Butlletí de la Societat Catalana de Matemàtiques
Vol. 21, núm. 2, 2006. Pàg. 197–211

Introducció als polinomis de Rédei

Simeon Ball

Resum Aquest article descriu algunes aplicacions dels polinomis de Rédei a problemes sorgits en l'àmbit de les geometries finites. Començarem amb una introducció als polinomis per Rédei per poder resoldre un problema de la factorització dels grups elementaris abelians. Llavors, continuarem amb les seves aplicacions, donades per Blokhuis, a problemes de conjunts bloquejadors a plans finits. Finalment, considerarem resultats de Brouwer-Schrijver i Alon-Tarsi en dimensions més grans.

Paraules clau: polinomis de Rédei, geometries finites.

Classificació MSC2000: 05.

1 Introducció

Els plans afí i projectiu reals són models geomètrics clàssics que tenen els seus anàlegs en el context de les *geometries finites*, en les quals el nombre de punts és finit. Tant des del punt de vista axiomàtic com des de la seva descripció algebraica, aquests models finits es corresponen exactament amb les versions clàssiques: simplement es tracta de substituir el cos $\mathbb{R}$ de les versions reals per un cos finit. Recordem que hi ha un cos finit únic de q elements per a cada q que és potència d'un nombre primer (i no n'hi ha cap si q no és una potència d'un nombre primer). Aquí denotarem per $\mathbb{F}_q$ el cos finit de q elements amb $q = p^r$, $r \geq 1$ i p primer.

Així, doncs, el pla afí sobre $\mathbb{F}_q$, que denotarem per $AG(2,q)$ (acrònim de l'anglès *affine geometry*), té per conjunt de punts les parelles (x,y) de $\mathbb{F}_q \times \mathbb{F}_q$, i per conjunt de rectes les solucions d'equacions del tipus $y = ax + b$ o $x = a$, $a, b \in \mathbb{F}_q$. D'aquesta manera cada dos punts determinen una única línia, i dues línies o no es tallen o ho fan en un únic punt. El pla afí es pot estendre al pla

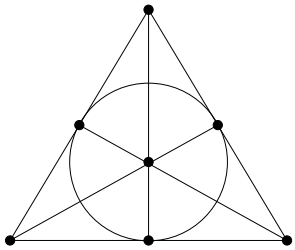

FIGURA 1: El pla de Fano.

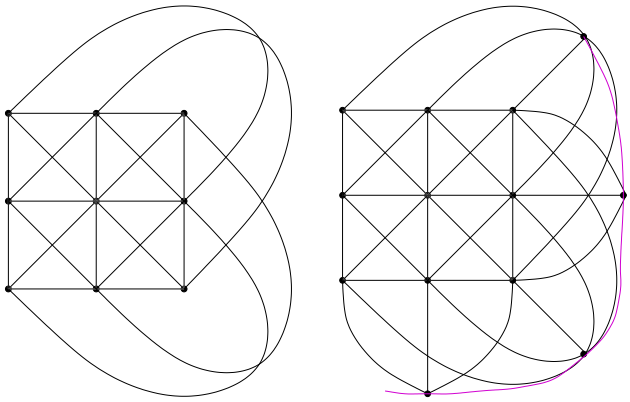

FIGURA 2: El pla afí i el pla projectiu sobre $\mathbb{F}_3$.

projectiu $PG(2,q)$ afegint un punt per a cada família de línies paral·leles i la línia formada per tots aquests punts. Des del punt de vista algebraic, els punts de $PG(2,q)$ es poden identificar amb els subespais de dimensió 1 de $(\mathbb{F}_q)^3$ i les línies són els subespais de dimensió 2. D'aquesta manera, cada dos punts determinen una única línia i cada dos línies es tallen exactament en un punt. L'exemple més senzill (i força important) de pla projectiu finit és el *pla de Fano*, $PG(2,2)$, dibuixat a la figura 1. A la figura 2 hi ha dibuixats el pla afí i el pla projectiu sobre $\mathbb{F}_3$.

Observem al pla de Fano de la figura 1 que cada línia conté tres punts i que cada punt és incident amb tres línies (una de les línies s'ha de dibuixar arrodonida; és per això que en el context de les geometries finites es parla de *línies* en lloc de *rectes*). Aquesta observació fa pensar en la mena de problemes que poden considerar-se en el context de les geometries finites: a més dels problemes geomètrics clàssics, en sorgeixen molts de nous relacionats amb l'enumeració.

Un cop establerts alguns dels elements sobre els quals formularem els nostres problemes, podem introduir un teorema ben bonic del matemàtic hongarès Lazslo Rédei (1900–1986) que és a l'origen del tema d'aquest article. Dos punts (a_1, a_2) i (a'_1, a'_2) al pla afí finit $AG(2, q)$ diem que determinen la direcció

$$\frac{a_2 - a'_2}{a'_1 - a_1},$$

si $a_1 \neq a'_1$, o la direcció ∞ si $a_1 = a'_1$. El teorema a què fèiem referència diu el que segueix:

1 TEOREMA (RÉDEI, [17]) *Sigui p un nombre primer senar i A un conjunt de p punts del pla afí $AG(2, p)$. Si A no és una línia, aleshores els punts de A determinen com a mínim $(p + 3)/2$ direccions.*

Per exemple, si cinc punts del pla afí $AG(2, 5)$ determinen menys de quatre direccions, aleshores només en determinen una: són tots sobre una mateixa línia (i són tots els punts d'aquesta línia ja que totes tenen exactament cinc punts).

L'objectiu d'aquest article és explicar el mètode de demostració que va introduir Rédei per a aquest i altres resultats, un mètode basat en la construcció de certs polinomis. Veurem com el mètode ha estat aplicat amb èxit a diversos problemes, particularment en els de trobar fites inferiors per al cardinal del nombre de punts d'un pla afí $AG(2, p)$ que calen per *trepitjar* totes les línies del pla, una de les aplicacions fonamentals dels polinomis de Rédei desenvolupada per Aart Blokhuis.

Els polinomis de Rédei formen part del que s'anomena *mètodes polinomials* en combinatòria. Hi ha molts exemples de les aplicacions de polinomis a la matemàtica discreta: posem per cas el polinomi de Tutte per matroides [13], el polinomi d'enumeració de pesos d'un codi [14], el polinomi de l'índex dels cicles d'un grup de permutacions [9] o, més rellevant per a les aplicacions que apareixen en aquest article, les aplicacions de l'anomenat *combinatorial Nullstellensatz* d'Alon [1]. Tot i això, els polinomis més usats en l'estudi de problemes sorgits en l'àmbit de les geometries finites van aparèixer per primera vegada en el llibre de Rédei [17]. És per això que s'anomenen *polinomis de Rédei*.

En general, tant si fem servir els polinomis de Rédei com si no, la manera d'aplicar els polinomis a un objecte geomètric és la següent: donat un subconjunt A de punts d'una geometria finita amb una certa propietat de regularitat, escrivim un polinomi f que ens tradueix les propietats geomètriques de A a propietats *algèbriques* de f. Procurem llavors obtenir més propietats de f que ens donin més informació geomètrica sobre A.

2 El treball inicial de Rédei

Per veure com Rédei va arribar a l'enunciat del teorema 1, repassem primer un dels problemes que l'ocupaven.

Sigui G un grup abelià finit. Diem que els conjunts $A, B \subset G$ formen una *factorització* de G si cada element $g \in G$ s'escriu de manera *única* com a $g = a + b$ amb $a \in A$ i $b \in B$. No és difícil trobar exemples de factoritzacions d'un grup abelià: prenem un subgrup propi A de G i prenem com a B un transversal de A, és a dir, un element de cada classe lateral de G mòdul A. L'objectiu de Rédei era el de classificar els grups abelians per als quals aquesta és l'única mena de factoritzacions possible.

Un dels casos més simples és aquell en què el grup és $G = (\mathbb{Z}/p\mathbb{Z})^2$, el producte de dos grups cíclics amb p elements, on p és primer i imparell.

Llevat de casos trivials, si $G = A + B$ és una factorització de G, aleshores tant A com B tenen p elements. Vegem com Rédei va formular el problema per concloure que un dels dos conjunts ha de ser un subgrup (o la classe lateral d'un subgrup).

Sigui $\epsilon \in \mathbb{C} \setminus \{1\}$, una arrel p-èsima de la unitat, $\epsilon^p = 1$. Sigui $\{a, b\}$ una base de G. Escrivint l'operació de G en forma multiplicativa,

$$G = \{a^i b^j \mid 0 \le i,\ j \le p-1\}.$$

Per a cada $z \in \mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ definim

$$\omega_z(a^i b^j) = \epsilon^{iz+j}.$$

Es verifica que $\omega_z(gh) = \omega_z(g)\omega_z(h)$. A més, per a cada h i cada z,

$$\omega_z(h) \sum_{g \in G} \omega_z(g) = \sum_{g \in G} \omega_z(gh) = \sum_{g \in G} \omega_z(g).$$

Per tant, $\sum_{g \in G} \omega_z(g) = 0$. Com que A i B formen una factorització de G, obtenim

$$0 = \sum_{g \in G} \omega_z(g) = \left(\sum_{a \in A} \omega_z(a) \right) \left(\sum_{b \in B} \omega_z(b) \right).$$

Per tant, un dels subconjunts A o B, diguem A, té la propietat que per almenys $(p+1)/2$ elements z de $\mathbb{Z}_p$,

$$0 = \sum_{a \in A} \omega_z(a) = \sum_{a \in A} \epsilon^{a_1 z + a_2}, \tag{1}$$

on $a = (a_1, a_2)$. Sigui S una seqüència de p arrels p-èsimes de la unitat amb la propietat que

$$\sum_{i=0}^{p-1} c_i \epsilon^i = 0,$$

on c_i és el nombre de vegades que apareix ϵ^i en S. Aleshores ϵ és una arrel del polinomi $f(X) = \sum_{i=0}^{p-1} c_i X^i \in \mathbb{Z}[X]$. D'altra banda, sigui $g(X) = (X^p - 1)/(X - 1)$; pel criteri d'Eisenstein, el polinomi $g(X+1)$ és irreductible a $\mathbb{R}[X]$ i, per tant,

$g(X)$ també ho és. Sigui $d = (f, g)$ el polinomi de $\mathbb{R}[X]$ que és el màxim comú divisor de f i g en $\mathbb{R}[X]$. Com que g és irreductible en $\mathbb{R}[X]$, el polinomi d és o bé 1 o bé un múltiple del polinomi g. Però en $\mathbb{C}$ els polinomis f i g tenen una arrel comuna i, per tant, $d \neq 1$. Concloem que f és múltiple de g i, a més, com que tenen el mateix grau i $\sum_{i=0}^{p-1} c_i = p$, els dos polinomis coincideixen. En particular $c_i = 1$ per a cada i. Tot això significa que

$$\{a_1 z + a_2 \mid a \in A\} = \{0, 1, \ldots, p-1\},$$

per almenys $(p+1)/2$ elements $z \in \mathbb{Z}_p$. El teorema de Rédei que exposarem a la secció següent demostra que un subconjunt A de $\mathbb{Z}_p^2$ amb aquesta propietat ha de ser una classe lateral.

3 Els polinomis de Rédei i el seu teorema

En lloc del grup $\mathbb{Z}_p$, Rédei fa servir el cos $\mathbb{F}_p$, que té els mateixos elements i la mateixa taula d'addició, però té, a més, l'operació de multiplicació mòdul p.

Recordem que, per a cada $c \in \mathbb{F}_p$, es satisfà $c^p = c$, i, per tant, $\prod_{c \in \mathbb{F}_p} (X - c) = X^p - X$. Denotarem per f° el grau d'un polinomi f.

A la demostració del teorema següent de Rédei es pot apreciar la idea central que és a la base de tot el desenvolupament posterior d'aquest mètode polinomial.

2 TEOREMA *Sigui A un subconjunt de $\mathbb{F}_p^2$ amb p elements i sigui N el conjunt dels elements $z \in \mathbb{F}_p$ amb la propietat que*

$$\{a_1 z + a_2 \mid a \in A\} = \{0, 1, \ldots, p-1\}.$$

Si $|N| \geq (p+1)/2$, aleshores A és una classe lateral.

PROVA Sigui

$$r(X, Y) = \prod_{a \in A} (X + a_1 Y + a_2).$$

Per hipòtesi, els elements $z \in N$ tenen la propietat

$$r(X, z) = \prod_{a \in A} (X + a_1 z + a_2) = \prod_{c \in \mathbb{F}_p} (X - c) = X^p - X.$$

Ara escrivim el polinomi r com a polinomi en X amb coeficients que són polinomis en Y

$$r(X, Y) = \sum_{j=0}^{|A|} \sigma_j(Y) X^{|A|-j}. \tag{2}$$

El grau del polinomi $r(X, Y)$ és $|A| = p$ i, per tant, el grau del polinomi $\sigma_j(Y)$ és menor o igual que j.

D'acord amb (2), si $z \in N$, aleshores $\sigma_j(z) = 0$ per a cada $j = 1, 2, \ldots, p-2$. Com que un polinomi no nul no pot tenir més arrels que el seu grau

$$\sigma_1 \equiv \sigma_2 \equiv \cdots \equiv \sigma_{|N|-1} \equiv 0\,,$$

llevat que $|N|$ sigui p.

Suposem que hi ha un element $z \notin N$. Aleshores

$$r(X,z) = \prod_{a \in A} (X + a_1 z + a_2) = X^p + \sum_{j=N}^{p} \sigma_j(z) X^{p-j} = X^p + s(X)\,, \qquad (3)$$

per a algun polinomi $s \neq -X$ de grau menor o igual que $p - N$.

Tots els factors de $r(X,z)$ són factors de $X^p - X$ i els que tenen multiplicitat més gran que 1 són factors de $r' = dr/dX$; per tant,

$$r(X,z) \mid (X^p - X) r'\,.$$

Les operacions en $\mathbb{F}_p$ són mòdul p i, per això, la derivada de r és $r' = pX^{p-1} + s' = s'$, la qual té grau com a màxim $p - N - 1$. La divisibilitat assegura

$$r(X,z) \mid (X^p - X - r(X,z)) r' = -(X + s(X)) s'\,.$$

Si $s' \neq 0$, aleshores el grau de r, que és igual a p, és com a màxim $2s^\circ - 1$. Això vol dir que $p \leq 2(p-N) - 1$ o $N \leq (p-1)/2$, cosa que contradiu la nostra hipòtesi.

Així, doncs, tenim $s' = 0$ i $s = c$ per algun $c \in \mathbb{F}_p$. Substituint a (3),

$$r(X,z) = \prod_{a \in A} (X + a_1 z + a_2) = X^p + c = (X + c)^p\,,$$

i, per tant,

$$A = \{(a_1, c - a_1 z) \mid a_1 \in \mathbb{F}_p\} = (0,c) + \{x(1,-z) \mid x \in \mathbb{F}_p\}.$$

En altres paraules, A és una classe lateral del subgrup additiu de $\mathbb{F}_p^2$ generat per $(1,-z)$. Notem que en aquest cas $\mathbb{F}_p \setminus N$ pot constar només d'un element.

Finalment tenim el cas que $N = \mathbb{F}_p$. Prenem dos elements $a = (a_1, a_2)$ i $a' = (a_1', a_2')$ de A. No hi ha cap element de $z \in \mathbb{F}_p$ tal que $a_1 z + a_2 = a_1' z + a_2'$, la qual cosa implica que $a_1 = a_1' = c$ per a algun $c \in \mathbb{F}_p$. Aleshores A és la classe lateral $(c,0) + \{(0,x) \mid x \in \mathbb{F}_p\}$ i obtenim la mateixa conclusió. □

La demostració anterior, de gran bellesa i enginy, fa intervenir el polinomi r que és un producte de polinomis lineals amb coeficients en un cos finit. Qualsevol polinomi d'aquest tipus s'anomena un *polinomi de Rédei*.

Hi ha d'altres maneres de descriure el teorema de Rédei. La propietat

$$\{a_1 z + a_2 \mid a \in A\} = \mathbb{F}_p$$

implica que no hi ha cap parell d'elements $a, a' \in A$ amb la propietat $a_1 z + a_2 = a_1' z + a_2'$, o sigui

$$-z = \frac{a_2 - a_2'}{a_1 - a_1'}.$$

En termes geomètrics, $-z$ no apareix com a direcció entre dos punts qualssevol (a_1, a_2), (a_1', a_2') de A. El teorema de Rédei, doncs, diu que, si un conjunt de p punts del pla afí $\mathrm{AG}(2, p)$ determina com a màxim $(p+1)/2$ direccions, aleshores és una línia. Aquest és l'enunciat del teorema 1.

El teorema de Rédei ens presenta un seguit de preguntes. Primer, la fita $(p+1)/2$ és la millor possible? La resposta a aquesta pregunta és afirmativa. Hi ha exemples de Megyesi on

$$A = \{(x, 0), (0, -y) \mid x, y \in \mathbb{F}_p \; x^d = 1 \; y^d \neq 1\}$$

que tenen d direccions no determinades, les arrels d-èsimes de la unitat. És clar que, per a això, cal que $\mathbb{F}_p$ tingui arrels d-èsimes de la unitat, que és el que passa quan d divideix $p-1$. Si escollim $d = (p-1)/2$, obtenim un exemple de conjunt que determina $(p+3)/2$ direccions (hi ha una direcció infinita) i que no és una classe lateral, fet que prova que la fita dels teoremes 1 i 2 és justa. Fixem-nos que, si escollim $d = p-1$, el conjunt A és una línia.

La segona pregunta pot ser què passa quan tenim menys direccions no determinades. Gács [10] va demostrar que, si $|N| \geq 2\lceil p - 1/6 \rceil + 1$, aleshores A està contingut en la unió de dues línies, és a dir, en la unió de *dues* classes laterals. Notem que, quan $p \equiv 1 \pmod 3$, hi ha un exemple de Megyesi amb $|N| = (p-1)/3$, que gairebé arriba a la fita de Gács. Hi ha un teorema de Szőnyi [19] que diu que, si A està contingut en la unió de dues línies i no determina com a mínim tres direccions, aleshores A és una generalització d'un exemple de Megyesi.

La tercera pregunta que ens podem plantejar és què passa quan substituïm el cos $\mathbb{F}_p$ per $\mathbb{F}_q$, el cos amb q elements on q és una potència d'un primer. Els resultats principals de [4] i [6] diuen que, si $|N| \geq (q+1)/2$, aleshores A és una classe lateral d'un subespai de dimensió r sobre $\mathbb{F}_{p^e}$, on $q = p^{er}$.

Una altra pregunta pot ser què passa quan A té més de p elements. Procurarem donar una resposta a aquesta pregunta en la propera secció.

4 El teorema de Blokhuis

El teorema de Blokhuis [5] és una generalització del teorema de Rédei per a conjunts de més de p elements. La prova segueix els mateixos passos que la del teorema de Rédei fent servir el lema següent de caràcter tècnic. Recordem que f° és el grau d'un polinomi f.

3 Lema *Sigui $r(X) = t(X)X^p + s(X)$ tal que el màxim comú divisor de s i t és 1, i els graus de s i t són com a màxim $(p-1)/2$. Si $r(X)$ és un polinomi de Rédei, és a dir, un producte de polinomis lineals a $\mathbb{F}_p[X]$, aleshores o bé $r = e(X+c)^p$ per a alguns elements $c, e \in \mathbb{F}_p$, o bé $r(X) = (X^p - X)t(X)$.*

PROVA Els factors de $r(X)$ són factors de $X^p - X$ i, per tant, són factors de $t(X^p - X) - r = -(tX + s)$. Els factors amb multiplicitat més gran que un de $r(X)$ són factors de $r' = dr/dX = X^p t' - s'$ i, per tant, són factors de $t'r - r't = t's - s't$. Com que $r(X)$ és un producte de polinomis lineals,

$$r(X) \mid -(Xt + s)(t's - s't).$$

A mà dreta de la divisibilitat el polinomi té grau com a màxim $(p+1)/2 + s^\circ + t^\circ - 1 \leq p - 1 + t^\circ$. A mà esquerra de la divisibilitat el polinomi r té grau $p + t$. Per tant, $(Xt + s)(ts' - t's) = 0$.

Si $s = -Xt$, aleshores $r = (X^q - X)t$.

Si $s't = t's$, aleshores t divideix t' (perquè $(s,t) = 1$) i, consegüentment, $t' = 0$ i $s' = 0$. Per tant, $t = e$ i $s = ec$ per a alguns elements $c, e \in \mathbb{F}_p$. □

4 TEOREMA *Sigui A un subconjunt de $\mathbb{F}_p^2$ amb $p + k$ elements i sigui N el conjunt dels elements $z \in \mathbb{F}_p$ amb la propietat que*

$$\{a_1 z + a_2 \mid (a_1, a_2) \in A\} \supseteq \mathbb{F}_p.$$

Si $|N| \geq (p+1)/2 + k$, aleshores A conté una classe lateral.

PROVA Sigui

$$r(X,Y) = \prod_{a \in A} (X + a_1 Y + a_2).$$

Per hipòtesi, si $z \in N$, aleshores

$$r(X,z) = \prod_{a \in A} (X + a_1 z + a_2) = (X^p - X)t(X),$$

per a algun polinomi $t(X)$ de grau k. Com abans, escrivim el polinomi r com a polinomi en X amb coeficients polinòmics en Y,

$$r(X,Y) = \sum_{j=0}^{|A|} \sigma_j(Y) X^{|A|-j}.$$

El grau del polinomi r és $|A|$ i, per tant, el polinomi $\sigma_j(Y)$ té grau menor o igual que j.

Suposem que $z \in N$. Hem vist que $\sigma_j(z) = 0$ per a $j = k+1, k+2, \ldots, q-2$. Com que un polinomi no nul no pot tenir més arrels que el seu grau,

$$\sigma_{k+1} \equiv \sigma_{k+2} \equiv \cdots \equiv \sigma_{|N|-1} \equiv 0.$$

Ara, suposem que $y \notin N$. Aleshores,

$$r(X,y) = \prod_{a \in A} (X + a_1 y + a_2) = \sum_{j=0}^{k} \sigma_j X^{p+k-j} + \sum_{j=N}^{p+k} \sigma_j X^{p+k-j} = t(X)X^p + s(X),$$

per a alguns polinomis s i t, on $s \neq -Xt$, $s^\circ \leq p - (N-k)$ i $t^\circ \leq k$.

Sigui $d(X)$ el màxim comú divisor de s i t.

Per hipòtesi, $|N| - k \geq (p+1)/2$ i, com que $|N| \leq p$, tenim $k \leq (p-1)/2$. A més, $s \neq -Xt$ i, per tant, el lema 3 implica que $r(X,z)/d = e(X+c)^p$.

Ara podem fer servir els mateixos raonaments de la prova del teorema de Rédei per concloure que A conté una classe lateral. □

El teorema de Blokhuis és important per les seves aplicacions als *conjunts bloquejadors* (en anglès, *blocking sets*) del pla projectiu $\mathrm{PG}(2,p)$. El pla projectiu $\mathrm{PG}(2,p)$ consta dels punts

$$\langle (x,y,z) \rangle = \{\lambda(x,y,z) \mid \lambda \in \mathbb{F}_p\},$$

on $x,y,z \in \mathbb{F}_p$ no són tots zero. És a dir, un punt és un subespai de dimensió u de l'espai vectorial $\mathbb{F}_p^3$ de dimensió tres sobre $\mathbb{F}_p$. Les línies són donades per equacions homogènies

$$aX + bY + cZ = 0\,.$$

Fixem-nos que, si considerem només els punts de $\mathrm{PG}(2,p)$ amb $z \neq 0$, recuperem el pla afí $\mathrm{AG}(2,p)$.

Un *conjunt bloquejador* B d'un pla és un conjunt de punts amb la propietat que cada línia és incident com a mínim, ambun punt de B. Com que al pla projectiu dues línies qualssevol es tallen, el conjunt de punts format per una línia és evidentment un conjunt bloquejador. Una conseqüència directa del teorema de Blokhuis és que qualsevol conjunt bloquejador *petit* ha de contenir un d'aquests bloquejadors trivials.

5 Corol·lari *Sigui B un conjunt bloquejador del pla projectiu $PG(2,q)$, on q és una potència d'un primer. Si $|B| < 3(q+1)/2$, aleshores B conté una línia del pla.*

Prova Podem suposar que B és un conjunt bloquejador minimal per inclusió.

Les línies definides per les equacions $Y = mX + cZ$ en el pla $\mathrm{PG}(2,q)$ són incidents amb el punt projectiu $\langle (1,m,0) \rangle$. Sigui N el conjunt d'elements $m \in \mathbb{F}_q$ tals que el punt $\langle (1,m,0) \rangle$ no pertany a B. Totes les línies $Y = mX + cZ$, $m \in N$, són incidents amb un punt $a = \langle (a_1,a_2,1) \rangle \in B$. Així, doncs, per a cada $c \in \mathbb{F}_p$ hi ha $a \in B$ tal que $c = -a_1 m + a_2$, o sigui

$$\{a_1(-m) + a_2 \mid a \in B\} \supseteq \mathbb{F}_p\,.$$

Podem suposar que el punt $\langle (0,1,0) \rangle \in B$ i, per tant, B té $p + 1 - |N|$ punts amb la tercera coordenada igual a zero. Sigui $|B| = p + k + (p + 1 - |N|)$. Aleshores $|N| = 2p + 1 + k - |B| \geq (p+1)/2 + k$, i el teorema 4 implica que B conté una línia. □

L'exemple de Megyesi amb $d = (p-1)/2$ es pot estendre a un exemple d'un conjunt bloquejador de $\mathrm{PG}(2,p)$ que no conté cap línia i que té exactament $3(p+1)/2$ elements. Per tant, la fita en el corol·lari 5 és la millor possible.

Si procurem substituir $\mathrm{PG}(2,p)$ per $\mathrm{PG}(2,q)$, on q és una potència d'un primer, el problema de decidir sobre l'optimalitat de la fita esdevé molt més complicat. Hi ha exemples de conjunt bloquejadors que tenen menys de $(p+1)/2$ punts i no contenen cap línia. La construcció següent és de Lunardon [15] i Polverino i Polito [16]. Sigui $q=p^h$ i sigui e un divisor de h. Les línies de $\mathrm{PG}(2,q)$, que són els subespais de dimensió 2 de $\mathbb{F}_q^3$, són subespais de dimensió $2h/e$ de $\mathbb{F}_{p^e}^{3h/e}$. Sigui U un subespai de $\mathbb{F}_{p^e}^{3h/e}$ de dimensió $h/e+1$. Sigui B els punts de $\mathrm{PG}(2,q)$, que són subespais de dimensió h/e, que tenen una intersecció no trivial amb U. Cada línia té una intersecció no trivial amb U i per tant és incident amb un punt de B. A més,

$$|B| \le \frac{(p^e)^{h/e+1}-1}{p^e-1} = q + \frac{q-1}{p^e-1} < 3(q+1)/2\,,$$

tret que p^e sigui 2.

Hi ha una conjectura que diu que tots els conjunts bloquejadors de $\mathrm{PG}(2,q)$ de mida menys que $3(q+1)/2$ són coneguts i es poden construir de la manera indicada en el paràgraf anterior. Szőnyi [18] va demostrar que, si B és un conjunt bloquejador amb $|B|<3(q+1)/2$, aleshores el nombre de punts de B incident amb cada línia és congruent amb 1 mòdul p. La conjectura, però, continua oberta.

5 Conjunts bloquejadors a l'espai afí $\mathrm{AG}(n,q)$

En aquesta secció obtindrem una fita inferior per a la mida d'un conjunt bloquejador del pla afí $\mathrm{AG}(2,p)$. De fet, obtindrem una fita més general. Substituïm p per qualsevol potència d'un primer q i 2 per qualsevol dimensió n. La fita inferior per a la mida d'un conjunt bloquejador d'$\mathrm{AG}(2,q)$ (o $\mathrm{AG}(n,q)$) no depén de si q és primer o no i, com veurem, és més gran que la fita en el cas projectiu.

Primer de tot, hem de parlar una mica d'un ideal de l'anell de polinomis $\mathbb{F}_q[X_1,\dots,X_n]$.

Sigui

$$I = \langle (X_1^q - X_1), \dots, (X_n^q - X_n) \rangle\,,$$

l'ideal generat pels polinomis de la forma $(X_i^q - X_i)$, $1 \le i \le n$; és a dir, I consta de tots els polinomis $f \in \mathbb{F}_q[X_1,\dots,X_n]$ que podem escriure com a

$$f = \sum_{i=0}^{n} (X_i^q - X_i) f_i\,,$$

per a alguns polinomis $f_i \in \mathbb{F}_q[X_1,\dots,X_n]$.

L'ideal I té la caracterització següent.

6 Lema *Un polinomi $f \in \mathbb{F}_q[X_1,\dots,X_n]$ té la propietat que*

$$f(x_1,x_2,\dots,x_n) = 0$$

per a cada $x \in \mathbb{F}_q^n$ si i només si $f \in I$.

PROVA La implicació ($\Leftarrow$) és evident. La implicació ($\Rightarrow$) es pot provar per inducció sobre el nombre de variables. Si $n = 1$, el polinomi $f(X) = (X^q - X)f_1$ per a algun polinomi f_1 si i només si $f(x) = 0$ per a cada $x \in \mathbb{F}_q$. Suposem $n > 1$. Podem escriure

$$f = \sum_{i=0}^{n-1} (X_i^q - X_i) f_i + h\,,$$

on el grau de X_i en h és com a màxim $q-1$ per a cada $i = 1, 2, \ldots, n-1$. Per la hipòtesi d'inducció, $f(X_1, \ldots, X_{n-1}, x_n) \in I$ per a cada $x_n \in \mathbb{F}_q$ i, per tant, $h(X_1, \ldots, X_{n-1}, x_n) \in I$, la qual cosa assegura que $h(X_1, \ldots, X_{n-1}, x_n) = 0$. Així, doncs, $X_n^q - X_n$ divideix h. □

L'espai afí de dimensió $n \geq 3$, $\mathrm{AG}(n, q)$, és una extensió del pla $\mathrm{AG}(2, q)$. Els seus punts tenen n coordenades de $\mathbb{F}_q$ i els seus hiperplans són donats per equacions de la forma

$$b_1X_1 + b_2X_2 + \ldots + b_nX_n = \delta,$$

on $\delta = 0, 1$. Un conjunt bloquejador d'$\mathrm{AG}(n, q)$ és un conjunt B amb la propietat que cada hiperplà passa per algun punt de B. El problema que es planteja és trobar una fita mínima per a la mida d'un conjunt bloquejador. La prova del teorema següent de Jamison [12] és de Brouwer i Schrijver [7].

7 TEOREMA *Un conjunt bloquejador d'$AG(n, q)$ té com a mínim $n(q-1)+1$ punts.*

PROVA Sigui B un conjunt bloquejador d'$\mathrm{AG}(n, q)$. Podem suposar, sense perdre la generalitat, que $(0, 0, \ldots, 0) \in B$. Sigui r el polinomi de Rédei de grau $|B|$, definit per

$$r(X) = \prod_{b \in B} (b_1X_1 + \ldots b_nX_n - 1)\,.$$

Per hipòtesi,

$$r(x_1, x_2, \ldots, x_n) = 0\,,$$

per a cada $x \in \mathbb{F}_q^n$ i $x \neq 0$. Notem que $r(0) \neq 0$. No obstant això, per a qualsevol $i \in \{1, \ldots, n\}$, el polinomi $X_i r(X) \in I$. Escrivim

$$r(X) = h(X) + \sum_{j=1}^{n} (X_j^q - X_j) f_j\,,$$

on el grau de h en qualsevol de les variables X_j és com a màxim $q-1$. Aleshores, $X_i r \in I$ implica $X_i h \in I$ i, per a les fites dels graus de h, el polinomi $X_i h \in \langle X_i^q - X_i \rangle$. Per tant, $X_i^q - X_i$ divideix $X_i h$ així que $X_i^{q-1} - 1$ divideix h. Consegüentment, h és un múltiple del polinomi

$$\prod_{i=1}^{n} (X_i^{q-1} - 1).$$

Com que $h(0) = r(0) \neq 0$, h és un polinomi diferent de zero. Per això, el grau de h és com a mínim $n(q-1)$. D'altra banda, el grau de r, $r^\circ = |A| - 1$, és com a mínim el grau de h.

La fita és la millor possible. El conjunt dels punts que tenen com a màxim una coordenada diferent de zero té la propietat desitjada i la seva mida és $n(q-1)+1$.

6 La conjectura de Jaeger

Sigui $GL(n,q)$ el conjunt de les matrius $n \times n$ no singulars amb coeficients a $\mathbb{F}_q$, on, com sempre, q és una potència d'un nombre primer. François Jaeger va proposar una conjectura simple i ben curiosa:

8 Conjectura (Jaeger) *Per a cada matriu A de $GL(n,q)$, hi ha un vector $v \in \mathbb{F}_q^n$ amb la propietat que v i Av no tenen cap coordenada zero.*

Jaeger va formular aquesta conjectura per al cas $q = 5$. En aquesta secció veurem una demostració de la conjectura en el cas en què q no és primer. El cas en què q és primer continua obert per a $q \geq 5$. Les matrius

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad \text{i} \quad \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

són contraexemples de la conjectura per als casos $q = 2$ i $q = 3$ respectivament.

En el cas $q = 2$ l'únic vector amb cap coordenada zero és $(1,1)$ i

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

i, per tant, o bé v o bé Av té una coordenada zero.

En el cas $q = 3$ sigui (x,y) un vector que no té cap coordenada zero, $xy \neq 0$. Com que $\mathbb{F}_3$ té només dos elements no zeros, o bé $x = y$ o bé $x = -y$. Així, doncs,

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+y \\ x-y \end{pmatrix},$$

i, per tant, o bé v o bé Av té una coordenada zero.

Per demostrar la conjectura de Jaeger en el cas en què q no és primer, adaptem la demostració feta per Alon i Tarsi [2]. Fa servir un altre ideal

$$I^* = \langle (X_1^{q-1} - 1), \ldots, (X_n^{q-1} - 1) \rangle,$$

que té la caracterització següent, que es demostra de manera anàloga al lema 6.

9 Lema *Un polinomi $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ té la propietat*

$$f(x_1, x_2, \ldots, x_n) = 0$$

per a cada $x \in (\mathbb{F}_q \setminus \{0\})^n$ si i només si $f \in I^*$.

El teorema següent no és enunciat en els termes de la conjectura de Jaeger, però veurem després com aquesta se'n dedueix.

10 TEOREMA *Sigui q no primer. Per a qualsevol parella de bases B i C de l'espai vectorial $\mathbb{F}_q^n$, existeix un hiperplà que no conté cap vector de $B \cup C$.*

PROVA Suposem el contrari: que cada hiperplà conté un vector de $B \cup C$. Podem suposar que una de les bases, diguem C, és la base canònica. Sigui

$$r(X) = \prod_{j=1}^{n} (b_{j1}X_1 + \cdots + b_{jn}X_n)\,,$$

on $b_j \in B$ i b_{jk} és la k-èsima coordenada de b_j. Els hiperplans que no són incidents amb cap punt de C tenen equacions

$$x_1X_1 + \cdots + x_nX_n = 0\,,$$

on $x \in (\mathbb{F}_q \setminus \{0\})^n$. Si cada hiperplà no incident amb cap punt de C és incident amb un punt de B, aleshores hi ha un $b_j \in B$ tal que

$$b_{j1}x_1 + \cdots + b_{jn}x_n = 0\,,$$

i, per tant, $r(x) = 0$, per a cada $x \in (\mathbb{F}_q \setminus \{0\})^n$.

Si aplicam el lema anterior, hi ha polinomis f_k tals que

$$r(X) = \sum_{k=1}^{n-1} (X_k^{q-1} - 1) f_k\,.$$

Com que B és una base, la matriu (b_{jk}) té una inversa (x_{ki}), és a dir, $\sum_{k=1}^{n} b_{jk}x_{ki} = \delta_{ji}$. Substituïm $X_k = \sum_{i=1}^{n} x_{ki}Y_i$ per deduir

$$Y_1Y_2\ldots Y_n = \sum_{k=1}^{n-1} \left(\left(\sum_{i=1}^{n} x_{ki}Y_i \right)^{q-1} - 1 \right) f_k\,.$$

A mà esquerra hi ha un terme $Y_1Y_2\ldots Y_n$ de grau n i, per tant, un dels termes $\left(\sum_{i=1}^{n} x_{ki}Y_i\right)^{q-1}$ ha de donar-nos un terme $Y_{i_1}\ldots Y_{i_{q-1}}$ amb coeficient diferent de zero. No obstant això, tots aquests termes tenen com a coeficient un múltiple de $(q-1)!$, que és zero si q no és primer.

11 COROL·LARI *Sigui q no primer. Per a cada matriu $A \in GL(n,q)$, hi ha un vector $v \in \mathbb{F}_q^n$ amb la propietat que v i Av no tenen cap coordenada zero.*

PROVA Per al teorema existeix un hiperplà donat per una equació

$$v_1X_1 + \cdots + v_nX_n = 0\,,$$

que no té cap incidència amb un vector de la base canònica. Per tant, $v_i \neq 0$ per a cada $i = 1,\ldots,n$. A més, no té cap incidència amb un vector de la base formada per les files de $A = (a_{jk})$. Això vol dir que, per a cada $j = 1,\ldots,n$,

$$a_{j1}v_1 + \ldots a_{jn}v_n \neq 0\,.$$

7 Consideracions finals

Si el tema interessa al lector, recomano l'article [20] per trobar més detalls sobre els conjunts bloquejadors en PG$(2, q)$ i més referències a articles que fan servir polinomis de Rédei. Els articles [3, 8] tenen més detalls sobre els conjunts bloquejadors d'AG(n, q).

8 Agraïments

A Oriol Serra per la seva ajuda. Al Ministeri de Ciència i Tecnologia pel seu suport mitjançant el Programa Ramón y Cajal.

Referències

[1] Alon, N. «Combinatorial Nullstellensatz». *Combin. Probab. Comput.*, 8 (1999), 7–29.

[2] Alon, N.; Tarsi, M. «A nowhere-zero point in linear mappings». *Combinatorica*, 9 (1989), 393–395.

[3] Ball, S. «On intersection sets in Desarguesian affine spaces». *European J. Combin.*, 21 (2000), 441–446.

[4] Ball, S. «The number of directions determined by a function over a finite field». *J. Combin. Theory Ser. A*, 104 (2003), 341–350.

[5] Blokhuis, A. «On the size of a blocking set in $PG(2, p)$» *Combinatorica*, 14 (1994), 111–114.

[6] Blokhuis, A.; Ball, S.; Brouwer, A. E.; Storme, L.; Szőnyi, T. «On the number of slopes of the graph of a function defined over a finite field». *J. Combin. Theory Ser. A*, 86 (1999), 187–196.

[7] Brouwer, A. E.; Schrijver, A. «The blocking number of an affine space». *J. Combin. Theory Ser. A*, 24 (1978), 251–253.

[8] Bruen, A. A. «Polynomial multiplicities over finite fields and intersection sets». *J. Combin. Theory Ser. A*, 60 (1992), 19–33.

[9] Cameron, P. J. «Cycle index, weight enumerator, and Tutte polynomial». *Electron. J. Combin.*, 9 (2002), nota 2. 10 p.

[10] Gács, A. «On a generalization of Rédei's theorem». *Combinatorica*, 23 (2003), 585–598.

[11] Jaeger, F. «Problema presentat en el *6th Hungar. Comb. Coll., Eger,* Hongria, 1981». A: Hajnal, A.; Lovász, L.; Sós, V. [ed.]. *Finite and Infinite Sets*. Amsterdam: North Holland, 1982, II, 879.

[12] Jamison, R. «Covering finite fields with cosets of subspaces». *J. Combin. Theory Ser. A*, 22 (1977), 253–266.

[13] Kung, J. P. S.; Noy, M.; Welsh, D. [ed.]. «Special issue dedicated to the Tutte polynomial». *Adv. in Appl. Math.*, 32, 2004.

[14] MacWilliams, F. J.; Sloane, N. J. A. *The theory of error-correcting codes*. Amsterdam: North-Holland, 1977.

[15] Lunardon, G. «Normal spreads». *Geom. Dedicata*, 75 (1999), 245–261.

[16] Polito, P.; Polverino, O. «On small blocking sets». *Combinatorica*, 18 (1997), 133–137.

[17] Rédei, L. *Lückenhafte Polynome über endlichen Körpen*. Basel: Birkhäuser-Verlag, 1970. [Traducció anglesa: *Lacunary Polynomials over finite fields*. Amsterdam: North-Holland, 1973]

[18] Szönyi, T. «Combinatorial problems for abelian groups arising from geometry». *Periodica Polytechnica*, 19 (1991), 91–100.

[19] Szönyi, T. «Blocking sets in Desarguesian affine and projective planes». *Finite Fields Appl.*, 3 (1997), 187–202.

[20] Szönyi, T.; Gács, A.; Weiner, Z. «On the spectrum of minimal blocking sets in PG$(2, q)$». *J. Geom*, 76 (2003), 256–281.

Departament de Matemàtica Aplicada IV
Universitat Politècnica de Catalunya
Jordi Girona, 1
08034 Barcelona
simeon@ma4.upc.edu