) el resultat següent, que diu com poden ser les estructures amb $\rho_2 \geq \rho_{STE}$.

Proposició 2.4.12 *Sigui* Γ *una estructura homogènia de rang* 3 *en un conjunt de* N *participants amb* $N \equiv 2, 4 (\mathrm{mod}\, 6)$. *Si per tots els participant* $p \in P$ *pels quals* $\deg(1,p) = N-1$ *es verifica* $\deg(2,p) \leq (N^2-4N+1)/2$ *llavors* $\rho_2 \geq \rho_{STE}$.

En el mateix treball [92] de D.R. Stinson, es presenta una fita per la taxa mitjana d'informació fent servir la mateixa tècnica:

$$\tilde{\rho}_{STE} = \frac{24}{5(N-1)(N-2)}$$

si $N \equiv 2, 4 (\mathrm{mod}\, 6)$. Aquesta fita és pitjor que la nostra fita $\tilde{\rho}_1$ ja que

$$\tilde{\rho}_1 = \frac{3N}{3|\Gamma_0| + \sum_{p\in P} \deg(1,p)} \geq \frac{3N}{3\binom{N}{3} + \sum_{p\in P} N - 1} =$$

$$\frac{3N}{N(N-1)(N-2)/2 + N(N-1)} = \frac{6}{N(N-1)} \geq \tilde{\rho}_{STE}$$

per valors $N \geq 10$. Pels valors de $N \not\equiv 2, 4 (\mathrm{mod}\, 6)$ es pot obtenir com abans fites a partir de la primera: $\rho_{STE} = 24/(5N(N+1))$ si $N \equiv 0 (\mathrm{mod}\, 6)$, $\rho_{STE} = 24/(5N(N-1))$ si $N \equiv 1, 3 (\mathrm{mod}\, 6)$ i $\rho_{STE} = 24/(5(N+1)(N+2))$ si $N \equiv 5 (\mathrm{mod}\, 6)$. En aquests tres casos és fàcil comprovar que $\tilde{\rho}_1$ és millor.

En el treball de H.M. Sun i S.P. Shieh [85] es presenta una fita per la taxa d'informació d'una estructura homogènia de rang 3 en un conjunt de N participants:

$$\rho_{S2} = \frac{6}{N^2 - 2N + 3}$$

de la qual es pot dir que és pitjor que ρ_1 per la majoria de les estructures d'accés. La concrecció d'aquest fet i la seva demostració és anàloga als resultats que ja hem enunciat anteriorment:

Proposició 2.4.13 *Sigui* Γ *una estructura homogènia de rang* 3 *llavors*

1. *Si per a tot participant* $p \in P$ *tenim que* $\deg(1,p) < N-1$ *llavors* $\rho_1 \geq \rho_{S2}$.
2. *Si per tots els participant* $p \in P$ *pels quals* $\deg(1,p) = N-1$ *es verifica* $\deg(2,p) \leq (N^2 - 4N + 5)/2$ *llavors* $\rho_1 \geq \rho_{S2}$.

Si comparem ρ_{S2} amb ρ_2 sempre és millor ρ_2 ja que $\deg(1,p) \leq \binom{N-1}{1}$, $\deg(2,p) \leq \binom{N-1}{2}$ i per tant

$$\rho_2 \geq \frac{3}{\frac{1}{\binom{2}{0}} + \frac{\binom{N-1}{1}}{\binom{2}{1}} + \frac{\binom{N-1}{2}}{\binom{2}{2}}} =$$

$$\frac{3}{\frac{1}{1} + \frac{N-1}{2} + \frac{(N-1)(N-2)/2}{1}} = \frac{6}{N^2 - 2N + 3} = \rho_{S2}$$

2.5 Fites superiors per les estructures homogènies de rang 3

Per trobar fites superiors de la taxa d'informació òptima per estructures homogènies de rang 3 seguirem un raonament semblant al que van fer servir Blundo, De Santis, De Simone i Vaccaro a l'article [20] per estructures homogènies de rang 2. Això és, construirem una estructura homogènia de rang 3 de la qual podrem fitar superiorment la seva taxa d'informació òptima. Aquest resultat només provarà que qualsevol fita inferior general per la taxa d'informació no podrà ser més gran que la fita superior que determinarem aplicada en aquesta estructura.

Sigui $n \equiv 0 \bmod 3$. Anomenarem *cicle generalitzat* de rang 3 i llargada n a l'estructura d'accés definida en el conjunt de participants $P = \mathbb{Z}_n$ que és la clausura de

$$\Gamma^0 = \{\{i, i+1, i+2\} \subset P | i \in \mathbb{Z}_n\}$$

S'observa que es tracta d'una estructura d'accés homogènia de rang 3. En aquesta estructura es pot fer una partició $P = S_0 \cup S_1 \cup S_2$ amb $S_i = \{j \in P | j \equiv i \bmod 3\}$ de tal manera que cada subconjunt minimal està format exactament per un element de cada part. Aquestes parts tenen igual cardinal.

Sigui ara una estructura d'accés homogènia de rang 3 en el conjunt P de cardinal $n \equiv 0 \bmod 3$ amb base Γ. Suposem que passa com abans, això és, existeix una partició $P = S_0 \cup S_1 \cup S_2$ en tres subconjunts d'igual cardinal de tal manera que cada subconjunt minimal està format exactament per un element de cada part. Donat $q \equiv 0 \bmod 3$ fem q còpies de l'estructura inicial $\Gamma_0, \ldots, \Gamma_{q-1}$ amb conjunts de participants $P_0, \ldots, P_{q-1}$ i particions $P_i = S_0^i \cup S_1^i \cup S_2^i$. Definim una nova estructura d'accés en el conjunt $P' = P_0 \cup \ldots \cup P_{q-1}$ amb base $\Gamma' = \Gamma_0 \cup \ldots \cup \Gamma_{q-1} \cup \bar{\Gamma}$ on $\bar{\Gamma}$ està definida de la manera següent:

Identifiquem els elements de S_j^i amb $0, 1, \ldots, \ell-1$ amb $n = 3\ell$. Els elements de $\bar{\Gamma}$ són la col·lecció de subconjunts de 3 elements següents

- Per $0 \leq i \leq q-3$ construïm els subconjunts formats per $j \in S_0^i$, $j \in S_1^{i+1}$ i $j \in S_2^{i+2}$
- Per $i = q-2$ construïm el subconjunt format per $j \in S_0^{q-2}$, $j \in S_1^{q-1}$ i $j - q/3 \in S_2^0$ (observem que $j - q/3$ és un enter que agafarem mòdul ℓ)
- Per $i = q-1$ construïm el subconjunt format per $j \in S_0^{q-1}$, $j - q/3 \in S_1^0$ i $j - q/3 \in S_2^1$ (amb el mateix comentari que hem fet abans)

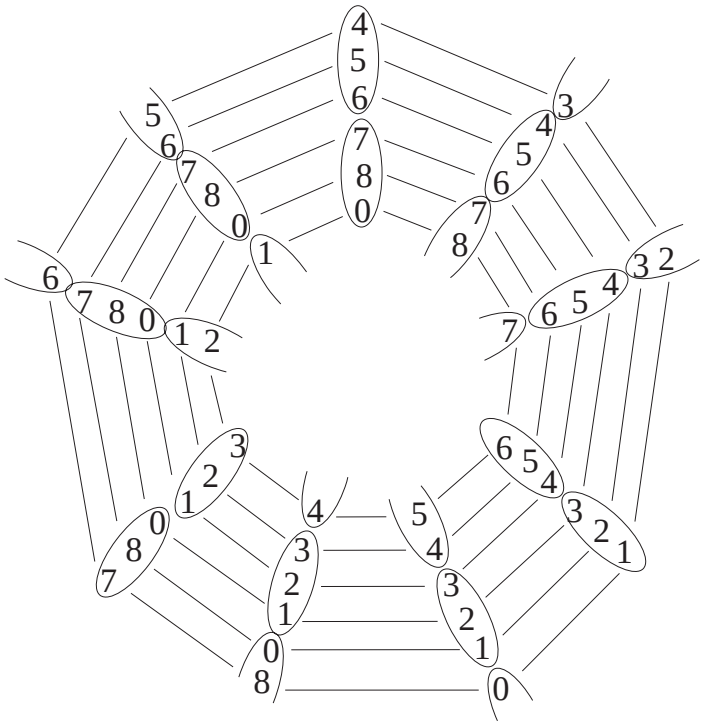

Figura 2.13: Exemple de construcció de Γ' a partir d'un cicle generalitzat de $n = 9$ elements amb $q = 6$ còpies.

A la Figura 3.13 hi ha la construcció de Γ' amb $q = 6$ còpies a partir del cicle generalitzat Γ^0 de $n = 9$ elements.

Comentem quines propietats té aquesta nova estructura. En primer lloc és homogènia de rang 3. El número de participants és nq. Hi ha una partició de $P' = S_0 \cup S_1 \cup S_2$ en tres subconjunts $S_0 = S_0^0 \cup S_0^1 \ldots \cup S_0^{q-1}$, $S_1 = S_1^0 \cup S_1^1 \ldots \cup S_1^{q-1}$, $S_2 = S_2^0 \cup S_2^1 \ldots \cup S_2^{q-1}$ d'igual cardinal de tal manera que cada subconjunt minimal està format exactament per un element de cada part.

A partir d'un cicle generalitzat de rang 3 i longitud $n \equiv 0 \bmod 3$ podem fer k vegades el procés anterior per $q \equiv 0 \bmod 3$ obtenint l'estructura que té per base Γ^k en el conjunt de participants P^k de nq^k elements.

Per aquesta estructura que hem definit trobarem una fita superior per la taxa d'informació òptima. Per tal de referir-nos més còmodament a les propietats de l'entropia i de la informació mútua que utilitzarem, fem un breu resum de les propietats més importants que ja s'ha referenciat a la Secció 2.8 junt

amb alguna altra que és conseqüencia immediata de les anteriors:

Propietat 1 $\sum_{i=1}^{n} H(X_i) = H(X_1 \dots X_n) + \sum_{i=2}^{n} H(X_i; X_1 \dots X_{i-1})$
Propietat 2 $H(XY) = H(X) + H(Y) - I(X;Y)$
Propietat 3 $I(X;Y) = I(Y;X)$
Propietat 4 $I(X;Y) \geq 0$
Propietat 5 $I(X;YZ) \geq I(X;Y)$
Propietat 6 Si A fa independent la successió d'elements B aleshores
$I(A;B) \geq |B|H(\mathcal{K})$ si $A \in \Gamma$
$I(A;B) \geq (|B|-1)H(\mathcal{K})$ si $A \notin \Gamma$
Propietat 7 Si Z fa independent la successió d'elements X aleshores
$I(XY;Z) \geq (|X|+1)H(\mathcal{K})$ si $Z \in \Gamma$
$I(XY;Z) \geq |X|H(\mathcal{K})$ si $Z \notin \Gamma$

Les propietats 1, 2, 3 i 4 han estat enunciades a la Secció 2.8. La propietat 6 és el Corol·lari 2.8.5 en la seva versió inicial de [20], és a dir el Teorema 2.8.7. Pel que fa a la propietat 7 es tracta de la propietat que afirma que $I(XY;Z) = I(X;Z) + I(Y;Z|X)$ després d'aplicar la propietat 6 i el Lema 2.8.3.

Hem de destacar que denotarem l'entropia de $A \cup B$ per $H(AB)$ i no pas $H(A \cup B)$ i per l'entropia $H(p)$ d'un participant p en lloc de $H(\{p\})$. Tots aquests abusos de llenguatge els farem també amb la informació mútua.

Els resultats que venen ara són lemes tècnics destinats a fitar superiorment la taxa d'informació de Γ^k. El primer lema és una fitació de la suma de les entropies dels elements del cicle generalitzat.

Lema 2.5.1 *El cicle generalitzat* Γ^0 *de rang* 3 *i longitud* $n \geq 9$ *verifica*

$$\sum_{p \in P^0} H(p) \geq H(P^0) + (n-2)H(\mathcal{K})$$

Demostració: Tenim que

$$\sum_{p \in P^0} H(p) = \sum_{i=0}^{n-1} H(i) = \sum_{i=0}^{3} H(i) + \sum_{i=4}^{n-1} H(i) =$$

$$H(0123) + \sum_{i=1}^{3} I(i; 01 \dots i-1) + H(4 \dots n-1) + \sum_{i=5}^{n-1} I(i; 4 \dots i-1)$$

aplicant la propietat 1 dues vegades. Fent servir la propietat 2 obtenim que $H(P^0) = H(01 \dots n-1) = H(0123) + H(4 \dots n-1) - I(0123; 4 \dots n-1)$ i per

tant,

$$\sum_{p\in P^0} H(p)-H(P^0) = \sum_{i=1}^{3} I(i;01\dots i-1)+\sum_{i=5}^{n-1} I(i;4\dots i-1)+I(01\dots 3;4\dots n-1)$$

Ara bé, per la propietat 4 i la 3 deduïm que $\sum_{i=1}^{3} I(i;01\dots i-1) \geq I(3;012) = I(012;3) \geq H(\mathcal{K})$ essent la darrera desigualtat certa per la propietat 6 ja que $\{0,1,2\} \in \Gamma^0$ fa independent $\{3\}$. Fent un raonament idèntic obtenim $\sum_{i=5}^{n-1} I(i;4\dots i-1) \geq \sum_{i=7}^{n-1} I(i;4\dots i-1) = \sum_{i=7}^{n-1} I(4\dots i-1;i) \geq \sum_{i=7}^{n-1} H(\mathcal{K}) = (n-7)H(\mathcal{K})$. Aplicant la propietat 7 amb $0,3,2$ la successió X, $Y=\{1\}$, $Z=\{4,\dots,n-1\}$ obtenim $I(0123;4\dots n-1) \geq 4H(\mathcal{K})$. Fent servir totes aquestes afitacions parcials surt que

$$\sum_{p\in P^0} H(p) - H(P^0) \geq (1+n-7+4)H(\mathcal{K}) = (n-2)H(\mathcal{K})$$

□

El segon lema tècnic calcula una fita de la suma de les entropies dels blocs de participants que es copien en la construcció de Γ^k .

Lema 2.5.2 *L'estructura* Γ^{k+1} *en el conjunt de participants* P^{k+1} *verifica*

$$\sum_{a=0}^{q-1} H(S_0^a S_1^a S_2^a) \geq H(P^{k+1}) + (q-3+\frac{nq^k}{3}(q-2))H(\mathcal{K})$$

Demostració: Aplicant la propietat 1 dues vegades obtenim

$$\sum_{a=0}^{q-1} H(S_0^a S_1^a S_2^a) = H(S_0^0 S_1^0 S_2^0 \dots S_0^3 S_1^3 S_2^3)+$$

$$\sum_{a=1}^{3} I(S_0^a S_1^a S_2^a; S_0^0 S_1^0 S_2^0 \dots S_0^{a-1} S_1^{a-1} S_2^{a-1}) + H(S_0^4 S_1^4 S_2^4 \dots S_0^{q-1} S_1^{q-1} S_2^{q-1})+$$

$$\sum_{a=5}^{q-1} I(S_0^a S_1^a S_2^a; S_0^4 S_1^4 S_2^4 \dots S_0^{a-1} S_1^{a-1} S_2^{a-1})$$

Ara per la propietat 2 l'entropia $H(S_0^0 S_1^0 S_2^0 \dots S_0^{q-1} S_1^{q-1} S_2^{q-1})$ val

$$H(S_0^0 S_1^0 S_2^0 \dots S_0^3 S_1^3 S_2^3) + H(S_0^4 S_1^4 S_2^4 \dots S_0^{q-1} S_1^{q-1} S_2^{q-1})-$$

$$I(S_0^0S_1^0S_2^0\dots S_0^3S_1^3S_2^3;S_0^4S_1^4S_2^4\dots S_0^{q-1}S_1^{q-1}S_2^{q-1})$$

Llavors

$$\sum_{a=0}^{q-1}H(S_0^aS_1^aS_2^a)-H(S_0^0S_1^0S_2^0\dots S_0^{q-1}S_1^{q-1}S_2^{q-1})=$$

$$\sum_{a=1}^{3}I(S_0^aS_1^aS_2^a;S_0^0S_1^0S_2^0\dots S_0^{a-1}S_1^{a-1}S_2^{a-1})+$$

$$\sum_{a=5}^{q-1}I(S_0^aS_1^aS_2^a;S_0^4S_1^4S_2^4\dots S_0^{a-1}S_1^{a-1}S_2^{a-1})+$$

$$I(S_0^0S_1^0S_2^0\dots S_0^3S_1^3S_2^3;S_0^4S_1^4S_2^4\dots S_0^{q-1}S_1^{q-1}S_2^{q-1})$$

Els dos primers sumatoris es poden afitar per la propietat 5

$$\sum_{a=1}^{3}I(S_0^aS_1^aS_2^a;S_0^0S_1^0S_2^0\dots S_0^{a-1}S_1^{a-1}S_2^{a-1})+$$

$$\sum_{a=5}^{q-1}I(S_0^aS_1^aS_2^a;S_0^4S_1^4S_2^4\dots S_0^{a-1}S_1^{a-1}S_2^{a-1})\geq$$

$$I(S_0^1S_1^1S_2^1;S_0^0S_1^0S_2^0)+I(S_0^5S_1^5S_2^5;S_0^4S_1^4S_2^4)+$$

$$\sum_{a=2,3,6,\dots,q-1}I(S_0^aS_1^aS_2^a;S_0^{a-2}S_1^{a-2}S_2^{a-2}S_0^{a-1}S_1^{a-1}S_2^{a-1})$$

Fent servir la propietat 7 i la propietat 4 amb $X=S_0^a$, $Y=S_1^aS_2^a$ i $Z=S_0^{a-2}S_1^{a-2}S_2^{a-2}S_0^{a-1}S_1^{a-1}S_2^{a-1}$ obtenim que és més gran que:

$$0+0+(\frac{nq^k}{3}+1)(2+q-6)H(\mathcal{K})=(\frac{nq^k}{3}+1)(q-4)H(\mathcal{K})$$

D'altra banda per la propietat 5 i per la propietat 7 amb $X=S_1^0S_0^3$, $Y=S_0^0S_2^0S_1^3S_2^3$ i $Z=S_0^4S_1^4S_2^4\dots S_0^{q-1}S_1^{q-1}S_2^{q-1}$ tenim

$$I(S_0^0S_1^0S_2^0\dots S_0^3S_1^3S_2^3;S_0^4S_1^4S_2^4\dots S_0^{q-1}S_1^{q-1}S_2^{q-1})\geq(\frac{2nq^k}{3}+1)H(\mathcal{K})$$

En resum obtenim que

$$\sum_{a=0}^{q-1}H(S_0^aS_1^aS_2^a)-H(S_0^0S_1^0S_2^0\dots S_0^{q-1}S_1^{q-1}S_2^{q-1})\geq$$

$$(\frac{nq^k}{3}+1)(q-4)H(\mathcal{K})+(\frac{2nq^k}{3}+1)H(\mathcal{K})=(q-3+\frac{nq^k}{3})H(\mathcal{K})$$

□

El lema següent ens dóna una fita de la suma de les entropies sobre cadascun dels participants de P^k en funció de l'entropia $H(P^k)$.

Lema 2.5.3 *L'estructura* Γ^k *en el conjunt de participants* P^k *verifica per* $k \geq 1$

$$\sum_{p\in P^k} H(p) \geq H(P^k)+(q^k(n-\frac{q+1}{q-1}+\frac{kn}{3})-\frac{2}{3}knq^{k-1}-\frac{q-3}{q-1})H(\mathcal{K})$$

Demostració: Raonem-ho per inducció sobre k. Per $k=0$ és cert pel Lema 3.5.1. Suposem que és cert per k i veiem que és cert per $k+1$ fent servir la hipòtesi d'inducció i el Lema 3.5.2:

$$\sum_{p\in P^{k+1}} H(p)=\sum_{a=0}^{q-1}\sum_{p\in P^k} H(p)\geq \sum_{a=0}^{q-1} H(S_0^aS_1^aS_2^a)+$$

$$q(q^k(n-\frac{q+1}{q-1}+\frac{kn}{3})-\frac{2}{3}knq^{k-1}-\frac{q-3}{q-1})H(\mathcal{K})\geq H(S_0^0S_1^0S_2^0\ldots S_0^{q-1}S_1^{q-1}S_2^{q-1})+$$

$$(q^{k+1}(n-\frac{q+1}{q-1}+\frac{kn}{3})-\frac{2kn}{3}q^k-q\frac{q-3}{q-1}+q-3+\frac{nq^k}{3}(q-2))H(\mathcal{K})=$$

$$H(P^{k+1})+(q^{k+1}(n-\frac{q+1}{q-1}+\frac{(k+1)n}{3})-\frac{2}{3}(k+1)nq^k-\frac{q-3}{q-1})H(\mathcal{K})$$

com volíem demostrar. □

Aquest darrer lema tècnic ens dóna una fita de la suma de les entropies de tots els participants sense fer intervenir cap més entropia llevat de l'entropia del conjunt de secrets.

Lema 2.5.4 *L'estructura* Γ^k *en el conjunt de participants* P^k *verifica per* $k \geq 1$

$$\sum_{p\in P^k} H(p)\geq (q^k(2n-\frac{q+1}{q-1}+\frac{(k-1)n}{3})-\frac{2}{3}(k-1)nq^{k-1}+\frac{2q}{q-1})H(\mathcal{K})$$

Demostració: Per $k \geq 1$ fent servir el Lema 3.5.3 tenim:

$$\sum_{p \in P^k} H(p) = \sum_{a=0}^{q-1} \sum_{p \in P^{k-1}} H(p) \geq$$

$$q(q^{k-1}(n - \frac{q+1}{q-1} + \frac{(k-1)n}{3}) - \frac{2(k-1)}{3} n q^{k-2} - \frac{q-3}{q-1}) H(\mathcal{K}) + \sum_{a=0}^{q-1} H(S_0^a S_1^a S_2^a)$$

Per la construcció de $\Gamma^k = \Gamma_0 \cup \ldots \cup \Gamma_{q-1} \cup \Gamma'$, sabem que si $S_0^a S_1^a S_2^a = \{p_1, \ldots, p_{nq^{k-1}}\}$, per a tot $i = 1, \ldots, nq^{k-1}$ existeix un únic $C_i \in \Gamma'$ tal que $p_i \in C_i$. Així tenim que $S_0^a S_1^a S_2^a$ fa independent la successió de nq^{k-1} subconjunts independents definida per:

$$B_i = (C_1 - \{p_1\}) \cup \ldots (C_i - \{p_i\})$$

A la Figura 3.14 s'il·lustra aquesta successió per $n = 9$, $k = 1$ i $q = 6$.

Per tant pel Corol·lari 2.8.5 obtenim

$$\sum_{p \in P^k} H(p) = \sum_{a=0}^{q-1} \sum_{p \in P^{k-1}} H(p) \geq$$

$$(q^k(n - \frac{q+1}{q-1} + \frac{(k-1)n}{3}) - \frac{2(k-1)}{3} n q^{k-1} - q\frac{q-3}{q-1}) H(\mathcal{K}) + q(nq^{k-1}+1) H(\mathcal{K}) =$$

$$(q^k(2n - \frac{q+1}{q-1} + \frac{(k-1)n}{3}) - \frac{2}{3}(k-1) n q^{k-1} + \frac{2q}{q-1}) H(\mathcal{K})$$

□

Ara ja podem enunciar una fita superior per a la taxa d'informació òptima per Γ^k:

Proposició 2.5.5 *La taxa d'informació òptima per l'estructura Γ^k en el conjunt de participants P^k verifica*

$$\rho^*(\Gamma^k) \leq \frac{n}{2n - \frac{q+1}{q-1} + \frac{(k-1)n}{3} - \frac{2n(k-1)}{3q} + \frac{2}{(q-1)q^{k-1}}}$$

Demostració: Com que

$$\sum_{p \in P^k} \log |\mathcal{S}_p| \geq \sum_{p \in P^k} \log H(p) \geq$$

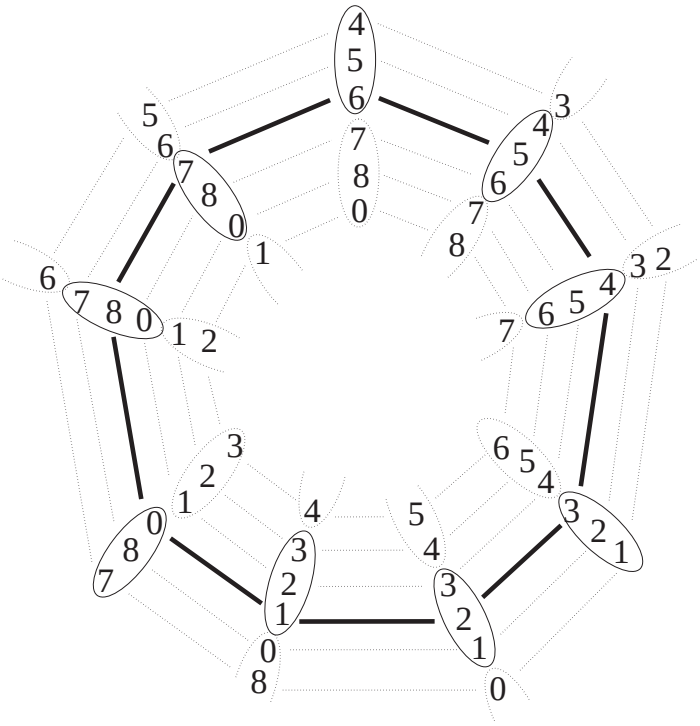

Figura 2.14: $S_0^a S_1^a S_2^a$ fa independent la successió $B_1, \ldots, B_9$ per $n = 9$, $k = 1$ i $q = 6$.

$$(q^k(2n - \frac{q+1}{q-1} + \frac{(k-1)n}{3}) - \frac{2}{3}(k-1)nq^{k-1} + \frac{2q}{q-1}) \log |\mathcal{K}|$$

llavors

$$\rho(\Gamma^k) \leq \tilde{\rho}(\Gamma^k) = \sup \frac{nq^k \log |\mathcal{K}|}{\sum_{p \in P^k} \log |\mathcal{S}_p|} \leq$$

$$\frac{nq^k}{q^k(2n - \frac{q+1}{q-1} + \frac{(k-1)n}{3}) - \frac{2}{3}(k-1)nq^{k-1} + \frac{2q}{q-1}} \leq$$

$$\frac{n}{2n - \frac{q+1}{q-1} + \frac{(k-1)n}{3} - \frac{2n(k-1)}{3q} + \frac{2}{(q-1)q^{k-1}}}$$

□

S'observa que els graus per aquesta estructura valen $\deg_{\Gamma^k}(2, p) = k + 3$, $\deg_{\Gamma^k}(1, p) = 2k + 4$, la qual cosa ens dóna una fita per a la taxa d'informació

$\rho^*(\Gamma^k) \geq 3/(2k+6)$ fent servir el Teorema 3.4.5. Podem fer una fitació més clara observant:

$$\rho^*(\Gamma^k) \leq \frac{n}{2n - \frac{q+1}{q-1} + \frac{(k-1)n}{3} - \frac{2n(k-1)}{3q} + \frac{2}{(q-1)q^{k-1}}} \leq$$

$$\frac{n}{2n - \frac{q+1}{q-1} + \frac{(k-1)n}{3} - \frac{2n(k-1)}{3q}} = \frac{1}{\frac{q-2}{3q}k + (\frac{5}{3} - \frac{q+1}{(q-1)n} + \frac{2}{3q})}$$

Per exemple per $q = 3$ obtenim:

$$\frac{3}{2k+6} \leq \rho^*(\Gamma^k) \leq \frac{3}{\frac{1}{3}k + (\frac{17}{3} - \frac{6}{n})}$$