Capítol 5

Conclusions

Les conclusions de la present memòria estan estructurades de la manera següent: en primer lloc hi ha la nostra aportació per a la taxa d'informació, després pels esquemes segurs enfront de l'acció de mentiders i finalitza amb les aportacions sobre les arrels cúbiques en un $\mathbb{Z}_m$.

El nostre treball sobre la taxa d'informació ha estat centrat en les dues vessants clàssicament estudiades: la caracterització de les estructures ideals i la fitació de la taxa d'informació. Relacionat íntimament amb el segon dels problemes està la generació d'esquemes amb una taxa raonable.

Ens hem dedicat a l'estudi d'estructures d'accés que són generalització de les més correntment estudiades: les de llindar i les definibles per un graf. Així hem estudiat 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 al càlcul de fites superiors i inferiors de la taxa d'informació, després de fer un estudi de l'estructura d'accés com a estructura combinatòria. Fem a continuació una breu descripció dels resultats obtinguts per a cadascuna d'aquestes estructures i dels principals problemes oberts.

Una de les estructures que més hem estudiat és l'estructura definida per pesos i llindar. Això és degut a que creiem que han de poder ser molt aplicables a situacions concretes, o si més no, constitueixen una opció més realista que els esquemes de llindar, ja que hi ha una jerarquia entre els participants quantificada mitjançant uns pesos. També ens ha decidit l'abscència de treballs dedicats a l'estudi d'aquest tipus d'estructura. Ens hem centrat primer en l'estudi dels pesos i llindar dels quals hem trobat que poden ser canviats per uns de naturals, definint la mateixa estructura. En el cas que l'estuctura sigui de rang 2 aconseguim caracteritzar totes les estructures que són definibles

per pesos i llindar. Així podem identificar quan una estructura de rang 2 és definible per pesos i llindar. A més som capaços de determinar els pesos i llindar mínims que defineixen l'estructura. A partir d'aquest coneixement íntim de l'estructura d'accés, podem trobar esquemes que la realitzen mitjançant la tècnica dels recobriments multipartits complets. D'aquesta manera trobem una fita inferior per la taxa d'informació òptima. Trobem també que l'estructura dual d'una estructura definida per pesos i llindar està definida per pesos i llindar. Així trobem una nova família d'estructures d'accés definibles per pesos i llindar (les que la seva dual és de rang 2) per a les quals determinem els pesos i llindar mínims, així com la seva caracterització. A partir de certes propietats obtingudes amb l'ús de l'estructura dual enunciem teoremes anàlegs als de caracterització i assignació de pesos mínims per una familia encara més àmplia derivada de la definida per pesos i llindar de rang 2 i de la seva dual. Finalment determinem una fita inferior per la taxa d'informació òptima.

Pel que fa a problemes oberts per a les estructures definibles per pesos i llindar no hem trobat una caracterització semblant a les de rang 2 vàlida per a tot rang. Tampoc hem trobat una manera de definir pesos i llindar mínims a partir d'uns pesos i llindar donats, per a tot rang. A la pregunta de si són ajustades les fites obtingudes per ús dels recobriments multipartits complets, no tenim resposta. La utilització de les darreres tècniques per fitar superiorment la taxa d'informació no ens han donat el fruit que esperàvem.

Com a generalització del cas particular de dos pesos, hem estudiat les estructures bipartites en les quals hi ha dues classes de participants que juguen un paper simètric. En aquestes estructures els participants d'una mateixa classe són intercanviables a tot arreu. Aquests fet ens ha semblat bastant real per les possibles aplicacions a més de ser més general que el de les estructures definides per dos pesos i llindar. Així en aquestes estructures que un subconjunt sigui autoritzat només depén de quants elements de la primera classe de participants i de la segona classe conté, però no pas de quins són en concret. Aquestes estructures admeten una representació gràfica bastant còmode. Hem caracteritzat les estructures bipartites ideals trobant que són exactament quatre famílies d'estructures, les que hem anomenat estructures de quasi llindar. Hem demostrat que, com passa en el cas de les estructures definides per un graf, dir que una estructura és ideal és equivalent a dir que és d'espai vectorial. A més hem vist que si una estructura bipartita no és de quasi llindar llavors la seva taxa d'informació és menor o igual que $2/3$, màxim assolible com hem mostrat amb un exemple concret. Tots aquests resultats es poden resumir en un teorema que afirma que per una estructura bipartita són equivalents dir que és de quasi llindar, dir que és d'espai vectorial, dir que és ideal i dir

que la taxa d'informació òptima és més gran que 2/3. Aquest teorema és un teorema calcat al teorema ben conegut per grafs que resulta de substituir *bipartita* per *definida per un graf* i *de quasi llindar* per *graf multipartit complet*. També tenim el conegut resultat que afirma que hi ha un interval prohibit per la taxa d'informació òptima (el $(2/3, 1)$). Mitjançant recobriments hem trobat fites inferiors per la taxa d'informació i hem aplicat la tècnica de la successió d'elements independents per fitar-la superiorment, trobant un algorisme que ens dóna una fita superior bastant raonable.

Problemes oberts que ens ha suggerit l'estudi de les estructures bipartites són els següents. Quines són les famílies d'estructures per les quals és equivalent ser ideal, d'espai vectorial i tenir taxa d'informació més gran que 2/3? Hi ha alguna estructura tal que la seva taxa d'informació òptima estigui a l'interval $(2/3, 1)$? Hi ha estructures ideals que no siguin implementables amb un esquema d'espai vectorial? Si és que n'hi ha, com es poden caracteritzar? També hi ha la possibilitat de generalitzar el nostre treball a estructures *n-partites*, cas que només hem estudiat en certs aspectes a més del cas d'estar definides per pesos i llindar.

Tornant a particularitzar hem estudiat els esquemes definits per dos pesos i llindar. En primer lloc hem trobat fites inferiors de la taxa d'informació òptima amb les tècniques ja fetes servir per a les estructures bipartites. A continuació hem trobat fites superiors pel cas de dos pesos com a particularització dels resultats trobats per estructures bipartites. Es generalitzen els resultats anteriors al cas que disposem d'una estructura definida per més de dos pesos. Aquestes fites superiors i inferiors no són coincidents per la majoria dels casos, per la qual cosa ens hem de plantejar en treballs futurs noves idees i estratègies per tal de millorar cadascuna de les fites. Fins ara hem fet servir fonamentalment una de les estructures per recobrir, però també hem comentat la possible utilització d'altres de forma que ens dóna fites en funció de la distància del taxista entre el punt T_m i T_M (els punts amb menor i més gran suma de coordenades, respectivament). Una de les possibilitats és fer servir qualsevol de les estructures de quasi llindar que hem provat a la secció anterior que són ideals. El cas de més de dos pesos és el que es veu encara més complicat ja que sembla que haurà de passar per l'estudi de les estructures *n-partites*. De tota manera hem donat uns resultats bàsics al respecte.

Com a generalització de les estructures definides per un graf i de les de llindar, ens hem plantejat l'estudi de les estructures homogènies de rang arbitrari. Recordem que tota estructura d'accés es pot posar com a reunió de subestructures homogènies. Hem fet dues construccions d'esquemes per a compartir secrets que ens han proporcionat noves fites inferiors per la taxa d'informació

òptima i per a la taxa d'informació mitjana òptima. Aquestes construccions fan ús de la λ-descomposició. No ens oblidem que també busquem esquemes que realitzin l'estructura de la forma més eficient possible. Les fites de la segona construcció són millors però proporcionen un esquema per a compartir secrets que maneja un conjunt de claus secretes molt gran, mentre que el conjunt de claus de la primera construcció és raonable. Aquestes fites milloren la majoria de les fites proposades fins ara. Per tal de fer el càlcul de les fites i de les comparacions entre elles i amb les anteriors ens hem vist obligats a definir el concepte de k-grau d'un participant en una estructura homogènia. Al final aquest paràmetre ha resultat tan natural que les fites que s'havien proposat fins ara es poden afinar fent servir aquest concepte.

Evidentment caldria veure que les fites que hem trobat són ajustades, com sabem que ho són pel cas de rang 2 (s'ha fet un intent a la mateixa memòria per justificar-ho). Caldria trobar d'altres alternatives que fossin igualment útils, tenint en compte la relació eficiència/complexitat de l'esquema, a l'hora de definir l'esquema per a una estructura homogènia. Si aquestes fites no són ajustades, caldria trobar-ne de millors. Una altra de les feines que queden per fer és l'extensió d'aquests resultats a estructures no necessàriament homogènies.

També hem fet un primer estudi de fitació superior de la taxa d'informació de les estructures homogènies de rang 3. La tècnica és paral·lela a la seguida per demostrar que la fita $2/(d+1)$ és ajustada per grafs de grau màxim d. Aquest procediment consisteix en crear una estructura d'accés per la qual es troba una fita superior de la taxa d'informació òptima. Els resultats d'aquesta fitació no han estat tan bons com en el cas de grafs, però s'observa que les fites inferiors obtingudes a la secció anterior i la fita superior obtinguda ara són properes i del mateix ordre. No sabem si l'estructura que hem definit és la més adient. Cal veure si encara es poden afinar més els càlculs. Cal fer la generalització per a una estructura de rang arbitrari.

El tema dels esquemes per a compartir secrets amb requeriments especials l'hem abordat pel cas d'esquemes segurs enfront l'acció de mentiders. El primer dels nostres resultats és trobar una fita per a la taxa òptima d'informació per esquemes que detecten mentiders (que no coneixen el secret) amb una certa probabilitat. Abans hem fet una definició formal de probabilitat de mentir i de seguretat en esquemes en els quals els mentiders no coneixen el secret repartit i en el cas que sí el coneixen. Aquesta fita i totes aquestes definicions han estat estudiades per altres autors només per estructures de llindar. Hem fet una proposta d'un esquema que realitza estructures d'accés d'espai vectorial (en particular també les de llindar) amb detecció de mentiders que no coneixen

el secret. La taxa òptima d'informació és asimptòticament òptima: 1/2. La comparació de la complexitat de càlcul de l'esquema amb l'únic proposat fins ara que té la taxa òptima (i que és vàlid només per esquemes de llindar), dóna una clara aventatge al nostre. Hem proposat un esquema per estructures de llindar que detecta mentiders que coneixen el secret. Aquest esquema és un esquema amb taxa d'informació 1/3. Fent ús d'esquemes d'espai vectorial hem proposat el primer esquema per a compartir secrets incondicionalment segur per a qualsevol estructura d'accés, generalitzant el primer dels nostres esquemes.

En el camp dels esquemes per a compartir secrets segurs enfront l'acció de mentiders relacionat amb els problemes principals de la taxa d'informació, cal trobar fitacions de la taxa d'informació amb els diferents requeriments que es poden demanar. Pels esquemes per a compartir secrets falta trobar esquemes que assoleixin la màxima fita possible de la taxa d'informació d'una forma pràctica (computacionalment parlant). Les propostes que han fet d'altres autors aporten solucions pel que fa a detecció, identificació o protecció del secret enfront dels mentiders, però només per estructures de llindar. Cal proposar esquemes que facin el mateix, però per estructures qualssevol i a ser possible amb una taxa d'informació raonable. Aquí sembla que s'hauria de començar a treballar en la introducció de les tècniques de recobriment per la millora de la taxa d'informació.

La memòria s'acaba amb un exposició del problema de l'existència i càlcul de l'arrel cúbica en un $\mathbb{Z}_m$. Es discuteix la qüestió de l'existència de l'arrel cúbica en un $\mathbb{Z}_p$ amb p primer. Es troba que hi ha dos casos segons que p sigui congruent amb -1 o amb 1 mòdul 3. Pel càlcul de les arrels cúbiques es troba un mètode molt simple pel primer cas i s'estudia el segon cas. Per aquest segon cas es generalitzen els mètodes pel càlcul de l'arrel quadrada de Peralta i de Tonelli-Shanks per arrels cúbiques. L'estudi de la complexitat indica que les parts no probabilístiques dels algorismes són de l'ordre de $\log^3 p$ pel primer i de $\log^4 p$ pel segon. S'han proposat algunes aplicacions criptogràfiques com ara al criptosistema de Rabin. Pel que fa al tema de l'arrel cúbica, hi ha moltes aplicacions possibles que caldria buscar entre les que té l'arrel quadrada: garbell cúbic (com a test de primalitat), ús d'aquests resultats en corbes el·líptiques, generador de nombres pseudo aleatoris (el de Blum-Blum-Shub) i les seves aplicacions criptogràfiques, tests de primalitat de Solovay-Strassen i de Lehman-Peralta, etc. Evidentment un dels problemes oberts sembla ser la generació d'un algorisme completament determinista pel càlcul de l'arrel cúbica a més d'intentar generalitzar els altres mètodes existents pel càlcul d'arrel quadrades: algorisme de Adleman-Manders-Miller, algorisme de Schoof

i l'algorisme de Lehmer. Caldria plantejar la generalització a arrels de qualsevol ordre.