Enumeració d'òrbites de n-conjunts d'espais projectius sota l'acció del grup lineal

Ricard Martí i Miras

Enumeració d'òrbites de n-conjunts d'espais projectius sota l'acció del grup lineal

Ricard Martí i Miras

Aquesta memòria ha estat realitzada per Ricard Martí i Miras sota la meva direcció, i constitueix la seva Tesi Doctoral per aspirar al grau de Doctor en Matemàtiques per la Universitat Autònoma de Barcelona

Bellaterra, març de 2006

Enric Nart

Als meus pares

Índex

Introducció

En aquesta memòria emprenem un estudi enumeratiu dels n-conjunts d'espais projectius sobre un cos finit k. Hi ha una doble motivació per estudiar aquests objectes. D'una banda, per una coneguda construcció de Tsfasman-Vlădut [TV91], els n-conjunts de punts k-racionals d'un espai projectiu determinen codis lineals sobre k (injectius si no hi ha repeticions entre els punts) i aquesta construcció permet establir una correspondència bijectiva entre òrbites de n-conjunts de punts k-racionals sota l'acció del grup lineal i classes d'isometria (també anomenades classes d'equivalència forta) de codis lineals. Des d'aquest punt de vista, ens interessem per n-conjunts de la forma $\{P_1, \ldots, P_n\}$ amb els P_i punts k-racionals d'un espai projectiu $\mathbb{P}^N$; és a dir, cada P_i admet coordenades homogènies amb valors al cos base k.

D'altra banda, els n-conjunts d'espais projectius tenen un estret lligam amb altres objectes geomètrics interessants. L'estudi d'aquests n-conjunts i els seus espais de moduli ha estat objecte de l'atenció de la geometria algebraica des de les seves etapes més clàssiques. Destaquen les contribucions de A. Coble a principis del segle passat. A [DO88] es pot trobar una extensa bibliografia sobre aquests treballs i una revisió dels mateixos en clau moderna. Centrant-nos en alguns dels casos més senzills, és ben sabut que, sobre un cos algebraicament tancat, els n-conjunts de $\mathbb{P}^1$ classifiquen corbes hiperel·líptiques [DO88, Cap. VIII], i els 7-conjunts del pla classifiquen corbes no hiperel·líptiques de gènere 3 dotades d'una estructura de 2-nivell [DO88, Cap. IX]. Si ens interessem per les propietats aritmètiques dels objectes geomètrics involucrats amb els n-conjunts, caldrà preocupar-se per la *racionalitat* d'aquests n-conjunts, és a dir, pel fet que el n-conjunt estigui definit sobre el cos base k; això vol dir que

$$\{\sigma(P_1), \ldots, \sigma(P_n)\} = \{P_1, \ldots, P_n\}, \quad \forall \sigma \in \mathrm{Gal}(\overline{k}/k),$$

de manera que per a cada membre P_i del n-conjunt tota l'òrbita de P_i per l'acció del grup de Galois ha d'estar continguda també al n-conjunt. Evidentment, els n-conjunts que hem mencionat abans, formats íntegrament per punts k-racionals són n-conjunts k-racionals, però són un tipus molt particular de n-conjunts k-racionals.

Per exemple, imaginem que els punts P_i són tots diferents, estan en una recta projectiva i els assignem una coordenada afí a_i a cadascun. Si la característica de k és senar podem associar aleshores al n-conjunt una corba hiperel·líptica donada per l'equació plana de Weierstrass

$$y^2 = (x - a_1)(x - a_2) \cdots (x - a_n).$$

Les corbes hiperel·líptiques k-definides venen donades en general per equacions de la forma $y^2 = f(x)$, on $f(x)$ és un polinomi separable arbitrari amb coeficients a k. Treballant amb n-conjunts de punts k-racionals només estem considerant corbes

amb la propietat (molt particular) que el polinomi $f(x)$ descompon completament a k. Veiem doncs la conveniència d'estendre el nostre estudi al cas de n-conjunts d'espais projectius que són racionals com a n-conjunt i no necessàriament punt a punt.

Atenent a la doble naturalesa dels n-conjunts i al fet que admetin o no repeticions dels seus punts, l'objectiu de la memòria és el d'obtenir fórmules explícites per a les següents quatre famílies de nombres:

$$T_N(n) := \left|\mathrm{PGL}_{N+1}(k)\backslash\backslash \binom{\mathbb{P}^N(k)}{n}\right|, \quad \overline{T}_N(n) := \left|\mathrm{PGL}_{N+1}(k)\backslash\backslash \left(\!\!\binom{\mathbb{P}^N(k)}{n}\!\!\right)\right|,$$

$$t_N(n) := \left|\mathrm{PGL}_{N+1}(k)\backslash\backslash \binom{\mathbb{P}^N}{n}(k)\right|, \quad \overline{t}_N(n) := \left|\mathrm{PGL}_{N+1}(k)\backslash\backslash \left(\!\!\binom{\mathbb{P}^N}{n}\!\!\right)(k)\right|,$$

on, en general, donat un conjunt finit X i un grup finit Γ que actua sobre X, denotem per $\Gamma\backslash\backslash X$ el conjunt d'òrbites d'aquesta acció; denotem per $\binom{X}{n}$, resp. $\left(\!\!\binom{X}{n}\!\!\right)$ el conjunt dels n-subconjunts, resp. n-multiconjunts de X i, finalment, denotem

$$\binom{\mathbb{P}^N}{n}(k) := \binom{\mathbb{P}^N(\overline{k})}{n}^{\mathrm{Gal}(\overline{k}/k)}, \quad \left(\!\!\binom{\mathbb{P}^N}{n}\!\!\right)(k) := \left(\!\!\binom{\mathbb{P}^N(\overline{k})}{n}\!\!\right)^{\mathrm{Gal}(\overline{k}/k)},$$

el nombre de n-conjunts i n-multiconjunts racionals de l'espai projectiu $\mathbb{P}^N$.

L'única referència que hem trobat a la literatura sobre els nombres $t_N(n)$, $\overline{t}_N(n)$ és l'article [LMNX02] on es donen fórmules explícites per als $t_1(n)$. En canvi, els nombres $T_N(n)$, $\overline{T}_N(n)$ han estat extensament estudiats; a [BFKWZ98] es fa un recull dels aspectes que concerneixen el seu càlcul i es dona una fórmula per a la seva funció generadora en termes de l'indicador de cicles de Pólya:

$$\begin{aligned} \sum_{n\in\mathbb{N}} T_N(n)x^n &= C(\mathrm{PGL}_{N+1},\mathbb{P}^N)_{|_{z_i=\frac{1}{1-x^i}}}, \\ \sum_{n\in\mathbb{N}} \overline{T}_N(n)x^n &= C(\mathrm{PGL}_{N+1},\mathbb{P}^N)_{|_{z_i=1+x^i}}, \end{aligned} \tag{1}$$

on $C(\mathrm{PGL}_{N+1},\mathbb{P}^N)$ és un determinat polinomi amb coeficients racionals, en indeterminades z_i, una per cada punt de $\mathbb{P}^N(k)$ (al capítol 1 en recordem la definició).

A més a més, H. Fripertinger va obtenir una descripció en termes combinatoris d'aquest indicador de cicles, que li va permetre implementar aquesta fórmula per obtenir taules amb els valors d'aquests nombres [Fri97], [Fri98].

En el capítol 1 de la memòria obtenim fórmules alternatives per als $T_2(n)$, $\overline{T}_2(n)$ i d'altres nombres relacionats, que compten el nombre de clases d'isometria de codis de dimensió tres amb certes propietats específiques. Les fórmules es basen en un recompte explícit del nombre de classes de conjugació d'elements de $\mathrm{PGL}_3(k)$ que donen lloc a permutacions de $\mathbb{P}^2(k)$ amb la mateixa descomposició en cicles i són prou mal·leables com per permetre obtenir expressions dels nombres $T_2(n)$, $\overline{T}_2(n)$ com a polinomis en q (on $k = \mathbb{F}_q$) amb coeficients racionals.

En els capítols 2 i 3 passem a estudiar el problema anàleg per als n-conjunts racionals. En el capítol 2 trobem fórmules explícites per al nombre total de n-conjunts racionals i en el capítol 3 estudiem el nombre d'òrbites sota l'acció del grup lineal. El resultat clau és el teorema 6.1, que calcula la funció zeta del quocient d'un espai projectiu per un automorfisme. A partir d'aquest resultat es pot imitar el procediment del capítol 1 per obtenir expressions explícites per als $t_2(n)$, $\overline{t}_2(n)$ com a polinomis en q amb coeficients enters.

Al capítol 4 desenvolupem aquestes idees per a un espai projectiu $\mathbb{P}^N$ de dimensió arbitrària. Els mètodes utilitzats en els capítols anteriors se sintetitzen en la classificació dels elements de $\mathrm{PGL}_{N+1}(k)$ en *subtipus* (hi ha un concepte més genèric de *tipus* d'un element de $\mathrm{PGL}_{N+1}(k)$, que també utilitzem) i en la construcció per a cada subtipus α d'un poset $\mathcal{L}(\alpha)$ amb pesos "dimensió" i "exponent" en cada node V, que permeten considerar un *indicador d'exponents*

$$\mathcal{L}(\mathrm{PGL}_{N+1}, \mathbb{P}^N) := \sum_{\alpha \in \mathcal{T}} N_\alpha \prod_{V \in \mathcal{L}(\alpha)} z_{\alpha,V} \in \mathbb{Q}[\{z_{\alpha,V}\}],$$

on $\mathcal{T}$ és el conjunt de tots els subtipus possibles i N_α compta el nombre de classes de conjugació de $\mathrm{PGL}_{N+1}(k)$ amb subtipus α fixat. Els posets $\mathcal{L}(\alpha)$ es construeixen a partir de subvarietats lineals γ-invariants *pròpies* (vegeu la definició a la secció 9), on $\gamma \in \mathrm{PGL}_{N+1}(k)$ és qualsevol automorfisme amb subtipus α. A partir d'aquest indicador d'exponents podem obtenir un resultat anàleg a (1)

$$\sum_{n \in \mathbb{N}} T_N(n) x^n = \mathcal{L}(\mathrm{PGL}_{N+1}, \mathbb{P}^N)_{|_{z_{\alpha,V} = h_{\alpha,V}(x)}},$$
$$\sum_{n \in \mathbb{N}} \overline{T}_N(n) x^n = \mathcal{L}(\mathrm{PGL}_{N+1}, \mathbb{P}^N)_{|_{z_{\alpha,V} = \overline{h}_{\alpha,V}(x)}},$$

per a funcions $h_{\alpha,V}(x)$, $\overline{h}_{\alpha,V}(x)$, que donem explícitament (vegeu el teorema 10.2).

L'avantatge d'aquest indicador d'exponents respecte de l'indicador de cicles de Pólya té una doble vessant. D'una banda, el polinomi $\mathcal{L}(\mathrm{PGL}_{N+1}, \mathbb{P}^N)$ té un nombre molt més reduit de variables i la implementació d'aquestes fórmules té una complexitat essencialment menor que la del càlcul de (1). D'altra banda, la seva concepció es pot estendre fàcilment al cas dels n-conjunts racionals. Considerem en la memòria un concepte anàleg de *G-subtipus* dels elements de $\mathrm{PGL}_{N+1}(k)$ i per a

cada G-subtipus α construim un poset $\mathcal{L}_G(\alpha)$ (la G fa referència a "Galois") amb pesos "dimensió", "exponent" i "grau" en cada node V, que permeten considerar un *G-indicador d'exponents*

$$\mathcal{L}_G(\mathrm{PGL}_{N+1}, \mathbb{P}^N) := \sum_{\alpha \in \mathcal{T}_G} N_{G,\alpha} \prod_{V \in \mathcal{L}_G(\alpha)} z_{\alpha,V} \in \mathbb{Q}[\{z_{\alpha,V}\}],$$

on $\mathcal{T}_G$ és el conjunt de tots els G-subtipus possibles i $N_{G,\alpha}$ compta el nombre de classes de conjugació de $\mathrm{PGL}_{N+1}(k)$ amb G-subtipus α fixat. A partir d'aquest G-indicador d'exponents podem obtenir un resultat anàleg a l'anterior

$$\sum_{n \in \mathbb{N}} t_N(n) x^n = \mathcal{L}_G(\mathrm{PGL}_{N+1}, \mathbb{P}^N)_{|_{z_{\alpha,V} = f_{\alpha,V}(x)}},$$

$$\sum_{n \in \mathbb{N}} \overline{t}_N(n) x^n = \mathcal{L}_G(\mathrm{PGL}_{N+1}, \mathbb{P}^N)_{|_{z_{\alpha,V} = \overline{f}_{\alpha,V}(x)}},$$

per a funcions $f_{\alpha,V}(x)$, $\overline{f}_{\alpha,V}(x)$, que donem explícitament (vegeu el teorema 10.5).

Per poder pensar que aquestes fòrmules són plenament satisfactòries des del punt de vista combinatori calen dues coses. En primer lloc cal obtenir una descripció intrínseca dels conjunts $\mathcal{T}$, $\mathcal{T}_G$ i dels posets $\mathcal{L}(\alpha)$, $\mathcal{L}_G(\alpha)$, en termes de dades combinatòries independents de l'estructura de grup de $\mathrm{PGL}_{N+1}(k)$; aquesta tasca s'acompleix a la secció 10.2 del capítol 4. Finalment, cal disposar també de fórmules explícites per als coeficients universals N_α, $N_{G,\alpha}$; aquesta tasca, que s'ha dut a terme en els capítols 1, 2 i 3 en el cas del pla projectiu, adquireix una gran complexitat en dimensions més grans i aquest càlcul ha quedat finalment fora de l'abast d'aquesta memòria. El problema combinatori de calcular aquests nombres N_α, $N_{G,\alpha}$ és força suggerent i esperem poder abordar-lo en una altra ocasió.

Agraeixo a l'Enric Nart el gran interés que ha mostrat per aquest treball, i la seva dedicació i paciència durant tot el procés d'evolució personal que ha significat per a mi atacar aquests problemes i anar seguint els camins, sovint inesperats i costeruts, que m'han dut a la seva comprensió i posterior resolució.

També vull expressar als meus pares i a la meva àvia un agraïment molt especial per l'ambient familiar agradable i afectuós que m'ha permès gaudir d'unes condicions favorables de treball. Sense el seu suport continuat i fidel la redacció d'aquesta memòria no hauria estat possible.

Capítol 1

Classes d'isometria de codis associats a n-conjunts del pla projectiu

Sigui Γ un grup finit actuant per l'esquerra sobre un conjunt finit $\mathcal{X}$ i denotem per $\Gamma\backslash\backslash\mathcal{X}$ el conjunt d'òrbites d'elements de $\mathcal{X}$ respecte d'aquesta acció. Aquest nombre d'òrbites es pot comptar utilitzant el lema de Cauchy-Frobenius [BFKWZ98, 3.1.6]:

$$|\Gamma\backslash\backslash\mathcal{X}| = \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}|\mathcal{X}_\gamma| = \sum_{\gamma\in\mathcal{C}}\frac{|\mathcal{X}_\gamma|}{|\Gamma_\gamma|}, \tag{2}$$

on $\mathcal{C}$ és un sistema de representants de classes de conjugació d'elements de Γ i

$$\mathcal{X}_\gamma := \{x\in\mathcal{X}|\gamma(x)=x\}, \quad \Gamma_\gamma := \{\rho\in\Gamma|\rho\gamma\rho^{-1}=\gamma\}.$$

Aquesta fórmula es pot aplicar al càlcul de nombres de classes d'isometria de certes famílies de codis lineals [BFKWZ98, 3.2]. Per exemple, donats un enter positiu N i un cos finit k, considerem $\Gamma = \mathrm{PGL}_{N+1}(k)$ actuant de manera natural sobre el conjunt $\mathcal{X}$ de n-subconjunts de l'espai projectiu $\mathbb{P}^N(k)$ (resp. sobre el conjunt $\mathcal{Y}$ de n-multiconjunts de $\mathbb{P}^N(k)$). Aleshores, els nombres $T_N(n) := |\Gamma\backslash\backslash\mathcal{X}|$ (resp. $\overline{T}_N(n) := |\Gamma\backslash\backslash\mathcal{Y}|$) compten classes d'isometria de tots els codis (resp. de tots els codis injectius) de longitud n i dimensió menor o igual que N, la matriu generadora dels quals no té cap columna nul·la. En els dos casos és possible obtenir (per a N fixat) una funció generadora per a aquests nombres d'òrbites en termes de l'indicador de cicles de Pólya ([BFKWZ98, 3.2.16]):

$$\sum_{n\in\mathbb{N}} T_N(n)x^n = C(\mathrm{PGL}_{N+1},\mathbb{P}^N)_{|_{z_i=\frac{1}{1-x^i}}},$$

$$\sum_{n\in\mathbb{N}} \overline{T}_N(n)x^n = C(\mathrm{PGL}_{N+1},\mathbb{P}^N)_{|_{z_i=1+x^i}}.$$

Recordem que, en general, per a qualsevol acció de Γ sobre $\mathcal{X}$ es defineix

$$C(\Gamma, \mathcal{X}) = \frac{1}{|\Gamma|} \sum_{\gamma \in \Gamma} \prod_{i=1}^{|\mathcal{X}|} z_i^{a_i(\gamma)} \in \mathbb{Q}[z_1,\, z_2,\, \ldots, z_{|\mathcal{X}|}],$$

on $a_i(\gamma)$ és el nombre de cicles de longitud i que apareixen en la descomposició en producte de cicles disjunts de γ actuant com a permutació de $\mathcal{X}$. Per a cada $\gamma \in \Gamma$, el vector $(a_1(\gamma), \ldots, a_{|\mathcal{X}|}(\gamma))$ s'anomena el *tipus de cicle* de γ.

Fripertinger [Fri97] ha obtingut a més a més una descripció general de l'índex $C(\mathrm{PGL}_{N+1}, \mathbb{P}^N)$, la qual ens permet construir taules dels valors de $T_N(n)$, $\overline{T}_N(n)$. Tanmateix, aquesta descripció és bastant embolicada i fins i tot per a valors petits de k el càlcul explícit d'aquests nombres requereix en diverses etapes l'aplicació d'algorismes.

L'objectiu d'aquest capítol és, en primer lloc, obtenir per a $\Gamma = \mathrm{PGL}_3(k)$ una descomposició explícita de $\mathcal{C}$ en una unió disjunta de famílies, $\mathcal{C} = \cup_\alpha \mathcal{C}_\alpha$, segons el tipus de cicle dels seus elements actuant sobre el pla projectiu $\mathbb{P}^2(k)$. El tipus de cicle de qualsevol γ depèn de la variació de l'estructura del conjunt de punts fixos entre les projectivitats del subgrup cíclic generat per γ.

Després, trobem fórmules per als cardinals:

$$c_\alpha := |\mathcal{C}_\alpha|, \quad g_\alpha := |\Gamma_\gamma|,\ \gamma \in \mathcal{C}_\alpha,$$

de cada subconjunt $\mathcal{C}_\alpha$ i els centralitzadors d'elements $\gamma \in \mathcal{C}_\alpha$ (que són constants per a elements de la mateixa família). Obtenim així fórmules explícites per als nombres:

$$N_\alpha := \sum_{\gamma \in \mathcal{C}_\alpha} \frac{1}{|\Gamma_\gamma|} = c_\alpha / g_\alpha.$$

Això ens permet obtenir fórmules per al nombre d'òrbites de l'acció de Γ sobre conjunts finits $\mathcal{X}$ quan els cardinals $|\mathcal{X}_\gamma|$ depenen només del tipus de cicle de γ actuant sobre $\mathbb{P}^2(k)$. De fet, per (2), s'obté:

$$|\Gamma \backslash\backslash \mathcal{X}| = \sum_\alpha N_\alpha x_\alpha,$$

on $x_\alpha := |\mathcal{X}_\gamma|$, per a $\gamma \in \mathcal{C}_\alpha$.

Com a aplicació, obtenim a les seccions 3.1 i 3.2 fórmules explícites per a $T_2(n)$, $\overline{T}_2(n)$ i per al nombre de classes d'isometria d'altres famílies de codis de dimensió tres. Fórmules anàlogues per a $T_1(n)$ han estat obtingudes a [LN99].

Alternativament, podem pensar que l'objectiu d'aquest capítol és proporcionar un càlcul molt concret de l'indicador de cicles de Pólya $C(\mathrm{PGL}_3, \mathbb{P}^2)$ i mostrar diverses aplicacions d'aquest càlcul.

Els resultats d'aquest capítol han estat publicats a [MN04].

1 Classes de conjugació i centralitzadors de PGL_3

Sigui k un cos. En aquesta secció trobem un sistema $\mathcal{C}$ de representants de classes de conjugació de $\Gamma := \mathrm{PGL}_3(k)$. Per a tot $\gamma \in \mathcal{C}$ estudiem el subgrup d'isotropia Γ_γ respecte de l'acció de Γ sobre ell mateix per automorfismes interns:

$$\Gamma_\gamma := \{\rho \in \Gamma \,|\, \rho^{-1}\gamma\rho = \gamma\} = \{\rho \in \Gamma \,|\, \gamma\rho = \rho\gamma\},$$

i calculem el seu cardinal quan k és un cos finit.

Classes de conjugació

Donada una matriu $A \in \mathrm{GL}_3(k)$, el polinomi característic $f_A(t)$ pertany a:

$$\mathcal{P} := \{f(t) \in k[t] \,|\, f(t) \text{ és mònic de grau 3 i } f(0) \neq 0\}.$$

Aquest conjunt $\mathcal{P}$ descompon en la unió disjunta de cinc famílies:

$$\begin{aligned}
\mathcal{P}_I &:= \{f(t) \in \mathcal{P} \,|\, f(t) \text{ és irreductible sobre } k\},\\
\mathcal{P}_{II} &:= \{f(t) \in \mathcal{P} \,|\, f(t) = (t-a)g(t),\ a \in k,\ g(t) \text{ irreductible sobre } k\},\\
\mathcal{P}_{III} &:= \{f(t) \in \mathcal{P} \,|\, f(t) \text{ té 3 arrels diferents a } k\},\\
\mathcal{P}_{IV} &:= \{f(t) \in \mathcal{P} \,|\, f(t) = (t-a)(t-b)^2,\ a,b \in k, a \neq b\},\\
\mathcal{P}_V &:= \{f(t) \in \mathcal{P} \,|\, f(t) = (t-a)^3,\ a \in k\},
\end{aligned}$$

i direm que una matriu A és del tipus I, II, III, IV o V segons si $f_A(t)$ pertany a cadascuna d'aquestes famílies. Considerem ara la següent acció de k^* respectivament sobre $\mathrm{GL}_3(k)$ i $\mathcal{P}$:

$$A^\lambda := \lambda A, \qquad f^\lambda(t) := \lambda^3 f(\frac{t}{\lambda}),$$

per a tot $\lambda \in k^*$, $A \in \mathrm{GL}_3(k)$, $f(t) \in \mathcal{P}$. Tenim clarament $f_{\lambda A}(t) = f_A^\lambda(t)$, de manera que la correspondència que assigna a cada matriu el seu polinomi característic indueix una aplicació exhaustiva ben definida:

$$f\colon \mathrm{PGL}_3(k) = (k^* \backslash\backslash \mathrm{GL}_3(k)) \longrightarrow k^* \backslash\backslash \mathcal{P}.$$

Clarament, aquesta aplicació factoritza a través del conjunt $\mathcal{C}$ de classes de conjugació de $\mathrm{PGL}_3(k)$:

$$f : \mathcal{C} \longrightarrow k^* \backslash\backslash \mathcal{P}.$$

A més, $x \in \bar{k}$ és una arrel de $f(t)$ si i només si λx és una arrel de $f^\lambda(t)$; per tant, l'acció de k^* sobre $\mathcal{P}$ respecta el tipus de factorització dels polinomis com a producte de polinomis irreductibles a $k[t]$. Així, encara té sentit dir que un element γ o una classe de conjugació de $\mathrm{PGL}_3(k)$ és de tipus $\mathrm{I}, \mathrm{II}, \mathrm{III}, \mathrm{IV}$ o V segons la subfamília de $\mathcal{P}$ a la qual $f_A(t)$ pertany, on A és qualsevol representant a $\mathrm{GL}_3(k)$ de γ o de qualsevol element de la classe de conjugació de γ.

Fixem ara un sistema de representants, que continuem denotant $\mathcal{C}$, de classes de conjugació de $\mathrm{PGL}_3(k)$, simplement triant representants de l'acció de k^* sobre una família de matrius amb forma normal de Jordan. Definim $\mathcal{C} = \mathcal{C}_I \cup \mathcal{C}_{II} \cup \mathcal{C}_{III} \cup \mathcal{C}_{IV} \cup \mathcal{C}_V$, on $\mathcal{C}_{IV} := \mathcal{C}'_{IV} \cup \mathcal{C}''_{IV}$ i:

$$\begin{aligned}
\mathcal{C}_I &:= \{ \begin{pmatrix} 0 & 0 & -a \\ 1 & 0 & -b \\ 0 & 1 & -c \end{pmatrix} \mid t^3 + ct^2 + bt + a \in k^* \backslash\backslash \mathcal{P}_I \}, \\
\mathcal{C}_{II} &:= \{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -b \\ 0 & 1 & -c \end{pmatrix} \mid t^2 + ct + b \text{ irreductible a } k[t] \}, \\
\mathcal{C}_{III} &:= \{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix} \mid (b,c) \in \mathcal{T} \}, \\
\mathcal{C}'_{IV} &:= \{ \begin{pmatrix} a & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid a \in k - \{0,1\} \}, \\
\mathcal{C}''_{IV} &:= \{ \begin{pmatrix} a & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \mid a \in k - \{0,1\} \}, \\
\mathcal{C}_V &:= \{ \gamma_V := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \gamma'_V := \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, 1 \},
\end{aligned}$$

on $\mathcal{T}$ és un conjunt de representants del conjunt quocient de

$$((k - \{0,1\}) \times (k - \{0,1\})) \setminus \Delta,$$

sent Δ el subconjunt diagonal, per l'acció de S_3 generada per:

$$(b,c) \sim (c,b), \qquad (b,c) \sim (cb^{-1}, b^{-1}) \sim (c^{-1}, bc^{-1}). \tag{3}$$

Com que l'aplicació f és exhaustiva i per a un polinomi característic separable la forma normal de Jordan queda unívocament determinada pel polinomi:

Lema 1.1. *Per a* $? \in \{I, II, III\}$*, la correspondència que assigna a cada matriu el seu polinomi característic indueix aplicacions bijectives:*

$$f : \mathcal{C}_? \longrightarrow k^* \backslash\backslash \mathcal{P}_?.$$

A [Hir79, 7.4], es pot trobar una descripció similar de $\mathcal{C}$ i un càlcul del nombre de classes de conjugació de cada tipus, quan $k = \mathbb{F}_q$ és un cos finit. De fet, el que necessitem és un refinament d'aquests càlculs. Dins cadascun d'aquests subconjunts volem comptar el nombre d'elements amb un tipus de cicle donat actuant com a permutacions de $\mathbb{P}^2(\mathbb{F}_q)$. Això s'aconseguirà a la secció 2.

Centralitzadors

Aquesta subsecció està dedicada al càlcul de Γ_γ. Donats $\gamma, \rho \in \mathrm{PGL}_3(k)$, podem considerar representants arbitraris $A, B \in \mathrm{GL}_3(k)$; la condició $\rho\gamma = \gamma\rho$ es tradueix en $AB = \lambda BA$, per a un cert $\lambda \in k^*$. Donats $A \in \mathrm{GL}_3(k)$ i $\lambda \in k^*$, considerem el k-espai vectorial:

$$V_{A,\lambda} := \{M \in M_3(k) \,|\, MA = \lambda AM\}.$$

Per a $\lambda = 1$, $V_A := V_{A,1}$ és una k-àlgebra, la dimensió de la qual depèn d'una manera ben coneguda de la forma normal de Jordan de A. De fet, estem interessats en els conjunts:

$$V^*_{A,\lambda} := V_{A,\lambda} \cap \mathrm{GL}_3(k),$$

ja que Γ_γ es pot expressar com la unió disjunta:

$$\Gamma_\gamma = \cup_{\lambda \in k^*} \left(k^* \backslash\backslash V^*_{A,\lambda}\right). \tag{4}$$

Observem que $V^*_{A,\lambda}$ no és buit si i només si A i λA són conjugats, i això passa només per a valors molt especials de λ i A:

Lema 1.2. *Suposem que* $A \in \mathrm{GL}_n(k)$ *i* λA *són conjugats a* $\mathrm{GL}_n(k)$*, per a un cert* $\lambda \in k^*$*. Aleshores,* $\lambda^n = 1$ *i el polinomi característic de* A *és del tipus:*

$$f_A(t) = (t^d + a_1) \cdots (t^d + a_r), \quad a_1, \ldots, a_r \in \overline{k}^*, \tag{5}$$

on d *és l'ordre del subgrup cíclic de* k^* *generat per* λ *i* $n = dr$*.*

Recíprocament, si $\lambda^n = 1$*,* $f_A(t)$ *és separable i té la forma indicada a (5), aleshores* A *i* λA *són conjugats a* $\mathrm{GL}_n(k)$*.*

Dem. Si A i λA són conjugats, el multiconjunt d'arrels del seu polinomi característic (comptant multiplicitats) ha de ser invariant sota multiplicació per λ. Com que cap d'aquestes arrels és zero, el multiconjunt de les arrels ha de ser una unió d'òrbites $\alpha, \lambda\alpha, \ldots, \lambda^{d-1}\alpha$ per a certs elements $\alpha \in \bar{k}$.

Recíprocament, si $f_A(t)$ és separable, la forma normal de Jordan de A queda unívocament determinada pel polinomi característic. Si $f_A(t)$ té la forma indicada a (5) i $\lambda^d = 1$, aleshores A i λA tenen el mateix polinomi característic i, en conseqüència, la mateixa forma normal de Jordan. ■

Per a les matrius A del tipus I totes les matrius no nul·les que pertanyen a V_A són invertibles:

Lema 1.3. *Siguin $A, B \in \mathrm{GL}_n(k)$ i suposem que el polinomi característic de A és irreductible sobre k. Sigui V el k-espai vectorial: $V = \{M \in M_n(k) \mid MA = BM\}$. Aleshores, tot $M \in V$ és o bé zero o bé invertible. En particular, $V \neq 0$ si i només si A i B són conjugats a $\mathrm{GL}_n(k)$. En aquest darrer cas, tenim $\dim_k V = n$.*

Dem. Les matrius A, B determinen dos homomorfismes d'anells $k[t] \longrightarrow M_n(k) = \mathrm{End}_k(k^n)$. Obtenim així dues estructures de $k[t]$-mòdul sobre k^n, que denotem per E_A, E_B. La condició $MA = BM$ implica que la multiplicació per M determina un homomorfisme $M\colon E_A \longrightarrow E_B$ de $k[t]$-mòduls. Per hipòtesi, el mòdul E_A és simple, per tant, o bé $\ker M = E_A$ o bé $\ker M = 0$. En el primer cas $M = 0$ i en el segon M és invertible.

En particular, $V \neq 0$ si i només si A i B són conjugats a $\mathrm{GL}_n(k)$. En aquest darrer cas, E_A i E_B són isomorfs com a $k[t]$-mòduls; aleshores

$$V = \mathrm{Hom}_{k[t]}(E_A, E_B) \simeq \mathrm{Hom}_{k[t]}(E_A, E_A).$$

Així, per demostrar que $\dim_k V = n$ podem suposar $A = B$. En aquest cas l'afirmació és ben coneguda. De fet, per a una matriu diagonal $D \in \mathrm{GL}_n(k)$ tal que totes les seves entrades a la diagonal són diferents, les matrius que commuten amb D són exactament totes les matrius diagonals; així, per a tota $A \in \mathrm{GL}_n(k)$ amb n valors propis diferents a k tenim $\dim_k V = n$. Per tant, el mateix és cert per a A que tingui polinomi característic irreductible, ja que estenent escalars per alguna extensió de cossos L de k, l'espai vectorial V esdevé un L-espai vectorial de dimensió n i la dimensió dels espais vectorials es preserva per extensió d'escalars. ■

Corol.lari 1.4. *Sigui $k = \mathbb{F}_q$ un cos finit. Suposem que $A \in \mathrm{GL}_n(k)$ té polinomi característic irreductible i sigui $\lambda \in k^*$ tal que A i λA són conjugats. Aleshores, $|V^*_{A,\lambda}| = q^n - 1$.*

Dem. $\dim_k V_{A,\lambda} = n$ i $V^*_{A,\lambda} = V_{A,\lambda} - \{0\}$, pel lema 1.3 aplicat a $B = \lambda A$. ■

Lema 1.5. *Sigui $k = \mathbb{F}_q$ un cos finit. Per a tot $\gamma \in \mathcal{C}$ d'ordre m tenim:*

$$|\Gamma_\gamma| = \begin{cases} 3(q^2+q+1), & si\ \gamma \in \mathcal{C}_I,\ m = 3, \\ q^2+q+1, & si\ \gamma \in \mathcal{C}_I,\ m > 3, \\ q^2-1, & si\ \gamma \in \mathcal{C}_{II}, \\ 3(q-1)^2, & si\ \gamma \in \mathcal{C}_{III},\ m = 3, \\ (q-1)^2, & si\ \gamma \in \mathcal{C}_{III},\ m > 3, \\ q(q-1)^2(q+1), & si\ \gamma \in \mathcal{C}'_{IV}, \\ q(q-1), & si\ \gamma \in \mathcal{C}''_{IV}, \\ q^3(q-1), & si\ \gamma = \gamma_V, \\ q^2, & si\ \gamma = \gamma'_V, \\ q^3(q-1)^2(q^2+q+1)(q+1), & si\ \gamma = 1. \end{cases}$$

Dem. Suposem primer que $\gamma \in \mathrm{PGL}_3(k)$ és del tipus I, II o III, i sigui A un representant de γ a $\mathrm{GL}_3(k)$. El $k[t]$-mòdul E_A definit com a la demostració del lema 1.3 és semisimple. La descomposició com a suma directa de mòduls simples és la següent:

$$E_A = \begin{cases} E_1, & \dim E_1 = 3, & \text{si } A \text{ és del tipus } I, \\ E_1 \oplus E_2, & \dim E_i = i,\ i = 1,2, & \text{si } A \text{ és del tipus } II, \\ E_1 \oplus E_2 \oplus E_3, & \dim E_i = 1,\ i = 1,2,3, & \text{si } A \text{ és del tipus } III. \end{cases}$$

Com que a cada descomposició entre els factors simples no n'hi ha dos d'isomorfs, tenim,

$$V^*_A = \mathrm{Aut}_{k[t]}(E_A) \simeq \oplus_i \mathrm{Aut}_{k[t]}(E_i).$$

Pel corol lari 1.4,

$$|V^*_A| = \begin{cases} q^3-1, & \text{si } A \text{ és del tipus } I, \\ (q-1)(q^2-1), & \text{si } A \text{ és del tipus } II, \\ (q-1)^3, & \text{si } A \text{ és del tipus } III. \end{cases}$$

Per a tot $\lambda \in A$, el mòdul $E_{\lambda A}$ admet una descomposició com a suma directa de mòduls simples, $E_{\lambda A} = \oplus_i E_i'$, del mateix tipus que A. Si a més A i λA són conjugats, els mòduls simples a la descomposició de E_A i $E_{\lambda A}$ són isomorfs: $E_i \simeq E_i'$ per a tot i, en cada cas. Així, $|V^*_{A,\lambda}| = |V^*_A|$, ja que

$$V^*_{A,\lambda} = \mathrm{Isom}(E_A, E_{\lambda A}) \simeq \oplus_i \mathrm{Isom}(E_i, E_i') \simeq \oplus_i \mathrm{Aut}(E_i).$$

Pel lema 1.2, A és conjugada a λA per a algun $\lambda \in k^*$, $\lambda \neq 1$, només si k conté una arrel cúbica de la unitat $\omega \neq 1$ i A té un polinomi característic de la forma: $f_A(t) = t^3 + a$, $a \in k^*$. Això és equivalent a $m = 3$. Aplicant (4), veiem que l'afirmació del lema és correcta per a γ del tipus I, II o III.

Sigui $\gamma \in \Gamma$ ara del tipus IV o V i sigui A qualsevol representant a $\mathrm{GL}_3(k)$. Pel lema 1.2 A és conjugada a λA, només per a $\lambda = 1$. Aleshores, per (4), $|\Gamma_\gamma| = |k^* \backslash\backslash V^*_A|$. Un senzill càlcul de V^*_A en cada cas permet acabar la demostració. ■

Remarca. Sigui μ_3 el subgrup de $\overline{k}^*$ format per les arrels cúbiques de la unitat. Si $q \not\equiv 1 \pmod 3$, tenim $\mu_3 \cap k = \{1\}$, i $k^* = (k^*)^3$; per tant, tots els elements de $\mathcal{C}$ d'ordre $m = 3$ són del tipus II (si $p \neq 3$) o V (si $p = 3$). Si $q \equiv 1 \pmod 3$, tenim $\mu_3 \subseteq k$ i $(k^* : (k^*)^3) = 3$; per tant, en aquest cas hi ha tres elements de $\mathcal{C}$ d'ordre 3, dos a $\mathcal{C}_I$ i un a $\mathcal{C}_{III}$, donats respectivament per:

$$\gamma = \begin{pmatrix} 0 & 0 & a \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & a^2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad \text{i} \quad \gamma = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix},$$

on $a \in k^* \setminus (k^*)^3$ i $\omega \in \mu_3 \setminus \{1\}$.

2 Acció de subgrups cíclics de PGL_3 sobre $\mathbb{P}^2$

Sigui $k = \mathbb{F}_q$ un cos finit amb q elements. Considerem l'acció natural del grup $\Gamma = \mathrm{PGL}_3(\mathbb{F}_q)$ sobre el pla projectiu $X := \mathbb{P}^2(\mathbb{F}_q)$.

L'objectiu d'aquesta secció és descompondre el nostre conjunt $\mathcal{C}$ de representants de classes de conjugació de Γ en una unió disjunta de famílies agrupant aquells γ amb el mateix tipus de cicle i comptar el nombre d'elements de cada família.

Sigui γ un element de Γ i sigui A un representant qualsevol de γ a $\mathrm{GL}_3(\mathbb{F}_q)$. Denotarem a tot arreu per $m = m(\gamma)$ l'ordre de γ com a element de Γ. El conjunt X_γ dels punts fixos de γ a $\mathbb{P}^2(\mathbb{F}_q)$ coincideix amb la imatge a $\mathbb{P}^2(\mathbb{F}_q)$ dels vectors propis de A a k^3. Més generalment, les rectes de $\mathbb{P}^2(\mathbb{F}_q)$ que són invariants per γ són imatge de subespais vectorials de k^3 de dimensió dos invariants per A. En particular, l'estructura d'aquest conjunt depèn només del tipus I, II, III, IV o V.

Més exactament, si denotem per $P_1 = (1,0,0), P_2 = (0,1,0), P_3 = (0,0,1)$, els tres punts fonamentals de $\mathbb{P}^2(\mathbb{F}_q)$ i per L_1, L_2, L_3 les tres rectes determinades, cada L_i pel parell de punts amb subíndex diferent de i, tenim (cf. [Hir79, 7.4]):

Punts fixos i rectes invariants de $\gamma \in \mathcal{C}$

tipus de γ	X_γ	rectes invariants de γ
I	$\emptyset$	cap
II	$\{P_1\}$	L_1
III	$\{P_1, P_2, P_3\}$	L_1, L_2, L_3
IV'	$L_1 \cup \{P_1\}$	L_1 i tota recta que passa per P_1
IV''	$\{P_1, P_3\}$	L_1, L_2
$\gamma = \gamma_V$	L_2	tota recta que passa per P_3
$\gamma = \gamma_V'$	$\{P_3\}$	L_1
$\gamma = 1$	X	totes les rectes

Taula 1

Per determinar el tipus de cicle de γ necessitem estudiar la variació de l'estructura dels conjunts X_{γ^r} de punts fixos de les projectivitats del subgrup cíclic generat per γ. A tal fi, la següent definició ens serà d'utilitat:

Definició 2.1. *Sigui L una recta invariant de γ. L'exponent de L, denotat* $\exp(L)$*, és el mínim divisor positiu d de $m(\gamma)$ tal que L és una recta de punts fixos de γ^d. Equivalentment, d és l'ordre de la projectivitat de L obtinguda per restricció de γ.*

Ara classifiquem els elements de $\mathcal{C}$ segons la configuració dels punts fixos i les rectes invariants, i els valors dels exponents d'aquestes rectes. Al final d'aquesta secció veurem que aquests invariants són suficients per determinar el tipus de cicle de γ.

Tipus I

Lema 2.2. *Sigui $\gamma \in \Gamma$ un element del tipus I i ordre m. Aleshores, tots els altres elements no trivials del subgrup cíclic generat per γ són del tipus I. Més exactament, $X_{\gamma^r} = \emptyset$, per a tot $1 \leq r < m$.*

Dem. Sigui $F(x) = x^q$ l'automorfisme de Frobenius de k. Denotem per $\alpha, \alpha_1 = F(\alpha), \alpha_2 = F^2(\alpha)$ els valors propis de A a l'extensió cúbica de k. Els valors propis de A^r són $\alpha^r, \alpha_1^r, \alpha_2^r$. Si $\alpha^r = a \in k$, aleshores:

$$a = F^i(a) = F^i(\alpha^r) = \alpha_i^r, \qquad \text{per a } i = 1, 2,$$

de manera que $A^r = aI_3$ i $\gamma^r = 1$. ■

Denotem per $\mathcal{C}_I(m)$ el subconjunt de $\mathcal{C}_I$ d'aquells elements d'ordre m, i sigui $c_I(m) := |\mathcal{C}_I(m)|$.

Lema 2.3. *Sigui $\gamma \in \Gamma$ un element del tipus I. Aleshores, l'ordre m de γ és un divisor de q^2+q+1 i $m \geq 3$. A més a més, per a tot divisor m de q^2+q+1, $m \geq 3$, tenim:*

$$c_I(m) = \begin{cases} \varphi(m), & si\ \ m = 3, \\ \varphi(m)/3, & si\ \ m > 3, \end{cases}$$

on φ és la funció "fi" d'Euler.

Dem. Sigui L l'extensió cúbica de k. Sobre $L^* - k^*$ tenim una acció doble pels dos grups k^* i $G := \mathrm{Gal}(L/k) = \{1, F, F^2\}$. La correspondència que assigna a cada $\alpha \in L^* - k^*$ el seu polinomi mònic irreductible indueix una aplicació bijectiva:

$$G\backslash\backslash(L^* - k^*) \longrightarrow \mathcal{P}_I,$$

la qual és compatible amb l'acció de k^* sobre ambdós conjunts. Així, obtenim una aplicació bijectiva:

$$k^*\backslash\backslash(G\backslash\backslash(L^* - k^*)) \longrightarrow k^*\backslash\backslash\mathcal{P}_I,$$

i aquest darrer conjunt és en bijecció amb $\mathcal{C}_I$ pel lema 1.1.

Com que Frobenius commuta amb la multiplicació per escalars a k, tenim una bijecció natural:

$$k^*\backslash\backslash(G\backslash\backslash(L^* - k^*)) \iff G\backslash\backslash(k^*\backslash\backslash(L^* - k^*)),$$

i aquest darrer conjunt es pot identificar amb $G\backslash\backslash((L^*/k^*) - \{1\})$. Aleshores, tenim una aplicació bijectiva:

$$G\backslash\backslash((L^*/k^*) - \{1\}) \longrightarrow \mathcal{C}_I. \tag{6}$$

Suposem que sota aquesta correspondència bijectiva un element $\gamma \in \mathcal{C}_I$ es correspon amb $\alpha \in L^*$; aleshores, l'ordre m de γ com a element de Γ és el mínim enter

positiu tal que $\alpha^m \in k^*$; és a dir, m coincideix amb l'ordre de α com a element de L^*/k^*. Com que això es un grup cíclic amb q^2+q+1 elements, necessàriament m és un divisor de q^2+q+1 i hi ha exactament $\varphi(m)$ elements d'ordre m en aquest grup.

Clarament, q^2+q+1 és sempre senar, de manera que m no pot ser mai igual a 2. Els elements de 3-torsió de L^*/k^* són exactament els elements fixos per l'acció de G:

$$\gamma^3 = 1 \Longleftrightarrow \alpha^3 \in k^* \Longleftrightarrow \exists \lambda \in k^* \text{ such that } F(\alpha) = \lambda\alpha.$$

Així, els dos elements d'ordre 3 de L^*/k^* estan en correspondència amb dos elements diferents a $\mathcal{C}_I$ sota la bijecció (6). D'altra banda, tots els elements a L^*/k^* d'ordre $m > 3$ tenen una òrbita de cardinal tres sota l'acció de G, de manera que proporcionen $\varphi(m)/3$ òrbites. Per la bijecció (6), aquest és el nombre d'elements a $\mathcal{C}_I$ d'ordre m. ■

Aquesta distinció entre els casos $m = 3$, $m > 3$ desapareix quan dividim $c_I(m)$ per $|\Gamma_\gamma|$ (que hem calculat al lema 1.5).

Corol.lari 2.4. *Per a tot divisor $m > 1$ de q^2+q+1,*

$$N_I(m) := \sum_{\gamma \in \mathcal{C}_I(m)} \frac{1}{|\Gamma_\gamma|} = \frac{c_I(m)}{|\Gamma_\gamma|} = \frac{\varphi(m)}{3(q^2+q+1)}.$$

Tipus II

Sigui K l'extensió quadràtica de k. Considerem $\gamma \in \mathcal{C}_{II}$ amb representant $A = \mathrm{diag}(1, B)$ a $\mathrm{GL}_3(\mathbb{F}_q)$, amb $B \in \mathrm{GL}_2(\mathbb{F}_q)$ tenint un parell $\alpha, \alpha' \in K$ de valors propis quadràtics conjugats. Denotem per $d = d(\gamma)$ l'exponent de l'única recta invariant de γ. Clarament,

$$d(\gamma) = \text{mínim enter positiu tal que } \alpha^d \in k^*.$$

Com que $\alpha^d = b \in k^*$ és fixat per Frobenius, tenim: $\alpha'^d = \alpha^d = b$, de manera que $B^d = bI_2$. Així, d és el mínim enter positiu tal que γ^d és, o bé 1, o bé del tipus IV'.

Les potències γ^r són representades per $\mathrm{diag}(1, B^r)$ a $\mathrm{GL}_3(\mathbb{F}_q)$; per tant, l'ordre m de γ és d vegades l'ordre de b a k^*.

Lema 2.5. *Per a γ del tipus II, siguin $P \in X$, $L \subseteq X$ respectivament el punt fix i la recta invariant de γ i sigui $d = d(\gamma)$ l'exponent de L. Aleshores, per a $1 \leq r < m$, tenim:*

$$X_{\gamma^r} = \begin{cases} \{P\}, & si\ d \nmid r, \quad (i\ \gamma^r\ és\ del\ tipus\ II), \\ L \cup \{P\}, & si\ d|r, \quad (i\ \gamma^r\ és\ del\ tipus\ IV'). \end{cases}$$

En particular, si $d = m$ tenim $X_{\gamma^r} = \{P\}$, per a tot $1 \leq r < m$. ■

Denotem com abans $G = \mathrm{Gal}(K/k)$. Procedint com al cas I, la correspondència que assigna a cada $\alpha \in K^* - k^*$ el polinomi $(x - 1)$ vegades el polinomi mònic irreductible de α, determina una aplicació bijectiva:

$$G\backslash\backslash(K^* - k^*) \longrightarrow k^*\backslash\backslash\mathcal{P}_{II},$$

i aquest darrer conjunt és en bijecció amb $\mathcal{C}_{II}$ pel lema 1.1.

Si $\alpha \in K^* - k^*$ correspon a $\gamma \in \mathcal{C}_{II}$, tenim:

$$d(\gamma) = \text{ ordre de la classe de } \alpha \text{ a } K^*/k^*,$$
$$\frac{m(\gamma)}{d(\gamma)} = \text{ ordre de } \alpha^{d(\gamma)} \text{ a } k^*.$$

En particular, $d(\gamma)|(q+1)$ i $m(\gamma) = d(\gamma)e$, $e|(q-1)$. Per a un parell donat d'enters positius, $d|(q+1)$, $d > 1$ i $m = de$, $e|(q-1)$, denotem:

$$\mathcal{C}_{II}(m,d) := \{\gamma \in \mathcal{C}_{II} \mid m(\gamma) = m, d(\gamma) = d\}, \quad c_{II}(m,d) := |\mathcal{C}_{II}(m,d)|.$$

Lema 2.6. *Per a tot parell d'enters positius, $e|(q-1)$, $d|(q+1)$, $d > 1$,*

$$c_{II}(de,d) = \begin{cases} \frac{1}{2}\varphi(d)\varphi(e), & si\ d\ senar, \\ 0, & si\ d\ parell\ i\ e|\frac{q-1}{2}, \\ \varphi(d)\varphi(e), & si\ d\ parell\ i\ e \nmid \frac{q-1}{2}. \end{cases}$$

Dem. Com que totes les òrbites de G que actuen sobre $K^* - k^*$ tenen dos elements, tenim:

$$c_{II}(de,d) = \frac{1}{2}|B(de,d)|,$$

per a tot d, e, on,

$$B(m,d) := \{\alpha \in K^* - k^* \mid m, d \text{ mínims satisfent } \alpha^d \in k^*, \alpha^m = 1\}.$$

Existeixen $\varphi(d)$ elements a K^*/k^* d'ordre d; per tant, existeixen $\varphi(d)(q-1)$ elements al conjunt:

$$T := \{\alpha \in K^* - k^* \mid d \text{ és el mínim enter positiu tal que } \alpha^d \in k^*\}.$$

Denotem $T_\lambda := \{\alpha \in T \mid \alpha^d = \lambda\}$, per a tot $\lambda \in k^*$. Els conjunts T i $B(de,d)$ descomponen en la unió disjunta:

$$T = \cup_{\lambda \in k^*} T_\lambda, \quad B(de,d) = \cup_{ord_{k^*}(\lambda)=e} T_\lambda. \tag{7}$$

La correspondència, $\alpha \mapsto \mu\alpha$ posa T_λ en bijecció amb $T_{\lambda\mu^d}$. Si d és senar, aleshores $(d, q-1) = 1$, ja que aquest nombre és un divisor senar de $(q+1, q-1)$. Per tant, $(k^*)^d = k^*$ i tots els conjunts T_λ tenen el mateix nombre d'elements. Per la primera descomposició de (7), tenim $|T_\lambda| = \frac{|T|}{q-1} = \varphi(d)$, per a tot $\lambda \in k^*$. Ara, aplicant la segona descomposició de (7) obtenim $|B(de,d)| = \varphi(e)\varphi(d)$.

Suposem ara que d és parell. En particular, q és senar i $(d, q-1) = 2$. Aleshores, $(k^*)^d = (k^*)^2$ i el valor de $|T_\lambda|$ és constant per a λ pertanyent respectivament al conjunt dels quadrats o no-quadrats de k^*. Ara, el conjunt T_1 és buit; de fet, si $d = 2d'$ i $\alpha^d = 1$, aleshores $\alpha^{d'} = \pm 1$, de manera que d no pot ser el mínim enter positiu tal que α^d pertany a k^*. Així, $|T_\lambda| = 0$ per a tot $\lambda \in (k^*)^2$ i $|T_\lambda| = \frac{|T|}{(q-1)/2} = 2\varphi(d)$, per a λ no-quadrat. Per la segona descomposició de (7), tenim $B(de,d) = \emptyset$ si e divideix $(q-1)/2$ i $|B(de,d)| = 2\varphi(d)\varphi(e)$ si e no divideix $(q-1)/2$. ■

Considerem nombres $N_{II}(m,d)$ anàlegs als anteriors:

Corol.lari 2.7. *Per a tot parell d'enters positius, $d|(q+1)$, $d > 1$ i $m = de$, amb $e|(q-1)$, tenim*

$$N_{II}(m,d) := \sum_{\gamma \in \mathcal{C}_{II}(m,d)} \frac{1}{|\Gamma_\gamma|} = \frac{c_{II}(d,e)}{|\Gamma_\gamma|} = \begin{cases} \dfrac{\varphi(d)\varphi(e)}{2(q^2-1)}, & \textit{si } d \textit{ senar,} \\ 0, & \textit{si } d \textit{ parell i } e|\frac{q-1}{2}, \\ \dfrac{\varphi(d)\varphi(e)}{q^2-1}, & \textit{si } d \textit{ parell i } e \nmid \frac{q-1}{2} \end{cases}$$

Tipus III

Sigui $\gamma \in \mathcal{C}_{III}$ amb representant a $\mathrm{GL}_3(\mathbb{F}_q)$ de la forma:

$$A = \mathrm{diag}(1,b,c), \quad b,c \in k - \{0,1\},\ b \neq c.$$

Com que $\gamma^{q-1} = 1$, l'ordre m de γ és un divisor de $q-1$. Els tres divisors d, e, f de $q-1$, tots més grans que 1, definits per:

$$d = \mathrm{ord}_{k^*}(b), \quad e = \mathrm{ord}_{k^*}(c), \quad f = \mathrm{ord}_{k^*}(\frac{b}{c}),$$

són els exponents respectius de les tres rectes invariants de γ. De fet, tota potència de γ amb exponent múltiple de d, e o f és o bé 1 o bé del tipus IV'. Clarament,

$$m = \mathrm{mcm}(d, e) = \mathrm{mcm}(d, f) = \mathrm{mcm}(e, f). \tag{8}$$

Lema 2.8. *Per a γ del tipus III i $1 \leq r < m$ tenim,*

$$X_{\gamma^r} = \begin{cases} \{P_1, P_2, P_3\}, & \textit{si ni } d \textit{ ni } e \textit{ ni } f \textit{ divideixen } r, \\ L_1 \cup \{P_1\}, & \textit{si } f \textit{ divideix } r, \\ L_2 \cup \{P_2\}, & \textit{si } e \textit{ divideix } r, \\ L_3 \cup \{P_3\}, & \textit{si } d \textit{ divideix } r. \end{cases}$$

Així, γ^r és del tipus III en el primer cas i del tipus V' en els altres casos.

Dem. Per (8), r no és múltiple comú de qualsevol parell d'enters de la tripleta d, e, f. ■

Com a les subseccions anteriors, volem comptar el nombre d'elements a $\mathcal{C}_{III}$ que tenen valors fixats d'aquests divisors (d, e, f). Tanmateix, aquesta terna depèn ara del representant escollit A de γ. Existeixen, en principi, sis representants del tipus $\mathrm{diag}(1, b', c')$ de les classes de γ a $\mathcal{C}_{III}$ (cf. (3)):

$$\begin{array}{lll} \mathrm{diag}(1, b, c), & \mathrm{diag}(1, cb^{-1}, b^{-1}), & \mathrm{diag}(1, c^{-1}, bc^{-1}), \\ \mathrm{diag}(1, c, b), & \mathrm{diag}(1, b^{-1}, cb^{-1}), & \mathrm{diag}(1, bc^{-1}, c^{-1}), \end{array} \tag{9}$$

i les ternes (d, e, f) associades a aquestes matrius són respectivament:

$$\begin{array}{lll} (d, e, f), & (f, d, e) & (e, f, d), \\ (e, d, f), & (d, f, e), & (f, e, d). \end{array}$$

Per tant, obtenim un invariant de γ si considerem la terna d, e, f ordenada per tamany, diguem: $d \geq e \geq f$.

Comptarem primer el nombre de matrius a $\mathrm{GL}_3(\mathbb{F}_q)$ que tenen ternes fixades. Per a un divisor fixat m of $q - 1$ i tres divisors (d, e, f) de m que satisfacin (8) denotem:

$$B(d, e, f) := \{(x, y) \in k^* \times k^* \mid d = \mathrm{ord}_{k^*}(x),\ e = \mathrm{ord}_{k^*}(y),\ f = \mathrm{ord}_{k^*}(xy^{-1})\},$$

i $b(d,e,f) := |B(d,e,f)|$. Observem que el valor de $b(d,e,f)$ és independent de l'ordenació de d,e,f.

Per a $\gamma = \mathrm{diag}(1,\omega,\omega^2)$, on ω és una arrel cúbica primitiva de 1, les sis matrius de (9) prenen només dos valors diferents: $\mathrm{diag}(1,\omega,\omega^2)$ i $\mathrm{diag}(1,\omega^2,\omega)$. En qualsevol altre cas, aquestes sis matrius són totes diferents. Aleshores, per a tota terna ordenada donada $d \geq e \geq f > 1$ de divisors de m que satisfacin (8), si denotem

$$\mathcal{C}_{III}(d,e,f) = \{\gamma \in \mathcal{C}_{III} \mid d(\gamma) = d,\ e(\gamma) = e,\ f(\gamma) = f\},$$

tenim:

$$c_{III}(d,e,f) := |\mathcal{C}_{III}(d,e,f)| = \begin{cases} 1 = \frac{1}{2}b(3,3,3), & \text{si } d = e = f = 3, \\ \frac{1}{6}b(m,m,m), & \text{si } d = e = f = m > 3, \\ \frac{1}{2}b(m,m,f), & \text{si } d = e = m > f > 1, \\ b(d,e,f), & \text{si } d > e > f > 1. \end{cases}$$

Per tant, és suficient trobar una fórmula per a $b(d,e,f)$.

Tots els elements $x, y, xy^{-1} \in k^*$ amb ordre fixat d,e,f pertanyen al subgrup cíclic μ_m de k^* format per les arrels m-èsimes de la unitat. Així, podem treballar al grup cíclic $\mathbb{Z}_m$ i pensar que:

$$b(d,e,f) = |\{(x,y) \in \mathbb{Z}_m \times \mathbb{Z}_m \mid d = \mathrm{ord}(x),\ e = \mathrm{ord}(y),\ f = \mathrm{ord}(x-y)\}|.$$

Pel teorema xinès dels residus, els nombres $b(d,e,f)$ determinen una funció multiplicativa de tres variables. Per a m una potència d'un nombre primer ℓ, la propietat (8) implica que almenys dos dels divisors d,e,f són iguals a m. Per tant, necessitem només calcular:

Lema 2.9. *Sigui $m = \ell^r$ una potència d'un nombre primer ℓ. Aleshores, per a tot divisor $f = \ell^j$, $0 \leq j \leq r$, tenim:*

$$b(m,m,f) = \begin{cases} \varphi(m)(\ell-2)\ell^{r-1}, & \text{si } f = m, \\ \varphi(m)\varphi(f), & \text{si } f < m. \end{cases}$$

Dem. Per a tot $y \in (\mathbb{Z}_m)^*$, denotem per $B_y = \{x \in (\mathbb{Z}_m)^* \mid \mathrm{ord}(x-y) = f\}$. Tots aquests conjunts B_y són en bijecció amb B_1 via l'aplicació, $x \to xy^{-1}$. Per tant, $b(m,m,f) = \varphi(m)|B_1|$.

Per a $m = \ell^r$ podem escriure els elements $x \in \mathbb{Z}_m$ de manera única com:

$$x = a_0 + a_1\ell + \cdots + a_{r-1}\ell^{r-1}, \quad 0 \leq a_i < \ell.$$

Suposem $f = m$; els elements x, $x-1$ són ambdós invertibles si i només si $a_0 \neq 0, 1$, per tant tenim $(\ell-2)\ell^{r-1}$ possibilitats per a x. D'altra banda, si $f < m$, l'element $x-1$ té ordre f si i només si:

$$x = 1 + a_{r-j}\ell^{r-j} + \cdots + a_{r-1}\ell^{r-1}, \quad a_{r-j} \neq 0,$$

i tenim $(\ell-1)\ell^{j-1}$ possibilitats. ■

D'ara endavant denotarem per v_ℓ la valoració ℓ-àdica associada a un nombre primer ℓ. Per trobar una expressió global per a $b(d,e,f)$ introduïm la següent terminologia.

Definició 2.10. *Diem que un enter positiu h és un divisor "ple" d'un enter m si h divideix m i $(h, m/h) = 1$; o, equivalentment, si $v_\ell(h) = v_\ell(m)$ per a tot factor primer ℓ de h.*

Diem que h és un divisor "buit" de m si h divideix m i $rad(h) = rad(m/h)$, o, equivalentment, si $v_\ell(h) < v_\ell(m)$ per a tot divisor primer ℓ de h.

Qualsevol divisor positiu d de m es pot escriure de manera única com a un producte: $d = Hh$, amb H un divisor ple de m i h un divisor buit de m.

Proposició 2.11. *Sigui m un enter positiu i siguin d, e, f divisors de m satisfent (8). Sigui*

$$\frac{def}{m^2} = Hh,$$

la descomposició de def/m^2 en un producte d'un divisor ple, H, i un divisor buit, h, de m. Aleshores,

$$b(d,e,f) = \varphi(m)\varphi(h)\psi(H),$$

on ψ és la funció multiplicativa determinada per $\psi(\ell^r) = (\ell-2)\ell^{r-1}$, per a tota potència d'un nombre primer.

Dem. Ambdues expressions són funcions multiplicatives i coincideixen per a m una potència d'un nombre primer pel lema 2.9. ■

Considerem, com abans, nombres $N_{III}(d,e,f) := \sum_{\gamma \in \mathcal{C}_{III}(d,e,f)} \frac{1}{|\Gamma_\gamma|}$, útils per compactificar la nostra fórmula final.

Corol.lari 2.12. *Amb les notacions anteriors, per a $d \geq e \geq f > 1$ enters que satisfacin (8) tenim,*

$$N_{III}(d,e,f) = \frac{c_{III}(d,e,f)}{|\Gamma_\gamma|} = \begin{cases} \dfrac{\varphi(m)\psi(m)}{6(q-1)^2}, & si\ d = e = f = m, \\ \dfrac{\varphi(m)\varphi(h)\psi(H)}{2(q-1)^2}, & si\ d = e = m > f, \\ \dfrac{\varphi(m)\varphi(h)\psi(H)}{(q-1)^2}, & si\ d > e > f. \end{cases}$$

Tipus IV i V

Per a $\gamma = \mathrm{diag}(a,1,1)$, $a \neq 0,1$, tenim $m = \mathrm{ord}_{k^*}(a)$. Per a tot $1 \leq r < m$, la potència γ^r és sempre del tipus IV'; així, el conjunt X_{γ^r} dels punts fixos de γ^r és:

$$X_{\gamma^r} = X_\gamma = L_1 \cup \{P_1\}.$$

En particular, totes les rectes invariants que passen per P_1 tenen exponent m.

Per a cada divisor d de $q-1$, $d > 1$, denotem per $\mathcal{C}'_{IV}(d)$ el subconjunt de $\mathcal{C}'_{IV}$ format pels γ que tenen ordre d. Clarament $|\mathcal{C}'_{IV}(d)| = \varphi(d)$.

Per a $\gamma = \mathrm{diag}(a, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix})$, $a \neq 0,1$, tenim $m = pd$, on $d = \mathrm{ord}_{k^*}(a)$. En aquest cas p i d són els exponents de les dues rectes invariants de γ. De fet, per a tot $1 \leq r < m$:

$$X_{\gamma^r} = \begin{cases} \{P_1, P_3\} & \text{si ni } p \text{ ni } d \text{ divideixen } r, \\ L_1 \cup \{P_1\} & \text{si } p \text{ divideix } r, \\ L_2 & \text{si } d \text{ divideix } r, \end{cases}$$

de manera que γ^r queda del tipus IV'' en el primer cas, canvia als tipus IV' en el segon cas i és conjugat a γ_V en el tercer cas.

Per a cada divisor d de $q-1$, $d > 1$, denotem per $\mathcal{C}''_{IV}(d)$ el subconjunt de $\mathcal{C}''_{IV}$ d'aquells γ que tenen ordre pd. Clarament $|\mathcal{C}''_{IV}(d)| = \varphi(d)$.

Corol.lari 2.13. *Sigui $d > 1$ un divisor positiu de $q-1$. Aleshores,*

$$N'_{IV}(d) := \sum_{\gamma \in \mathcal{C}'_{IV}(d)} \frac{1}{|\Gamma_\gamma|} = \frac{\varphi(d)}{q(q-1)^2(q+1)},$$

$$N''_{IV}(d) := \sum_{\gamma \in \mathcal{C}''_{IV}(d)} \frac{1}{|\Gamma_\gamma|} = \frac{\varphi(d)}{q(q-1)}.$$

La matriu γ_V té ordre $m = p$ i totes les potències no-trivials de γ_V són conjugades a γ_V; així, per a tot $1 \leq r < m$ tenim, $\mathcal{X}_{\gamma_V^r} = X_{\gamma_V} = L_2$. En particular, totes les rectes invariants, excepte L_2, tenen exponent m.

Finalment, la matriu γ'_V té ordre p si p és senar i ordre 4 si $p = 2$. Per a tot $1 \leq r < p$ tenim en aquest cas:

$$X_{(\gamma'_V)^r} = \begin{cases} \{P_3\} & \text{si } p > 2 \text{ or } r \text{ is odd,} \\ L_1 & \text{si } p = 2 \text{ i } r = 2, \end{cases}$$

de manera que $(\gamma'_V)^r$ és respectivament conjugat a γ'_V, γ_V.

Per donar una formulació global a les nostres fórmules, definim:

$$N_V := \frac{1}{|\Gamma_{\gamma_V}|} = \frac{1}{q^3(q-1)}, \qquad N'_V := \frac{1}{|\Gamma_{\gamma'_V}|} = \frac{1}{q^2},$$
$$N_1 = \frac{1}{|\Gamma|} = \frac{1}{q^3(q-1)^2(q^2+q+1)(q+1)}.$$

Tipus de cicle

El tipus de cicle de $\gamma \in \Gamma$ actuant com a permutació de $\mathbb{P}^2(\mathbb{F}_q)$ queda determinat pels cardinals de les òrbites:

$$O_\gamma(P) = \{P, \gamma(P), \ldots, \gamma^{m-1}(P)\},$$

de tots els punts $P \in \mathbb{P}^2(\mathbb{F}_q)$ pel subgrup cíclic generat per γ. El resultat següent és probablement ben conegut, però per la manca d'una referència precisa en donem una curta demostració.

Lema 2.14. *Sigui $P \in \mathbb{P}^2(\mathbb{F}_q)$ i sigui $\gamma \in \Gamma$ un element d'ordre $m > 1$. Aleshores,*

$$|O_\gamma(P)| = \begin{cases} 1 & \textit{si } \gamma(P) = P, \\ d & \textit{si } \gamma(P) \neq P \textit{ i } P \textit{ pertany a una recta } \gamma\textit{-invariant d'exponent } d, \\ m & \textit{si } P \textit{ no pertany a cap subvarietat lineal } \gamma\textit{-invariant pròpia.} \end{cases}$$

Dem. El cardinal $r = |O_\gamma(P)|$ és el mínim enter positiu tal, que P és un punt fix de γ^r. Ara, la subvarietat lineal generada per $O_\gamma(P)$,

$$V = \langle\, P, \gamma(P), \ldots \gamma^{r-1}(P) \,\rangle \subseteq \mathbb{P}^2(\mathbb{F}_q)$$

és γ-invariant i és fixada (punt a punt) per γ^r. Tenim, doncs, $\gamma^r_{|V} = \mathrm{id}_V$, i r coincideix amb l'ordre de $\gamma_{|V}$. ■

En particular, el tipus de cicle de γ queda determinat per la configuració dels punts fixos i les rectes invariants, i pels exponents d'aquestes rectes. Així, la partició de $\mathcal{C}$ en subfamílies que descriuen les diferents possibilitats per a aquestes configuracions i exponents coincideix amb la classificació dels elements de $\mathcal{C}$ segons el seu tipus de cicle. Dos elements de $\mathrm{PGL}_3(k)$ amb la mateixa configuració de subvarietats invariants i exponents direm que tenen el mateix *subtipus*. Recordem que aquesta partició de $\mathcal{C}$ en famílies segons el seu subtipus és:

$$\mathcal{C} = \left(\bigcup_{m\in Z_I} \mathcal{C}_I(m)\right) \cup \left(\bigcup_{(m,d)\in Z_{II}} \mathcal{C}_{II}(m,d)\right) \cup \left(\bigcup_{(d,e,f)\in Z_{III}} \mathcal{C}_{III}(d,e,f)\right) \cup \\ \cup \left(\bigcup_{d\in Z_{IV}} (\mathcal{C}'_{IV}(d) \cup \mathcal{C}''_{IV}(d))\right) \cup \mathcal{C}_V,$$

on

$$Z_I := \{m \in \mathbb{Z} \mid m|q^2+q+1,\ m \geq 3\},$$

$$Z_{II} := \{(m,d) \in \mathbb{Z}^2 \mid d|(q+1,m),\ d>1, \tfrac{m}{d}|(q-1)\},$$

$$Z_{III} := \{(d,e,f) \in \mathbb{Z}^3 \mid d \geq e \geq f > 1, \\ \mathrm{mcm}(d,e) = \mathrm{mcm}(d,f) = \mathrm{mcm}(e,f)|(q-1)\},$$

$$Z_{IV} := \{d \in \mathbb{Z} \mid d|(q-1),\ d>1\}.$$

3 Òrbites de n-conjunts de $\mathbb{P}^2$ per l'acció de PGL_3

Sigui p un nombre primer, q una potència de p i $k = \mathbb{F}_q$ un cos finit amb q elements. Una altra vegada, denotem el grup $\mathrm{PGL}_3(\mathbb{F}_q)$ simplement per Γ. Sigui

$$\mathcal{X} := \binom{\mathbb{P}^2(\mathbb{F}_q)}{n}$$

el conjunt dels n-subconjunts de $\mathbb{P}^2(\mathbb{F}_q)$. Els elements de $\mathcal{X}$ són famílies no-ordenades $\{P_1,\ldots,P_n\}$ de n punts diferents de $\mathbb{P}^2(\mathbb{F}_q)$.

El nostre objectiu és comptar el nombre d'òrbites del conjunt finit $\mathcal{X}$ per l'acció de Γ. Després dels càlculs de la secció 1, per aplicar la fórmula (2) només necessitem

comptar $|\mathcal{X}_\gamma|$ per a cada $\gamma \in \mathcal{C}$. Com que qualsevol element de $\mathcal{X}_\gamma$ és una unió disjunta d'òrbites pel subgrup cíclic generat per γ, queda clar que $|\mathcal{X}_\gamma|$ depèn només del subtipus de γ. Així, aquests cardinals s'haurien d'expressar només en termes dels invariants que determinen el tipus de cicle.

Hem vist a la secció 2 que només les rectes L_1, L_2, L_3 poden ser les rectes invariants d'exponent menor que $m(\gamma)$ dels diferents elements $\gamma \in \mathcal{C}$. Segons el lema 2.14, una estratègia general per comptar $|\mathcal{X}_\gamma|$ és pensar que els n punts estan distribuïts en un cert nombre s de punts fixos de γ, certs nombres s_1 i/o s_2 i/o s_3 d'òrbites dins L_1, L_2, L_3 i un cert nombre s_0 d'òrbites que no intersecten aquestes rectes. Així, considerem particions de n del tipus:

$$n = s + \sum_i s_i d_i + s_0 m,$$

on d_i són els possibles exponents de L_i i hem de comptar per a cada valor de s, s_i i s_0 el nombre de tries possibles d'aquestes òrbites. Obtenim:

Lema 3.1. *Sigui γ un element de Γ d'ordre m. Denotem el cardinal $|\mathcal{X}_\gamma|$ respectivament per $x_I(m)$, $x_{II}(m,d)$, $x_{III}(d,e,f)$, $x'_{IV}(d)$, $x''_{IV}(d)$, x_V, x'_V, x_1, segons la subfamília de $\mathcal{C}$ (descrita a la secció 2) a la qual la classe de conjugació de γ pertany. Amb el conveni que $\binom{a}{b} = 0$ si a o b no són enters o b és negatiu, tenim:*

$$x_I(m) = \begin{pmatrix} (q^2+q+1)/m \\ n/m \end{pmatrix}.$$

$$x_{II}(m,d) = \sum_{s=0}^{1} \sum_{s_1=0}^{(q+1)/d} \binom{(q+1)/d}{s_1} \binom{(q^2-1)/m}{(n-ds_1-s)/m},$$

$$x_{III}(d,e,f) = \sum_{s=0}^{3} \sum_{s_1=0}^{(q-1)/d} \sum_{s_2=0}^{(q-1)/e} \sum_{s_3=0}^{(q-1)/f}$$
$$\binom{3}{s} \binom{(q-1)/d}{s_1} \binom{(q-1)/e}{s_2} \binom{(q-1)/f}{s_3} \binom{(q-1)^2/m}{(n-ds_1-es_2-fs_3-s)/m},$$

on $m = \mathrm{mcm}(d,e) = \mathrm{mcm}(d,f) = \mathrm{mcm}(e,f)$.

$$x'_{IV}(d) = \sum_{s=0}^{q+2} \binom{q+2}{s} \binom{(q^2-1)/d}{(n-s)/d}.$$

$$x''_{IV}(d) = \sum_{s=0}^{2} \sum_{s_1=0}^{q/p} \sum_{s_2=0}^{(q-1)/d} \binom{2}{s} \binom{q/p}{s_1} \binom{(q-1)/d}{s_2} \binom{(q^2-q)/pd}{(n-ps_1-ds_2-s)/pd}.$$

$$x_V = \sum_{s=0}^{q+1} \binom{q+1}{s} \binom{q^2/p}{(n-s)/p}$$

$$x'_V = \begin{cases} \sum_{s=0}^{1} \binom{(q^2+q)/p}{(n-s)/p}, & si\ p > 2, \\ \sum_{s=0}^{1} \sum_{s_1=0}^{q/2} \binom{q/2}{s_1} \binom{q^2/4}{(n-2s_1-s)/4}, & si\ p = 2. \end{cases}$$

$$x_1 = |\mathcal{X}| = \binom{q^2+q+1}{n}. \qquad \blacksquare$$

Remarca 3.2. *Quan una recta invariant L_1, L_2 or L_3 té exponent m és possible simplificar aquestes fórmules, simplement ignorant la recta i pensant que els seus punts es comporten com un punt general (com fèiem amb les altres rectes invariants en els casos IV' i V). Tenim, per exemple,*

$$x_{II}(m,m) = \sum_{s=0}^{1} \binom{(q^2+q)/m}{(n-s)/m},$$

$$x_{III}(m,m,m) = \sum_{s=0}^{3} \binom{3}{s} \binom{(q^2+q-2)/m}{(n-s)/m}$$

$$x_{III}(m,m,f) = \sum_{s=0}^{3} \sum_{s_1=0}^{(q-1)/f} \binom{3}{s} \binom{(q-1)/f}{s_1} \binom{(q^2-1)/m}{(n-fs_1-s)/m}.$$

Ara ja som capaços d'escriure una fórmula explícita per a $T_2(n) = |\Gamma \backslash\backslash \mathcal{X}|$:

$$T_2(n) = \sum_{\gamma \in \mathcal{C}_I} \frac{|\mathcal{X}_\gamma|}{|\Gamma_\gamma|} + \sum_{\gamma \in \mathcal{C}_{II}} \frac{|\mathcal{X}_\gamma|}{|\Gamma_\gamma|} + \sum_{\gamma \in \mathcal{C}_{III}} \frac{|\mathcal{X}_\gamma|}{|\Gamma_\gamma|} + \sum_{\gamma \in \mathcal{C}_{IV}} \frac{|\mathcal{X}_\gamma|}{|\Gamma_\gamma|} + \sum_{\gamma \in \mathcal{C}_V} \frac{|\mathcal{X}_\gamma|}{|\Gamma_\gamma|}, \qquad (10)$$

on,

$$\sum_{\gamma \in \mathcal{C}_I} \frac{|\mathcal{X}_\gamma|}{|\Gamma_\gamma|} = \sum_{m \in Z_I} N_I(m) x_I(m),$$

$$\begin{aligned}
\sum_{\gamma\in\mathcal{C}_{II}} \frac{|\mathcal{X}_\gamma|}{|\Gamma_\gamma|} &= \sum_{(m,d)\in Z_{II}} N_{II}(m,d)x_{II}(m,d),\\
\sum_{\gamma\in\mathcal{C}_{III}} \frac{|\mathcal{X}_\gamma|}{|\Gamma_\gamma|} &= \sum_{(d,e,f)\in Z_{III}} N_{III}(d,e,f)x_{III}(d,e,f),\\
\sum_{\gamma\in\mathcal{C}_{IV}} \frac{|\mathcal{X}_\gamma|}{|\Gamma_\gamma|} &= \sum_{d\in Z_{IV}} (N'_{IV}(d)x'_{IV}(d) + N''_{IV}(d)x''_{IV}(d)),\\
\sum_{\gamma\in\mathcal{C}_{V}} \frac{|\mathcal{X}_\gamma|}{|\Gamma_\gamma|} &= N_V x_V + N'_V x'_V + N_1 x_1.
\end{aligned}$$

Tot i que la fórmula sembla molt enrevessada, proporciona per a cada valor de n una expressió explícita de $T_2(n)$ com a polinomi en q amb coeficients racionals. Aquesta és una diferència essencial respecte dels altres mètodes que podem trobar a la literatura per comptar aquests nombres, com per exemple els de [BFKWZ98], [Fri97], [Fri98], on per obtenir taules per a aquests nombres necessiten fixar el valor de q. A la secció següent explicitarem la fórmula per a $n = 7$.

D'altra banda, aquesta fórmula dóna el valor de $|\Gamma\backslash\backslash\mathcal{X}|$ per a qualsevol acció de Γ sobre un conjunt $\mathcal{X}$ amb la propietat que els cardinals $|\mathcal{X}_\gamma|$ depenen només del subtipus de γ. Això passa en molts exemples. A la secció 3.2 desenvoluparem alguns exemples que donen lloc a fórmules per al nombre de classes d'isometria de diferents famílies de codis de dimensió tres.

3.1 Enumeració de les configuracions de 7 punts del pla

Volem explicitar la fórmula (10) per a $n = 7$. Obtindrem, doncs, el nombre de configuracions de 7 punts del pla, identificant les configuracions que difereixen en un automorfisme del pla. Procedirem de manera independent per a cada tipus.

D'ara endavant convindrem en denotar, per a enters arbitraris d, N:

$$[x]_{d|N} = \begin{cases} x, & \text{si } d|N,\\ 0, & \text{en cas contrari.}\end{cases}$$

Tipus I

Recordem que

$$Z_I = \{m \in \mathbb{Z} \mid m|q^2+q+1,\ m>1\}, \quad N_I(m) = \frac{\varphi(m)}{3(q^2+q+1)}.$$

Totes les òrbites de punts de $\mathbb{P}^2$ tenen cardinal m; per tant, només el cas $m = 7$ entra en joc i:

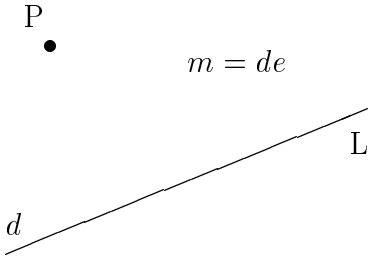
$$\sum_{m \in Z_I} N_I(m) x_I(m) = \left[\frac{\varphi(7)}{3(q^2+q+1)} \frac{q^2+q+1}{7} \right]_{7|q^2+q+1} = \left[\frac{2}{7} \right]_{7|q^2+q+1}$$

Tipus II

Recordem que $Z_{II} := \{(de, d) \in \mathbb{Z}^2 \mid d|(q+1),\ d > 1,\ e|(q-1),\ e \geq 1\}$,

$$N_{II}(de, d) = \begin{cases} \dfrac{\varphi(d)\varphi(e)}{2(q^2-1)}, & \text{si } d \text{ senar}, \\ 0, & \text{si } d \text{ parell i } e|\frac{q-1}{2}, \\ \dfrac{\varphi(d)\varphi(e)}{q^2-1}, & \text{si } d \text{ parell i } e \nmid \frac{q-1}{2} \end{cases}$$

Tota γ d'aquest tipus té un únic punt fix P i una recta invariant L d'exponent d, que no passa pel punt fix. Fora d'aquest punt i aquesta recta els punts tenen òrbites de cardinal $m = de$, amb $e|(q-1)$.



Veiem, doncs, que només els casos $d = 2, 3, 4, 5, 6, 7$ entren en joc. Estudiem-los un per un. Abans, fem la següent observació:

Lema 3.3. *Si q és senar, tenim:*

$$\sum_{e|(q-1),\ e\nmid(q-1)/2} \varphi(e) = \frac{q-1}{2}.$$

Dem.

$$\sum_{e|(q-1),\ e\nmid(q-1)/2} \varphi(e) = \sum_{e|(q-1)} \varphi(e) - \sum_{e|(q-1)/2} \varphi(e) = q-1-\frac{q-1}{2} = \frac{q-1}{2}.$$

■

Suposem $d=7$. Si $e=1$, totes les òrbites de tots els punts del pla, tret del punt fix, tenen cardinal 7. Si $e>1$, els nostres 7 punts han de formar una única òrbita continguda a la recta L. Tenim doncs, una contribució a la suma (10) de:

$$\frac{3}{q^2-1}\left[\frac{q^2+q}{7}+\sum_{e|(q-1),e>1}\varphi(e)\frac{q+1}{7}\right]_{7|q+1} = \left[\frac{6}{7}\right]_{7|q+1}.$$

Suposem $d=6$. Com que d és parell i $d|(q+1)$, forçosament q és senar i necessàriament $e>1$ per a tot enter $e|(q-1)$, $e\nmid(q-1)/2$. Per tant, els nostres 7-conjunts del pla γ-invariants han de contenir el punt fix P i sis punts han de pertànyer a la recta invariant L. Per tant, aquest cas contribueix a la suma (10) en:

$$\frac{\varphi(6)}{q^2-1}\sum_{e|(q-1),\ e\nmid(q-1)/2}\varphi(e)\frac{q+1}{6} = \left[\frac{1}{6}\right]_{6|q+1}.$$

En els casos $d=5,4$ no poden haver 7-conjunts γ-invariants. Suposem $d=3$. Tots els 7-conjunts invariants consten del punt fix P i un 6-conjunt invariant. Separem el recompte en tres casos: quan $e=1$ tots els punts del pla, tret de P, s'agrupen en tripletes invariants; quan $e=2$ cal comptar els 6-conjunts invariants de punts fora de la recta L; finalment en el cas $e\geq 2$ comptem també totes les possibles parelles de tripletes invariants dins de la recta L. En total, la contribució a (10) és:

$$\frac{1}{q^2-1}\left[\binom{(q^2+q)/3}{2}+\left[\frac{q^2-1}{6}\right]_{2|q-1}+\sum_{e|(q-1),e>1}\varphi(e)\binom{(q+1)/3}{2}\right]_{3|q+1} =$$

$$= \left[\frac{q^2+3q-4}{18}\right]_{3|q+1}+\left[\frac{1}{6}\right]_{3|q+1,p>2}.$$

Finalment, si $d=2$ tornem a tenir e parell, $e\geq 2$, com en el cas $d=6$. El cas genèric és comptar tres òrbites de cardinal 2 dins de la recta L i en el cas $e=2$ (que

només es pot donar si $4|(q+1)$) tenim la contribució extra dels 6-conjunts invariants formats per una quarteta invariant fora de la recta L i un parell invariant dins de L. En total,

$$\frac{1}{q^2-1}\left[\sum_{e|(q-1),\ e\nmid(q-1)/2}\varphi(e)\binom{(q+1)/2}{3}+\left[\frac{q^2-1}{4}\cdot\frac{q+1}{2}\right]_{4|q+1}\right]_{2|q+1}=$$

$$=\left[\frac{(q-1)(q-3)}{96}\right]_{2|q+1}+\left[\frac{q+1}{8}\right]_{4|q+1}.$$

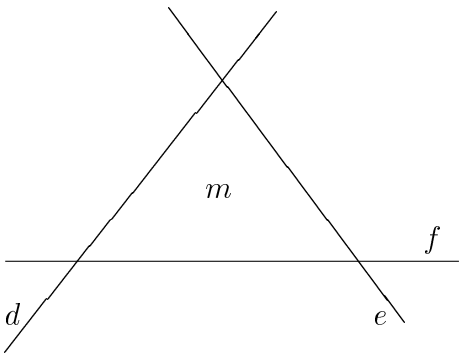
Tipus III

Recordem que

$$Z_{III}:=\{(d,e,f)\in\mathbb{Z}^3\mid d\geq e\geq f>1,\\ m:=\operatorname{mcm}(d,e)=\operatorname{mcm}(d,f)=\operatorname{mcm}(e,f)|(q-1)\},$$

$$N_{III}(d,e,f)=\begin{cases}\dfrac{\varphi(m)\psi(m)}{6(q-1)^2}, & \text{si } d=e=f=m,\\ \dfrac{\varphi(m)\varphi(h)\psi(H)}{2(q-1)^2}, & \text{if } d=e=m>f,\\ \dfrac{\varphi(m)\varphi(h)\psi(H)}{(q-1)^2}, & \text{if } d>e>f,\end{cases}$$

Recordem també la disposició de les tres rectes invariants amb exponents respectius d, e, f



En aquest cas tenim necessàriament: $\{d,\ e,\ f\} \cap \{2,\ 3,\ 4,\ 5,\ 6,\ 7\} \neq \emptyset$. Distingim diversos casos. Hi ha un recompte que es repeteix diverses vegades i que val la pena discutir en general.

Lema 3.4. *Sigui ℓ un nombre primer i denotem per Z_{III}^{ℓ} el conjunt de tripletes $(d,e,f) \in Z_{III}$ tals, que $\ell \in \{d,\ e,\ f\}$ però $(d,\ e,\ f) \neq (\ell,\ell,\ell)$. Aleshores,*

$$\sum_{(d,e,f)\in Z_{III}^{\ell}} N_{III}(d,e,f) = \left[\frac{\varphi(\ell)(q-1-\ell)}{2(q-1)^2}\right]_{\ell|q-1}.$$

Dem. Posem $q-1 = \ell^t Q$, amb $\ell \nmid Q$ i $m = \ell^r F$, amb $r \leq t$, $F|Q$. Les tripletes (d,e,f) que pertanyen a Z_{III}^{ℓ} són:

r	(d,e,f)	F	def/m^2	$N_{III}(d,e,f)$
$r=1$	$(\ell,F,\ell F)$	$F>1$	1	$\dfrac{\varphi(\ell F)}{(q-1)^2}$
$r=1$	$(\ell,\ell F,\ell F)$	$F>1$	$\ell = H$	$\dfrac{\varphi(\ell F)\psi(\ell)}{2(q-1)^2}$
$r>1$	$(\ell,\ell^r F,\ell^r F)$	$F\geq 1$	$\ell = h$	$\dfrac{\varphi(\ell^r F)\varphi(\ell)}{2(q-1)^2}$

Taula 2

Notem que: $N_{III}(\ell,F,\ell F) + N_{III}(\ell,\ell F,\ell F) = \dfrac{\varphi(\ell)\varphi(F)\ell}{2(q-1)^2}$. Per tant, separant els sumands que corresponen a $r=1$ (on caldrà restar de la suma general el sumand corresponent a $F=1$) dels de $r>1$ tenim:

$$\sum_{(d,e,f)\in Z_{III}^{\ell}} N_{III}(d,e,f) = \frac{\varphi(\ell)}{2(q-1)^2}\left[-\ell + \sum_{F|Q}\varphi(F)\left(\ell + \sum_{r=2}^{t}\varphi(\ell^r)\right)\right]_{\ell|q-1} =$$

$$= \frac{\varphi(\ell)}{2(q-1)^2}\left[-\ell + Q\left(\ell + \ell^t - 1 - \varphi(\ell)\right)\right]_{\ell|q-1} = \frac{\varphi(\ell)(q-1-\ell)}{2(q-1)^2}.$$

■

Suposem que un dels tres divisors d ó e ó f val 7. En el cas $d = e = f = 7$, tenim $m = 7$ i tots els punts del pla, excepte els 3 punts fixos, s'agrupen en 7-òrbites invariants. La contribució a la suma (10) d'aquest cas és:

$$\left[\frac{5}{(q-1)^2} \cdot \frac{q^2+q-2}{7}\right]_{7|q-1} = \left[\frac{5(q+2)}{7(q-1)}\right]_{7|q-1}.$$

En la resta dels casos, reflectits a la Taula 2 prenent $\ell = 7$, tenim $m > 7$ i hi ha una única recta d'exponent 7. Comptarem només la contribució dels 7-conjunts continguts en aquesta recta d'exponent 7.[1] Pel lema 3.4, com que $x_{III}(d,e,f) = (q-1)/7$ en tots aquests casos, tenim una contribució a la suma (10) de:

$$\frac{q-1}{7} \cdot \frac{\varphi(7)(q-8)}{2(q-1)^2} = \left[\frac{3(q-8)}{7(q-1)}\right]_{7|q-1}.$$

Suposem ara que un dels tres divisors d ó e ó f val 6. Posem $q-1 = 2^t 3^u Q$, amb $(6,Q) = 1$ i $m = 2^r 3^s F$, amb $0 < r \leq t$, $0 < s \leq u$, $F|Q$.

Com abans, distingim els casos $(6,6,3)$ i $(6,3,2)$ com a especials, ja que fora d'aquests casos els 7-conjunts invariants hauran de tenir 6 punts en una mateixa recta d'exponent 6.

En el cas $(6,3,2)$ tenim $m = 6$, $def/m^2 = 1$, $N_{III}(6,3,2) = 2/(q-1)^2$. Tots els punts del pla s'agrupen en 6-òrbites, excepte els $2q+1$ punts que pertanyen a la reunió de les dues rectes d'exponent 2 i 3. Considerem només 7-conjunts que contenen un dels tres punts fixos i una d'aquestes 6-òrbites, o bé una tripleta invariant i dos parells invariants, o bé una tripleta invariant, un parell invariant i dos punts fixos:[2]

$$\frac{2}{(q-1)^2}\left[3\,\frac{q^2-q}{6} + \frac{q-1}{3}\binom{(q-1)/2}{2} + 3\,\frac{q-1}{3}\cdot\frac{q-1}{2}\right]_{6|q-1} =$$

$$= \left[\frac{q^2+20q-9}{12(q-1)}\right]_{6|q-1}.$$

En el cas $(6,6,3)$ tenim $m = 6$, $def/m^2 = H = 3$, $N_{III}(6,6,3) = 1/(q-1)^2$. Tots els punts del pla, excepte els $q+2$ formats per la recta d'exponent 3 i el punt fix exterior, s'agrupen en 6-òrbites. Comptem només la contribució dels 7-conjunts formats per un punt fix i una d'aquestes 6-òrbites:[2]

[1] Per a $(d,e,f) = (42,7,6), (35,7,5), (28,7,4), (21,7,3), (14,7,2)$, hi ha d'altres possibilitats per als 7-conjunts invariants, que seran comptades més endavant en els casos 6, 5, 4, 3, $2 \in \{d,e,f\}$ respectivament.

[2] La contribució de dues tripletes a la recta d'exponent 3 i un punt fix ja la comptarem en el cas $3 \in \{d, e, f\}$. La contribució de dos parells invariants a la recta d'exponent 2 i tres punts fixos, o bé tres parells invariants i un punt fix, la comptarem en el cas $2 \in \{d, e, f\}$.

$$\frac{3}{(q-1)^2}\left[\frac{q^2-1}{6}\right]_{6|q-1} = \left[\frac{q+1}{2(q-1)}\right]_{6|q-1}.$$

La resta de casos presenta les següents possibilitats:

$r,\ s$	(d,e,f)	F	def/m^2	$N_{III}(d,e,f)$
$r=s=1$	$(6,F,6F)$	$F>1$	1	$\frac{2\varphi(F)}{(q-1)^2}$
$r=s=1$	$(6,2F,6F)$	$F\geq 1$	$2=H$	0
$r=s=1$	$(6,3F,6F)$	$F>1$	$3=H$	$\frac{2\varphi(F)}{(q-1)^2}$
$r=s=1$	$(6,6F,6F)$	$F\geq 1$	$6=H$	0
$r=s=1$	$(6,2F,3F)$	$F>1$	1	$\frac{2\varphi(F)}{(q-1)^2}$
$r=1,\ s>1$	$(6,3^sF,2\cdot 3^sF)$	$F\geq 1$	$3=h$	$\frac{2\varphi(3^sF)}{(q-1)^2}$
$r=1,\ s>1$	$(6,2\cdot 3^sF,2\cdot 3^sF)$	$F\geq 1$	$6,\ H=2,\ h=3$	0
$r>1,\ s=1$	$(6,2^rF,3\cdot 2^rF)$	$F\geq 1$	$2=h$	$\frac{2\varphi(2^rF)}{(q-1)^2}$
$r>1,\ s=1$	$(6,3\cdot 2^rF,3\cdot 2^rF)$	$F\geq 1$	$6,\ H=3,\ h=2$	$\frac{\varphi(2^rF)}{(q-1)^2}$
$r>1,\ s>1$	$(6,2^r3^sF,2^r3^sF)$	$F\geq 1$	$6=h$	$\frac{\varphi(2^r3^sF)}{(q-1)^2}$

Taula 3

Cal avaluar la contribució dels 7-conjunts que tenen un punt fix i una 6-òrbita continguda a l'única recta d'exponent 6. Sumant sobre tot r, s, F (i descomptant el sumand corresponent a $r=s=F=1$) tenim:

$$\sum_{(d,e,f)\in\text{Taula 3}} N_{III}(d,e,f) =$$

$$= \frac{1}{(q-1)^2}\left(-6+\sum_{F|Q}\varphi(F)\left(6+\sum_{s=2}^{u}2\varphi(3^s)+\sum_{r=2}^{t}3\varphi(2^r)+\sum_{r,\,s\geq 2}\varphi(2^r3^s)\right)\right) =$$

$$= \frac{1}{(q-1)^2}\left(-6+Q\left(6+\sum_{D|2^t3^u,\,D\neq 1,2,3,6}\varphi(D)\right)\right) = \frac{q-7}{(q-1)^2}. \quad (11)$$

Com que $x_{III}(d,e,f) = 3(q-1)/6$ per a tots aquest tipus (el 3 que multiplica té en compte la variació dels tres punts fixos), tenim una contribució de:

$$\left[\frac{q-7}{2(q-1)}\right]_{6|q-1}.$$

El cas en que $5 \in \{d,\, e,\, f\}$ és completament anàleg al cas en que $7 \in \{d,\, e,\, f\}$. En el cas $(5,5,5)$ tenim $m = 5$ i una contribució:

$$3\frac{3\varphi(5)}{6(q-1)^2}\left[\frac{q^2+q-2}{5}\right]_{5|q-1} = \left[\frac{6(q+2)}{5(q-1)}\right]_{5|q-1}.$$

En la resta de casos hi ha una única recta invariant d'exponent 5 i comptem l'aportació els 7-conjunts invariants que tenen 2 punts fixos i 5 punts invariants en aquesta recta d'exponent 5. Pel lema 3.4 tenim una contribució de:

$$\left[\frac{6(q-6)}{5(q-1)}\right]_{5|q-1}.$$

Per a $(35,7,5)$ i $(30,6,5)$ hi ha altres possibilitats per als 7-conjunts, que ja han estat comptades en els casos anteriors. Per a $(20,5,4)$, $(15,5,3)$ i $(10,5,2)$ hi ha també altres possibilitats: 4-conjunts o 6-conjunts invariants a la recta d'exponent menor que 5 completats amb punts fixos, que seran comptades més endavant. En el cas excepcional $(10,5,2)$ es pot donar a més a més la possibilitat d'un 5-conjunt invariant i un 2-conjunt invariant. Per considerar aquesta contribució cal afegir als termes calculats:

$$\frac{\varphi(10)}{(q-1)^2}\left[\frac{q-1}{5}\cdot\frac{q-1}{2}\right]_{10|q-1} = \left[\frac{2}{5}\right]_{10|q-1}.$$

Suposem ara $4 \in \{d,\, e,\, f\}$. Posem $q-1 = 2^tQ$, Q senar, $t \geq 2$, $m = 2^rF$, $F|Q$, $t \geq r \geq 2$. Distingim, el cas $(4,4,2)$ de la resta de casos, que són:

r	(d,e,f)	F	def/m^2	$N_{III}(d,e,f)$
$r=2$	$(4,F,4F)$	$F>1$	1	$\dfrac{2\varphi(F)}{(q-1)^2}$
$r=2$	$(4,2F,4F)$	$F>1$	$2=h$	$\dfrac{2\varphi(F)}{(q-1)^2}$
$r=2$	$(4,4F,4F)$	$F\geq 1$	$4=H$	0
$r>2$	$(4,2^rF,2^rF)$	$F\geq 1$	$4=h$	$\dfrac{\varphi(2^rF)}{(q-1)^2}$

Taula 4

En el cas $(4,4,2)$, es té:

$$m=4, \quad def/m^2=2=h, \quad N_{III}(4,4,2)=1/(q-1)^2.$$

Tots els punts fora de la recta d'exponent 2 i el punt fix exterior s'agrupen en 4-conjunts invariants. Comptem la contribució dels 7-conjunts formats per un d'aquests 4-conjunts i 3 punts fixos, o bé un punt fix, un parell invariant a la recta d'exponent 2 i un dels 4-conjunts invariants:[3]

$$\frac{1}{(q-1)^2}\left[\frac{q^2-1}{4}+3\,\frac{q^2-1}{4}\cdot\frac{q-1}{2}\right]_{4|q-1}=\frac{1}{q-1}\left[\frac{3q^2+2q-1}{8}\right]_{4|q-1}.$$

En la resta de casos els 7-conjunts invariants consten d'una quarteta invariant continguda a l'única recta d'exponent 4, i els tres punts fixos. La contribució és:

$$\sum_{(d,e,f)\in\text{Taula 4}} N_{III}(d,e,f)\,\frac{q-1}{4}=$$

$$\frac{1}{(q-1)^2}\cdot\frac{q-1}{4}\left[-4+\sum_{F|Q}\varphi(F)\left(4+\sum_{r=3}^{t}\varphi(2^r)\right)\right]_{4|q-1}=\left[\frac{q-5}{4(q-1)}\right]_{4|q-1}. \quad (12)$$

[3]La contribució de tres parells invariants i un punt fix, o dos parells invariants i tres punts fixos serà comptada dins del cas $2\in\{d,\,e,\,f\}$.

Ens queda el cas $(12,4,3)$, on també poden haver 7-conjunts invariants partits en una tripleta i una quarteta invariant. Cal afegir als termes calculats fins ara:

$$\frac{\varphi(12)}{(q-1)^2}\left[\frac{q-1}{4}\cdot\frac{q-1}{3}\right]_{12|q-1}=\left[\frac{1}{3}\right]_{12|q-1}.$$

Anem pel cas $3\in\{d,\,e,\,f\}$. Comptem la contribució del cas $(3,3,3)$ apart:

$$3\,\frac{1}{3(q-1)^2}\left[\binom{(q^2+q-2)/3}{2}\right]_{3|q-1}=\left[\frac{(q^3+3q^2-3q-10)}{18(q-1)}\right]_{3|q-1}.$$

I comptem els casos en que considerem dues tripletes invariants dins de la mateixa recta d'exponent 3 i un punt fix. Pel lema 3.4 això representa una contribució de:

$$3\,\frac{q-4}{(q-1)^2}\left[\binom{(q-1)/3}{2}\right]_{3|q-1}=\left[\frac{(q-4)^2}{6(q-1)}\right]_{3|q-1}.$$

Finalment, considerem el cas $2\in\{d,\,e,\,f\}$. Com que $N_{III}(2,2,2)=0$, el cas $(2,2,2)$ no aporta res. En la resta de casos es té $m>2$ i hi ha una única recta invariant d'exponent 2. La contribució de diverses possibilitats dels casos $(14,7,2)$, $(6,6,2)$, $(10,5,2)$, $(4,4,2)$, $(6,3,2)$ ja s'han comptat; l'única aportació que queda per comptar és la de tres parells invariants a la recta d'exponent 2 i un punt fix, o bé dos parells invariants en aquesta recta i 3 punts fixos. Pel lema 3.4 contribueixen amb:

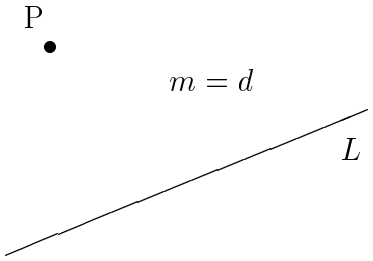
$$\frac{q-3}{2(q-1)^2}\left[3\binom{(q-1)/2}{3}+\binom{(q-1)/2}{2}\right]_{2|q-1}=\left[\frac{(q-3)^3}{32(q-1)}\right]_{2|q-1}.$$

Tipus IV

Recordem que $Z_{IV}=\{d\in\mathbb{Z}\mid d|(q-1),\ d>1\}$,

$$N'_{IV}(d)=\frac{\varphi(d)}{q(q-1)^2(q+1)},\quad N''_{IV}(d)=\frac{\varphi(d)}{q(q-1)}.$$

Pel tipus IV' tenim una recta L de punts fixos i un punt exterior P també fix. Fora d'aquests $q+2$ punts fixos totes les òrbites tenen cardinal $m=d$.



Per a qualsevol $d \in Z_{IV}$ tenim la possibilitat de considerar 7 punts fixos. Això contribueix amb:

$$\frac{1}{q(q-1)^2(q+1)}\left(\sum_{d|q-1,\, d>1}\varphi(d)\binom{q+2}{7}\right) = \frac{(q-2)^2(q+2)(q-3)(q-4)}{7!(q-1)}.$$

Fora d'aquesta situació tenim forçosament $d \in \{2, 3, 4, 5, 6, 7\}$. En els casos $d = 7, 6, 5, 4$ podem considerar una d-tupla invariant fora de $L \cup \{P\}$ i la resta de punts fixos. En el cas $d = 3$ podem considerar 1 o 2 tripletes invariants fora de $L \cup \{P\}$ i en el cas $d = 2$ podem considerar 1 o 2 o 3 parells invariants fora de $L \cup \{P\}$. En total tenim la contribució de:

$$\frac{1}{q(q-1)^2(q+1)}\left(\varphi(7)\left[\frac{(q^2-1)}{7}\right]_{7|q-1} + \varphi(6)\left[\frac{(q^2-1)}{6}(q+2)\right]_{6|q-1} +\right.$$

$$+\varphi(5)\left[\frac{(q^2-1)}{5}\binom{q+2}{2}\right]_{5|q-1} + \varphi(4)\left[\frac{(q^2-1)}{4}\binom{q+2}{3}\right]_{4|q-1} +$$

$$+\varphi(3)\left[\frac{(q^2-1)}{3}\binom{q+2}{4} + \binom{(q^2-1)/3}{2}(q+2)\right]_{3|q-1} +$$

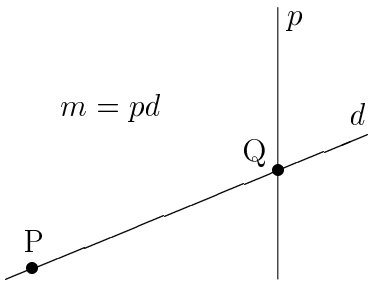
$$\left.+\left[\binom{(q^2-1)/2}{3}(q+2) + \binom{(q^2-1)/2}{2}\binom{q+2}{3} + \frac{q^2-1}{2}\binom{q+2}{5}\right]_{2|q-1}\right) =$$

$$= \frac{1}{q(q-1)}\left(\left[\frac{6}{7}\right]_{7|q-1} + \left[\frac{q+2}{3}\right]_{6|q-1} + \left[\frac{2(q+2)(q+1)}{5}\right]_{5|q-1} +\right.$$

$$+\left[\frac{(q+2)(q+1)q}{12}\right]_{4|q-1}+\left[\frac{(q+2)(q^3+4q^2-q-16)}{36}\right]_{3|q-1}+$$

$$+\left[\frac{(q+2)(q+1)q(q-1)(q-2)}{240}\right]_{2|q-1}\Bigg).$$

Pel tipus IV'' tenim dues rectes invariants, L_d, L_p, d'exponents respectius d, p. El punt Q d'intersecció és un punt fix i la recta L_d té encara una altre punt fix P. Fora d'aquestes dues rectes totes les òrbites tenen cardinal $m = pd$.



Considerem com a contribució genèrica la que aporten els 7-conjunts continguts a la recta d'exponent $d \in \{2,\ 3,\ 5,\ 6,\ 7\}$.

$$\frac{1}{q(q-1)}\Bigg(\varphi(7)\left[\frac{q-1}{7}\right]_{7|q-1}+2\varphi(6)\left[\frac{q-1}{6}\right]_{6|q-1}+\varphi(5)\left[\frac{q-1}{5}\right]_{5|q-1}+$$

$$+2\varphi(3)\left[\binom{(q-1)/3}{2}\right]_{3|q-1}+2\varphi(2)\left[\binom{(q-1)/2}{3}\right]_{2|q-1}\Bigg)=$$

$$=\frac{1}{q}\left(\left[\frac{6}{7}\right]_{7|q-1}+\left[\frac{2}{3}\right]_{6|q-1}+\left[\frac{4}{5}\right]_{5|q-1}+\left[\frac{2(q-4)}{9}\right]_{3|q-1}+\left[\frac{(q-3)(q-5)}{24}\right]_{2|q-1}\right).$$

Les altres possibilitats corresponent a valors molt concrets de la característica: $p \in \{2,\ 3,\ 5,\ 7\}$. Per a cada valor de p comptem la contribució del 7-conjunts continguts a $L_p \cup \{P\}$, repetida per a tot valor de $d \in Z_{IV}$:

$$\frac{1}{q(q-1)}\sum_{d|q-1,d>1}\varphi(d)\left(\left[\frac{q}{7}\right]_{7|q}+\left[\frac{q}{5}\right]_{5|q}+2\left[\binom{q/3}{2}\right]_{3|q}+2\left[\binom{q/2}{3}\right]_{2|q}\right)=$$

$$=\frac{q-2}{q-1}\left(\left[\frac{1}{7}\right]_{7|q}+\left[\frac{1}{5}\right]_{5|q}+\left[\frac{q-3}{9}\right]_{3|q}+\left[\frac{(q-2)(q-4)}{24}\right]_{2|q}\right).$$

Finalment, comptem la contribució del 7-conjunts que tenen òrbites invariants de les dues rectes i els que consten d'un punt fix i una 6-òrbita invariant fora de les dues rectes (en aquest cas necessàriament $d=2$, $p=3$ ó $d=3$, $p=2$).

$$\frac{1}{q(q-1)}\left(\left[\frac{q}{5}\cdot\frac{q-1}{2}\right]_{5|q}+\right.$$

$$+\varphi(4)\left[\frac{q}{3}\cdot\frac{q-1}{4}\right]_{3|q,\,4|q-1}+\left[\frac{q}{3}\cdot\binom{(q+1)/2}{2}+2\,\frac{q^2-q}{6}\right]_{3|q}+$$

$$\left.+\varphi(5)\left[\frac{q}{2}\cdot\frac{q-1}{5}\right]_{2|q,\,5|q-1}+\varphi(3)\left[\frac{q-1}{3}\binom{q/2}{2}+\frac{q}{2}\cdot\frac{q-1}{3}+2\,\frac{q^2-q}{6}\right]_{2|q,\,3|q-1}\right)=$$

$$=\left[\frac{1}{10}\right]_{5|q}+\left[\frac{1}{6}\right]_{3|q,\,4|q-1}+\left[\frac{q+9}{24}\right]_{3|q}+\left[\frac{2}{5}\right]_{2|q,\,5|q-1}+\left[\frac{q+10}{12}\right]_{2|q,\,3|q-1}.$$

Tipus V

Recordem que:

$$N_V=\frac{1}{q^3(q-1)},\qquad N_V'=\frac{1}{q^2},\qquad N_1=\frac{1}{q^3(q-1)^2(q^2+q+1)(q+1)}.$$

Per a γ_V tenim una recta L de punts fixos i fora d'ella les òrbites invariants tenen totes cardinal $m=p$. Tenim doncs una contribució genèrica de:

$$\frac{1}{q^3(q-1)}\binom{q+1}{7}=\frac{(q+1)(q-2)(q-3)(q-4)(q-5)}{5040\,q^2},$$

aportada pels 7-conjunts formats íntegrament per punts fixos, i una contribució que serà específica de característiques petites, $p \in \{2, 3, 5, 7\}$:

$$\frac{1}{q^3(q-1)}\left(\left[\frac{q^2}{7}\right]_{7|q}+\left[\frac{q^2}{5}\cdot\binom{q+1}{2}\right]_{5|q}+\left[\frac{q^2}{3}\cdot\binom{q+1}{4}+\binom{q^2/3}{2}(q+1)\right]_{3|q}+\right.$$

$$\left.+\left[\frac{q^2}{2}\cdot\binom{q+1}{5}+\binom{q^2/2}{2}\binom{q+1}{3}+\binom{q^2/2}{3}(q+1)\right]_{2|q}\right)=$$

$$=\frac{1}{q(q-1)}\left(\left[\frac{1}{7}\right]_{7|q}+\left[\frac{(q+1)q}{10}\right]_{5|q}+\left[\frac{(q+1)(q^3+q^2+2q-12)}{72}\right]_{3|q}+\right.$$

$$\left.+\left[\frac{(q+1)(11q^4-11q^3-29q^2+4q+40)}{240}\right]_{2|q}\right).$$

Per a γ'_V tenim una recta invariant L d'exponent p, que conté un únic punt fix P. Fora d'ella les òrbites invariants tenen totes cardinal $m = p$, si $p > 2$ i $m = 4$, si $p = 2$. Si $p > 2$, tenim doncs $q^2 + q$ punts agrupats en òrbites invariants de cardinal p, que contribueixen en:

$$\frac{1}{q^2}\left(\left[\frac{q^2+q}{7}\right]_{7|q}+\left[\binom{(q^2+q)/3}{2}\right]_{3|q}\right)=\left[\frac{q+1}{7q}\right]_{7|q}+\left[\frac{(q+1)(q^2+q-3)}{18q}\right]_{3|q}.$$

Per a $p = 2$ tenim, en canvi,

$$\frac{1}{q^2}\left[\frac{q^2}{4}\cdot\frac{q}{2}+\binom{q/2}{3}\right]_{2|q}=\left[\frac{7q^2-6q+8)}{48q}\right]_{2|q}.$$

Finalment, la contribució de $\gamma = 1$ és:

$$N_1\binom{q^2+q+1}{7}=\frac{(q^2+q+1)(q+2)(q^2+q-3)(q^2+q-4)(q^2+q-5)}{5040\,q^2(q-1)}.$$

La suma de totes les contribucions de tots els tipus dóna com a resultat, per a $n = 7$ i $p = 2$:

$$T_2(7) = \frac{q^6+7q^5+9q^4+183q^3+632q^2-364q+1344}{5040}+$$

$$+[\frac{q^2+18q+20}{36}]_{3|q-1}+[\frac{16}{5}]_{5|q-1}+[\frac{6}{7}]_{7|q-1},$$

mentre que per a $n=7$ i $p>2$ tenim:

$$T_2(7) = \frac{q^6+7q^5+9q^4+183q^3+1157q^2+56q-201}{5040}+[\frac{q^2+10q-15}{72}]_{3|q}+$$

$$+[\frac{q^2+18q+77}{36}]_{3|q-1}+[\frac{4q+13}{12}]_{4|q-1}+[\frac{1}{3}]_{12|q-1}+[\frac{1}{6}]_{12|q-9}+$$

$$+[\frac{16}{5}]_{5|q-1}+[\frac{2}{5}]_{5|q}+[\frac{8}{7}]_{7|q-1}+[\frac{6}{7}]_{7|q+1}+[\frac{2}{7}]_{7|q}+[\frac{2}{7}]_{7|q^2+q+1}.$$

3.2 Classes d'isometria de codis de dimensió tres

Remetem a [BFKWZ98, 3.2, 3.3] per a les motivacions que porten a la consideració de diferents famílies de codis injectius de longitud n sense coordenades universalment nul.les. La Taula 5 recull la nostra notació per al nombre de classes d'isometria d'aquestes famílies de codis, i la seva connexió amb el nombre d'òrbites de Γ quan actua sobre diferents conjunts de famílies de punts del pla projectiu (cf. loc. cit.).

Codis injectius de longitud n

dimensió ≤ 3	$T_2(n) = \lvert\Gamma\backslash\backslash\mathcal{X}\rvert$	$\mathcal{X}$ = conjunt de n-subconjunts de $\mathbb{P}^2(\mathbb{F}_q)$
dimensió 3	$S_2(n) = \lvert\Gamma\backslash\backslash\mathcal{Y}\rvert$	$\mathcal{Y}$ = conjunt de n-subconjunts de $\mathbb{P}^2(\mathbb{F}_q)$ no continguts a cap recta
dimensió 3 indecomponibles	$R_2(n) = \lvert\Gamma\backslash\backslash\mathcal{Z}\rvert$	$\mathcal{Z}$ = conjunt de n-subconjunts de $\mathbb{P}^2(\mathbb{F}_q)$ no continguts a la unió de recta i punt

Taula 5

Anàlogament, $\overline{T}_2(n)$, $\overline{S}_2(n)$, $\overline{R}_2(n)$ denoten el nombre de classes d'isometria de codis que satisfan les respectives condicions descrites a la taula, però oblidant la condició d'injectivitat. Aquestes classes d'isometria es poden expressar com $|\Gamma\backslash\backslash\mathcal{X}|$, considerant que $\mathcal{X}$ sigui el conjunt dels n-multiconjunts de $\mathbb{P}^2(\mathbb{F}_q)$, resp. no continguts a cap recta, resp. no continguts a la unió d'una recta i un punt.

A (10) hem trobat una fórmula explícita per a $T_2(n)$. En aquesta fórmula, els conjunts Z_I, Z_{II}, Z_{III}, Z_{IV} i els nombres $N_I(m)$, $N_{II}(m,d)$, $N_{III}(d,e,f)$, $N'_{IV}(d)$, $N''_{IV}(d)$, N_V, N'_V, N_1 són universals; és a dir, depenen només de l'acció de Γ sobre $\mathbb{P}^2(\mathbb{F}_q)$ i no sobre el conjunt particular $\mathcal{X}$ que consideràvem.

Denotem per un moment $\mathcal{X} = \left(\!\!\binom{\mathbb{P}^2(\mathbb{F}_q)}{n}\!\!\right)$ el conjunt dels n-multiconjunts de $\mathbb{P}^2(\mathbb{F}_q)$. Clarament, un multiconjunt fixat per un cert $\gamma \in \Gamma$ és una unió disjunta de γ-òrbites de punts de $\mathbb{P}^2(\mathbb{F}_q)$, permetent repeticions d'òrbites. Així, $|\mathcal{X}_\gamma|$ depèn només del subtipus de γ i es pot calcular amb exactament les mateixes fórmules del lema 3.1 reemplaçant a tot arreu els coeficients binomials $\binom{n}{r}$ per coeficients multinomials $\left(\!\!\binom{n}{r}\!\!\right)$. D'aquesta manera també obtenim un càlcul explícit de $\overline{T}_2(n)$.

De la mateixa manera, tan aviat com siguem capaos de calcular els cardinals $|\mathcal{Y}_\gamma|$, $|\mathcal{Z}_\gamma|$, la fórmula (10) ens donarà un càlcul explícit de $S_2(n)$, $R_2(n)$, i només reemplaçant coeficients binomials per coeficients multinomials, la mateixa expressió ens donarà fórmules per a $\overline{S}_2(n)$, $\overline{R}_2(n)$.

Clarament, tenim $S_2(n) = T_2(n) - T_1(n)$. Una fórmula explícita per a $T_1(n)$ va ser trobada a [LN99]; així, juntant-la amb el càlcul de $T_2(n)$ fet a la secció 3, seríem capaços d'escriure una fórmula per a $S_2(n)$. Tanmateix, per exemplificar el caràcter universal de la fórmula (10) obtindrem el valor de $S_2(n)$ calculant $|\mathcal{Y}_\gamma|$. De fet, és trivial calcular $|\mathcal{Y}_\gamma|$ i $|\mathcal{Z}_\gamma|$ després del lema 3.1 i l'observació següent, que és evident:

Lema 3.5. *Sigui $\mathcal{X}$ el conjunt dels n-subconjunts de $\mathbb{P}^2(\mathbb{F}_q)$ i sigui $x \in \mathcal{X}_\gamma$ un n-subconjunt invariant per un cert $\gamma \in \Gamma$. Siguin L una recta i Q un punt de $\mathbb{P}^2(\mathbb{F}_q)$. Aleshores,*

(a) Si $x \subseteq L$ i $n > 1$, aleshores L és una recta γ-invariant.

(b) Si $x \subseteq L \cup \{Q\}$, $x \nsubseteq L$ i $n > 3$, aleshores L és una recta γ-invariant i Q és un punt fix de γ. ■

Corol.lari 3.6. *Sigui $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ com a la Taula 5, amb $n > 3$. Per a tot $\gamma \in \Gamma$ denotem el cardinal $|\mathcal{X}_\gamma|$ respectivament per $x_I(m)$, $x_{II}(m,d)$, $x_{III}(d,e,f)$, $x'_{IV}(d)$, $x''_{IV}(d)$, x_V, x'_V, x_1, com fèiem al lema 3.1. Amb una notació similar per a $|\mathcal{Y}_\gamma|$, $|\mathcal{Z}_\gamma|$ i el conveni que $\binom{a}{b} = 0$ si a o b no són enters o b és negatiu, tenim:*

$$z_I(m) = y_I(m) = x_I(m),$$

$$y_{II}(m,d) = x_{II}(m,d) - \binom{(q+1)/d}{n/d}, \quad z_{II}(m,d) = y_{II}(m,d) - \binom{(q+1)/d}{(n-1)/d}$$

$$y_{III}(d,e,f) = x_{III}(d,e,f) - \sum_{s=0}^{2} \binom{2}{s} \left[\binom{(q-1)/d}{(n-s)/d} + \binom{(q-1)/e}{(n-s)/e} + \binom{(q-1)/f}{(n-s)/f} \right],$$

$$z_{III}(d,e,f) = y_{III}(d,e,f) - \sum_{s=0}^{2} \binom{2}{s} \left[\binom{(q-1)/d}{(n-1-s)/d} + \binom{(q-1)/e}{(n-1-s)/e} + \binom{(q-1)/f}{(n-1-s)/f} \right],$$

$$y'_{IV}(d) = x'_{IV}(d) - \binom{q+1}{n} - (q+1) \sum_{s=0}^{2} \binom{2}{s} \binom{(q-1)/d}{(n-s)/d},$$

$$z'_{IV}(d) = y'_{IV}(d) - \binom{q+1}{n-1} - q(q+1) \sum_{s=0}^{2} \binom{2}{s} \binom{(q-1)/d}{(n-1-s)/d},$$

$$y''_{IV}(d) = x''_{IV}(d) - \sum_{s=0}^{2} \binom{2}{s} \binom{(q-1)/d}{(n-s)/d} - \sum_{s=0}^{1} \binom{q/p}{(n-s)/p},$$

$$z''_{IV}(d) = y''_{IV}(d) - \sum_{s=0}^{1} \binom{q/p}{(n-1-s)/p},$$

$$y_V = x_V - \binom{q+1}{n} - q \sum_{s=0}^{1} \binom{q/p}{(n-s)/p}, \quad z_V = y_V - q \sum_{s=0}^{1} \binom{q/p}{(n-1-s)/p},$$

$$z'_V = y'_V = x'_V - \sum_{s=0}^{1} \binom{q/p}{(n-s)/p},$$

$$y_1 = x_1 - (q^2+q+1) \binom{q+1}{n}, \quad z_1 = y_1 - (q^2+q+1)q^2 \binom{q+1}{n-1}.$$

Dem. Després del lema 3.5, només hem de descomptar de $|\mathcal{X}_\gamma|$ el nombre de n-subconjunts γ-invariants continguts a una recta invariant i els continguts a la unió d'una recta invariant i un punt fix. Una ullada a la Taula 1 clarifica tots els càlculs. ■

Obtenim de (10) un càlcul explícit de $S_2(n)$ i $R_2(n)$. Com abans, per a qualsevol valor donat de n, és possible obtenir una expressió explícita d'aquests valors com a

polinomi en q amb coeficients racionals. Per exemple, petits retocs als càlculs de la secció 3.1 permeten obtenir, per a $n = 7$ i $p = 2$:

$$S_2(7) = \frac{q^6 + 7q^5 + 8q^4 + 197q^3 + 456q^2 + 420q + 384}{5040} + [\frac{q^2 + 14q + 36}{36}]_{3|q-1} +$$
$$+ [\frac{14}{5}]_{5|q-1} + [\frac{3}{7}]_{7|q-1},$$

$$R_2(7) = \frac{q^6 + 7q^5 + 8q^4 + 190q^3 + 414q^2 + 588q + 272}{5040} + [\frac{q^2 + 14q + 40}{36}]_{3|q-1} +$$
$$+ [2]_{5|q-1} + [\frac{3}{7}]_{7|q-1},$$

i per a $n = 7$, $p > 2$:

$$S_2(7) = \frac{q^6 + 7q^5 + 8q^4 + 197q^3 + 981q^2 + 1050q - 1896}{5040} + [\frac{q^2 + 6q - 3}{72}]_{3|q} +$$
$$+ [\frac{q^2 + 14q + 81}{36}]_{3|q-1} + [\frac{4q + 13}{12}]_{4|q-1} + [\frac{1}{3}]_{12|q-1} + [\frac{1}{6}]_{12|q-9} +$$
$$+ [\frac{14}{5}]_{5|q-1} + [\frac{2}{5}]_{5|q} + [\frac{5}{7}]_{7|q-1} + [\frac{3}{7}]_{7|q+1} + [\frac{1}{7}]_{7|q} + [\frac{2}{7}]_{7|q^2+q+1},$$

$$R_2(7) = \frac{q^6 + 7q^5 + 8q^4 + 190q^3 + 939q^2 + 903q - 2008}{5040} + [\frac{q^2 + 6q + 13}{72}]_{3|q} +$$
$$+ [\frac{q^2 + 14q + 85}{36}]_{3|q-1} + [\frac{2q + 5}{6}]_{4|q-1} + [\frac{1}{3}]_{12|q-1} + [\frac{1}{6}]_{12|q-9} +$$
$$+ [2]_{5|q-1} + [\frac{1}{5}]_{5|q} + [\frac{5}{7}]_{7|q-1} + [\frac{3}{7}]_{7|q+1} + [\frac{1}{7}]_{7|q} + [\frac{2}{7}]_{7|q^2+q+1}.$$

Capítol 2

La varietat de n-conjunts d'una varietat

A més de proporcionar una representació geomètrica de la teoria de codis lineals, els n-conjunts d'espais projectius tenen un estret lligam amb d'altres objectes geomètrics interessants. L'estudi d'aquests n-conjunts i els seus espais de moduli ha estat objecte de l'atenció de la geometria algebraica des de les seves etapes més clàssiques. Destaquen les contribucions d'A. Coble a principis del segle passat. A [DO88] es pot trobar una extensa bibliografia sobre aquests treballs i una revisió dels mateixos en clau moderna. Centrant-nos en alguns dels casos més senzills, és ben sabut que, sobre un cos algebraicament tancat, els n-conjunts de $\mathbb{P}^1$ classifiquen corbes hiperel·líptiques [DO88, Cap. VIII], i els 7-conjunts del pla classifiquen corbes no hiperel·líptiques de gènere 3 dotades d'una estructura de 2-nivell [DO88, Cap. IX].

Si ens interessem per les propietats aritmètiques dels objectes geomètrics involucrats amb els n-conjunts, caldrà preocupar-se per la *racionalitat* d'aquests n-conjunts, és a dir, pel fet que el n-conjunt estigui definit sobre un determinat cos, que no serà necessàriament algebraicament tancat. Per exemple, suposem que k és un cos perfecte i tenim un n-conjunt $\{a_1, \ldots, a_n\}$ de $\mathbb{A}^1(\overline{k})$; aquest n-conjunt està definit sobre k (o, equivalentment, el n-conjunt és k-racional) si:

$$\{\sigma(a_1), \ldots, \sigma(a_n)\} = \{a_1, \ldots, a_n\}, \quad \forall \sigma \in \mathrm{Gal}(\overline{k}/k),$$

de manera que per a cada membre a_i del n-conjunt tota l'òrbita de a_i per l'acció del grup de galois ha d'estar continguda també al n-conjunt. Evidentment, els n-conjunts formats íntegrament per elements $a_1, \ldots, a_n \in k$ són k-definits, però són un tipus molt particular de n-conjunts k-definits.

Per exemple, la fórmula per a $\overline{T}_{n2}$ obtinguda a [LN99] compta n-conjunts de $\mathbb{P}^1(k)$ classificats per l'acció del grup lineal, on k és un cos finit. Si n és parell i la característica de k és senar, podem interpretar aquesta fórmula (essencialment) com un recompte de classes de k-isomorfisme de corbes hiperel·líptiques de gènere $g = (n-2)/2$, *que tinguin tots els punts de Weierstrass racionals*; la corba associada al n-conjunt $\{a_1, \ldots, a_n\}$ vindria donada per l'equació plana de Weierstrass:

$$y^2 = (x - a_1)(x - a_2) \cdots (x - a_n).$$

Estem, doncs, lluny de tenir controlades totes les corbes hiperel·líptiques d'aquest gènere, que vindran donades per equacions de la forma:

$$y^2 = f(x),$$

on $f(x)$ és un polinomi separable arbitrari de grau n amb coeficients a k. Treballant amb n-conjunts de punts k-definits només estem considerant corbes amb la propietat (molt particular) que el polinomi $f(x)$ descompon completament a k. A l'article [LMNX02] es va calcular el nombre de n-conjunts k-racionals de $\mathbb{P}^1$ classificats per l'acció del grup lineal, obtenint d'aquesta manera el veritable nombre total de classes de k-isomorfisme de corbes hiperel·líptiques de gènere fixat.

Veiem, doncs, la necessitat d'estendre els càlculs del capítol anterior al cas de n-conjunts d'espais projectius que són racionals com a n-conjunt i no necessàriament punt a punt. Separarem aquesta tasca en dues parts. En aquest capítol trobarem fórmules pel nombre de n-conjunts racionals d'una varietat algebraica qualsevol, que farem més explícites en el cas de subvarietats lineals d'espais afins i projectius. En el capítol següent estudiarem com comptar les òrbites d'aquests n-conjunts racionals sota l'acció del grup lineal.

4 Punts racionals de la varietat de n-conjunts

Fixem un cos finit $k = \mathbb{F}_q$ i una clausura algebraica $\overline{k}$ de k. Denotem per $G = \mathrm{Gal}(\overline{k}/k)$ el grup de Galois absolut de k. El grup G és isomorf al grup procíclic $\hat{\mathbb{Z}}$ i està generat topològicament (respecte de la topologia profinita) per l'automorfisme de Frobenius:

$$\sigma \colon \overline{k} \longrightarrow \overline{k}, \quad \sigma(x) = x^q, \ \forall x \in \overline{k}.$$

Per a tot enter $r \geq 1$ denotem per $k_r = \mathbb{F}_{q^r}$ l'única extensió de grau r de k dins $\overline{k}$.

Considerem una varietat algebraica V definida sobre k. Denotem respectivament per:

$$\binom{V}{n}, \qquad \left(\!\binom{V}{n}\!\right),$$

la varietat dels n-conjunts de punts de V i la varietat dels n-multiconjunts de punts de V. Els punts d'aquestes varietats són famílies no-ordenades de n punts de V:

$$\binom{V}{n}(k_r) = \binom{V(\overline{k})}{n}^{\mathrm{Gal}(\overline{k}/k_r)}, \quad \left(\!\binom{V}{n}\!\right)(k_r) = \left(\!\binom{V(\overline{k})}{n}\!\right)^{\mathrm{Gal}(\overline{k}/k_r)}, \ \forall r \geq 1.$$

La varietat $\left(\!\!\left(\begin{smallmatrix} V \\ n \end{smallmatrix}\right)\!\!\right)$ es pot identificar a la varietat $(V\times \overset{n)}{\cdots} \times V)/S_n$, producte simètric de V amb ella mateixa n vegades, i la varietat $\binom{V}{n}$ es pot identificar amb l'obert de $\left(\!\!\left(\begin{smallmatrix} V \\ n \end{smallmatrix}\right)\!\!\right)$ format pels n-conjunts que no presenten repeticions. De fet, $\binom{V}{n}$ és el lloc no-singular de $\left(\!\!\left(\begin{smallmatrix} V \\ n \end{smallmatrix}\right)\!\!\right)$, ja que és fàcil comprovar que una S_n-òrbita de $V\times \overset{n)}{\cdots} \times V$ és singular en el quocient per l'acció de S_n si i només si hi ha repeticions entre els punts.

En aquest capítol volem calcular el nombre de punts k-racionals d'aquestes dues varietats. Denotem aquests nombres:

$$a_V(n) := \left|\binom{V}{n}(k)\right| = \left|\binom{V(\overline{k})}{n}^G\right|, \quad \bar{a}_V(n) := \left|\left(\!\!\left(\begin{smallmatrix} V \\ n \end{smallmatrix}\right)\!\!\right)(k)\right| = \left|\left(\!\!\left(\begin{smallmatrix} V(\overline{k}) \\ n \end{smallmatrix}\right)\!\!\right)^G\right|.$$

Convindrem sempre en què $a_V(0) = 1 = \bar{a}_V(0)$.

Veurem en primer lloc com aquests nombres $a_V(n)$, $\bar{a}_V(n)$ estan determinats per la funció zeta $Z(V/k, x)$ de V. Després utilitzarem aquesta relació per donar fórmules explícites per a $a_V(n)$ per a $V = \mathbb{A}^N$, $\mathbb{P}^N$ i certes subvarietats seves.

En alguns casos també calcularem la funció zeta de la varietat $\binom{V}{n}$.

Revisió de la funció zeta

La funció zeta de V/k és una sèrie formal en una indeterminada:

$$\mathrm{Z}(V/k, x) = \exp\left(\sum_{r\geq 1} \frac{N_r}{r} x^r\right),$$

on $N_r := N_r(V) := |V(k_r)|$. Es tracta d'un objecte global que codifica la informació que es pugui desprendre dels nombres N_r de punts racionals de V sobre les diferents extensions de k.

Aquesta sèrie, que d'entrada pertany a $\mathbb{Q}[\![x]\!]$, té sempre coeficients enters i admet una expressió com a quocient de dos polinomis amb coeficients enters.

Veiem alguns exemples de funcions zeta. Per a $V = \mathbb{A}^N$, tenim $N_r = q^{Nr}$ i:

$$\log\, \mathrm{Z}(\mathbb{A}^N/k, x) = \sum_{r\geq 1} \frac{(q^N x)^r}{r} = -\log(1 - q^N x),$$

de manera que:

$$\mathrm{Z}\left(\mathbb{A}^N/k, x\right) = \frac{1}{1-q^N x}.$$

Amb el mateix raonament obtenim:

$$\mathrm{Z}\left((\mathbb{A}^N - \{*\})/k, x\right) = \frac{1-x}{1-q^N x},$$

$$\mathrm{Z}\left(\mathbb{P}^N/k, x\right) = \frac{1}{(1-x)(1-qx)\cdots(1-q^N x)}.$$

Definició 4.1. *Donat $P \in V(\overline{k})$, denotem per:*

$$O_G(P) = \{P, \sigma(P), \sigma^2(P), \dots\},$$

l'òrbita de P sota l'acció del grup de Galois G.

Definim el grau del punt P com: $\deg(P) = |O_G(P)|$. *Equivalentment,* $\deg(P)$ *és el mínim enter r tal que $P \in V(k_r)$.*

Denotarem també:

$$b_r := \frac{1}{r}\left|\{P \in V(\overline{k}) \mid \deg(P) = r\}\right| = \left|\{O_G(P) \mid \deg(P) = r\}\right|.$$

Les famílies $\{N_r\}_{r\geq 1}$ i $\{b_r\}_{r\geq 1}$ es determinen l'una a l'altra. Tenim clarament:

$$N_r = \sum_{d|r} d\, b_d, \tag{13}$$

i, per la fórmula d'inversió de Möbius:

$$b_r = \frac{1}{r}\sum_{d|r} \mu\left(\frac{r}{d}\right) N_d.$$

Aquestes relacions es poden englobar en una expressió de la funció zeta com a producte infinit:

$$Z(V/k) = \prod_{d\geq 1}(1-x^d)^{-b_d}. \tag{14}$$

En efecte, prenent logaritmes als dos costats d'aquesta igualtat, veiem que equival a:

$$\sum_{r\geq 1}\frac{N_r}{r}\,x^r = -\sum_{d\geq 1} b_d \log(1-x^d) = \sum_{d\geq 1} b_d \sum_{e\geq 1}\frac{x^{de}}{e}.$$

Igualant els termes en x^r, aquesta igualtat equival a (13). La identitat (14) permet deduir immediatament que els coeficients de $Z(V/k, x)$ són tots enters. En efecte, recordem que, per a b enter positiu, tenim:

$$(1-x)^{-b} = 1 + \left(\!\!\binom{b}{1}\!\!\right) x + \left(\!\!\binom{b}{2}\!\!\right) x^2 + \cdots + \left(\!\!\binom{b}{r}\!\!\right) x^r + \cdots, \tag{15}$$

on $\left(\!\!\binom{b}{r}\!\!\right) = \binom{b+r-1}{r}$ compta el nombre de combinacions amb repetició de b objectes, agafats de r en r. La identitat (14) també permet expressar la funció zeta d'una manera completament anàloga a la funció zeta de Riemann (que és la funció zeta de l'esquema $\mathrm{Spec}(\mathbb{Z})$):

$$\mathrm{Z}(V/k, x) = \prod_{v \in V} (1 - x^{\deg(v)})^{-1},$$

on ara els $v \in V$ són els punts tancats de V com a esquema.

La funció generadora dels $a_V(n)$, $\bar{a}_V(n)$

D'entrada, és clar que aquests nombres $a_V(n)$, $\bar{a}_V(n)$ estan determinats per la funció zeta de V. En efecte, si pensem un n-conjunt o n-multiconjunt k-definit de V com a una reunió de diferents òrbites galoisianes de diferents graus, arribem a una expressió per a $a_V(n)$, $\bar{a}_V(n)$ que només depèn dels valors $b_1, b_2, \ldots, b_n$:

$$a_V(n) = \sum_{r_1 + 2r_2 + \cdots + nr_n = n} \binom{b_1}{r_1} \binom{b_2}{r_2} \cdots \binom{b_n}{r_n}, \tag{16}$$

$$\bar{a}_V(n) = \sum_{r_1 + 2r_2 + \cdots + nr_n = n} \left(\!\!\binom{b_1}{r_1}\!\!\right) \left(\!\!\binom{b_2}{r_2}\!\!\right) \cdots \left(\!\!\binom{b_n}{r_n}\!\!\right), \tag{17}$$

on $0 \leq r_i$ representa el nombre de G-òrbites de grau i de cada n-conjunt o n-multiconjunt, i entenem que $\binom{b_i}{r_i} = 0$ si $r_i > b_i$. Aquestes expressions no serveixen com a "fórmules explícites" per als $a_V(n)$, $\bar{a}_V(n)$ perquè la seva avaluació és extremament ineficient. De tota manera, ens fa veure que pot ser interesssant considerar les funcions generadores potencials:

$$f_V(x) := 1 + a_V(1)x + a_V(2)x^2 + \cdots + a_V(n)x^n + \cdots,$$

$$\bar{f}_V(x) := 1 + \bar{a}_V(1)x + \bar{a}_V(2)x^2 + \cdots + \bar{a}_V(n)x^n + \cdots,$$

que permeten englobar (16), (17) per a tots els valors de n en identitats:

$$f_V(x) = (1+x)^{b_1}(1+x^2)^{b_2}\cdots(1+x^r)^{b_r}\cdots,$$

$$\bar{f}_V(x) = (1-x)^{-b_1}(1-x^2)^{-b_2}\cdots(1-x^r)^{-b_r}\cdots,$$

les quals, tenint en compte (14), ens permeten deduir relacions que expressen d'una manera prou satisfactòria la dependència dels $a_V(n)$, $\bar{a}_V(n)$ respecte de la funció zeta de V:

Teorema 4.2. *Per a tota varietat k-definida V:*

$$f_V(x) = \mathrm{Z}(V/k,x)/\,\mathrm{Z}(V/k,x^2), \qquad \bar{f}_V(x) = \mathrm{Z}(V/k,x).$$

En la resta del capítol ens limitem a aplicar aquest teorema per obtenir diferents resultats sobre els $a_V(n)$. Per començar, deixem anotat el càlcul explícit de $f_{\mathbb{A}^N}(x)$ i $f_{\mathbb{P}^N}(x)$, que se'n desprèn immediatament:

$$f_{\mathbb{A}^N}(x) = \frac{1-q^Nx^2}{1-q^Nx}, \tag{18}$$

$$f_{\mathbb{P}^N}(x) = \frac{(1-x^2)(1-qx^2)\cdots(1-q^Nx^2)}{(1-x)(1-qx)\cdots(1-q^Nx)}. \tag{19}$$

A la secció 5 utilitzarem aquestes expressions per deduir fórmules explícites per als $a_V(n)$ per a $V = \mathbb{A}^N$, $\mathbb{P}^N$ i certes subvarietats seves.

Una altra conseqüència immediata del Teorema 4.2 és el caràcter multiplicatiu de $f_V(x)$ respecte d'unions disjuntes:

Corol.lari 4.3. *Sigui $W \subseteq V$ una subvarietat (localment tancada) de V, també k-definida, i sigui $U = V \setminus W$ la subvarietat complementària. Aleshores:*

$$f_V(x) = f_W(x)f_U(x). \tag{20}$$

Dem. Tenim clarament $N_r(V) = N_r(W) + N_r(U),\ \forall r \geq 1$, de manera que:

$$\mathrm{Z}(V/k,x) = \mathrm{Z}(W/k,x)\,\mathrm{Z}(U/k,x),$$

i l'afirmació es desprèn automàticament del Teorema 4.2. ■

La relació (20) es tradueix en:

$$a_V(n) = \sum_{e=0}^{n} a_W(e)a_U(n-e), \tag{21}$$

i aquesta relació es podia haver deduït independentment del fet que, essent W k-definida, tenim, per a tot $P \in V(\overline{k})$:

$$O_G(P) \cap W \neq \emptyset \implies O_G(P) \subseteq W,$$

i anàlogament per a U, de manera que tot n-conjunt G-invariant de V s'expressa de manera única com la reunió d'un determinat e-conjunt G-invariant W i un $(n-e)$-conjunt G-invariant de U:

$$\{P_1, \ldots, P_n\} = (\{P_1, \ldots, P_n\} \cap W) \cup (\{P_1, \ldots, P_n\} \cap U)\,.$$

Podem utilitzar la relació (20) per expressar $f_V(x)$ en termes de les funcions generadores d'una estratificació de V; per exemple:

$$f_{\mathbb{P}^N}(x) = f_{\mathbb{A}^N}(x) \cdot f_{\mathbb{A}^{N-1}}(x) \cdots f_{\mathbb{A}^1}(x) \cdot f_{\mathbb{A}^0}(x).$$

I també, per obtenir la funció generadora de certs oberts complementaris de subvarietats lineals. Per exemple,

$$f_{V\setminus\{*\}}(x) = f_V(x) \cdot f_{\{*\}}(x)^{-1} = (1+x)^{-1} \cdot f_V(x), \tag{22}$$

o, si $L \subseteq \mathbb{A}^N$ és un hiperplà,

$$f_{\mathbb{A}^N\setminus L}(x) = f_{\mathbb{A}^N(x)} \cdot f_L(x)^{-1} = f_{\mathbb{A}^N}(x) \cdot f_{\mathbb{A}^{N-1}}(x)^{-1} = \frac{(1-q^N x^2)(1-q^{N-1}x)}{(1-q^N x)(1-q^{N-1}x^2)}. \tag{23}$$

I, a més, un cas que necessitarem més endavant; si L, $L' \subseteq \mathbb{A}^N$ són dos hiperplans no-paral·lels de $\mathbb{A}^N$, amb $N \geq 2$,

$$f_{\mathbb{A}^N\setminus(L\cup L')}(x) = f_{\mathbb{A}^N}(x) \cdot f_{L\cup L'}(x)^{-1} = f_{\mathbb{A}^N}(x) \cdot f_L(x)^{-1} \cdot f_{L'\setminus(L\cap L')}(x)^{-1} =$$

$$= f_{\mathbb{A}^N}(x) \cdot f_{\mathbb{A}^{N-1}}(x)^{-1} \left(\frac{f_{\mathbb{A}^{N-1}}(x)}{f_{\mathbb{A}^{N-2}}(x)}\right)^{-1} = \frac{f_{\mathbb{A}^N}(x) f_{\mathbb{A}^{N-2}}(x)}{f_{\mathbb{A}^{N-1}}(x)^2} =$$

$$= \frac{(1-q^N x^2)(1-q^{N-2}x^2)(1-q^{N-1}x)^2}{(1-q^N x)(1-q^{N-2}x)(1-q^{N-1}x^2)^2}. \tag{24}$$

5 Fórmules explícites

En aquesta secció obtenim fórmules explícites per als $a_V(n)$ per a certes varietats V que ens interessen. Els càlculs són una conseqüència immediata de l'expressió de la funció generadora $f_V(x)$ com a quocient de dos polinomis, obtinguda a la secció anterior.

5.1 Subvarietats de $\mathbb{A}^N$

Proposició 5.1. *Per a tot $N \geq 0$,*

$$a_{\mathbb{A}^N}(n) = \begin{cases} q^{nN}, & \text{si } n \leq 1, \\ q^{nN} - q^{(n-1)N}, & \text{si } n \geq 2. \end{cases}$$

Dem. Apliquem (18):

$$f_{\mathbb{A}^N}(x) = \frac{1 - q^N x^2}{1 - q^N x} = q^{-N} + x + \frac{1 - q^{-N}}{1 - q^N x} = q^{-N} + x + (1 - q^{-N}) \sum_{n \geq 0} q^{Nn} x^n.$$

■

Per a $N = 1$, el valor $a_{\mathbb{A}^1}(n)$ compta el nombre de polinomis mònics i separables de grau n amb coeficients a $\mathbb{F}_q$. L'expressió $a_{\mathbb{A}^1}(n) = q^n - q^{n-1}$, per a $n \geq 2$, es pot trobar a la literatura en diferents llocs [BG01], [LMNX02]. Pensem que la fórmula que recull la Proposició 5.1 per a $N > 1$ és original.

Proposició 5.2. *Per a tot $N \geq 1$,*

$$a_{\mathbb{A}^N \setminus \{*\}}(n) = \frac{q^N - 1}{q^N + 1}(q^{nN} - (-1)^n), \quad \forall n \geq 1.$$

Dem. Apliquem (22):

$$f_{\mathbb{A}^N \setminus \{*\}}(x) = \frac{1 - q^N x^2}{(1 + x)(1 - q^N x)} = 1 + (q^N - 1)\frac{x}{(1 + x)(1 - q^N x)} =$$

$$= 1 + \frac{q^N - 1}{q^N + 1}\left(\frac{-1}{1 + x} + \frac{1}{1 - q^N x}\right),$$

i les dues fraccions dins del parèntesi són de la forma $c/(1-ax)$, amb terme general $c\,a^n$. ■

Per a $N=1$ aquesta fórmula per a $a_{\mathbb{A}^1\setminus\{*\}}(x)$ va ser obtinguda a [LMNX02] seguint un mètode diferent.

Proposició 5.3. *Sigui $L\subseteq\mathbb{A}^N$ un hiperplà. Aleshores:*

$$a_{\mathbb{A}^N\setminus L}(n)=\begin{cases}\dfrac{(q-1)(q^N-1)}{q^{N+1}-1}\left(q^{nN}-q^{n(N-1)/2}\right), & \text{si } 0<n \text{ parell},\\ \dfrac{(q-1)(q^N-1)}{q^{N+1}-1}\left(q^{nN}+\dfrac{q-1}{q^N-1}\,q^{(n+1)(N-1)/2}\right), & \text{si } n \text{ senar}.\end{cases}$$

Dem. Apliquem (23):

$$f_{\mathbb{A}^N\setminus L}(n)=\frac{(1-q^Nx^2)(1-q^{N-1}x)}{(1-q^Nx)(1-q^{N-1}x^2)}=1+(q^N-q^{N-1})\frac{x-x^2}{(1-q^Nx)(1-q^{N-1}x^2)}=$$

$$=1+\frac{q^N-q^{N-1}}{q^{N+1}-1}\left(\frac{q-q^{-(N-1)}}{1-q^Nx}+\frac{-q+q^{-(N-1)}+(q-1)x}{1-q^{N-1}x^2}\right)=$$

$$=1+\frac{q-1}{q^{N+1}-1}\left(\frac{q^N-1}{1-q^Nx}+\frac{1-q^N+(q^N-q^{N-1})x}{1-q^{N-1}x^2}\right).$$

D'altra banda, si descomponem la darrera fracció:

$$\frac{1-q^N+(q^N-q^{N-1})x}{1-q^{N-1}x^2}=\frac{A}{1-q^{(N-1)/2}x}+\frac{B}{1+q^{(N-1)/2}x},$$

tenim:

$$A+B=1-q^N,\quad A-B=q^{(N-1)/2}(q-1),$$

i el terme general d'aquesta fracció és:

$$\begin{cases}(A+B)q^{n(N-1)/2}=(1-q^N)q^{n(N-1)/2}, & \text{si } n \text{ parell},\\ (A-B)q^{n(N-1)/2}=(q-1)q^{(n+1)(N-1)/2}, & \text{si } n \text{ senar}.\end{cases}$$

Això acaba la demostració. ■

Proposició 5.4. *Sigui $W \subseteq \mathbb{A}^2$ la unió de dues rectes no paral·leles del pla afí. Aleshores, per a n parell, $n > 0$, tenim:*

$$a_{\mathbb{A}^2\setminus W}(n) = \frac{(q^4-1)(q-1)^2}{(q^3-1)^2}\left(q^{2n} - q^{n/2}\left(\frac{n}{2}\,\frac{(q^3-1)(q-1)}{q^4-1}+1\right)\right),$$

mentre que, per a n senar, el valor de $a_{\mathbb{A}^2\setminus W}(n)$ és:

$$\frac{(q^4-1)(q-1)^2}{(q^3-1)^2}\left(q^{2n} + q^{(n-1)/2}\left(\frac{n-1}{2}\,\frac{(q^3-1)(q^2-1)}{q^4-1} - \frac{(q-1)(2q^2+q+1)}{q^4-1}\right)\right).$$

Dem. Apliquem (24):

$$f_{\mathbb{A}^2\setminus W}(x) = \frac{(1-q^2x^2)(1-x^2)(1-qx)^2}{(1-q^2x)(1-x)(1-qx^2)^2} = \frac{(1+x)(1-qx)^3(1+qx)}{(1-q^2x)(1-qx^2)^2} =$$

$$= 1 + (q-1)^2\frac{x-q^2x^4}{(1-q^2x)(1-qx^2)^2} = 1 + \frac{q-1}{(q^2+q+1)^2}\cdot\left(\frac{q^3+q^2+q+1}{1-q^2x}+\right.$$

$$\left.+\frac{q(q^2+q+2)(q^2x^3+x^2)-(2q^2+q+1)x-(q^3+q^2+q+1)}{(1-qx^2)^2}\right).$$

Expressem com a suma de fraccions elementals la darrera fracció.

$$\frac{q(q^2+q+2)(q^2x^3+x^2)-(2q^2+q+1)x-(q^3+q^2+q+1)}{(1-qx^2)^2} =$$

$$= \frac{Ax+B}{(1-\sqrt{q}\,x)^2} + \frac{Cx+D}{(1+\sqrt{q}\,x)^2}. \quad (25)$$

El terme general del terme de la dreta és (per (15)):

$$n(A+(-1)^{n-1}C)q^{(n-1)/2} + (n+1)(B+(-1)^nD)q^{n/2}.$$

Ara, de la relació (25) deduïm immediatament:

$$A+C = q^4+q^3+2q^2, \qquad A-C = \frac{\sqrt{q}}{2}(q^3+2q^2+2q+3),$$
$$B+D = -(q^3+q^2+q+1), \qquad B-D = -\frac{1}{2\sqrt{q}}(q^4+q^3+4q^2+q+1).$$

Això permet acabar els càlculs sense més entrebancs. ■

5.2 Espais projectius

Recordem (19):

$$f_{\mathbb{P}^N}(x) = \frac{(1-x^2)(1-qx^2)\cdots(1-q^Nx^2)}{(1-x)(1-qx)\cdots(1-q^Nx)} =$$

$$= \frac{\prod_{0\leq i\leq[\frac{N}{2}]}(1+q^ix)\prod_{1\leq i\leq N,\, i\text{ senar}}(1-q^ix^2)}{\prod_{\frac{N}{2}<i\leq N}(1-q^ix)}.$$

Ara, $f_{\mathbb{P}^N}(x)$ és una funció racional amb una diferència de $N+1$ entre els graus del numerador i del denominador. Per tant,

$$f_{\mathbb{P}^N}(x) = A(x) + \frac{B(x)}{C(x)},\ \deg A(x) = N+1,\ \deg B(x) < \deg C(x).$$

Hi haurà una expressió homogènia per al terme general de la fracció $B(x)/C(x)$, obtinguda en descompondre-la com a suma de fraccions elementals, però els coeficients del polinomi $A(x)$ distorsionaran aquesta expressió genèrica per a $a_{\mathbb{P}^N}(n)$, $n \leq N+1$. També podem observar que el denominador té grau $\lceil\frac{N}{2}\rceil$, de manera que l'expressió genérica per als $a_{\mathbb{P}^N}(n)$ serà de la forma:

$$a_{\mathbb{P}^N}(n) = \sum_{\frac{N}{2}<i\leq N} \lambda_i q^{in},\ \forall n > N+1. \tag{26}$$

No tenim clar que es pugui donar una expressió més compacta per als valors dels $a_{\mathbb{P}^N}(n)$; ens limitarem, doncs, en el que segueix a donar fórmules explícites per als λ_i. Abans, donarem el càlcul complet dels $a_{\mathbb{P}^N}(n)$ per a $N = 1, 2$.

El cas $N = 1$ va ser resolt a [LMNX02], però ara en podem donar una demostració molt més senzilla:

Proposició 5.5.

$$a_{\mathbb{P}^1}(n) = \begin{cases} q+1, & si\ n=1, \\ q^2, & si\ n=2, \\ q^n - q^{n-2}, & si\ n\geq 3 \end{cases}$$

Dem.

$$f_{\mathbb{P}^1}(x) = \frac{(1+x)(1-qx^2)}{1-qx} = x^2 + (1+q^{-1})x + q^{-2} + \frac{1-q^{-2}}{1-qx}.$$

■

Proposició 5.6.

$$a_{\mathbb{P}^2}(n) = \begin{cases} q^2+q+1, & si\ \ n=1, \\ q^4+q^3+q^2, & si\ \ n=2, \\ q^6+q^5+q^4-q^2-q, & si\ \ n=3, \\ \dfrac{(q^4-1)(q^3-1)}{q^6(q-1)}q^{2n}, & si\ \ n\geq 4. \end{cases}$$

Dem.

$$f_{\mathbb{P}^2}(x) = \frac{(1+x)(1+qx)(1-qx^2)}{1-q^2x} =$$
$$= x^3 + \frac{q^3-1}{q^2(q-1)}x^2 + \frac{q^3-1}{q^4(q-1)}x - \frac{(q^4-1)(q^3-1)}{q^6(q-1)} + 1 + \frac{(q^4-1)(q^3-1)}{q^6(q-1)}\frac{1}{1-q^2x}.$$

■

Necessitem també fórmules explícites per als $a_V(n)$, per a

$$V = \mathbb{P}^1 \setminus \{Q, Q'\}, \qquad V = \mathbb{P}^2 \setminus \{Q, Q', Q''\},$$

on $Q \in \mathbb{P}^1(k_2)\setminus\mathbb{P}^1(k)$, $Q \in \mathbb{P}^2(k_3)\setminus\mathbb{P}^2(k)$, respectivament, i Q', Q'' són els conjugats galoisians de Q.

Proposició 5.7. *Per a $V = \mathbb{P}^1 \setminus \{Q, Q'\}$ i tot enter $n > 0$:*

$$a_V(n) = \begin{cases} \dfrac{q+1}{q^2+1}\left(q^{n+1} - q^n + (-1)^{(n-1)/2}(q+1)\right), & si\ \ n\ senar, \\ \dfrac{q^2-1}{q^2+1}\left(q^n - (-1)^{n/2}\right), & si\ \ n\ parell. \end{cases}$$

Dem. Aquesta fórmula es troba a [LMNX02, Lemma 2.1]. De tota manera, ara veiem que és conseqüència immediata del fet que la funció generadora és

$$f_{\mathbb{P}^1\setminus\{Q,Q'\}}(x) = f_{\mathbb{P}^1}(x)(1+x^2)^{-1}.$$

■

Proposició 5.8. *Per a* $V = \mathbb{P}^2 \setminus \{Q, Q', Q''\}$ *i tot enter* $n > 0$*:*

$$a_V(n) = \begin{cases} \dfrac{(q^2+q+1)(q^2+1)}{q^6+1}\,((q^2-1)q^{2n} + (-1)^{(n-1)/3}), & si\ n \equiv 1 \pmod 3, \\ \dfrac{(q^2+q+1)(q^2+1)}{q^6+1}\,((q^2-1)q^{2n} + (-1)^{(n-2)/3}q^2), & si\ n \equiv 2 \pmod 3, \\ \dfrac{(q^2+q+1)(q^4-1)}{q^6+1}\,(q^{2n} - (-1)^{n/3}), & si\ n \equiv 0 \pmod 3. \end{cases}$$

Dem. La funció generadora és:

$$f_V(x) = f_{\mathbb{P}^2}(x)(1+x^3)^{-1} = 1 + (q^2+q+1)\frac{x-x^3}{(1-q^2x)(1+x^3)} =$$

$$= 1 + \frac{q^2+q+1}{q^6+1}\left(\frac{A}{1-q^2x} + \frac{Bx^2+Cx+D}{1+x^3}\right),$$

amb

$$A = q^4 - 1, \quad B = q^2(q^2+1), \quad C = q^2+1, \quad D = -A.$$

■

Tractem finalment el cas N-dimensional. Introduïm una família de constants que depenen de q:

Notació. Per a qualsevol nombre natural r, denotem:

$$\Lambda(r) := (1-q^{-1})(1-q^{-2})\cdots(1-q^{-r}) = q^{-r(r+1)/2}(q-1)(q^2-1)\cdots(q^r-1),$$

si $r \geq 1$, i convenim en considerar $\Lambda(0) = 1$.

Proposició 5.9.

$$a_{\mathbb{P}^N}(n) = \sum_{\frac{N}{2}<i\leq N} \frac{(-1)^{N-i}\Lambda(2i)}{\Lambda(2i-N-1)\Lambda(i)\Lambda(N-i)}\, q^{in-(N-i)(N-i+1)/2}, \quad \forall n > N+1.$$

Dem. Denotem $P(x) = (1-x)(1-qx)\cdots(1-q^N x)$. Volem trobar les úniques constants λ_i que satisfan:

$$\frac{P(x^2)}{P(x)} \in \sum_{i=0}^{N} \frac{\lambda_i}{1-q^i x} + \mathbb{Z}[x].$$

Aquesta relació equival a:

$$P(x^2) \;\in\; \sum_{i=0}^{N} \lambda_i \frac{P(x)}{1-q^i x} \;+\; P(x)\,\mathbb{Z}[x],$$

i, donant el valor $x = q^{-i}$, podem aïllar λ_i:

$$\lambda_i = \frac{P(q^{-2i})}{[P(x)/(1-q^i x)]_{x=q^{-i}}}.$$

Obtenim $\lambda_i = 0$ per a $i = 0, 1, \ldots, \left[\frac{N}{2}\right]$, com ja havíem observat a (26), i:

$$\lambda_i = \left(\prod_{r=0}^{N}(1-q^{r-2i})\right) \Big/ \left(\prod_{s=0,\, s\neq i}^{N}(1-q^{s-i})\right), \quad \frac{N}{2} < i \leq N.$$

El numerador d'aquesta fracció és:

$$\Lambda(2i)/\Lambda(2i-N-1),$$

i el denominador, separant els factors amb $s < i$ dels factors amb $s > i$, el podem expressar com:

$$\prod_{s=0}^{i-1}(1-q^{s-i}) = \Lambda(i), \qquad \prod_{s=i+1}^{N}(1-q^{s-i}) = (-1)^{N-i}\Lambda(N-i)q^{(N-i)(N-i+1)/2}.$$

Si introduïm aquestes expressions en la fórmula (26), acabem la demostració. ■

5.3 Corbes el·líptiques

Tot i que en aquesta memòria només utilitzarem aquestes fórmules explícites per a varietats lineals i els seus complementaris, calcularem $a_E(n)$ per a una corba el·líptica E k-definida, per la curiositat de veure quina mena de fórmules s'obtenen.

La funció zeta d'una corba el·líptica té la forma [Sil86]:

$$\mathrm{Z}(E/k, x) = \frac{1 - tx + qx^2}{(1-x)(1-qx)},$$

on t és un enter que satisfà la desigualtat de Hasse-Weil:

$$|t| \leq 2\sqrt{q},$$

i coincideix amb la traça de l'endomorfisme de Frobenius de E operant sobre el mòdul de Tate de la corba E. Pel Teorema 4.2, tenim, doncs:

$$f_E(x) = \frac{1 - tx + qx^2}{1 - tx^2 + qx^4} f_{\mathbb{P}^1}(x) = \frac{1 - tx + qx^2}{1 - tx^2 + qx^4} \cdot \frac{(1+x)(1-qx^2)}{1-qx} = 1 + N_1 \frac{x - qx^4}{(1 - tx^2 + qx^4)(1-qx)},$$

on $N_1 := N_1(E) = q + 1 - t$ és el nombre $|E(k)|$ de punts k-racionals de la corba. Podem expressar aquesta fracció com:

$$\frac{x - qx^4}{(1 - tx^2 + qx^4)(1-qx)} = \frac{(e+1)x^3 + q^{-1}(e+1)x^2 + (1-qe)x - e}{1 - tx^2 + qx^4} + \frac{e}{1-qx},$$

on $e = (q^2 - 1)/(q^3 + 1 - tq)$.

Siguin π, π' les arrels a $\overline{\mathbb{Q}}$ del polinomi $P(x) = x^2 - tx + q$, i denotem per $K = \mathbb{Q}(\pi)$ el cos quadràtic imaginari (si $|t| < 2\sqrt{q}$) generat per π. A través de l'elecció d'un isomorfisme $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} \simeq K$, podem pensar que π és l'element que es correspon amb l'endomorfisme de Frobenius de E. Tenim, clarament:

$$1 - tx + qx^2 = (1 - \pi x)(1 - \pi' x).$$

Hem de considerar, doncs, una descomposició:

$$\frac{(e+1)x^3 + q^{-1}(e+1)x^2 + (1-qe)x - e}{1 - tx^2 + qx^4} = \frac{A}{1 - \sqrt{\pi}x} + \frac{B}{1 + \sqrt{\pi}x} + \frac{C}{1 - \sqrt{\pi'}x} + \frac{D}{1 + \sqrt{\pi'}x}$$

El terme general d'aquesta fracció és, doncs:

$$A\pi^{n/2} + (-1)^n B\pi^{n/2} + C(\pi')^{n/2} + (-1)^n D(\pi')^{n/2} = \\ = \begin{cases} (A+B)\pi^{n/2} + (C+D)(\pi')^{n/2}, & \text{si } n \text{ parell}, \\ (A-B)\pi^{n/2} + (C-D)(\pi')^{n/2}, & \text{si } n \text{ senar}. \end{cases}$$

El càlcul explícit de A, B, C, D ens dóna:

$$A+B = \frac{q^{-1}(e+1) - \pi e}{\pi - \pi'}, \qquad A-B = \pi^{1/2}\frac{\pi^{-1}(e+1) + 1 - qe}{\pi - \pi'},$$
$$C+D = \frac{q^{-1}(e+1) - \pi' e}{\pi' - \pi}, \qquad C-D = (\pi')^{1/2}\frac{(\pi')^{-1}(e+1) + 1 - qe}{\pi' - \pi}$$

Notació. Per a qualsevol natural r, denotem:

$$t_r := \pi^r + (\pi')^r = t(E_{|k_r}) = q^r + 1 - N_r(E),$$
$$s_r := (\pi^{r+1} - (\pi')^{r+1})/(\pi - \pi') = \pi^r + \pi^{r-1}\pi' + \cdots + \pi(\pi')^{r-1} + (\pi')^r,$$

si $r \geq 1$, i convenim en què $t_0 = s_0 = 1$, $s_{-1} = 0$. Clarament, $t_r, s_r \in \mathbb{Z}$, ja que són enters algebraics invariants per l'acció de galois del cos quadràtic K. Les següents relacions entre aquests nombres són molt fàcils de comprovar (tenint en compte que $\pi + \pi' = t$ i $\pi\pi' = q$):

$$s_r = t_r + qt_{r-2} + q^2 t_{r-4} + \cdots,$$
$$s_r = t_r + qs_{r-2},$$
$$s_r = ts_{r-1} - qs_{r-2},$$

per a tot $r \geq 1$.

Amb aquestes notacions es dedueix immediatament de les consideracions anteriors:

Proposició 5.10. *Considerant $e = (q^2-1)/(q^3+1-qt)$:*

$$a_E(n) = \begin{cases} N_1\left(eq^n + q^{-1}(e+1)s_{(n-2)/2} - es_{n/2}\right), & \textit{si } n \textit{ parell, } n > 0, \\ N_1\left(eq^n + (e+1)s_{(n-3)/2} + (1-qe)s_{(n-1)/2}\right), & \textit{si } n \textit{ senar.} \end{cases}$$

Per exemple, podem calcular fàcilment:

$$a_E(1) = N_1,\ a_E(2) = qN_1,\ a_E(3) = (q^2+t)N_1,\ a_E(4) = q(q^2+t-1)N_1.$$

Els valors s_r són especialment fàcils de calcular per a les corbes el·líptiques supersingulars, és a dir, les que satisfan $p|t$, on p és la característica de k.

Per exemple, si $t = 0$, tenim que $\pi = \sqrt{-q}, \pi' = -\sqrt{-q}$ i:

$$s_r = \begin{cases} 0, & \text{si } r \text{ senar,} \\ (-q)^{r/2}, & \text{si } r \text{ parell,} \end{cases}$$

de manera que, per a les corbes supersingulars amb $t = 0$, tindrem:

$$a_E(n) = N_1 \begin{cases} e(q^n - (-q)^{n/4}), & n \equiv 0 \pmod 4,\ n > 0, \\ eq^n + (1-qe)(-q)^{(n-1)/4}, & n \equiv 1 \pmod 4, \\ eq^n - (e+1)(-q)^{(n-6)/4}, & n \equiv 2 \pmod 4, \\ eq^n + (e+1)(-q)^{(n-3)/4}, & n \equiv 3 \pmod 4. \end{cases}$$

5.4 Funció zeta de la varietat de n-conjunts

A les seccions anteriors hem obtingut resultats sobre el nombre de punts racionals de la varietat $\binom{V}{n}$, amb la idea de variar n i considerar funcions generadores adequades. Aquests resultats no semblen el camí més adequat per calcular $\mathrm{Z}(\binom{V}{n}/k, x)$. En principi, $\mathrm{Z}(\binom{V}{n}/k, x)$ ha de dependre només de $\mathrm{Z}(V/k, x)$, però no està clar com establir una relació entre aquestes dues sèries formals. El Teorema 4.2 ens dóna una relació una mica estrafolària, de l'estil:

$$\prod_{n\geq 1} \mathrm{Z}\left(\binom{V}{n}/k, x^n\right) = \prod_{n\geq 1} \exp\left(\frac{1}{n}\frac{\mathrm{Z}(V/k_n, x^n)}{\mathrm{Z}(V/k_n, x^{2n})}\right),$$

que no sembla tenir cap utilitat.

La idea d'utilitzar descomposicions $V = W \sqcup U$ per expressar $\mathrm{Z}(\binom{V}{n}/k, x)$ en termes de subvarietats tampoc sembla funcionar. La relació (20) (o, equivalentment, la relació (21)) es tradueix en:

$$\mathrm{Z}(\binom{V}{n}/k, x) = \prod_{e=0}^{n} \mathrm{Z}(\binom{W}{e} \times \binom{U}{n-e}/k, x),$$

però aquesta relació tampoc té massa utilitat perquè, en general, és complicat expressar la relació entre la funció zeta d'un producte $X \times Y$ i la funció zeta dels factors. Clarament,

$$b_r(X \times Y) = \prod_{\mathrm{mcm}(e,d)=r} b_d(X) b_e(Y),$$

i no sembla senzill treballar amb aquesta relació.

Ens limitem, doncs, a exhibir el càlcul d'algunes $\mathrm{Z}(\binom{V}{n}/k, x)$ que s'obtenen immediatament de les fórmules explícites de la secció anterior. Per al càlcul de $\mathrm{Z}(\binom{\mathbb{P}^2}{n}/k, x)$ utilitzem la proposició 5.6 i la identitat:

$$\frac{(q^4-1)(q^3-1)}{q^6(q-1)}\, q^{2n} = q^{2n} + q^{2n-1} + q^{2n-2} - q^{2n-4} - q^{2n-5} - q^{2n-6}.$$

Proposició 5.11.

$$\mathrm{Z}(\binom{\mathbb{A}^N}{n}/k, x) = \frac{1 - q^{(n-1)N}x}{1 - q^{nN}x}, \qquad \forall n > 1,$$

$$\mathrm{Z}(\binom{\mathbb{P}^1}{n}/k, x) = \frac{1 - q^{n-2}x}{1 - q^{n}x}, \qquad \forall n > 2,$$

$$\mathrm{Z}(\binom{\mathbb{P}^2}{n}/k, x) = \frac{(1 - q^{2n-6}x)(1 - q^{2n-5}x)(1 - q^{2n-4}x)}{(1 - q^{2n-2}x)(1 - q^{2n-1}x)(1 - q^{2n}x)}, \quad \forall n > 3.$$

Capítol 3

Òrbites de n-conjunts racionals de $\mathbb{P}^N$ per l'acció de PGL_{N+1}

Sigui V una varietat algebraica k-definida i $\Gamma \subseteq \mathrm{Aut}(V)$ un subgrup finit del grup d'automorfismes algebraics k-definits de V. En aquest capítol ens proposem estudiar els nombres:

$$t_V(n) := \left| \Gamma \backslash\backslash \binom{V}{n}(k) \right|,$$

de Γ-òrbites de n-conjunts k-definits de punts de V. Ens interessarem especialment pel cas $V = \mathbb{P}^N$, $\Gamma = \mathrm{PGL}_{N+1}(k)$, i denotarem $t_N(n) := t_{\mathbb{P}^N}(n)$; aquests nombres compten els punts k-valorats del functor $X := \mathrm{PGL}_{N+1} \backslash \mathbb{P}^N$, que no és representable per un esquema, ja que, per a les extensions L de k, l'aplicació natural $X(k) \to X(L)$ no és injectiva en general.

Sota condicions molt generals (per exemple, si V és quasi-projectiva), per a qualsevol $\gamma \in \Gamma$ existeix el quocient:

$$V/\gamma := V/\langle\, \gamma \,\rangle$$

a la categoria de les varietats algebraiques k-definides [Har92]. Per exemple, si $V = \mathrm{Spec}(A)$ és una varietat afí, aleshores el quocient V/γ també és afí i és representat per la varietat $\mathrm{Spec}(A^\gamma)$, que té per anell de coordenades el subanell $A^\gamma \subseteq A$ de les funcions γ-invariants.

Per a $\Gamma = \mathrm{PGL}_2(k)$ i $V = \mathbb{P}^1$, els nombres $t_1(n)$ van ser determinats a [LMNX02], on van ser utilitzats per trobar fórmules explícites per al nombre de corbes hiperel·líptiques k-definides de gènere g fixat. El fet clau que permetia el càlcul dels $t_1(n)$ era que la corba $\mathbb{P}^1/\gamma$ torna a ser isomorfa a $\mathbb{P}^1$ (pel teorema de Lüroth). Aquest fet deixa de ser cert en dimensió superior, com tot especialista en teoria d'invariants sap molt bé. De fet, no costa gaire trobar exemples de superfícies quocient de $\mathbb{A}^2$ i $\mathbb{P}^2$ per l'acció d'un automorfisme lineal, que no són isomorfes a $\mathbb{A}^2$ o $\mathbb{P}^2$, respectivament.

Recordem que el grup $\mathrm{Aff}_N(k)$ de les afinitats k-definides de $\mathbb{A}^N$ està format pels automorfismes de $\mathbb{A}^N$ de la forma:

$$x \mapsto Ax + b, \quad A \in \mathrm{GL}_N(k),\ b \in \mathbb{A}^N(k).$$

A la secció 6 obtenim el resultat clau que permet calcular els $t_V(n)$, per a $V = \mathbb{A}^N$, $\mathbb{P}^N$, i $\Gamma = \mathrm{Aff}_N(k)$, $\mathrm{PGL}_{N+1}(k)$, respectivament. Utilitzant el Lema de Cauchy-Frobenius, el problema es redueix a calcular el nombre de punts fixos del subgrup cíclic generat per un element γ de $\mathrm{Aff}_N(k)$, $\mathrm{PGL}_{N+1}(k)$, respectivament; i això és possible gràcies al fet que les varietats $\mathbb{A}^N/\gamma$ i $\mathbb{P}^N/\gamma$, tot i que en general no són isomorfes a $\mathbb{A}^N$, $\mathbb{P}^N$, respectivament, mantenen la funció zeta d'aquests espais.

Teorema 6.1.

$$\mathrm{Z}\left((\mathbb{A}^N/\gamma)/k, x\right) = \mathrm{Z}(\mathbb{A}^N/k, x),\ \forall \gamma \in \mathrm{Aff}_N(k),$$

$$\mathrm{Z}\left((\mathbb{P}^N/\gamma)/k, x\right) = \mathrm{Z}(\mathbb{P}^N/k, x),\ \forall \gamma \in \mathrm{PGL}_{N+1}(k).$$

Com a conseqüència dels Teoremes 4.2 i 6.1, tenim:

Corol.lari 6.2. *Per a tot $n, N \in \mathbb{N}$, tenim:*

$$\left|\binom{\mathbb{A}^N/\gamma}{n}(k)\right| = \left|\binom{\mathbb{A}^N}{n}(k)\right|,\ \forall \gamma \in \mathrm{Aff}_N(k),$$

$$\left|\binom{\mathbb{P}^N/\gamma}{n}(k)\right| = \left|\binom{\mathbb{P}^N}{n}(k)\right|,\ \forall \gamma \in \mathrm{PGL}_{N+1}(k).$$

A la secció 7 utilitzem aquest resultat per obtenir fórmules explícites per als $t_{\mathbb{A}^2}(n)$ i $t_{\mathbb{P}^2}(n)$, amb l'esperit del capítol 1. També expressarem $t_{\mathbb{P}^2}(7)$ com un polinomi en q, que ara tindrà coeficients enters.

Al capítol següent veurem com aquests resultats ens permeten obtenir una expressió per a la funció generadora dels $t_{\mathbb{A}^N}(n)$ i $t_{\mathbb{P}^N}(n)$ en termes d'un objecte similar a l'índex de cicles de Pólya, a l'estil de [Fri97].

6 Funció zeta del quocient de $\mathbb{P}^N$ per un automorfisme

El nostre objectiu en aquesta secció és provar el Teorema 6.1. Obtindrem la prova mitjançant un recompte explícit del nombre de punts racionals de $\mathbb{A}^N/\gamma$ i $\mathbb{P}^N/\gamma$. Més precisament, el Teorema 6.1 és una conseqüència immediata del següent resultat:

Proposició 6.3. *Per a qualsevol cos finit $k = \mathbb{F}_q$:*

$$|(\mathbb{A}^N/\gamma)(k)| = q^N, \ \forall \gamma \in \mathrm{Aff}_N(k),$$

$$|(\mathbb{P}^N/\gamma)(k)| = \frac{q^{N+1}-1}{q-1}, \ \forall \gamma \in \mathrm{PGL}_{N+1}(k).$$

Provarem primer la Proposició 6.3 per a $\mathbb{A}^N$ i deduirem el resultat sobre $\mathbb{P}^N$ via la relació natural entre $\mathbb{P}^N$ i $\mathbb{A}^{N+1}$.

Seguim denotant per σ l'automorfisme de Frobenius, que és un generador topològic del grup de Galois absolut $G = \mathrm{Gal}(\overline{k}/k)$. Tots els operadors de $\mathrm{Aff}_N(k)$ i $\mathrm{PGL}_N(k)$ commuten amb l'acció de σ pel fet de ser k-definits:

$$\sigma(\gamma(P)) = \gamma^\sigma(\sigma(P)) = \gamma(\sigma(P)).$$

Fixem $\gamma \in \mathrm{Aff}_N(k)$ i denotem $m = \mathrm{ord}(\gamma)$. Volem comptar el cardinal del conjunt:

$$(\mathbb{A}^N/\gamma)(k) = \{O_\gamma(P), P \in \mathbb{A}^N(\overline{k}) \mid \sigma(O_\gamma(P)) = O_\gamma(P)\}.$$

Considerem, per a qualsevol $\rho \in \mathrm{Aff}_N(k)$:

$$C_\rho := \{P \in \mathbb{A}^N(\overline{k}) \mid \sigma(P) = \rho(P)\}$$

La prova del Lema 6.5 mostrarà en particular que aquests conjunts són finits. Al Lema 6.6 veurem a més que tots tenen el mateix cardinal. Fem observar que, en variar ρ, aquests conjunts no són pas disjunts; per exemple, els punts fixos de ρ a $\mathbb{A}^N(k)$ pertanyen a C_{ρ^i}, per a tot $i \geq 1$. Notem també que:

$$P \in C_\rho, \ \gamma\rho = \rho\gamma \ \Rightarrow \ O_\gamma(P) \subseteq C_\rho, \tag{27}$$

ja que:

$$\sigma(\gamma^i(P)) = \gamma^i(\sigma(P)) = \gamma^i\rho(P) = \rho\gamma^i(P).$$

Caracteritzem el fet que una γ-òrbita $O_\gamma(P)$ sigui k-definida de la següent manera:

Lema 6.4. *Siguin $\gamma \in \mathrm{Aff}_N(k)$ una afinitat d'ordre m, i $P \in \mathbb{A}^N(\overline{k})$. La γ-òrbita $O_\gamma(P)$ és k-definida sii existeix $0 \leq i < m$ tal que $\sigma(P) = \gamma^i(P)$ (és a dir, $P \in C_{\gamma^i}$).*

Dem. Si $\sigma(O_\gamma(P)) = O_\gamma(P)$, tenim $\sigma(P) \in O_\gamma(P) = \{P, \gamma(P), \ldots, \gamma^{m-1}(P)\}$.

Recíprocament, $\sigma(P) = \gamma^i(P)$ implica que $\sigma(O_\gamma(P)) = O_\gamma(P)$; en efecte, per a qualsevol enter j, tenim:

$$\sigma(\gamma^j(P)) = \gamma^j(\sigma(P)) = \gamma^{i+j}(P),$$

de manera que $\sigma(O_\gamma(P)) \subseteq O_\gamma(P)$ i com que aquests conjunts finits tenen el mateix cardinal, coincideixen. ■

Lema 6.5.

$$|(\mathbb{A}^N/\gamma)(k)| = \frac{1}{m} \sum_{0 \leq i < m} |C_{\gamma^i}|.$$

Dem. Considerem la unió disjunta (formal) dels C_{γ^i} i establim l'aplicació:

$$\begin{array}{rccc} O_\gamma\colon & \coprod_{0 \leq i < m} C_{\gamma^i} & \longrightarrow & (\mathbb{A}^N/\gamma)(k) \\ & P & \mapsto & O_\gamma(P) \end{array}$$

Pel lema anterior, $O_\gamma(P)$ és k-definida sii $P \in \cup_{0 \leq i < m} C_{\gamma^i}$, de manera que aquesta aplicació està ben definida i és exhaustiva. Per provar el lema només cal veure que cada γ-òrbita $O_\gamma(P)$ k-definida té exactament m antiimatges. Considerem $O_\gamma(P) \in (\mathbb{A}^N/\gamma)(k)$ i sigui $D = |O_\gamma(P)|$; clarament, $D|m$ i, com que $\sigma(P) \in O_\gamma(P) = \{P, \gamma(P), \ldots, \gamma^{D-1}(P)\}$, existeix un únic $0 \leq i < D$ tal que $P \in C_{\gamma^i}$. Per (27), tenim $O_\gamma(P) \subseteq C_{\gamma^i}$, de manera que els D integrants de $O_\gamma(P)$ són les antiimatges de $O_\gamma(P)$ per l'aplicació O_γ restringida a C_{γ^i}. Ara bé, aquests mateixos punts pertanyen també a

$$C_{\gamma^{i+D}}, C_{\gamma i+2D}, \ldots, C_{\gamma^{i+(\frac{m}{D}-1)D}},$$

i a cap altre C_{γ^j}. Per tant, $O_\gamma(P)$ té exactament $D\frac{m}{D} = m$ antiimatges. ■

La primera afirmació de la Proposició 6.3 quedarà provada si veiem:

Lema 6.6.

$$|C_\gamma| = q^N, \ \forall \gamma \in \mathrm{Aff}_N(k).$$

Dem. Posem $\gamma(x) = Ax + b$, amb $A \in \mathrm{GL}_N(k)$, $b \in k^N$. Treballant amb les coordenades adequades, podem suposar que A és una matriu de Jordan (k-racional), és a dir,

$$A = \mathrm{diag}(A_1, \ldots, A_r),$$

on cada A_i és un bloc de Jordan:

$$A_i = \begin{pmatrix} B & & & & & \\ J & B & & & & \\ & J & B & & & \\ & & & \ddots & & \\ & & & & B & \\ & & & & J & B \end{pmatrix} \in \mathrm{GL}_{N_i}(k), \tag{28}$$

on B, J són matrius de la forma:

$$B = \begin{pmatrix} 0 & & & & -a_s \\ 1 & 0 & & & -a_{s-1} \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & -a_2 \\ & & & 1 & -a_1 \end{pmatrix}, \qquad J = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix}, \tag{29}$$

amb $x^s + a_1 x^{s-1} + \cdots + a_s$ polinomi irreductible a $k[x]$, que depèn de A_i. La component A_i és semisimple només quan $N_i = s$ i $A_i = B$.

Si trenquem els punts de $\mathbb{A}^N$ (treballant en les noves coordenades) en:

$$x = (x_1, x_2, \ldots, x_r),\ x_i \in k^{N_i},\ N_1 + \cdots + N_r = N,$$

l'acció de γ descompon:

$$\gamma(x) = (A_1 x_1 + b_1, \ldots, A_r x_r + b_r).$$

(De fet, podríem suposar $b_i = 0$ sempre que la matriu B del bloc A_i sigui $B \neq (1) \in GL_1(k)$, però no farem ús d'aquesta remarca.)

Ara, la condició $\gamma(x) = \sigma(x)$ equival a:

$$A_i x_i + b_i = \sigma(x_i),\ i = 1, \ldots, r,$$

de manera que podem reduir la prova al cas en què A és un bloc de Jordan. Un cop feta aquesta suposició, si A pren la forma considerada a (28), amb $N = ts$, trencant els punts de $\mathbb{A}^N$ en coordenades:

$$x = (x_1, \ldots, x_t),\ x_i \in k^s,$$

tenim:

$$\gamma(x) = (Bx_1 + b_1, Jx_1 + Bx_2 + b_2, \ldots, Jx_{i-1} + Bx_i + b_i, \ldots, Jx_{t-1} + Bx_t + b_t),$$

de manera que la igualtat $\gamma(x) = \sigma(x)$ es tradueix en:

$$\begin{aligned} Bx_1 + b_1 &= \sigma(x_1), \\ Bx_2 + (b_2 + Jx_1) &= \sigma(x_2), \\ \cdots\cdots & \cdots \\ Bx_t + (b_t + Jx_{t-1}) &= \sigma(x_t). \end{aligned} \tag{30}$$

Veiem, doncs, que podem reduir la prova al cas de l'afinitat $\gamma(x) = Bx + b$; perquè sabríem aleshores que a la primera equació de (30) hi ha q^t possibilitats per a x_1, per a cadascun d'aquests possibles valors de x_1 la segona equació té q^t possibilitats per a x_2, etc.

Així, doncs, suposem d'ara endavant que $N = s$ i $\gamma(x) = Bx + b$, amb B donada per (29). Denotem per $f(x) = x^N + a_1 x^{N-1} + \cdots + a_N$ el polinomi característic de B, que és irreductible a $k[x]$ per hipòtesi. Si $N = 1$ i $B = (1)$, la relació $\gamma(x) = \sigma(x)$ es tradueix en $x^q = x + b$, aquesta equació té q arrels a $\overline{k}$ i l'afirmació del lema és correcta. Llevat del cas d'una traslació 1-dimensional, la nostra afinitat γ tindrà punts fixos k-definits i, prenent-ne un d'ells com a origen de coordenades, podem suposar $b = 0$. En aquest cas, la relació $\gamma(x) = \sigma(x)$ es tradueix en:

$$\begin{aligned} -a_N x_N &= \sigma(x_1), \\ x_1 - a_{N-1} x_N &= \sigma(x_2), \\ \cdots\cdots & \cdots \\ x_{N-1} - a_1 x_N &= \sigma(x_N). \end{aligned} \tag{31}$$

Es comprova immediatament que les $N - 1$ darreres relacions equivalen a:

$$\begin{aligned} x_{N-1} &= a_1 x_N + \sigma(x_N), \\ \cdots & \cdots\cdots \\ x_{N-i} &= a_i x_N + a_{i-1}\sigma(x_N) + \cdots + a_1 \sigma^{i-1}(x_N) + \sigma^i(x_N), \\ \cdots & \cdots\cdots \\ x_1 &= a_{N-1} x_N + a_{N-2}\sigma(x_N) + \cdots + a_1 \sigma^{N-2}(x_N) + \sigma^{N-1}(x_N). \end{aligned}$$

i, un cop expressades les $N - 1$ primeres coordenades com a una combinació lineal de x_N i els seus conjugats galoisians, la primera equació de (31) equival a:

$$\sigma^N(x_N) + a_1 \sigma^{N-1}(x_N) + \cdots + a_{N-1}\sigma(x_N) + a_N x_N = 0.$$

Aquesta equació és un polinomi separable de grau q^N i té, per tant, q^N solucions a $\overline{k}$. ■

Un cop resolt el cas de $\mathbb{A}^N$, podem acabar la prova de la Proposició 6.3 deduint l'afirmació sobre el nombre de punts k-racionals de $\mathbb{P}^N/\gamma$ de l'afirmació anàloga per a $\mathbb{A}^{N+1}$.

Considerem $\gamma \in \mathrm{PGL}_{n+1}(k)$ i fem una elecció d'un representant de γ a $\mathrm{GL}_{N+1}(k)$, que continuarem denotant per γ. Tenim un morfisme natural de varietats algebraiques:

$$\pi : (\mathbb{A}^{N+1}/\gamma) \setminus \{0\} \longrightarrow \mathbb{P}^N/\gamma,$$

induït pel morfisme natural $\mathbb{A}^{N+1} \setminus \{0\} \longrightarrow \mathbb{P}^N$.

Notem que $\{0\}$ es refereix a la γ-òrbita formada exclusivament per l'origen de $\mathbb{A}^{N+1}$, que és un punt fix de γ.

És evident que punts de la mateixa γ-òrbita a $\mathbb{A}^{N+1}$ van a parar a punts de la mateixa γ-òrbita a $\mathbb{P}^N$. De tota manera, fem observar que aquestes γ-òrbites tenen, en general, longituds diferents; per exemple, si $P \in \mathbb{A}^{N+1}$ és un vector propi de γ, de valor propi $\lambda \in k^*$, tenim:

$$|O_\gamma(P)| = \mathrm{ord}_{k^*}(\lambda) \quad (\text{a } \mathbb{A}^{N+1}), \qquad |O_\gamma(P)| = 1 \quad (\text{a } \mathbb{P}^N).$$

Per distingir l'òrbita projectiva de l'afí, denotarem (només en aquest paràgraf) la primera per $O_\gamma^{\mathrm{pr}}(P)$.

Lema 6.7. *La següent aplicació natural és exhaustiva:*

$$(\mathbb{A}^{N+1}/\gamma)(k) \setminus \{0\} \longrightarrow (\mathbb{P}^N/\gamma)(k).$$

Dem. Considerem $O_\gamma^{\mathrm{pr}}(P) \in (\mathbb{P}^N/\gamma)(k)$. Fent una elecció de coordenades homogènies per a P, podem escriure $P = (x_0, \ldots, x_N)$ amb:

$$\sigma(P) = \lambda\gamma^i(P),$$

per a alguns $\lambda \in k^*$ i $0 \leq i < m$. Per comprovar l'exhaustivitat de l'aplicació seria suficient veure que, per a alguna altra elecció de coordenades homogènies, tenim la mateixa relació amb $\lambda = 1$; aleshores, pel Lema 6.4, el mateix punt, pensat com a punt de $\mathbb{A}^{N+1} \setminus \{0\}$, donarà lloc a una γ-òrbita k-definida de $\mathbb{A}^{N+1} \setminus \{0\}$, que es projecta sobre la nostra γ-òrbita projectiva fixada.

Volem, doncs, comprovar que existeix $\mu \in \overline{k}^*$ tal que $\tilde{P} := \mu P$ (pensat com a punt afí) satisfà $\sigma(\tilde{P}) = \gamma^i(\tilde{P})$. Com que:

$$\sigma(\tilde{P}) = \sigma(\mu)\sigma(P) = \sigma(\mu)\lambda\gamma^i(P) = \sigma(\mu)\lambda\mu^{-1}\gamma^i(\tilde{P}),$$

volem que $\lambda^{-1} = \sigma(\mu)\mu^{-1} = \mu^{q-1}$. L'existència d'aquest $\mu \in \overline{k}^*$ està, doncs, garantida. ■

Ens falta controlar quantes antiimatges té cada γ-òrbita projectiva per l'aplicació del Lema 6.7. En general, per a qualssevol P, $Q \in \mathbb{A}^{N+1}(\overline{k}) \setminus \{0\}$, tenim:

$$\pi(O_\gamma(P)) = \pi(O_\gamma(Q)) \Leftrightarrow \exists i \in \mathbb{N},\ \exists \mu \in \overline{k}^* :\ Q = \mu\gamma^i(P) \Leftrightarrow$$
$$\Leftrightarrow \exists \mu \in \overline{k}^* :\ O_\gamma(Q) = \mu O_\gamma(P) = O_\gamma(\mu P).$$

Per a qualsevol $P \in \mathbb{A}^{N+1}(\overline{k}) \setminus \{0\}$, considerem el següent subgrup de $\overline{k}^*$:

$$\Lambda_P := \{\lambda \in \overline{k}^* \mid \lambda O_\gamma(P) = O_\gamma(P)\}.$$

Genèricament, tindrem $\Lambda_P = \{1\}$. En tot cas, Λ_P és un subgrup multiplicatiu finit de $\overline{k}^*$ i, per tant, és cíclic.

Lema 6.8. *Sigui $P \in \mathbb{A}^{N+1}(\overline{k}) \setminus \{0\}$ tal que $O_\gamma(P)$ és k-definida. Aleshores:*

a) $\Lambda_P \leq k^*$.

b) Per a tot $\mu \in \overline{k}^*$, tenim:

$$O_\gamma(\mu P) \text{ és } k\text{-definida } \Leftrightarrow \frac{\sigma(\mu)}{\mu} \in \Lambda_P.$$

Dem. Sigui $\lambda \in \Lambda_P$. Per hipòtesi, existeixen $i, j \in \mathbb{N}$ tals que:

$$\sigma(P) = \gamma^i(P), \quad \lambda P = \gamma^j(P).$$

D'aquí deduïm:

$$\lambda\sigma(P) = \lambda\gamma^i(P) = \gamma^i(\lambda P) = \gamma^{i+j}(P) = \gamma^j(\sigma(P)) =$$
$$= \sigma(\gamma^j(P)) = \sigma(\lambda P) = \sigma(\lambda)\sigma(P),$$

de manera que $\lambda = \sigma(\lambda)$, i, per tant, $\lambda \in k^*$. Això prova a). Pel que fa a b), per a qualsevol $\mu \in \overline{k}^*$, tenim:

$$\sigma(O_\gamma(\mu P)) = \sigma(\mu O_\gamma(P)) = \sigma(\mu)\sigma(O_\gamma(P)) = \sigma(\mu)O_\gamma(P),$$

i això coincideix amb $O_\gamma(\mu P) = \mu O_\gamma(P)$ si i només si $\sigma(\mu)\mu^{-1}O_\gamma(P) = O_\gamma(P)$. ■

El següent resultat clou la prova de la Proposició 6.3:

Lema 6.9. *A través de l'aplicació:*

$$(\mathbb{A}^{N+1}/\gamma)(k) \setminus \{0\} \longrightarrow (\mathbb{P}^N/\gamma)(k),$$

cada element de $(\mathbb{P}^N/\gamma)(k)$ té $q-1$ antiimatges.

Dem. Sigui $P \in \mathbb{A}^{N+1}(\overline{k}) \setminus \{0\}$ tal que $O_\gamma(P)$ és k-definida. Volem veure que entre les infinites òrbites $O_\gamma(\mu P)$, amb $\mu \in \overline{k}^*$, n'hi ha exactament $q-1$ que són k-definides.

Pel Lema 6.8, Λ_P és un subgrup de k^*. Sigui $e = |\Lambda_P|$. Pel Lema 6.8, hi ha exactament $e(q-1)$ valors de $\mu \in \overline{k}^*$ per als quals l'òrbita $O_\gamma(\mu P)$ és k-definida. (En efecte: per a cada $\lambda \in \Lambda_P$ cal considerar les $q-1$ solucions de l'equació:

$$\mu^{q-1} = \sigma(\mu)\mu^{-1} = \lambda.)$$

Finalment, entre aquests $e(q-1)$ valors de μ, tenim:

$$O_\gamma(\mu P) = O_\gamma(\mu' P) \Leftrightarrow \mu'\mu^{-1} \in \Lambda_P \Leftrightarrow \mu' \in \mu\Lambda_P,$$

de manera que per a cada valor de μ n'hi ha e que donen lloc a la mateixa òrbita afí. Per tant, obtenim $q-1$ òrbites diferents. ■

7 Fórmules explícites per als $t_2(n)$

Per simplicitat, denotem $\Gamma = \mathrm{PGL}_3(k)$ i:

$$\mathcal{X}_V(n) := \binom{V}{n}(k), \qquad \mathcal{X}(n) := \binom{\mathbb{P}^2}{n}(k).$$

Com hem vist al Capítol 1, podem comptar els $t_V(n) := |\Gamma \backslash\backslash \mathcal{X}_V(n)|$ pel Lema de Cauchy-Frobenius:

$$t_V(n) = \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma} |\mathcal{X}_{V,\gamma}(n)| = \sum_{\gamma\in\mathcal{C}} \frac{|\mathcal{X}_{V,\gamma}(n)|}{|\Gamma_\gamma|},$$

on $\mathcal{X}_{V,\gamma}(n) = \{x \in \mathcal{X}_V(n) \mid \gamma(x) = x\}$, Γ_γ és el centralitzador de γ dins Γ i $\mathcal{C}$ és un sistema de representants de classes de conjugació de Γ.

Qüestió. *Per a $\Gamma = \mathrm{PGL}_3(k)$ i $V = \mathbb{P}^2$, al capítol 1 hem dividit el conjunt $\mathcal{C} = \coprod_\alpha \mathcal{C}_\alpha$ en "subtipus", que agrupaven les projectivitats $\gamma \in \mathcal{C}$ que tenien el mateix tipus de cicle actuant com a permutació de $\mathbb{P}^2(k)$.*

Depèn $|\mathcal{X}_\gamma(n)| := |\mathcal{X}_{\mathbb{P}^2,\gamma}(n)|$ només del subtipus de γ?

En cas afirmatiu, podríem aplicar la fórmula universal que hem obtingut al capítol 1 i tindríem una fórmula de l'estil:

$$t_2(n) = \sum_\alpha N_\alpha x_\alpha(n), \tag{32}$$

on $x_\alpha(n) := |\mathcal{X}_\gamma(n)|$ per a tot $\gamma \in \mathcal{C}_\alpha$.

Ara, un element $x \in \mathcal{X}_\gamma(n)$ és una unió k-definida d'òrbites projectives $O_\gamma(P)$, amb $P \in \mathbb{P}^2(\overline{k})$. Cada òrbita $O_\gamma(P)$ és un cicle de γ com a permutació de $\mathbb{P}^2(\overline{k})$, de manera que $|\mathcal{X}_\gamma(n)|$ depèn del subtipus de γ sobre les diferents extensions finites de k.

La qüestió anterior es tradueix, doncs, en: determina el subtipus de γ sobre k el subtipus de γ sobre totes les extensions finites k_r? La resposta és: per a γ dels tipus III, IV, V, sí; però per a γ dels tipus I, II no està clar, d'entrada. En efecte, es comprova immediatament que, per a γ dels tipus III, IV ó V, la configuració de punts fixos i rectes invariants de γ (cf. Taula 1 del Capítol 1) i els exponents d'aquestes rectes invariants són dades que no canvien en considerar γ com a un element dels diferents $\mathrm{PGL}_3(k_r)$; en canvi, si γ és del tipus I, aleshores passa a ser del tipus III a les extensions k_r, amb $3|r$, i, si γ és del tipus II, passa a ser del tipus III, a les extensions k_r, amb $2|r$.

No obstant això, veurem a continuació que, amb petites modificacions, podem salvar l'esperit de la fórmula universal del Capítol 1 i trobar una fórmula molt similar a (32).

Abans de procedir a calcular $x_\alpha(n)$ cas per cas, deixem anotada una observació crucial, que utilitzarem constantment en el que segueix, i que és una conseqüència immediata del Corol·lari 6.2:

Corol.lari 7.1. *Siguin $V = \mathbb{A}^N$ (resp. $V = \mathbb{P}^N$), $\gamma \in \mathrm{Aff}_N(k)$ (resp. $\gamma \in \mathrm{PGL}_{N+1}(k)$) i $W \subsetneq V$ una subvarietat lineal γ-invariant amb la propietat que, sobre l'obert $U := V \setminus W$ tots els punts $\overline{k}$-racionals tenen la γ-òrbita de la mateixa longitud, $m = \mathrm{ord}(\gamma)$. Aleshores,*

$$|\mathcal{X}_{U,\gamma}(mn)| = |\mathcal{X}_U(n)|.$$

Dem. Un mn-conjunt γ-invariant i σ-invariant de U es correspon biunívocament amb un n-conjunt σ-invariant de U/γ i, pel Corol.lari 6.2, $|\mathcal{X}_{U/\gamma}(n)| = |\mathcal{X}_U(n)|$. ■

7.1 Càlcul dels $|\mathcal{X}_\gamma(n)|$

Càlcul de $|\mathcal{X}_\gamma(n)|$ per a γ del tipus V

Per a $\gamma = 1$, tenim $|\mathcal{X}_1(n)| = a_{\mathbb{P}^2}(n)$, que ha estat calculat a la Proposició 5.6.

Per a $\gamma = \gamma_V$, la recta L_2 té tots els seus punts fixos i fora d'ella totes les γ-òrbites tenen cardinal p (vegeu la Taula 1).

Com que L_2 és γ-invariant i σ-invariant, un n-conjunt γ-invariant i σ-invariant es reparteix necessàriament en un n_0-conjunt γ-invariant i σ-invariant dins la recta

L_2 i un pn_1-conjunt γ-invariant i σ-invariant fora de la recta L_2, amb $n_0 + pn_1 = n$. Tenim, doncs,

$$|\mathcal{X}_\gamma(n)| = \sum_{n_0+pn_1=n} |\mathcal{X}_{L_2}(n_0)||\mathcal{X}_{(\mathbb{P}^2\setminus L_2),\gamma}(pn_1)|.$$

Identificant L_2 amb $\mathbb{P}^1$ i $\mathbb{P}^2 \setminus L_2$ amb $\mathbb{A}^2$, γ es restringeix a una afinitat de $\mathbb{P}^2 \setminus L_2$. Pel corol·lari 7.1, tenim:

$$|\mathcal{X}_\gamma(n)| = \sum_{n_0+pn_1=n} |\mathcal{X}_{\mathbb{P}^1}(n_0)||\mathcal{X}_{\mathbb{A}^2}(n_1)|. \tag{33}$$

Per a $\gamma = \gamma'_V$, tenim un únic punt fix P_3 i una única recta invariant L_1, d'exponent p. Fora de L_1, les γ-òrbites tenen cardinal

$$m = \mathrm{ord}(\gamma) = \begin{cases} p, & \text{si } p \text{ senar,} \\ 4, & \text{si } p = 2. \end{cases}$$

Els n-conjunts γ-invariants i k-definits es reparteixen entre $\{P_3\} \cup (L_1 \setminus \{P_3\}) \cup (\mathbb{P}^2 \setminus L_1)$. Identificant $\{P_3\} = \mathbb{A}^0$, $L_1 \setminus \{P_3\} = \mathbb{A}^1$ i $\mathbb{P}^2 \setminus L_1 = \mathbb{A}^2$, obtenim, raonant com abans:

$$|\mathcal{X}_\gamma(n)| = \sum_{\substack{n_0 + pn_1 + mn_2 = n, \\ 0 \le n_0 \le 1}} |\mathcal{X}_{\mathbb{A}^1}(n_1)||\mathcal{X}_{\mathbb{A}^2}(n_2)|. \tag{34}$$

Podem introduir la funció generadora:

$$F_\gamma(x) := \sum_{n\ge 1} |\mathcal{X}_\gamma(n)| x^n,$$

i les fórmules anteriors es reinterpreten com:

$$\begin{aligned} F_1(x) &= f_{\mathbb{P}^2}(x), \\ F_{\gamma_V}(x) &= f_{\mathbb{P}^1}(x) f_{\mathbb{A}^2}(x^p), \\ F_{\gamma'_V}(x) &= f_{\mathbb{A}^0}(x) f_{\mathbb{A}^1}(x^p) f_{\mathbb{A}^2}(x^m). \end{aligned}$$

Càlcul de $|\mathcal{X}_\gamma(n)|$ per a γ del tipus IV

Per a γ del tipus IV', tenim $L_1 \cup \{P_1\}$ com a conjunt de punts fixos i, fora d'aquest conjunt, totes les γ-òrbites tenen cardinal $m = \mathrm{ord}(\gamma)$. Raonant com abans, obtenim:

$$|\mathcal{X}_\gamma(n)| = \sum_{\substack{n_0+n_1+mn_2=n,\\ 0\le n_0\le 1}} |\mathcal{X}_{\mathbb{P}^1}(n_1)||\mathcal{X}_{\mathbb{A}^2\setminus\{*\}}(n_2)|, \tag{35}$$

amb funció generadora:

$$F_\gamma(x) = (1+x) f_{\mathbb{P}^1}(x) f_{\mathbb{A}^2\setminus\{*\}}(x^m).$$

Per a γ del tipus IV'', tenim P_1, P_3 com a punts fixos, L_1, L_2 com a rectes invariants, d'exponent respectiu p i d (un divisor de $q-1$). Fora de $L_1 \cup L_2$, totes les γ-òrbites tenen cardinal pd. Tenim:

$$|\mathcal{X}_\gamma(n)| = \sum_{\substack{n_0+pn_1+dn_2+pdn_3=n,\\ 0\le n_0\le 2}} \binom{2}{n_0} |\mathcal{X}_{\mathbb{A}^1}(n_1)||\mathcal{X}_{\mathbb{A}^1\setminus\{*\}}(n_2)||\mathcal{X}_{\mathbb{A}^2\setminus L}(n_3)|, \tag{36}$$

on L representa una recta de $\mathbb{A}^2$. La funció generadora és:

$$F_\gamma(x) = (1+x)^2 f_{\mathbb{A}^1}(x^p) f_{\mathbb{A}^1\setminus\{*\}}(x^d) f_{\mathbb{A}^2\setminus L}(x^{pd}).$$

Càlcul de $|\mathcal{X}_\gamma(n)|$ per a γ del tipus III

Per a γ del tipus III, tenim P_1, P_2, P_3 com a punts fixos i L_1, L_2, L_3 com a rectes invariants, d'exponents respectius d, e, f. Fora de $L_1 \cup L_2 \cup L_3$, les γ-òrbites tenen cardinal $m = \mathrm{mcm}(d,e,f)$. Obtenim

$$|\mathcal{X}_\gamma(n)| = \sum_{\substack{n_0+fn_1+en_2+dn_3+mn_4=n,\\ 0\le n_0\le 3}} \binom{3}{n_0} |\mathcal{X}_{\mathbb{A}^1\setminus\{*\}}(n_1)||\mathcal{X}_{\mathbb{A}^1\setminus\{*\}}(n_2)||\mathcal{X}_{\mathbb{A}^1\setminus\{*\}}(n_3)||\mathcal{X}_{\mathbb{A}^2\setminus W}(n_4)|, \tag{37}$$

on W representa la unió de dues rectes no paral·leles de $\mathbb{A}^2$. La funció generadora és:

$$F_\gamma(x) = (1+x)^3 f_{\mathbb{A}^1\setminus\{*\}}(x^f) f_{\mathbb{A}^1\setminus\{*\}}(x^e) f_{\mathbb{A}^1\setminus\{*\}}(x^d) f_{\mathbb{A}^2\setminus W}(x^m).$$

Càlcul de $|\mathcal{X}_\gamma(n)|$ per a γ del tipus II

Per a γ del tipus II, tenim una configuració diferent de punts fixos, rectes invariants i exponents, sobre els diferents cossos k_r, segons r sigui parell o senar. Per a r senar, tenim P_1 com a únic punt fix, L_1 com a única recta invariant, d'exponent d (un divisor de $q+1$), determinat per:

$$d = \min\{s \in \mathbb{N} \mid \alpha^s \in k\},$$

on $\alpha \in k_2 \setminus k$ és una arrel del factor quadràtic irreductible que divideix el polinomi característic de γ. Fora de $L_1 \cup \{P_1\}$ les γ-òrbites tenen cardinal $m = de = \mathrm{ord}_{k_2^*}(\alpha)$, on $e = \mathrm{ord}_{k^*}(\alpha^d)|(q-1)$.

Per a r parell, γ és conjugada a $\mathrm{diag}(1, \alpha, \alpha')$, on $\alpha' \in k_2 \setminus k$ és l'arrel conjugada de α. Per tant, és del tipus III i té tres punts fixos P_1, Q, Q', on Q, Q' són k_2-definits i conjugats galoisians (les direccions dels vectors propis de $\mathbb{A}^3$ de valors propis α, α') i tres rectes invariants L_1, L, L', on L, L' són també k_2-definides i conjugades galoisianes l'una de l'altra. L'exponent de L_1 continua sent d, mentre que l'exponent de L, L' és $m = de = \mathrm{ord}_{k_2^*}(\alpha) = \mathrm{ord}_{k_2^*}(\alpha')$.

Per tant, fora de $L_1 \cup \{P_1\}$ tenim sempre γ-òrbites de longitud m i només dins L_1 hem de tenir en compte l'existència de la γ-òrbita k-definida $\{Q, Q'\}$. Deixant que $0 \leq n_1 \leq 1$ indiqui si considerem $x \in \mathcal{X}_\gamma(n)$ contenint $\{Q, Q'\}$ ($n_1 = 1$) o no ($n_1 = 0$), obtenim:

$$|\mathcal{X}_\gamma(n)| = \sum_{\substack{n_0 + 2n_1 + dn_2 + mn_3 = n, \\ 0 \leq n_0, n_1 \leq 1}} |\mathcal{X}_{L_1 \setminus \{Q,Q'\},\gamma}(dn_2)||\mathcal{X}_{\mathbb{P}^2 \setminus (L_1 \cup \{P_1\}),\gamma}(mn_3)|,$$

i, aleshores, pel Corol·lari 7.1, tenim:

$$|\mathcal{X}_\gamma(n)| = \sum_{\substack{n_0 + 2n_1 + dn_2 + mn_3 = n, \\ 0 \leq n_0, n_1 \leq 1}} |\mathcal{X}_{\mathbb{P}^1 \setminus \{Q,Q'\}}(n_2)||\mathcal{X}_{\mathbb{A}^2 \setminus \{*\}}(n_3)|, \tag{38}$$

on continuem denotant per Q, Q' un parell qualsevol de punts k_2-definits tals que el 2-conjunt $\{Q,\ Q'\}$ és k-definit. La funció generadora dels $|\mathcal{X}_\gamma(n)|$ és:

$$F_\gamma(x) = (1+x)(1+x^2) f_{\mathbb{P}^1 \setminus \{Q,Q'\}}(x^d) f_{\mathbb{A}^2 \setminus \{*\}}(x^m).$$

Càlcul de $|\mathcal{X}_\gamma(n)|$ per a γ del tipus I

Per a γ del tipus I i k_r amb $3 \nmid r$, no hi ha punts fixos ni rectes invariants, i tota γ-òrbita té cardinal $m|q^2+q+1$, on $m = \min\{s \in \mathbb{N} \mid \alpha^s \in k\}$, sent $\alpha \in k_3 \setminus k$ una arrel del polinomi característic de γ.

En canvi, si $3|r$, γ és conjugada a $\mathrm{diag}(\alpha, \alpha', \alpha'')$ i és del tipus III, amb tres punts fixos Q, Q', Q'' (les tres direccions a $\mathbb{A}^3(k_3)$ dels vectors propis de valor propi respectiu α, α', α'') i tres rectes invariants L, L', L'', que són les rectes que s'obtenen unint Q, Q', Q'' de dos en dos. De tota manera, l'exponent d'aquestes tres rectes és m, i, per tant, fora de la terna $\{Q, Q', Q''\}$, que és γ-invariant i k-definida, les γ-òrbites continuen tenint totes cardinal m. Tenim, per tant:

$$|\mathcal{X}_\gamma(n)| = \sum_{\substack{3n_0 + mn_1 = n,\\ 0 \leq n_0 \leq 1}} |\mathcal{X}_{\mathbb{P}^2\setminus\{Q,Q',Q''\}}(n_1)|, \tag{39}$$

on $\{Q, Q', Q''\}$ és qualsevol terna k-definida amb Q, Q', Q'' no-alineats i k_3-definits, però no k-definits. La funció generadora és:

$$F_\gamma(x) = (1 + x^3) f_{\mathbb{P}^2\setminus\{Q,Q',Q''\}}(x^m).$$

En conclusió, podem respondre afirmativament a la qüestió plantejada a l'inici de la secció: els valors $|\mathcal{X}_\gamma(n)|$ depenen només del subtipus de γ, ja que aquest determina tots els paràmetres que descriuen les fórmules (33), (34), (35), (36), (37), (38) i (39). En els tipus III, IV i V l'expressió per a $|\mathcal{X}_\gamma(n)|$ depèn només del tipus de cicle de γ actuant com a permutació de $\mathbb{P}^2(k)$, i en els tipus I i II intervé també l'acció de γ sobre $\mathbb{P}^2(k_2)$ o $\mathbb{P}^2(k_3)$, però aquesta acció també està determinada pel subtipus de γ. Finalment, doncs, la fórmula (32) té sentit.

No obstant, veurem al capítol següent que això deixa de ser cert en dimensió superior.

7.2 Enumeració dels 7-conjunts racionals del pla

A la secció anterior hem expressat tots els valors $|\mathcal{X}_\gamma(n)|$ en termes dels nombres $a_V(n)$, per a certes subvarietats V del pla. En tots els casos, a la secció 5 hem trobat fórmules explícites per a aquests $a_V(n)$. Això ens permet obtenir fórmules explícites per als $t_2(n)$ en la forma de polinomis en q, que en aquesta ocasió tindran coeficients enters. A l'estil de la secció 3.1, explicitem ara aquestes fórmules en el cas $n = 7$. Recordem que $t_2(7)$ compta el nombre de 7-conjunts racionals del pla, classificats sota l'acció del grup lineal.

Tipus I

Recordem que

$$Z_I = \{m \in \mathbb{Z} \mid m|q^2 + q + 1,\ m > 1\}, \quad N_I(m) = \frac{\varphi(m)}{3(q^2 + q + 1)}.$$

Apliquem (39). Els únics parells $(n_0,\, n_1)$ satisfent:

$$3n_0 + m\, n_1 = 7, \qquad 0 \le n_0 \le 1, \qquad m \in Z_I,$$

són $(n_0,\, n_1) = (0, 1)$, quan $m = 7$ divideix $q^2 + q + 1$. El cas $(n_0,\, n_1) = (1, 1)$ amb $m = 4$ no es pot donar ja que $q^2 + q + 1$ és sempre senar. Denotant $x_I(m) := |\mathcal{X}_\gamma(7)|$ per a γ del subtipus $m \in Z_I$, i aplicant (39):

$$\sum_{m \in Z_I} N_I(m) x_I(m) = \left[\frac{\varphi(7)}{3(q^2+q+1)} (q^2+q+1) \right]_{7 | q^2+q+1} = [2]_{7 | q^2+q+1}\,.$$

Tipus II

Recordem que $Z_{II} = \{(de, d) \in \mathbb{Z}^2 \mid d | (q+1),\ d > 1,\ e | (q-1),\ e \ge 1\}$,

$$N_{II}(de, d) = \begin{cases} \dfrac{\varphi(d)\varphi(e)}{2(q^2-1)}, & \text{si } d \text{ senar}, \\ 0, & \text{si } d \text{ parell i } e | \frac{q-1}{2}, \\ \dfrac{\varphi(d)\varphi(e)}{q^2-1}, & \text{si } d \text{ parell i } e \nmid \frac{q-1}{2}. \end{cases}$$

Apliquem (38). Considerem famílies d'enters no-negatius $(n_0,\, n_1,\, n_2,\, n_3)$ satisfent:

$$n_0 + 2n_1 + d\, n_2 + de\, n_3 = 7, \qquad 0 \le n_0,\, n_1 \le 1, \qquad (de, d) \in Z_{II}.$$

Com que $n_0 + 2n_1 \le 3$, a la força $(n_2,\, n_3) \ne (0, 0)$ i, per tant, $d \le 7$. Estudiem els casos $d = 2, 3, 4, 5, 6, 7$ un per un.

Suposem $d = 7$. Tenim les següents possibilitats per a $(n_0,\, n_1,\, n_2,\, n_3)$:

$$(n_0,\, n_1,\, n_2,\, n_3) = (0, 0, 0, 1),\ e = 1, \qquad (n_0,\, n_1,\, n_2,\, n_3) = (0, 0, 1, 0),\ e \ge 1.$$

Denotem $x_{II}(m, d) := |\mathcal{X}_\gamma(7)|$ per a γ del subtipus $(m, d) \in Z_{II}$. Aplicant (38), obtenim una contribució a la suma (10) de:

$$\frac{\varphi(7)}{2(q^2-1)} \left[q^2 - 1 + \sum_{e | (q-1)} \varphi(e)(q+1) \right]_{7 | q+1} = [6]_{7 | q+1}\,.$$

Suposem $d = 6$. Com que d és parell i $d|(q+1)$, forçosament q és senar; d'altra banda, necessàriament $e > 1$ per a tot enter $e \nmid (q-1)/2$. Per tant, l'única possibilitat és $(n_0,\, n_1,\, n_2,\, n_3) = (1, 0, 1, 0)$. Per (38) aquest cas contribueix a la suma (10) en:

$$\frac{\varphi(6)}{q^2-1} \sum_{e|(q-1),\ e\nmid(q-1)/2} \varphi(e)(q+1) = [1]_{6|q+1}\,,$$

on hem aplicat el Lema 3.3 per calcular aquest sumatori.

Suposem $d = 5$. Tenim les següents possibilitats per a $(n_0,\, n_1,\, n_2,\, n_3)$:

$$(0,1,0,1),\ e=1, \qquad (0,1,1,0),\ e \geq 1,$$

que, per (38), contribueixen a la suma (10) en:

$$\frac{\varphi(5)}{2(q^2-1)} \left[q^2 - 1 + \sum_{e|(q-1)} \varphi(e)(q+1) \right]_{5|q+1} = [4]_{5|q+1}\,.$$

El cas $d = 4$ és idèntic al cas $d = 6$. Necessàriament $(n_0,\, n_1,\, n_2,\, n_3) = (1, 1, 1, 0)$, que contribueix en:

$$\frac{\varphi(4)}{q^2-1} \sum_{e|(q-1),\ e\nmid(q-1)/2} \varphi(e)(q+1) = [1]_{4|q+1}\,.$$

Per a $d = 3$ tenim les següents possibilitats per a $(n_0,\, n_1,\, n_2,\, n_3)$:

$$(1,0,2,0),\ e \geq 1, \qquad (1,0,0,2),\ e=1, \qquad (1,0,1,1),\ e=1, \qquad (1,0,0,1),\ e=2,$$

que, per (38) i les fórmules explícites de la secció 5, contribueixen:

$$\frac{\varphi(3)}{2(q^2-1)} \left[\sum_{e|(q-1)} \varphi(e)(q^2-1) + (q^2-1)^2 + (q+1)(q^2-1) + \left[q^2-1\right]_{2|q-1} \right]_{3|q+1} =$$
$$= \left[q^2+2q-1\right]_{3|q+1} + [1]_{3|q+1,\,p>2}\,.$$

Finalment, si $d = 2$ tornem a tenir e parell, $e > 1$, com en el cas $d = 6$, i les següents possibilitats per a $(n_0,\, n_1,\, n_2,\, n_3)$:

$(1,0,3,0),\ e\geq 1, \qquad (1,0,1,1),\ e=2, \qquad (1,1,2,0),\ e\geq 1, \qquad (1,1,0,1),\ e=2.$

Agrupem els casos amb $e\geq 1$ i els casos amb $e=2$ per separat. Apliquem (38), el Lema 3.3 i les fórmules explícites de la secció 5, per obtenir una contribució respectivament de:

$$\frac{1}{q^2-1}\left[\sum_{e|(q-1),\ e\nmid (q-1)/2}\varphi(e)\left((q+1)(q^2-q-1)+q^2-1\right)\right]_{2|q+1}=\left[\frac{q^2-2}{2}\right]_{2|q+1},$$

$$\frac{1}{q^2-1}\left[(q+1)(q^2-1)+q^2-1\right]_{4|q+1}=[q+2]_{4|q+1}\,.$$

Tipus III

Recordem que

$$Z_{III}=\{(d,e,f)\in\mathbb{Z}^3\mid d\geq e\geq f>1,\\ m:=\mathrm{mcm}(d,e)=\mathrm{mcm}(d,f)=\mathrm{mcm}(e,f)|(q-1)\},$$

$$N_{III}(d,e,f)=\begin{cases}\dfrac{\varphi(m)\psi(m)}{6(q-1)^2}, & \text{si } d=e=f=m,\\ \dfrac{\varphi(m)\varphi(h)\psi(H)}{2(q-1)^2}, & \text{si } d=e=m>f,\\ \dfrac{\varphi(m)\varphi(h)\psi(H)}{(q-1)^2}, & \text{si } d>e>f.\end{cases}$$

Apliquem (37). Considerem famílies d'enters no-negatius $(n_0,\,n_1,\,n_2,\,n_3,\,n_4)$ satisfent:

$$n_0+f\,n_1+e\,n_2+d\,n_3+m\,n_4=7, \qquad 0\leq n_0\leq 3, \qquad (d,e,f)\in Z_{III}.$$

Tenim necessàriament: $\{d,\,e,\,f\}\cap\{2,\,3,\,4,\,5,\,6,\,7\}\neq\emptyset$.

Suposem que un dels tres divisors d, e ó f val 7. En el cas $d=e=f=7$, tenim $m=7$ i tots els punts $\overline{k}$-racionals del pla, excepte els 3 punts fixos, s'agrupen en 7-òrbites invariants. En aquest cas, en comptes d'aplicar (37), és més rendible aplicar directament el Corol·lari 7.1 per obtenir una contribució a la suma (10) de:

$$\left[\frac{\varphi(7)\psi(7)}{6(q-1)^2}\, a_{\mathbb{P}^2\setminus\{P_1,P_2,P_3\}}(1)\right]_{7|q-1} = \left[\frac{5}{(q-1)^2}(q^2+q-2)\right]_{7|q-1} = \left[\frac{5(q+2)}{q-1}\right]_{7|q-1}.$$

En la resta dels casos, tenim $m > 7$ i hi ha una única recta d'exponent 7. Aplicant el Lema 3.4 i el Corol·lari 7.1, podem comptar la contribució dels 7-conjunts invariants continguts en aquesta recta:

$$\sum_{(d,e,f)\in Z^7_{III}} N_{III}(d,e,f)x_{III}(d,e,f) = \sum_{(d,e,f)\in Z^7_{III}} N_{III}(d,e,f)a_{\mathbb{A}^1\setminus\{*\}}(1) =$$

$$= \left[\frac{6(q-8)}{2(q-1)^2}\,(q-1)\right]_{7|q-1} = \left[\frac{3(q-8)}{q-1}\right]_{7|q-1}.$$

Com hem fet a la secció 3.1, comptarem més endavant les altres possibilitats que es presenten en els casos $e = 7 > f > 1$.

Suposem ara que un dels tres divisors d, e ó f val 6. Com fèiem a la secció 3.1, considerem independentment els casos $(6,6,3)$ i $(6,3,2)$.

En el cas $(6,3,2)$ tenim $m = 6$, $def/m^2 = 1$, $N_{III}(6,3,2) = 2/(q-1)^2$. Deixem per als casos $2,\, 3 \in \{d,\, e,\, f\}$ el recompte de la contribució de les següents possibilitats per a $(n_0,\, n_1,\, n_2,\, n_3,\, n_4)$:

$$(1,3,0,0,0), \qquad (1,0,2,0,0), \qquad (3,2,0,0,0).$$

Comptem ara només la contribució de:

$$(1,0,0,1,0), \qquad (1,0,0,0,1), \qquad (2,1,1,0,0), \qquad (0,2,1,0,0). \tag{40}$$

Agrupem els dos primers casos. Els punts $\overline{k}$-racionals de $\mathbb{P}^2 \setminus (L \cup L')$ s'agrupen tots en 6-òrbites invariants. Pel Corol·lari 7.1 tenim una contribució de:

$$\frac{\varphi(6)}{(q-1)^2}\left[3\, a_{\mathbb{P}^2\setminus(L\cup L')}(1)\right]_{6|q-1} = \frac{2}{(q-1)^2}\left[3(q^2-q)\right]_{6|q-1} = \left[\frac{6q}{q-1}\right]_{6|q-1}.$$

Aplicant (37) i la proposició 5.2, els altres dos casos de (40) contribueixen amb:

$$\frac{\varphi(6)}{(q-1)^2}\left[3\,(q-1)^2 + (q-1)^2(q-1)\right]_{6|q-1} = [2q+4]_{6|q-1}.$$

En el cas $(6,6,3)$ tenim $m = 6$, $def/m^2 = H = 3$, $N_{III}(6,6,3) = 1/(q-1)^2$. El cas $(n_0,\, n_1,\, n_2,\, n_3,\, n_4) = (1,2,0,0,0)$ serà comptat quan considerem $3 \in \{d,\, e,\, f\}$. La resta de possibilitats són:

$$(1,0,1,0,0), \qquad (1,0,0,1,0), \qquad (1,0,0,0,1).$$

Es poden unificar pensant que a $\mathbb{P}^2 \setminus (L \cup \{P\})$ tots els punts $\overline{k}$-racionals s'agrupen en 6-òrbites invariants. Aplicant el Corol·lari 7.1 tenim una contribució de:

$$\frac{1}{(q-1)^2}\left[3\, a_{\mathbb{P}^2\setminus(L\cup\{P\})}(1)\right]_{6|q-1} = \frac{1}{(q-1)^2}\left[3\,(q^2-1)\right]_{6|q-1} = \left[\frac{3(q+1)}{q-1}\right]_{6|q-1}.$$

La resta de casos es recull a la Taula 3 de la secció 3.1. En tots ells, $m > 6$ i hi ha una única recta invariant d'exponent 6 (en els casos $(6,6,6)$ i $(6,6,2)$ tenim $N_{III} = 0$). Pel corol·lari 7.1 la contribució és:

$$\sum_{(d,e,f)\neq(6,6,3),\,(6,3,2)} N_{III}(d,e,f)\, 3\, a_{\mathbb{A}^1\setminus\{*\}}(1) = \left[\frac{3(q-7)}{q-1}\right]_{6|q-1},$$

on hem utilitzat el càlcul (11) que hem fet a la secció 3.1 de $\sum N_{III}(d,e,f)$, quan el sumatori s'estén als casos recollits en la Taula 3.

El cas en que $5 \in \{d,\, e,\, f\}$ és completament anàleg al cas en que $7 \in \{d,\, e,\, f\}$. Comptarem només l'aportació dels 7-conjunts invariants que consten de dos punts fixos i un 5-conjunt invariant. En el cas $(5,5,5)$ tenim $m = 5$ i una contribució:

$$\left[\frac{\varphi(5)\psi(5)}{6(q-1)^2}\, 3\,(q^2+q-2)\right]_{5|q-1} = \left[\frac{6(q+2)}{q-1}\right]_{5|q-1}.$$

En la resta de casos tenim $m > 5$ i hi ha una única recta d'exponent 5. Pel Lema 3.4 tenim una contribució de:

$$\sum_{(d,e,f)\in Z^5_{III}} N_{III}(d,e,f)\, 3\, a_{\mathbb{A}^1\setminus\{*\}}(1) = \left[\frac{4(q-6)}{2(q-1)^2}\, 3(q-1)\right]_{5|q-1} = \left[\frac{6(q-6)}{q-1}\right]_{5|q-1}.$$

La contribució extra del cas excepcional $(10,5,2)$ és:

$$\frac{\varphi(10)}{(q-1)^2}\left[(q-1)(q-1)\right]_{10|q-1} = [4]_{10|q-1}.$$

Suposem ara $4 \in \{d,\, e,\, f\}$. En el cas $(4,4,2)$, es té $m = 4$, $def/m^2 = 2 = h$, $N_{III}(4,4,2) = 1/(q-1)^2$. La contribució de $(n_0,\, n_1,\, n_2,\, n_3,\, n_4) = (1,3,0,0,0)$, $(3,2,0,0,0)$ la deixem per al cas en que $2 \in \{d,\, e,\, f\}$. La resta de possibilitats són:

$$\begin{array}{lll} (1,1,1,0,0), & (1,1,0,1,0), & (1,1,0,0,1), \\ (3,0,1,0,0), & (3,0,0,1,0), & (3,0,0,0,1). \end{array} \tag{41}$$

Unifiquem les tres primeres en la situació de considerar 7-conjunts formats per un punt fix, un 2-conjunt a l'única recta d'exponent 2 i un 4-conjunt a $\mathbb{P}^2 \setminus (L \cup \{P\})$. Pel Corol·lari 7.1 contribueixen en:

$$\frac{1}{(q-1)^2}\left[3\,(q-1)(q^2-1)\right]_{4|q-1} = [3q+3]_{4|q-1}\,.$$

Unifiquem les tres darreres possibilitats de (41) considerant 7-conjunts formats pels 3 punts fixos i un 4-conjunt invariant a $\mathbb{P}^2\setminus(L\cup\{P\})$. Pel Corol·lari 7.1 contribueixen en:

$$\frac{1}{(q-1)^2}\left[(q^2-1)\right]_{4|q-1} = \left[\frac{q+1}{q-1}\right]_{4|q-1}.$$

En la resta de casos, recollits a la Taula 4 de la secció 3.1, tenim $m > 4$ i i hi ha una única recta d'exponent 4. Contribueixen amb:

$$\sum_{(d,e,f)\neq(4,4,2)} N_{III}(d,e,f)\, a_{\mathbb{A}^1\setminus\{*\}}(1) = \left[\frac{q-5}{q-1}\right]_{4|q-1},$$

on hem utilitzat el càlcul (12) que hem fet a la secció 3.1 de $\sum N_{III}(d,e,f)$, quan el sumatori s'estén als casos recollits en la Taula 4.

Ens queda el cas $(12,4,3)$, on també poden haver 7-conjunts invariants partits en una tripleta i una quarteta invariant. Cal afegir $[4]_{12|q-1}$ als termes calculats fins ara.

Anem al cas $3 \in \{d,\, e,\, f\}$. Comptem la contribució del cas $(3,3,3)$ apart. Pel Corol·lari 7.1, el nombre de parells de 3-conjunts invariants de $\mathbb{P}^2 \setminus \{P_1,P_2,P_3\}$ coincideix amb $a_{\mathbb{P}^2\setminus\{P_1,P_2,P_3\}}(2)$. Aquest valor el podem obtenir descomptant de $a_{\mathbb{P}^2}(2)$ (calculat a la Proposició 5.6) tots els parells de punts k-racionals que involucren algun dels tres punts P_1, P_2, P_3:

$$a_{\mathbb{P}^2\setminus\{P_1,P_2,P_3\}}(2) = a_{\mathbb{P}^2}(2) - 3 - 3(q^2+q-2) = q^4+q^3-2q^2-3q+3.$$

Ara ja podem comptabilitzar la contribució del cas $(3,3,3)$:

$$\left[\frac{1}{3(q-1)^2}\,3\,a_{\mathbb{P}^2\setminus\{P_1,P_2,P_3\}}(2)\right]_{3|q-1} =$$
$$= \left[\frac{1}{(q-1)^2}(q^4+q^3-2q^2-3q+3)\right]_{3|q-1} = \left[q^2+3q+3\right]_{3|q-1}.$$

En la resta de casos tenim $m>3$ i hi ha una única recta d'exponent 3. Pel Lema 3.4 tenim una contribució de:

$$\sum_{(d,e,f)\in Z^3_{III}} N_{III}(d,e,f)\,3\,a_{\mathbb{A}^1\setminus\{*\}}(2) = [3(q-4)]_{3|q-1}.$$

Finalment, considerem el cas $2\in\{d,\,e,\,f\}$. Com que $N_{III}(2,2,2)=0$, el cas $(2,2,2)$ no aporta res. En la resta de casos es té $m>2$ i hi ha una única recta invariant d'exponent 2. La contribució de diverses possibilitats dels casos $(14,7,2)$, $(6,6,2)$, $(10,5,2)$, $(4,4,2)$, $(6,3,2)$ ja s'han comptat; l'única aportació que queda per comptar és la de tres parells invariants a la recta d'exponent 2 i un punt fix, o bé dos parells invariants en aquesta recta i 3 punts fixos. Pel Lema 3.4 i el Corol·lari 7.1, aquests casos contribueixen amb:

$$\sum_{(d,e,f)\in Z^2_{III}} N_{III}(d,e,f)\left(3\,a_{\mathbb{A}^1\setminus\{*\}}(3)+a_{\mathbb{A}^1\setminus\{*\}}(2)\right) =$$
$$= \left[\frac{q-3}{2(q-1)^2}\left(3(q-1)(q^2-q+1)+(q-1)^2\right)\right]_{2|q-1} =$$
$$= \left[\frac{(q-3)(3q^2-2q+2)}{2(q-1)}\right]_{2|q-1}.$$

Tipus IV

Recordem que $Z_{IV}=\{d\in\mathbb{Z}\mid d|(q-1),\ d>1\}$, $m=d$,

$$N'_{IV}(d)=\frac{\varphi(d)}{q(q-1)^2(q+1)},\quad N''_{IV}(d)=\frac{\varphi(d)}{q(q-1)}.$$

Atenent a (35), per tractar el tipus IV' hem de considerar tripletes $(n_0,\,n_1,\,n_2)$ satisfent:

$$n_0 + n_1 + d\,n_2 = 7, \qquad 0 \le n_0 \le 1, \qquad d \in Z_{IV}.$$

Atenent al nombre de punts fixos dels 7-conjunts, tenim les següents possibilitats per a $(n_0,\, n_1,\, n_2)$:

$$\begin{array}{lll}
(0,7,0),\ (1,6,0), & d \text{ arbitrari} & 7 \text{ punts fixos,} \\
(0,5,1),\ (1,4,1), & d = 2 & 5 \text{ punts fixos,} \\
(0,4,1),\ (1,3,1), & d = 3 & 4 \text{ punts fixos,} \\
\left.\begin{array}{ll} (0,3,1),\ (1,2,1), & d = 4 \\ (0,3,2),\ (1,2,2), & d = 2 \end{array}\right\} & & 3 \text{ punts fixos,} \\
(0,2,1),\ (1,1,1), & d = 5 & 2 \text{ punts fixos,} \\
\left.\begin{array}{ll} (0,1,1),\ (1,0,1), & d = 6 \\ (0,1,2),\ (1,0,2), & d = 3 \\ (0,1,3),\ (1,0,3), & d = 2 \end{array}\right\} & & 1 \text{ punt fix,} \\
(0,0,1), & d = 7 & 0 \text{ punts fixos.}
\end{array}$$

Agrupant els casos en funció del valor de d i aplicant (35), tenim contribucions respectives de:

$$\frac{1}{q(q-1)^2(q+1)} \left(\sum_{d|q-1,\, d>1} \varphi(d)\,(a_{\mathbb{P}^1}(7) + a_{\mathbb{P}^1}(6)) \right) = \\ = \frac{(q-2)(q^7+q^6-q^5-q^4)}{q(q-1)^2(q+1)} = \frac{q^3(q-2)(q+1)}{q-1},$$

$$\frac{\varphi(2)}{q(q-1)^2(q+1)}(q^2-1)\cdot \\ \cdot \left[(q^5+q^4-q^3-q^2) + (q^2-1)(q^3+q^2-q) + (q^4-q^2+1)(q+2)\right]_{2|q-1} = \\ = \left[\frac{3q^5+4q^4-4q^3-4q^2+2q+2}{q(q-1)}\right]_{2|q-1},$$

$$\frac{\varphi(3)}{q(q-1)^2(q+1)} \left[(q^2-1)(q^4+q^3-q^2-q) + (q^2-1)^2(q+2)\right]_{3|q-1} = \\ = \left[\frac{2(q^3+3q^2+4q+2)}{q}\right]_{3|q-1},$$

$$\frac{\varphi(4)}{q(q-1)^2(q+1)}\,[(q^2-1)(q^3+q^2-q)]_{4|q-1} = \left[\frac{2(q^2+q-1)}{q-1}\right]_{4|q-1},$$

$$\frac{\varphi(5)}{q(q-1)^2(q+1)}\,[(q^2-1)(q^2+q+1)]_{5|q-1} = \left[\frac{4(q^2+q+1)}{q(q-1)}\right]_{5|q-1},$$

$$\frac{\varphi(6)}{q(q-1)^2(q+1)}\,[(q^2-1)(q+2)]_{6|q-1} = \left[\frac{2(q+2)}{q(q-1)}\right]_{6|q-1},$$

$$\frac{\varphi(7)}{q(q-1)^2(q+1)}\,[q^2-1]_{7|q-1} = \left[\frac{6}{q(q-1)}\right]_{7|q-1}.$$

Atenent a (36), per tractar el tipus IV'' considerem quartetes (n_0, n_1, n_2, n_3) satisfent:

$$n_0 + p\,n_1 + d\,n_2 + pd\,n_3 = 7, \qquad 0 \le n_0 \le 2, \qquad d \in Z_{IV}.$$

Si imposem $n_1 = n_3 = 0$, tenim les següents possibilitats, genèriques en p:

$$(0,0,1,0),\ d=7; \qquad (1,0,1,0),\ d=6; \qquad (2,0,1,0),\ d=5;$$

$$(1,0,2,0),\ d=3; \qquad (1,0,3,0),\ d=2.$$

La contribució d'aquests casos és:

$$\frac{1}{q(q-1)}\Big([\varphi(7)(q-1)]_{7|q-1} + [2\varphi(6)(q-1)]_{6|q-1} + [\varphi(5)(q-1)]_{5|q-1} +$$

$$+ \left[2\varphi(3)(q-1)^2\right]_{3|q-1} + \left[2\varphi(2)(q-1)(q^2-q+1)\right]_{2|q-1}\Big) =$$

$$= \frac{1}{q}\left([6]_{7|q-1} + [4]_{6|q-1} + [4]_{5|q-1} + [4(q-1)]_{3|q-1} + \left[2(q^2-q+1)\right]_{2|q-1}\right).$$

Considerem ara les possibilitats corresponents a $n_1 n_3 \neq 0$, que es donen només per a $p \in \{2,\ 3,\ 5,\ 7\}$. Les possibilitats per a $(n_0,\ n_1,\ n_2,\ n_3)$ són:

$$
\begin{array}{lll}
(0,1,0,0), & & p=7,\ d \text{ arbitrari},\\
(2,1,0,0), & & p=5,\ d \text{ arbitrari},\\
(0,1,1,0), & & p=5,\ d=2,\\
(1,2,0,0), & & p=3,\ d \text{ arbitrari},\\
(2,1,1,0), & (0,1,2,0), \ (1,0,0,1), & p=3,\ d=2,\\
(0,1,1,0), & & p=3,\ d=4,\\
(1,3,0,0), & & p=2,\ d \text{ arbitrari},\\
(2,1,1,0), & (0,2,1,0), \ (1,0,0,1), & p=2,\ d=3,\\
(0,1,1,0), & & p=2,\ d=5.
\end{array}
$$

Comptem primer els casos en què d és arbitrari:

$$
\frac{1}{q(q-1)} \sum_{d|q-1, d>1} \varphi(d) \left([q]_{7|q} + [q]_{5|q} + \left[2(q^2-q)\right]_{3|q} + \left[2(q^3-q^2)\right]_{2|q} \right) =
$$

$$
= \left[\frac{q-2}{q-1}\right]_{7|q} + \left[\frac{q-2}{q-1}\right]_{5|q} + [2(q-2)]_{3|q} + [2q(q-2)]_{2|q}\,.
$$

La resta de casos contribueixen a la suma (10) amb:

$$
\frac{1}{q(q-1)} \Big([q(q-1)]_{5|q} +
$$

$$
+ [\varphi(4) q(q-1)]_{3|q,\,4|q-1} + \left[q(q-1) + q(q-1)^2 + 2(q^2-q)\right]_{3|q} +
$$

$$
+ [\varphi(5) q(q-1)]_{2|q,\,5|q-1} + \varphi(3) \left[(q^2-q)(q-1) + q(q-1) + 2(q^2-q)\right]_{2|q,\,3|q-1} \Big) =
$$

$$
= [1]_{5|q} + [2]_{3|q,\,4|q-1} + [q+2]_{3|q} + [4]_{2|q,\,5|q-1} + [2q+4]_{2|q,\,3|q-1}\,.
$$

Tipus V

Recordem que

$$
N_V = \frac{1}{q^3(q-1)}, \qquad N'_V = \frac{1}{q^2}, \qquad N_1 = \frac{1}{q^3(q-1)^2(q^2+q+1)(q+1)}.
$$

Atenent a (33), per tractar el cas γ_V hem de considerar parells $(n_0,\, n_1)$ satisfent: $n_0 + p\, n_1 = 7$. El cas $(n_0,\, n_1) = (7, 0)$ és genèric en p i aporta a la suma (10) una contribució de:

$$\frac{1}{q^3(q-1)}(q^7 - q^5) = q^2(q+1).$$

La resta de possibilitats són:

$$\begin{array}{llll} (0,1), & p=7 & (2,1), & p=5, \\ (1,2),\ (4,1), & p=3 & (1,3),\ (3,2), (5,1), & p=2, \end{array}$$

i la seva contribució és:

$$\begin{aligned} &\frac{1}{q^3(q-1)}\Big(\big[q^2\big]_{7|q} + \big[q^2\cdot q^2\big]_{5|q} + \big[(q+1)(q^4-q^2) + (q^4-q^2)q^2\big]_{3|q} + \\ &\quad + \big[(q+1)(q^6-q^4) + (q^3-q)(q^4-q^2) + (q^5-q^3)q^2\big]_{2|q}\Big) = \left[\frac{1}{q(q-1)}\right]_{7|q} + \\ &\qquad + \left[\frac{q}{q-1}\right]_{5|q} + \left[\frac{(q+1)(q^2+q+1)}{q}\right]_{3|q} + \big[(q+1)(3q^2+q-1)\big]_{2|q}\,. \end{aligned}$$

Atenent a (34), per tractar el cas γ'_V considerem tripletes (n_0, n_1, n_2) satisfent:

$$n_0 + p\, n_1 + m\, n_2 = 7, \quad 0 \le n_0 \le 1, \quad m = p \text{ (resp. } m = 4\text{), si } p > 2 \text{ (resp. } p = 2\text{).}$$

Les possibilitats per a $(n_0,\, n_1,\, n_2)$ són:

$$\begin{array}{ll} (0,1,0),\ (0,0,1), & p=7, \\ (1,2,0),\ (1,0,2),\ (1,1,1), & p=3, \\ (1,3,0),\ (1,1,1), & p=2, \end{array}$$

i la seva contribució és:

$$\begin{aligned} &\frac{1}{q^2}\Big(\big[q^2+q\big]_{7|q} + \big[(q^2-q) + (q^4-q^2) + q\cdot q^2\big]_{3|q} + \big[(q^3-q^2+q\cdot q^2\big]_{2|q}\Big) = \\ &\qquad = \left[\frac{q+1}{q}\right]_{7|q} + \left[\frac{q^3+q^2-1}{q}\right]_{3|q} + \big[2q-1\big]_{2|q}\,. \end{aligned}$$

Finalment, la contribució de $\gamma = 1$ és:

$$N_1\, a_{\mathbb{P}^2}(7) = N_1\, q^8 \frac{(q^4-1)(q^3-1)}{q-1} = \frac{q^5(q^2+1)}{q-1}.$$

La suma de totes les contribucions de tots els tipus dóna com a resultat, per a $n = 7$ i $p = 2$:

$$t_2(7) = q^6 + q^5 + 3q^4 + 6q^3 + 8q^2 - 1 +$$

$$+ [2(q^2+6q+4)]_{3|q-1} + [4]_{5|q+1} + [20]_{5|q-1} + [6]_{7|q-1},$$

mentre que, per a $n = 7$ i $p > 2$, tenim:

$$t_2(7) = q^6 + q^5 + 3q^4 + 6q^3 + 11q^2 + 4q +$$

$$+ [2(q^2+6q+9)]_{3|q-1} + [4]_{5|q+1} + [20]_{5|q-1} + [4q+6]_{4|q-1} + [8]_{7|q-1} + [6]_{7|q+1} +$$

$$+ [4]_{12|q-1} + [2]_{7|q^2+q+1} + [q^2+4q-1]_{3|q} + [2]_{3|q,\,4|q-1} + [3]_{5|q} + [2]_{7|q}.$$

7.3 Integralitat dels coeficients

L'aspecte dels resultats anteriors ens condueix a conjecturar que els $t_N(n)$ es podran expressar sempre com a certs "polinomis en q" amb coeficients enters. Per precisar aquesta afirmació introduïm la següent:

Definició 7.2. *Sigui K un anell i q una indeterminada. Un q-polinomi amb coeficients a K és una expressió formal:*

$$P(x) = [P_1(x)]_{q \equiv a_1 \pmod{M_1}} + \cdots + [P_r(x)]_{q \equiv a_r \pmod{M_r}}, \tag{42}$$

amb $a_1, \ldots, a_r$, $M_1, \ldots, M_r$ enters, $M_1, \ldots, M_r \neq 0$, i $P_1(x), \ldots, P_r(x) \in K[x]$.

Denotarem per $K[x]_q$ l'anell de tots els q-polinomis.

El fet de fixar un valor numèric de q determina un homomorfisme d'anells av: $K[x]_q \longrightarrow K[x]$, que resulta d'assignar a cada expressió (42) el polinomi que resulta de sumar els $P_i(x)$ que satisfan $q \equiv a_i \pmod{M_i}$. Donat un q-polinomi

$P(x) \in K[x]_q$ escriurem $P(q) \in K$ per indicar l'"avaluació absoluta" que consisteix en avaluar en q el polinomi $\mathrm{av}(P(x))$.

Conjectura. *Per a qualsevol parell d'enters positius N, n, existeix un q-polinomi amb coeficients enters $P(x) := P_{N,n,p}(x)$, que depèn del parell (N,n) i de la característica p de k, satisfent $t_N(n) = P(q)$.*

Per a $N = 1, 2$, podem comprovar aquesta conjectura utilitzant les fórmules explícites. Per a $N > 2$ això no és possible, i caldria buscar una raó més profunda que expliqui aquest fet.

Veiem per exemple el cas $N = 1$. Si $n = 1, 2$, és evident. Per a $n > 2$, a [LMNX02, Thm. 2.2] es prova la fórmula $t_1(n) = q^{n-3} + P_1(q) + P_2(q) + P_3(q)$, on $P_1(x)$, $P_2(x)$, $P_3(x)$ són q-polinomis amb coeficients racionals:

$$P_1(x) = \frac{1}{2(x+1)} \sum_{e=0}^{2} \binom{2}{e} \sum_{m|(q-1,n-e),\ m>1} \varphi(m) \left(x^{\frac{n-e}{m}} - (-1)^{\frac{n-e}{m}} \right),$$

$$P_2(x) = \tfrac{1}{x} \sum_{e=0}^{1} \left(\left[x^{\frac{n-e}{p}-1}(x-1) \right]_{n \equiv e(p)} + [1]_{n-e=p} \right),$$

$$P_3(x) = \frac{1}{2(x^2+1)} \sum_{e \in \{0,2\}} \sum_{m|(q+1,n-e),\, m>1} \varphi(m) \left(x^{\frac{n-e}{m}+1} - x^{\frac{n-e}{m}} + (-1)^{[\frac{n-e-m}{2m}]} x + (-1)^{[\frac{n-e}{2m}]} \right).$$

Notem que en aquestes expressions els respectius denominadors $x+1$, x, x^2+1 desapareixen, ja que:

$$x+1 \mid \left(x^{\frac{n-e}{m}} - (-1)^{\frac{n-e}{m}} \right), \qquad x \mid \left(\left[x^{\frac{n-e}{p}-1}(x-1) \right]_{n \equiv e(p)} + [1]_{n-e=p} \right),$$

$$x^2+1 \mid \left(x^{\frac{n-e}{m}+1} - x^{\frac{n-e}{m}} + (-1)^{[\frac{n-e-m}{2m}]} x + (-1)^{[\frac{n-e}{2m}]} \right).$$

Notem també que $P_2(x)$ és un polinomi de debò:

$$P_2(x) = [x^{\frac{n}{p}-2}(x-1)]_{p|n, p \neq n} + [1]_{p=n} + [x^{\frac{n-1}{p}-2}(x-1)]_{p|(n-1), p \neq n-1} + [1]_{p=n-1},$$

que depèn de p, n, i que els possibles valors de $P_2(x)$ tenen sempre coeficients enters. Per tant, la conjectura es redueix en aquest cas a comprovar que $P_1(x) + P_3(x) \in \mathbb{Z}[x]_q$.

L'únic obstacle perquè els coeficients d'aquests dos q-polinomis siguin tots enters és el factor $1/2$ que hi ha davant el sumatori. Per a $P_1(x)$, aquest denominador 2

és neutralitzat pel factor $\binom{2}{e}$ quan $e = 1$. Un cop suposat que $e = 0, 2$, tant per a $P_1(x)$ com per a $P_3(x)$, tenim en els dos casos un sumatori sobre un paràmetre $m > 1$, i en cada sumand amb $m > 2$ el denominador 2 és neutralitzat pel factor $\varphi(m)$, que és parell. Per tant, ens podem reduir a estudiar el sumand corresponent a $m = 2$. Si n és senar o q és parell, aquest sumand no apareix i ja tenim directament $P_1(x)$, $P_3(x) \in \mathbb{Z}[x]_q$. Per a n parell i q senar, fixant-nos en el sumand amb $m = 2$, podem dir:

$$P_1(x) \equiv \frac{\left(x^{n/2} - (-1)^{n/2} + x^{(n-2)/2} - (-1)^{(n-2)/2}\right)}{2(x+1)} = \frac{1}{2}x^{(n-2)/2} \pmod{\mathbb{Z}[x]_q},$$

$$P_3(x) \equiv \frac{1}{2(x^2+1)}\left(x^{(n/2)+1} - x^{n/2} + (-1)^{[(n-2)/4]}x + (-1)^{[n/4]} + \right.$$
$$\left. + x^{((n-2)/2)+1} - x^{(n-2)/2} + (-1)^{[(n-4)/4]}x + (-1)^{[(n-2)/4]}\right) \pmod{\mathbb{Z}[x]_q},$$

Posant $n = 2M$, aquesta darrera expressió val:

$$P_3(x) \equiv \begin{cases} \frac{1}{2(x^2+1)}\left(x^{M+1} - x^{M-1} - (-1)^{M/2}2x\right) \pmod{\mathbb{Z}[x]_q}, & \text{si } M \text{ parell}, \\ \frac{1}{2(x^2+1)}\left(x^{M+1} - x^{M-1} + (-1)^{(M-1)/2}2\right) \pmod{\mathbb{Z}[x]_q}, & \text{si } M \text{ senar}. \end{cases}$$

Tenim clarament:

$$\frac{x^{M+1} - x^{M-1} - (-1)^{M/2}2x}{x^2+1} \equiv \frac{x^{M+1} + x^{M-1} - 2x(x^{M-2} + (-1)^{M/2})}{x^2+1} \equiv$$
$$\equiv \frac{x^{M+1} + x^{M-1}}{x^2+1} \equiv x^{M-1} \pmod{2\mathbb{Z}[x]_q},$$

$$\frac{x^{M+1} - x^{M-1} + (-1)^{(M-1)/2}2}{x^2+1} \equiv \frac{x^{M+1} + x^{M-1} - 2(x^{M-1} - (-1)^{(M-1)/2})}{x^2+1} \equiv$$
$$\equiv \frac{x^{M+1} + x^{M-1}}{x^2+1} \equiv x^{M-1} \pmod{2\mathbb{Z}[x]_q}.$$

Per tant, $P_3(x) \equiv \frac{1}{2}x^{M-1} \pmod{\mathbb{Z}[x]_q}$ en qualsevol cas, i

$$P_1(x) + P_3(x) \equiv 0 \pmod{\mathbb{Z}[x]_q},$$

com volíem demostrar.

En el cas $N = 2$ hem pogut comprovar la conjectura de manera similar, treballant amb les expressions explícites per a $t_2(n)$ que hem obtingut en aquest capítol. De tota manera, els càlculs són molt més llargs i enrevessats. Com que, a més a més, són poc il·lustratius, hem preferit no incloure'ls en la memòria.

Capítol 4

Funcions generadores dels nombres d'òrbites de n-conjunts

Recordem les funcions generadores que hem utilitzat en capítols anteriors i les que volem estudiar en aquest capítol.

Per a qualsevol conjunt finit Y:

$$\sum_{n\geq 0}\left|\binom{Y}{n}\right|x^n=(1+x)^{|Y|},\qquad \sum_{n\geq 0}\left|\left(\!\!\binom{Y}{n}\!\!\right)\right|x^n=(1-x)^{-|Y|}.$$

D'altra banda, per al nombre de punts k-racionals de les varietats $\binom{V}{n}$ i $\left(\!\!\binom{V}{n}\!\!\right)$ tenim les funcions generadores (cf. Teorema 4.2):

$$\sum_{n\geq 0}\left|\binom{V}{n}(k)\right|x^n=\frac{\mathrm{Z}(V/k,x)}{\mathrm{Z}(V/k,x^2)},\quad \sum_{n\geq 0}\left|\left(\!\!\binom{V}{n}\!\!\right)(k)\right|x^n=\mathrm{Z}(V/k,x).$$

Si el grup finit Γ opera sobre el conjunt finit Y, aleshores podem expressar la funció generadora dels $\left|\Gamma\backslash\backslash\binom{Y}{n}\right|$ i els $\left|\Gamma\backslash\backslash\left(\!\!\binom{Y}{n}\!\!\right)\right|$ en termes de l'indicador de cicles de Pólya [BFKWZ98, 3.2.16]:

$$\sum_{n\geq 1}\left|\Gamma\backslash\backslash\binom{Y}{n}\right|x^n=C(\Gamma,Y)_{|z_i=1+x^i},$$

$$\sum_{n\geq 1}\left|\Gamma\backslash\backslash\left(\!\!\binom{Y}{n}\!\!\right)\right|x^n=C(\Gamma,Y)_{|z_i=(1-x^i)^{-1}}.$$

Tanmateix, l'indicador de cicles de Pólya no és gaire adequat per a expressar les funcions generadores dels nombres:

$$t_V(n) := \left|\Gamma\backslash\backslash \binom{V}{n}(k)\right|, \qquad \bar{t}_V(n) := \left|\Gamma\backslash\backslash \left(\!\binom{V}{n}\!\right)(k)\right|,$$

per a Γ un subgrup finit del grup de k-automorfismes de la varietat V. D'entrada, l'acció de γ com a permutació de $V(k)$ no determina els $|\mathcal{X}_{V,\gamma}(n)|$ (vegeu la secció 7, ja que intervenen punts de $V(\overline{k})$. Podríem utilitzar l'indicador de cicles de Γ actuant sobre $V(\overline{k})$ o sobre $V(k_r)$, per a r prou gran, però aleshores obtenim polinomis amb un nombre astronòmic de variables (sobre $V(\overline{k})$, obtenim polinomis amb infinites variables).

En aquest capítol trobarem fórmules per a les funcions generadores dels $t_N(n) := t_{\mathbb{P}^N}(n)$ i $\bar{t}_N(n) := \bar{t}_{\mathbb{P}^N}(n)$, respecte de $\Gamma = \mathrm{PGL}_{N+1}(k)$, i també les expressarem en termes d'un *G-indicador d'exponents*:

$$\mathcal{L}_G(\Gamma, \mathbb{P}^N) = \sum_{\alpha\in\mathcal{T}_G} N_{G,\alpha} \prod_{V\in\mathcal{L}_G(\alpha)} z_{\alpha,V} \in \mathbb{Q}[\{z_{\alpha,V}\}],$$

anàleg al de Pólya. La idea és que per a cada element $\gamma \in \Gamma$ es construeix un poset $\mathcal{L}_G(\alpha)$ format per certes subvarietats lineals γ-invariants i *pròpies* (cf. secció 9) de $\mathbb{P}^N$. Els elements γ que donen lloc (essencialment) al mateix poset constitueixen un *G-subtipus* α. El conjunt $\mathcal{T}_G$ recull els possibles G-subtipus i les constants $N_{G,\alpha}$ compten quants γ hi ha de cada G-subtipus. L'avantatge d'aquest indicador d'exponents respecte de l'indicador de cicles de Pólya és doble: d'una banda $\mathcal{L}_G(\Gamma, \mathbb{P}^N)$ té un nombre molt més reduït de variables; de l'altra, la descripció de $\mathcal{T}_G$ i $\mathcal{L}_G(\alpha)$ es fa en termes de dades combinatòries explícites que ja recullen (i fan innecessari tenir en compte) l'efecte de l'acció dels diferents γ com a permutacions de $\mathbb{P}^N$. El còmput dels $N_{G,\alpha}$ per a un valor arbitrari de la dimensió N és complicat i no l'hem considerat en aquesta memòria.

A la secció 10 provem el resultat principal d'aquesta memòria:

$$\sum_{n\in\mathbb{N}} t_N(n)x^n = \mathcal{L}_G(\Gamma, \mathbb{P}^N)_{|z_{\alpha,V}=h(x)}, \qquad \sum_{n\in\mathbb{N}} \bar{t}_N(n)x^n = \mathcal{L}_G(\Gamma, \mathbb{P}^N)_{|z_{\alpha,V}=\bar{h}(x)},$$

per a funcions adequades $h(x)$, $\bar{h}(x)$ (vegeu el Teorema 10.5).

De fet, aquest tractament és extensible al càlcul de funcions generadores per als nombres

$$T_N(n) := \left|\Gamma\backslash\backslash \binom{\mathbb{P}^N(k)}{n}\right|, \qquad \overline{T}_N(n) := \left|\Gamma\backslash\backslash \left(\!\binom{\mathbb{P}^N(k)}{n}\!\right)\right|,$$

i d'una manera completament anàloga obtenim una generalització dels resultats del capítol 1 a dimensió N arbitrària (tret del còmput de les constants N_α, anàlogues

a les anteriors, que compten el nombre de $\gamma \in \Gamma$ del mateix subtipus). Cal utilitzar en aquest cas uns indicadors similars:

$$\mathcal{L}(\Gamma, \mathbb{P}^N) = \sum_{\alpha \in \mathcal{T}} N_\alpha \prod_{V \in \mathcal{L}(\alpha)} z_{\alpha,V} \in \mathbb{Q}[\{z_{\alpha,V}\}],$$

que donen lloc a resultats similars:

$$\sum_{n \in \mathbb{N}} T_N(n) x^n = \mathcal{L}(\Gamma, \mathbb{P}^N)_{|z_{\alpha,V} = f(x)}, \qquad \sum_{n \in \mathbb{N}} \overline{T}_N(n) x^n = \mathcal{L}(\Gamma, \mathbb{P}^N)_{|z_{\alpha,V} = \bar{f}(x)},$$

per a funcions adequades $f(x)$, $\bar{f}(x)$ (vegeu el Teorema 10.2).

8 Generalitats sobre conjunts parcialment ordenats

En aquesta secció revisem algunes nocions sobre posets, extretes de [Sta99], que utilitzarem al llarg del capítol.

Definició 8.1. *Un poset és un conjunt parcialment ordenat ("Partially Ordered Set").*

Exemples

$[n] := \{1, \ldots, n\}$, amb l'ordre usual.

$\mathbf{B}_n := 2^{[n]}$, el conjunt de les parts de $[n]$, amb la inclusió com a relació d'ordre.

$\mathbf{D}_n := \{\text{divisors positius de } n\}$, amb la divisibilitat com a relació d'ordre.

$\mathbf{D}_{\mathbb{N}} := \{\text{enters positius}\}$, amb la divisibilitat com a relació d'ordre.

Definició 8.2. *Siguin P, Q posets. Diem que una aplicació $\phi : P \longrightarrow Q$ és un morfisme de posets si $x \leq y \Rightarrow \phi(x) \leq \phi(y)$.*

Diem que ϕ és un isomorfisme de posets si és bijectiva i ϕ, ϕ^{-1} son morfismes de posets. Escrivim $P \simeq Q$ per denotar que P i Q són isomorfs.

Definició 8.3. *Sigui P un poset. Un subposet de P és qualsevol subconjunt $Q \subseteq P$, dotat de la relació d'ordre induïda:*

$$x \leq_Q y \Leftrightarrow x \leq y.$$

Definició 8.4. *Sigui P un poset i siguin x, $y \in P$, amb $x \leq y$. L'interval (tancat) $[x, y]$ és el conjunt*

$$[x, y] = \{z \in P \mid x \leq z \leq y\}.$$

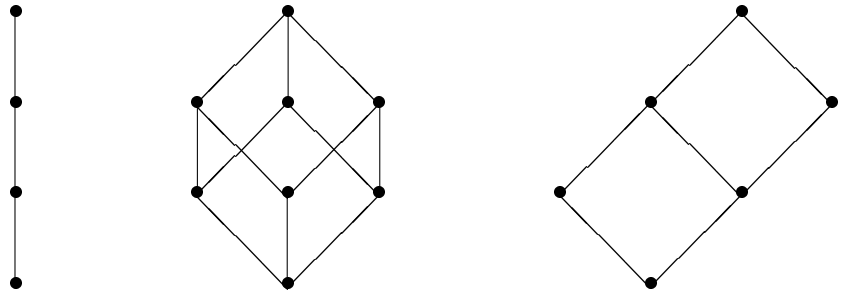
Si $x \not\leq y$, aleshores no definim l'interval $[x, y]$. Per tant, el conjunt buit no és un interval (tancat).

Definició 8.5. *Diem que un poset és localment finit si tot interval és finit.*

Definició 8.6. *Sigui P un poset i siguin x, $y \in P$. Diem que y "cobreix" x si $y > x$ i $[x, y] = \{x, y\}$.*

Un diagrama de Hasse d'un poset P és un graf amb vèrtexs els elements de P i arestes que indiquen els cobriments. Donats x, $y \in P$, si y cobreix x, aleshores x s'escriu exactament a un nivell inferior respecte y.

Exemples de diagrames de Hasse



$[4]$ $\quad$ $\mathbf{B}_3$ $\quad$ $\mathbf{D}_{12}$

Definició 8.7. *Sigui P un poset. Diem que P té un element zero, i el denotem per $\hat{0}$, si $\exists \hat{0} \in P$ tal que $\hat{0} \leq x$, $\forall x \in P$. Diem que P té un element u, i el denotem per $\hat{1}$, si $\exists \hat{1} \in P$ tal que $x \leq \hat{1}$, $\forall x \in P$.*

Observem que, els elements $\hat{0}$, $\hat{1}$, si existeixen, són únics.

Definició 8.8. *Una cadena és un poset totalment ordenat. La longitud d'una cadena C és $\ell(C) := |C| - 1$.*

Una cadena d'un poset P és una cadena que és un subposet de P. Definim la longitud (o el rang) d'un poset P com:

$$\ell(P) := \sup\{\ell(C) | C \text{ cadena de } P\}.$$

Diem que una cadena C d'un poset P està saturada si: donats x, $y \in C$, $\nexists z \in P \setminus C$ tal que $x < z < y$ i $C \cup \{z\}$ és una cadena de P.

Definició 8.9. *Una multicadena d'un poset P és una cadena de P amb elements repetits, és a dir, un multiconjunt tal que el conjunt subjacent és una cadena de P.*

La longitud d'una multicadena C és $\ell(C) := |C| - 1$.

L'àlgebra d'incidències d'un poset localment finit

Sigui K un cos. Sigui P un poset localment finit. Denotem per $\mathrm{Int}(P)$ el conjunt d'intervals de P, és a dir,

$$\mathrm{Int}(P) := \{[x,y] \mid x,y \in P,\ x \leq y\}.$$

Definim $I(P,K) := \mathrm{Apl}(\mathrm{Int}(P),K)$, el conjunt de totes les aplicacions de $\mathrm{Int}(P)$ a K.

Donada $\chi \in I(P,K)$, escriurem $\chi(x,y) := \chi([x,y])$.

$I(P,K)$ és una K-àlgebra amb l'estructura natural de K-e.v. i el producte

$$(\chi\xi)(x,y) := \sum_{x\leq z\leq y} \chi(x,z)\xi(z,y).$$

És una K-àlgebra associativa amb identitat

$$1(x,y) := \delta(x,y) := \begin{cases} 1 & \text{si } x = y, \\ 0 & \text{si } x \neq y. \end{cases}$$

Podem pensar $\chi \in I(P,K)$ com a una suma formal

$$\sum_{[x,y]\in \mathrm{Int}(P)} \chi(x,y)[x,y].$$

Aleshores el producte és l'extensió bilineal de l'aparellament

$$[x,y]\cdot[z,w] = \begin{cases} [x,w] & \text{si } y = z, \\ 0 & \text{si } y \neq z. \end{cases}$$

D'ara endavant, denotarem simplement $I(P) := I(P,\mathbb{C})$.

Exemple

Sigui P un poset finit. Etiquetem els seus elements $x_1,\ldots,x_n$ de manera que $x_i < x_j \Rightarrow i < j$.

Si $\chi \in I(P,K)$, posem $\chi(x_i,x_j) := 0$ si $x_i \not\leq x_j$. Aleshores $I(P,K)$ s'identifica amb la subàlgebra de $M_n(K)$ de les matrius $M = (m_{ij})$ amb $m_{ij} = 0$ sempre que $x_i \not\leq x_j$ (en particular, M és triangular superior). L'isomorfisme s'obté considerant $m_{ij} = \chi(x_i,x_j)$.

Proposició 8.10. *Sigui K un cos. Sigui $\chi \in I(P,K)$. Aleshores les afirmacions següents són equivalents:*

a) χ té invers per la dreta.
b) χ té invers per l'esquerra.
c) χ té invers pels dos costats.
d) $\chi(x,x) \neq 0$, $\forall x \in P$.

A més, si χ^{-1} existeix, $\chi^{-1}(x,y)$ depèn només de l'acció de χ sobre $[x,y]$.

Demostració.

$$\chi\xi = \delta \Leftrightarrow \begin{cases} \chi(x,x)\xi(x,x) = 1, & \forall x \in P, \\ \xi(x,y) = -\frac{1}{\chi(x,x)} \sum_{x<z\leq y} \chi(x,z)\xi(z,y), & \forall x < y \text{ a } P. \end{cases}$$

Per tant, χ té invers per la dreta sii $\chi(x,x) \neq 0,\ \forall x \in P$; i, en aquest cas, $\chi^{-1}(x,y)$ depèn només de $[x,y]$. Anàlogament, $\chi(x,x) \neq 0,\ \forall x \in P$ també equival a tenir invers per l'esquerra. □

Fórmula d'inversió de Möbius

Definició 8.11. *Sigui P un poset localment finit. La funció zeta de P és l'element de $I(P)$ donat per $\zeta(x,y) = 1,\ \forall [x,y] \in \mathrm{Int}(P)$.*

Les següents observacions són clares:

$$\zeta^k(x,y) = \sum_{x=x_0\leq x_1\leq\cdots\leq x_k=y} 1 = |\{\text{multicadenes } x = x_0 \leq x_1 \leq \cdots \leq x_k = y\}|,$$
$$(\zeta - 1)^k(x,y) = |\{\text{cadenes } x = x_0 < x_1 < \cdots < x_k = y\}|.$$

La funció de Möbius de P és, per definició, $\mu = \zeta^{-1}$.
Com hem vist a la demostració de la proposició anterior:

$$\mu(x,x) = 1,\ \forall x \in P; \qquad \mu(x,y) = -\sum_{x<z\leq y} \mu(z,y),\ \forall x < y \text{ a } P. \tag{43}$$

En particular, $\mu(x,y) = -1$ sempre que y cobreix x.
Sigui P un poset on tots els conjunts

$$\left\langle\, y \,\right\rangle := \{x \in P \mid x \leq y\}$$

siguin finits. Per a qualsevol parell de funcions $f,\, g\colon P \longrightarrow \mathbb{C}$, tenim la següent *fórmula d'inversió*:

$$g(x) = \sum_{y\leq x} f(y),\ \forall x \in P \iff f(x) = \sum_{y\leq x} g(y)\mu(y,x),\ \forall x \in P.$$

En efecte, $\mathbb{C}^P$ és un $\mathbb{C}$-espai vectorial on actua $I(P)$ per la dreta:

$$(f\chi)(x) := \sum_{y\leq x} f(y)\chi(y,x),\ \forall \chi \in I(P).$$

La fórmula d'inversió diu: $g = f\zeta \iff g\mu = f$, la qual cosa és evident.

Exemples.

(1) Sigui $\hat{1} = S_1 \cup S_2 \cup \cdots \cup S_n$ una descomposició d'un conjunt finit en reunió de subconjunts. Considerem el poset P format per les possibles interseccions d'alguns d'aquests subconjunts (incloent la intersecció buida $\hat{1}$), ordenats per inclusió.

Per a cada $T \in P$, denotem:

$$f(T) := |T \setminus \cup_{T'<T} T'|, \quad g(T) := |T|.$$

Clarament, $g(T) = \sum_{T' \leq T} f(T')$, $\forall T \in P$, de manera que, per inversió de Möbius,

$$0 = f(\hat{1}) = \sum_{T \in P} g(T)\mu(T, \hat{1}) \implies g(\hat{1}) = -\sum_{T<\hat{1}} |T|\mu(T, \hat{1}).$$

que és, essencialment, el principi d'inclusió-exclusió.

(2) Considerem $P = \mathbb{N}$, amb la relació d'ordre usual. Tenim, per (43):

$$\mu(i,j) = \begin{cases} 1, & i = j, \\ -1, & i+1 = j, \\ 0, & \text{en altre cas.} \end{cases}$$

La fórmula d'inversió en aquest cas és

$$g(n) = \sum_{i=1}^{n} f(i), \ \forall n > 0 \iff f(n) = \begin{cases} g(n) - g(n-1), & n > 1, \\ g(1), & n = 1. \end{cases}$$

En altres paraules, els operadors Σ, Δ (amb Σ convenientment inicialitzat) són inversos l'un de l'altre. Aquest és l'anàleg, en el terreny de les diferències finites, del teorema fonamental del càlcul.

Producte de posets

El poset producte $(P \times Q, \leq)$ és el poset que té $P \times Q$ per conjunt i l'ordre:

$$(x, y) \leq (x', y') \iff x \leq x' \text{ a } P \text{ i } y \leq y' \text{ a } Q.$$

Proposició 8.12 (teorema del producte). *Siguin P, Q posets localment finits. Tenim:*

$$(x, y) \leq (x', y') \text{ a } P \times Q \implies \mu_{P\times Q}((x, y), (x', y')) = \mu_P(x, x')\mu_Q(y, y').$$

Exemple.

(1) $\mathbf{B}_n \simeq [2]\times \overset{n}{\cdots} \times[2] =: [2]^n$ via la identificació entre $\mathbf{B}_n$ i $\{1,2\}^n$ que consisteix en assignar a una n-tupla de 1's i 2's el subconjunt format pels i tals, que en la posició i apareix un 2.

Clarament, $\mu(1,1) = \mu(2,2) = 1$, $\mu(1,2) = -1$. Per tant, tenim calculada la funció de Möbius de $\mathbf{B}_n$:

$$\mu(T,S) = (-1)^{|S-T|} = (-1)^{\ell(T,S)}, \quad \text{sempre que } T \subseteq S.$$

La fórmula d'inversió es converteix en:

$$g(S) = \sum_{T\subseteq S} f(T) \iff f(S) = \sum_{T\subseteq S} (-1)^{|S-T|} f(T).$$

(2) Considerem $P = [n_1+1]\times\cdots\times[n_k+1]$. Identifiquem els elements de P amb k-tuples $(a_1,a_2,\ldots,a_k) \in \mathbb{N}$ tals, que $0 \le a_i \le n_i$. L'ordre és el natural en cada component. Pel teorema del producte,

$$\mu((a_1,\ldots,a_k),(b_1,\ldots,b_k)) = \begin{cases} (-1)^{(b_1-a_1)+\cdots+(b_k-a_k)}, & b_i - a_i = 0,1,\ \forall i, \\ 0, & \text{en altre cas.} \end{cases}$$

Si $N = p_1^{n_1}\cdots p_k^{n_k}$, on els p_i són primers diferents, P és isomorf al poset $\mathbf{D}_N$ dels divisors positius de N. Tenim, doncs, per a tot $r|s|N$,

$$\mu(r,s) = \begin{cases} (-1)^t, & \text{si } s/r \text{ és producte de } t \text{ primers diferents}, \\ 0, & \text{en altre cas.} \end{cases}$$

Aquesta és la funció clàssica de Möbius $\mu(s/r)$. La fórmula d'inversió és la clàssica:

$$g(n) = \sum_{d|n} f(d),\ \forall n|N \iff f(n) = \sum_{d|n} g(d)\mu(\frac{n}{d}),\ \forall n|N.$$

9 Poset de les subvarietats invariants pròpies

Sigui k un cos finit. Fixem un nombre natural $N \ge 1$ i un automorfisme de $\mathbb{P}^N$, $\gamma \in \mathrm{PGL}_{N+1}(k)$. Denotem també per $\gamma \in \mathrm{GL}_{N+1}(k)$ l'elecció d'un representant de γ en el grup lineal afí.

Conveni. El terme *subvarietat lineal* s'aplicarà exclussivament per indicar subvarietats lineals irreductibles no buides de $\mathbb{P}^N$.

Les subvarietats lineals $V \subseteq \mathbb{P}^N(\overline{k})$ que són γ-invariants es corresponen amb els subespais vectorials γ-invariants de $\mathbb{A}^{N+1}(\overline{k}) \setminus \{0\}$.

Definició 9.1. *Si $V \subseteq \mathbb{P}^N(\overline{k})$ és una subvarietat lineal γ-invariant, definim el seu "exponent" com:*

$$\exp(V) := \mathrm{ord}(\gamma_{|V}).$$

Notem que, si tenim una inclusió $V \subseteq W$ de subvarietats lineals γ-invariants, aleshores $\exp(V) | \exp(W)$.

El poset $\mathcal{L}_\gamma$ format per les subvarietats lineals γ-invariants de $\mathbb{P}^N(\overline{k})$, ordenades respecte la inclusió, no és localment finit. Per exemple, per a $N = 2$ i γ del tipus IV', l'interval $[P_1, \mathbb{P}^2]$ conté infinits elements: P_1, $\mathbb{P}^2$ i totes les rectes que passen per P_1. O també, si V és un pla de punts fixos per γ i $P \in V$, l'interval $[P, V]$ també és infinit.

Definició 9.2. *Diem que una subvarietat lineal invariant $V \subseteq \mathbb{P}^N(\overline{k})$ és "pròpia" si $\exp(V) < \exp(W)$, $\forall W$ subvarietat lineal invariant, $W \supsetneq V$.*

En el primer exemple anterior, les rectes que passen per P_1 no són pròpies, ja que tenen el mateix exponent que $\mathbb{P}^2$. En el segon exemple anterior, els punts Q i les rectes L del pla V tampoc són propis, ja que tenen el mateix exponent que V: $\exp(Q) = \exp(L) = \exp(V) = 1$.

Notem que $\mathbb{P}^N$ és propi, ja que la condició $W \supsetneq \mathbb{P}^N$ és buida.

Notació. Denotem per $\mathcal{L}_\gamma^{\mathrm{pr}}$ el poset format per les subvarietats lineals pròpies γ-invariants de $\mathbb{P}^n(\overline{k})$, amb la inclusió com a relació d'ordre.

En aquesta secció veurem que $\mathcal{L}_\gamma^{\mathrm{pr}}$ és un poset finit i determinarem la seva estructura. Comencem revisant els subespais lineals invariants de $\mathbb{A}^{N+1}(\overline{k})$. Recordem la primera descomposició:

Teorema 9.3. *Si $P_\gamma(x) = (x - \lambda_1)^{n_1} \cdots (x - \lambda_r)^{n_r}$ és el polinomi característic de γ, tenim la descomposició*

$$\mathbb{A}^{N+1}(\overline{k}) = V_1 \oplus \cdots \oplus V_r, \quad \text{on } \ V_i = \mathrm{Ker}(\gamma - \lambda_i)^{n_i}, \ i = 1, \ldots, r. \tag{44}$$

Cada subespai V_i és γ-invariant i els únics subespais γ-invariants de $\mathbb{A}^{N+1}(\overline{k})$ són els de la forma:

$$W = W_1 \oplus \cdots \oplus W_r, \tag{45}$$

amb els $W_i \subseteq V_i$ γ-invariants.

Per tant, és suficient estudiar el cas d'un sol valor propi. Denotem genèricament $V := \mathrm{Ker}(\gamma - \lambda)^n$.

En coordenades adequades, γ ve donada per una matriu amb s blocs de Jordan:

$$\begin{pmatrix} \lambda & 0 & 0 & \cdots & 0 \\ 1 & \lambda & 0 & \cdots & 0 \\ 0 & 1 & \lambda & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & \lambda \end{pmatrix}$$

de mida variable, a la diagonal. Tornem a tenir:

$$V = U_1 \oplus \cdots \oplus U_s,$$

on els U_κ estan formats pels vectors de la forma $(0, 0, \ldots, 0, *, *, \ldots, *, 0, 0, \ldots, 0)$; aquests subespais són γ-invariants i a les coordenades $(*, *, \ldots, *)$ hi opera el κ-èsim bloc de Jordan.

És fàcil determinar els subespais γ-invariants de cada U_κ. Posem genèricament $U = U_\kappa$, $\dim(U) = e$.

Lema 9.4. *Sigui $v_1 \in U$ tal que $(\gamma - \lambda)^{e-1}(v_1) \neq 0$. Aleshores els elements*

$$v_1, v_2 := (\gamma - \lambda)(v_1), \ldots, v_e := (\gamma - \lambda)^{e-1}(v_1)$$

són una base de U i els únics subespais γ-invariants de U són:

$$U^{(j)} := \mathrm{Ker}(\gamma - \lambda)^{e-j} \cap U = \left\langle v_{j+1}, \ldots, v_e \right\rangle, \quad j = 0, 1, \ldots, e,$$

entenent que $U^{(e)} = \{0\}$. A més a més, denotant igualment per $U^{(j)}$ la corresponent subvarietat lineal invariant de $\mathbb{P}^N$, tenim:

$$\exp(U^{(j)}) = p^{\delta_j}, \quad \textit{on } \delta_j := \min\{t \in \mathbb{N} \mid p^t \geq e - j\}.$$

Tanmateix, ara no és cert que els subespais γ-invariants de V siguin de la forma:

$$T_1 \oplus \cdots \oplus T_s,$$

on cada T_κ és un subespai γ-invariant de U_κ. Per exemple, si els s blocs de Jordan són iguals, aleshores $e := \dim(U_\kappa)$ és constant i tenim subespais γ-invariants de la forma:

$$T = \{(x_1, \ldots, x_e, a_1 x_1, \ldots, a_1 x_e, a_2 x_1, \ldots, a_2 x_e, \ldots, a_{s-1} x_1, \ldots, a_{s-1} x_e) \mid x_1, \ldots, x_e \in \overline{k}\},$$

on $a_1, a_2, \ldots, a_{s-1} \in \overline{k}$ són escalars fixats. No obstant això, si ens centrem en els subespais γ-invariants propis, aquests són fàcils de determinar. Notem que:

$$\exp(V) = \max\{\exp(U_\kappa)\} = p^\delta, \text{on } \delta = \min\{t \in \mathbb{N} \mid p^t \geq e_1, \ldots, e_s\}.$$

Per tant, un subespai γ-invariant T de V té necessàriament $\exp(T) = p^\nu$, amb $0 \leq \nu \leq \delta$. Per a cada valor de ν en aquest interval, hi ha un subespai γ-invariant màxim amb exponent p^ν:

$$V^{(\nu)} := \bigoplus_{\kappa=1}^{s} U_\kappa^{(j_\kappa)},$$

on j_κ és el mínim natural que satisfà $p^\nu \geq e_\kappa - j_\kappa$; per tant, aquest és l'únic subespai γ-invariant propi, per a cada $0 \leq \nu \leq \delta$.

Lema 9.5. *Suposem que $V = \mathrm{Ker}(\gamma - \lambda)^n$, amb $\exp(V) = p^\delta$. Aleshores, els únics subespais γ-invariants propis de V són:*

$$0 \subsetneq V^{(0)} \subsetneq V^{(1)} \subsetneq \cdots \subsetneq V^{(\delta)} = V.$$

Denotarem $V_{ss} := V^{(0)}$. És el subespai semisimple, generat pels vectors propis de valor propi λ. Geomètricament, V_{ss} és la subvarietat (irreductible en aquest cas) de $\mathbb{P}^N$ formada pels punts fixos de γ.

Això ens permetrà determinar fàcilment els subespais γ-invariants propis en el cas general (cf. Teorema 9.8). Calculem primer l'exponent de qualsevol subvarietat γ-invariant.

Lema 9.6. *Sigui $W \subseteq \mathbb{A}^{N+1}(\overline{k})$ una subvarietat lineal γ-invariant donada per (44) i (45). Denotem:*

$$\exp(V_i) = p^{\delta_i}, \quad \exp(W_i) = p^{\epsilon_i}, \quad \epsilon_i \leq \delta_i.$$

Aleshores,

1. $\exp(W) = p^\epsilon D$, *on* $\epsilon = \max\{\epsilon_1, \ldots, \epsilon_r\}$ *i*

   $$D := D(W) := D(\lambda_{i_1}, \ldots, \lambda_{i_t}) := \min\{d \in \mathbb{N} \mid \lambda_{i_1}^d = \lambda_{i_2}^d = \cdots = \lambda_{i_t}^d\},$$

   essent $\lambda_{i_1}, \ldots, \lambda_{i_t}$ els valors propis de $\gamma_{|W}$ (és a dir, $i_1, \ldots, i_t$ són els índexs pels quals $W_i \neq 0$). Notem que $p \nmid D$ en qualsevol cas.

2. *Si W és propi, cada factor W_i és propi com a subespai γ-invariant de V_i.*

Demostració. La primera afirmació és evident. Provem la segona; si W_i no és propi, tenim:

$$0 \subsetneq W_i \subsetneq W_i' \subseteq V_i, \quad \text{amb} \quad \exp(W_i') = p^{\epsilon_i} = \exp(W_i).$$

Per tant, W no és propi, ja que:

$$W \subsetneq W_1 \oplus \cdots \oplus W_{i-1} \oplus W_i' \oplus W_{i+1} \oplus \cdots \oplus W_r$$

i aquests dos subespais tenen el mateix exponent. □

Per exemple,

$$\exp(\mathbb{P}^N) = p^{\delta} D(\lambda_1, \ldots, \lambda_r), \qquad \delta := \max\{\delta_1, \ldots, \delta_r\}.$$

El recíproc de la segona afirmació d'aquest lema no és cert. Per exemple, si $D := D(\lambda_2, \ldots, \lambda_r)$ i tenim

$$\lambda_1^D = \lambda_2^D, \qquad \epsilon_1 \leq \max\{\epsilon_2, \ldots, \epsilon_r\},$$

aleshores:

$$D(\lambda_1, \ldots, \lambda_r) = D(\lambda_2, \ldots, \lambda_r), \qquad \max\{\epsilon_1, \ldots, \epsilon_r\} = \max\{\epsilon_2, \ldots, \epsilon_r\},$$

i, per a qualssevol $W_2, \ldots, W_r$ propis, el subespai

$$W = 0 \oplus W_2 \oplus \cdots \oplus W_r,$$

no és propi, ja que $W_1 \oplus \cdots \oplus W_r$ té el mateix exponent.

Elements propis d'un poset, respecte d'un morfisme a un altre poset

Necessitem el concepte de "propi" en un context més general.

Definició 9.7. *Sigui $\phi : P \longrightarrow Q$ un morfisme entre dos posets P i Q. Diem que $x \in P$ és "propi" respecte de ϕ (o ϕ-propi) si $\phi(x) < \phi(y)$, $\forall x < y$.*

Denotem per P_ϕ^{pr} el poset induït que obtenim en quedar-nos només amb els elements propis de P respecte de ϕ.

Per exemple, si $P = \mathcal{L}_\gamma$, $Q = \mathbf{D}_\mathbb{N}$ i $\phi = \exp\colon \mathcal{L}_\gamma \longrightarrow \mathbf{D}_\mathbb{N}$ és el morfisme que associa a cada subvarietat V el seu exponent, obtenim el concepte de propi estudiat al paràgraf anterior.

Apliquem aquest concepte més general de propi al cas següent: prenem $P = \mathbf{B}_r$, el poset dels subconjunts de $\{1, \ldots, r\}$, amb la relació d'ordre donada per la inclusió. Prenem $Q = \mathbf{D}_\mathbb{N}$, respectivament $Q = \mathbb{N}$, i considerem els morfismes

$$D\colon \mathbf{B}_r \longrightarrow \mathbf{D}_\mathbb{N}, \qquad \delta\colon \mathbf{B}_r \longrightarrow \mathbb{N},$$

donats per:

$$\Lambda := \{i_1, \ldots, i_t\} \longmapsto D(\Lambda) := D(\lambda_{i_1}, \ldots, \lambda_{i_t}), \quad \delta(\Lambda) := \max\{\delta_{i_1}, \ldots, \delta_{i_t}\}.$$

Fem notar que aquestes definicions depenen de l'element $\gamma \in \Gamma$ que tenim fixat, amb valors propis $\lambda_1, \ldots, \lambda_r$.

Teorema 9.8. *Sigui $\Lambda \in \mathbf{B}_r$ un element D-propi i siguin $D := D(\Lambda)$, $\delta := \delta(\Lambda)$. Aleshores els següents subespais γ-invariants són propis amb exponents respectius $D, pD, \ldots, p^\delta D$:*

$$\emptyset \subsetneq V_\Lambda^{(0)} \subsetneq V_\Lambda^{(1)} \subsetneq \cdots \subsetneq V_\Lambda^{(\delta)}, \qquad V_\Lambda^{(\nu)} := \bigoplus_{i \in \Lambda} V_i^{(\nu)}.$$

A més a més, variant Λ entre tots els elements D-propis de $\mathbf{B}_r$ obtenim d'aquesta manera tots els subespais γ-invariants propis de $\mathbb{P}^N$.

Demostració. Suposem que Λ és D-propi i provem que cada $V_\Lambda^{(\nu)}$ és propi. Considerem $V_\Lambda^{(\nu)} \subseteq W$, amb W γ-invariant i $\exp(V_\Lambda^{(\nu)}) = \exp(W)$, i comprovem que forçosament $V_\Lambda^{(\nu)} = W$.

Sigui $\Lambda_W \subseteq \Lambda_\gamma := \{\lambda_1, \ldots, \lambda_r\}$ tal, que $W = \oplus_{j \in \Lambda_W} W_j$, amb $W_j \subseteq V_j$ γ-invariant i $W_j \neq 0$. Pel Lema 9.6, tenim:

$$\exp(V_\Lambda^{(\nu)}) = p^\nu D(\Lambda), \qquad \exp(W) = p^\epsilon D(\Lambda_W).$$

Tenim, doncs, $D(\Lambda) = D(\Lambda_W)$, amb la qual cosa, $\Lambda = \Lambda_W$ pel caràcter propi de Λ. D'altra banda, tenim també:

$$\epsilon = \nu \geq \epsilon_j, \ \forall j \in \Lambda \implies W_j = V_j^{(\nu)}, \ \forall j \in \Lambda,$$

ja que $V_j^{(\nu)}$ és el màxim subespai γ-invariant de V_j amb exponent p^ν. Com que $V_j^{(\nu)} \subseteq W_j$ per hipòtesi, tenim la igualtat $W_j = V_j^{(\nu)}$.

Recíprocament, suposem que W és pròpia i sigui $\Lambda_W = \{\lambda_{i_1}, \ldots, \lambda_{i_t}\}$ el conjunt de valors propis pels quals $W_i \neq 0$. Pel Lema 9.6, cada subespai W_i és propi i, pel Lema 9.5, $W_i = V_i^{(\nu_i)}$, per a algun $0 \leq \nu_i \leq \delta_i$. Volem provar dues coses: que Λ_W és propi i que $\nu_{i_1} = \nu_{i_2} = \cdots = \nu_{i_t}$. Ara, si

$$\nu_{i_j} < \nu := \max\{\nu_{i_1}, \ldots, \nu_{i_t}\},$$

tindríem $W \subsetneq V_{\Lambda_W}^{(\nu)}$ i, en canvi, $\exp(W) = \exp(V_{\Lambda_W}^{(\nu)})$, amb la qual cosa W no seria pròpia. Finalment, si $\Lambda_W \subsetneq \Lambda$, amb $D(\Lambda_W) = D(\Lambda)$, tindríem també $W = V_{\Lambda_W}^{(\nu)} \subsetneq V_\Lambda^{(\nu)}$ i W tampoc seria pròpia. □

Corol.lari 9.9. *Sigui $\delta = \delta(\{1, \ldots, r\})$. Tenim una identificació natural:*

$$\mathcal{L}_\gamma^{\mathrm{pr}} \hookrightarrow [\delta] \times \mathbf{B}_r^{\mathrm{pr}},$$

essent la imatge el subposet format pels (ν, Λ) amb $\nu \leq \delta(\Lambda)$. En particular, $\mathcal{L}_\gamma^{\mathrm{pr}}$ és un poset finit.

Corol.lari 9.10. *El poset $\mathcal{L}_\gamma^{\mathrm{pr}}$ és un reticle.*

Demostració. Pel corol·lari anterior és suficient provar que el poset $\mathbf{B}(\lambda_1,\ldots,\lambda_r)^{\mathrm{pr}}$ és un reticle. El conjunt total $\hat{1}$ és sempre propi; per [Sta99, 3.3.1] és suficient comprovar que la intersecció de dos elements propis és un element propi. Considerem Λ_0, Λ_1, $\Lambda_2 \subseteq \Lambda$ disjunts dos a dos i tals, que $\Lambda_0 \cup \Lambda_1$ i $\Lambda_0 \cup \Lambda_2$ són propis. Provem que necessàriament Λ_0 és propi. Suposem que $D(\Lambda_0 \cup \{\lambda\}) = D(\Lambda_0)$; en particular,

$$D(\Lambda_0 \cup \Lambda_1 \cup \{\lambda\}) = D(\Lambda_0 \cup \Lambda_1), \qquad D(\Lambda_0 \cup \Lambda_2 \cup \{\lambda\}) = D(\Lambda_0 \cup \Lambda_2).$$

Com que aquests conjunts són propis tenim $\lambda \in \Lambda_0 \cup \Lambda_1$ i $\lambda \in \Lambda_0 \cup \Lambda_2$ i, com que els tres conjunts eren disjunts dos a dos, forçosament $\lambda \in \Lambda_0$. □

Acabem aquesta secció amb una propietat crucial de les subvarietats γ-invariants i pròpies. Recordem que σ denota l'automorfisme de Frobenius de $\overline{k}$ i k_n denota l'única extensió de grau n de k dins $\overline{k}$. Recordem també que el *grau* d'una subvarietat $V \subseteq \mathbb{P}^N(\overline{k})$ és el mínim exponent r tal, que $\sigma^r(V) = V$, o, equivalentment, el mínim nombre natural r tal que V és k_r-definida. El denotarem $r = \deg(V)$.

Proposició 9.11. *Sigui V una subvarietat γ-invariant i pròpia de $\mathbb{P}^N$, de grau r. Aleshores,*

$$V \cap \sigma^i(V) = \emptyset, \quad \forall\, 0 < i < r.$$

Demostració. Suposem que $0 < i < r$ i denotem per W la mínima subvarietat lineal que conté V i $\sigma^i(V)$; clarament, W és també γ-invariant. Com que γ commuta amb σ, tenim $\exp(V) = \exp(\sigma^i(V))$. Ara, si fos $V \cap \sigma^i(V) \neq \emptyset$, tindríem $V \subsetneq W$ i $\exp(V) = \exp(W)$, en contra de la hipòtesi de que V és pròpia. □

Corol.lari 9.12. *Sigui V una subvarietat γ-invariant i pròpia de $\mathbb{P}^N$, de grau r. Sigui $V_G := V \cup \sigma(V) \cup \cdots \cup \sigma^{r-1}(V)$ la varietat algebraica k-definida determinada per V. Aleshores,*

$$\mathrm{Z}(V_G/k, x) = \mathrm{Z}(V/k_r, x^r).$$

Demostració. Volem provar la identitat de sèries formals:

$$\sum_{m\geq 1} \frac{|V_G(k_m)|}{m} x^m = \sum_{n\geq 1} \frac{|V(k_{rn})|}{n} x^{rn}. \tag{46}$$

D'entrada és clar que $r \nmid m \implies V_G(k_m) = \emptyset$. En efecte,

$$P \in V_G(k_m) \implies P \in \sigma^i(V),\ \sigma^m(P) = P \implies P \in \sigma^i(V) \cap \sigma^{i+m}(V),$$

i això implica que $r | m$ per la proposició anterior.

Per tant, fent el canvi $m = rn$ en la sèrie de l'esquerra de (46) i tenint en compte (també per la proposició anterior) que $|V_G(k_{rn})| = r|V(k_{rn})|$, comprovem que la sèrie coincideix amb la de la dreta. □

10 Funcions generadores i indicadors d'exponents

Sigui k un cos finit i $\gamma \in \Gamma := \mathrm{PGL}_{N+1}(k)$. Considerem el poset $\mathcal{L}_\gamma^{\mathrm{pr}}$ de les subvarietats γ-invariants pròpies de $\mathbb{P}^N(\overline{k})$, amb la inclusió com a relació d'ordre.

Per a cada $V \in \mathcal{L}_\gamma^{\mathrm{pr}}$, definim

$$V^0 := V \setminus \cup_{W<V} W.$$

Podem considerar una estratificació de $\mathbb{P}^N$:

$$\mathbb{P}^N = \coprod_{V \in \mathcal{L}_\gamma^{\mathrm{pr}}} V^0.$$

Fem notar que, per a tot $P \in V^0$, la γ-òrbita $O_\gamma(P)$ té cardinal $\exp(V)$ (la demostració del Lema 2.14 és vàlida en qualsevol dimensió). Això fa que puguem aplicar el Corol·lari 7.1 per comptar el nombre de Γ-òrbites de diferents tipus de n-conjunts.

10.1 Teoremes principals

Enumeració d'òrbites de n-conjunts de punts k-racionals

Denotem per $\mathcal{L}_\gamma^{\mathrm{pr}}(k)$ el subposet de $\mathcal{L}_\gamma^{\mathrm{pr}}$ format per les subvarietats k-definides.

Teorema 10.1. *La funció generadora dels $T_N(n)$, resp. $\overline{T}_N(n)$, és:*

$$\sum_{\gamma \in \mathcal{C}} \frac{1}{|\Gamma_\gamma|} \prod_{V \in \mathcal{L}_\gamma^{\mathrm{pr}}(k)} h_{V^0}(x^{\exp(V)}), \tag{47}$$

on, per a qualsevol subvarietat $U \subseteq \mathbb{P}^N(k)$, denotem:

$$h_U(x) := (1+x)^{|U(k)|}, \quad \textit{resp.} \quad h_U(x) := (1-x)^{-|U(k)|}.$$

Demostració. Per a $X = \binom{\mathbb{P}^N(k)}{n}$, resp. $X = \left(\!\!\binom{\mathbb{P}^N(k)}{n}\!\!\right)$, aplicant el Corol·lari 7.1 obtenim la següent generalització del Lema 3.1:

$$|X_\gamma| = \sum_{\sum_{V \in \mathcal{L}_\gamma^{\mathrm{pr}}(k)} n_V \exp(V) = n} \left(\prod_{V \in \mathcal{L}_\gamma^{\mathrm{pr}}(k)} \binom{|V^0(k)|}{n_V} \right),$$

resp.

$$|X_\gamma| = \sum_{\sum_{V \in \mathcal{L}_\gamma^{\mathrm{pr}}(k)} n_V \exp(V) = n} \left(\prod_{V \in \mathcal{L}_\gamma^{\mathrm{pr}}(k)} \left(\!\!\binom{|V^0(k)|}{n_V}\!\!\right) \right).$$

El lema de Cauchy-Frobenius (2) acaba la demostració. □

Podem aspirar a simplificar aquesta expressió de la funció generadora a partir de les idees del capítol 1. D'entrada, cal classificar les classes de conjugació de Γ en *subtipus*. Introduïm la següent relació d'equivalència sobre $\mathcal{C}$: diem que dues classes de conjugació γ, γ' són *del mateix subtipus* si existeix un isomorfisme de posets:

$$\phi\colon \mathcal{L}_{\gamma}^{\mathrm{pr}}(k) \xrightarrow[\sim]{} \mathcal{L}_{\gamma'}^{\mathrm{pr}}(k),$$

que preserva el *pes* $(\dim(V), \exp(V))$ de cada vèrtex V del poset. El conjunt quocient $\mathcal{T} := \mathcal{C}/\sim$ l'anomenem *conjunt dels possibles subtipus*, i denotem per $\mathrm{st}\colon \mathcal{C} \to \mathcal{T}$ l'aplicació quocient, que assigna a cada $\gamma \in \mathcal{C}$ el seu subtipus.

Per a cada subtipus $\alpha \in \mathcal{T}$ podríem descriurem de manera intrínseca el poset (amb pes $(\dim(V), \exp(V))$ en cada vèrtex) $\mathcal{L}(\alpha) := \mathcal{L}_{\gamma}^{\mathrm{pr}}(k)$, on $\mathrm{st}(\gamma) = \alpha$. Aleshores, si comptem el nombre de γ amb el mateix subtipus, afectat del pes $|\Gamma_\gamma|^{-1}$:

$$N_\alpha := \sum_{\gamma \in \mathrm{st}^{-1}(\alpha)} \frac{1}{|\Gamma_\gamma|},$$

obtenim una fórmula molt més explícita per a la funció generadora que ens ocupa:

Teorema 10.2. *La funció generadora dels $T_N(n)$, resp. $\overline{T}_N(n)$, és:*

$$\sum_{\alpha \in \mathcal{T}} N_\alpha \prod_{V \in \mathcal{L}(\alpha)} h_{V^0}(x^{\exp(V)}),$$

on, per a qualsevol subvarietat $U \subseteq \mathbb{P}^N(k)$, denotem:

$$h_U(x) := (1+x)^{|U(k)|}, \quad \textit{resp.} \quad h_U(x) := (1-x)^{-|U(k)|}.$$

Al capítol 1 hem obtingut fórmules explícites per a aquests N_α en dimensió 2. Un càlcul similar en dimensió arbitrària sembla prou enredat i no el treballarem en aquesta memòria.

Un inconvenient de la fórmula del Teorema 10.2 és la dificultat de calcular $h_{V^0}(x)$. En els casos que estem tractant ara es redueix a calcular $|V^0(k)|$ i a tal fi podem utilitzar inversió de Möbius en el poset $\mathcal{L}_{\gamma}^{\mathrm{pr}}(k)$. Clarament,

$$|V(k)| = \sum_{W \leq V} |W^0(k)| \implies |V^0(k)| = \sum_{W \leq V} \mu(W,V)|W(k)| = \\ = \sum_{W \leq V} \mu(W,V) \frac{q^{\dim(W)} - 1}{q-1},$$

on $\dim(W)$ indica la dimensió afí.

Per acabar, podem especular també sobre l'existència d'un *indicador d'exponents* $\mathcal{L}(\Gamma, X) \in \mathbb{Q}[z_1, \ldots, z_r]$ definible per a qualsevol grup finit Γ actuant sobre una varietat algebraica V, que permeti calcular la funció generadora dels $\left|\Gamma\backslash\backslash \binom{V(k)}{n}\right|$ o dels $\left|\Gamma\backslash\backslash \left(\!\binom{V(k)}{n}\!\right)\right|$. Per al cas particular de $\Gamma = \mathrm{PGL}_{N+1}(k)$ i $V = \mathbb{P}^N$, hem vist que cal considerar:

$$\mathcal{L}(\Gamma, \mathbb{P}^N) = \sum_{\alpha \in \mathcal{T}} N_\alpha \prod_{V \in \mathcal{L}(\alpha)} z_{\alpha,V},$$

i la funció generadora que ens interessa és $\mathcal{L}(\Gamma, \mathbb{P}^N)_{|z_{\alpha,V} = h_{V\,0}(x^{\exp(V)})}$.

L'avantatge d'aquest indicador d'exponents respecte de l'indicador de cicles de Pólya és múltiple: d'una banda, $\mathcal{L}(\Gamma, \mathbb{P}^N)$ té un nombre molt més reduït de variables; de l'altra, a la secció 10.2 obtindrem una descripció de $\mathcal{T}$ i $\mathcal{L}(\alpha)$ en termes de dades combinatòries explícites que ja recullen (i fan innecessari tenir en compte) l'efecte de l'acció dels diferents γ com a permutacions de $\mathbb{P}^N$; finalment, aquest indicador d'exponents admet una generalització natural que permet resoldre d'una manera completament anàloga l'enumeració de les òrbites de n-conjunts racionals.

Enumeració d'òrbites de n-conjunts racionals

Cal substituir el poset $\mathcal{L}^{\mathrm{pr}}_\gamma(k)$ per un poset que contempli totes les subvarietats lineals γ-invariants i no només les k-definides. Per a $G := \mathrm{Gal}(\overline{k}/k)$ definim,

$$\mathcal{L}^{\mathrm{pr}}_{\gamma,G} := G\backslash\backslash\mathcal{L}^{\mathrm{pr}}_\gamma.$$

Cada vèrtex d'aquest nou poset és una G-òrbita $\{V, \sigma(V), \ldots, \sigma^{r-1}(V)\}$, on $r = \deg(V)$. Cada subvarietat de la mateixa òrbita té la mateixa dimensió, el mateix exponent i el mateix grau. En particular, cada element V d'aquest poset té un pes $(\dim(V), \exp(V), \deg(V))$ i tots els elements són propis respecte del morfisme que assigna a cada element el seu exponent. Podem pensar que $\mathcal{L}^{\mathrm{pr}}_{\gamma,G}$ coincideix amb $(G\backslash\backslash\mathcal{L}_\gamma)^{\mathrm{pr}}$. Clarament, el poset $\mathcal{L}^{\mathrm{pr}}_\gamma(k)$ es pot identificar al subposet de $\mathcal{L}^{\mathrm{pr}}_{\gamma,G}$ format pels elements V que tenen $\deg(V) = 1$.

Considerem un n-conjunt $\Sigma \subseteq \mathbb{P}^N$, k-definit i γ-invariant. Per a cada punt $P \in \Sigma$, l'òrbita $(G \cdot \gamma)P$ sota l'acció simultània de G i γ està continguda a Σ. Ara, si P pertany a una varietat V γ-invariant de grau r, necessàriament aquesta òrbita $(G \cdot \gamma)P$ està continguda dins la unió:

$$V_G := \bigcup_{0 \le s < r} \sigma^s(V).$$

Aquesta varietat algebraica V_G és k-definida i, pel Teorema 4.2 i el Corol·lari 9.12, coneixem les funcions generadores $f_{V_G}(x)$, $\bar{f}_{V_G}(x)$ dels nombres $\left|\binom{V_G}{n}(k)\right|$, resp. $\left|\left(\!\binom{V_G}{n}\!\right)(k)\right|$:

Corol.lari 10.3. $f_{V_G}(x) = f_V(x^{\deg(V)})$, *resp.* $\bar{f}_{V_G}(x) = \bar{f}_V(x^{\deg(V)})$, *on*

$$f_V(x) = \frac{\mathrm{Z}(V/k_r, x)}{\mathrm{Z}(V/k_r, x^2)}, \quad \textit{resp.} \quad \bar{f}_V(x) = \mathrm{Z}(V/k_r, x),$$

és la funció generadora dels $\left|\binom{V}{n}(k_r)\right|$, *resp.* $\left|\left(\!\binom{V}{n}\!\right)(k_r)\right|$.

Prenent $X = \binom{\mathbb{P}^N}{n}(k)$, resp. $X = \left(\!\binom{\mathbb{P}^N}{n}\!\right)(k)$, tenim ara

$$|X_\gamma| = \sum_{\sum_{V\in\mathcal{L}^{\mathrm{pr}}_{\gamma,G}} n_V \exp(V)=n} \left(\prod_{V\in\mathcal{L}^{\mathrm{pr}}_{\gamma,G}} \binom{|V^0|}{n_V}(k)\right),$$

resp.

$$|X_\gamma| = \sum_{\sum_{V\in\mathcal{L}^{\mathrm{pr}}_{\gamma,G}} n_V \exp(V)=n} \left(\prod_{V\in\mathcal{L}^{\mathrm{pr}}_{\gamma,G}} \left(\!\binom{|V^0|}{n_V}\!\right)(k)\right).$$

Els arguments utilitzats en la prova del Teorema 10.1 permeten provar d'idèntica manera:

Teorema 10.4. *La funció generadora dels* $t_N(n)$, *resp.* $\bar{t}_N(n)$, *és:*

$$\sum_{\gamma\in\mathcal{C}} \frac{1}{|\Gamma_\gamma|} \prod_{V\in\mathcal{L}^{\mathrm{pr}}_{\gamma,G}} f_{V^0}(x^{\exp(V)\deg(V)}),$$

on, per a qualsevol subvarietat $U \subseteq \mathbb{P}^N$ *de grau* r, *denotem:*

$$f_U(x) := \frac{\mathrm{Z}(U/k_r, x)}{\mathrm{Z}(U/k_r, x^2)}, \quad \textit{resp.} \quad \bar{f}_U(x) := \mathrm{Z}(U/k_r, x).$$

Podem considerar també el corresponent concepte de subtipus. Diem que dos elements $\gamma, \gamma' \in \Gamma$ són del mateix G-subtipus si existeix un isomorfisme de posets,

$$\phi\colon \mathcal{L}^{\mathrm{pr}}_{\gamma,G} \xrightarrow[\sim]{} \mathcal{L}^{\mathrm{pr}}_{\gamma',G},$$

que preserva el pes $(\dim(V), \exp(V), \deg(V))$ de cada vèrtex V del poset. Denotem per $\mathcal{T}_G$ el conjunt dels possibles G-subtipus i per $\mathrm{st}_G(\gamma) \in \mathcal{T}_G$ el G-subtipus de cada $\gamma \in \mathrm{GL}_{N+1}(k)$.

A la secció 10.2 descriurem de manera intrínseca (i.e. en termes de dades combinatòries senzilles, que depenen només de N) un poset $\mathcal{L}_G(\alpha) \simeq \mathcal{L}^{\mathrm{pr}}_{\gamma,G}$, per a cada $\alpha \in \mathcal{T}_G$, amb pes $(\dim(V), \exp(V), \deg(V))$ en cada vèrtex, on $\mathrm{st}_G(\gamma) = \alpha$. Considerant els corresponents *coeficients universals* (diferents dels del cas anterior)

$$N_{G,\alpha} := \sum_{\alpha \in \mathrm{st}_G^{-1}(\alpha)} \frac{1}{|\Gamma_\gamma|},$$

obtenim una fórmula molt més explícita per a la funció generadora que ens ocupa:

Teorema 10.5. *La funció generadora dels $t_N(n)$, resp. $\bar{t}_N(n)$, és:*

$$\sum_{\alpha \in \mathcal{T}_G} N_{G,\alpha} \prod_{V \in \mathcal{L}_G(\alpha)} f_{V^0}(x^{\exp(V)\deg(V)}),$$

on, per a qualsevol subvarietat $U \subseteq \mathbb{P}^N$ de grau r, denotem:

$$f_U(x) := \frac{\mathrm{Z}(U/k_r, x)}{\mathrm{Z}(U/k_r, x^2)}, \qquad \textit{resp.} \qquad \bar{f}_U(x) := \mathrm{Z}(U/k_r, x).$$

Aquest es pot considerar el resultat principal de la memòria. També podem expressar la funció generadora en termes d'un G-indicador d'exponents anàleg al que hem introduït al paràgraf anterior:

$$\mathcal{L}_G(\Gamma, \mathbb{P}^N)_{|z_{\alpha,V} = f_{V^0}(x^{\exp(V)\deg(V)})},$$

on ara:

$$\mathcal{L}_G(\Gamma, \mathbb{P}^N) = \sum_{\alpha \in \mathcal{T}_G} N_{G,\alpha} \prod_{V \in \mathcal{L}_G(\alpha)} z_{\alpha,V}.$$

Com abans, també podem calcular $f_{V^0}(x)$ usant inversió de Möbius. Si denotem $g_V(x) := f_{V^0}(x)$, aleshores, pel Corol.lari 4.3, tenim:

$$f_V(x) = \prod_{W \leq V} g_W(x).$$

Podem pensar f_V, g_V com a funcions $\mathcal{L}^{\mathrm{pr}}_{\gamma,G} \to \mathbb{Q}[\![x]\!]$, i aplicar la inversió de Möbius:

$$g_V = \prod_{W \leq V} (f_W)^{\mu(W,V)}.$$

Aquest punt de vista té l'avantatge de què el resultat pren una forma que només depèn de $\dim(W)$, ja que $W \simeq \mathbb{P}^{\dim(W)}$ i coneixem explícitament $\mathrm{Z}(\mathbb{P}^{\dim(W)}/k, x)$.

Posets semipropis

En el Teorema 10.1 podem substituir el poset $\mathcal{L}_\gamma^{\rm pr}(k)$ per qualsevol poset $\mathcal{L}$ satisfent $\mathcal{L}_\gamma^{\rm pr}(k) \subseteq \mathcal{L} \subseteq \mathcal{L}_\gamma(k)$, entenent que el subposet $\mathcal{L}$ manté el pes $(\dim(V), \exp(V))$ de cada vèrtex V. En efecte, considerem per exemple el poset $\mathcal{L} = \mathcal{L}_\gamma^{\rm pr}(k) \cup \{V\}$ obtingut adjuntant a $\mathcal{L}_\gamma^{\rm pr}(k)$ qualsevol subvarietat no pròpia V; per a qualsevol $W \supseteq V$, amb W pròpia del mateix exponent que V, en la fórmula (47) el factor $h_{W^0}(x^{\exp(W)})$ és substituït per:

$$h_{W^0 \setminus V^0}(x^{\exp(W)}) h_{V^0}(x^{\exp(W)}),$$

i, per la multiplicativitat de la funció $h_U(x)$ respecte d'unions disjuntes, obtenim el mateix resultat. Ja havíem comentat una observació similar a la Remarca 3.2 i l'hem utilitzada abastament a les seccions 7.1 i 7.2.

Definició 10.6. *Un subposet $\mathcal{L}$ satisfent $\mathcal{L}_\gamma^{\rm pr}(k) \subseteq \mathcal{L} \subseteq \mathcal{L}_\gamma(k)$ direm que és semipropi respecte de l'exponent.*

Hem de pensar que el poset $\mathcal{L}_\gamma^{\rm pr}(k)$ conté els mínims ingredients necessaris perquè la fórmula (47) sigui correcta, però pot ser substituït per qualsevol subposet semipropi. Podríem substituir-lo, per exemple, pel poset total $\mathcal{L}_\gamma(k)$, però la fórmula es tornaria impracticable; per exemple, quan γ tingués una varietat 3-dimensional V de punts fixos, estaríem fent intervenir en la fórmula cada punt, cada recta i cada pla de V de manera individualitzada.

D'altra banda, necessitem que la descripció del poset en termes combinatoris sigui senzilla, i en aquest aspecte el concepte de propi pot complicar les coses. Per aquest motiu, en la secció següent modificarem convenientment el concepte de subtipus i el poset $\mathcal{L}(\alpha)$ que associarem a cada subtipus α serà semipropi (i molt proper a $\mathcal{L}_\gamma^{\rm pr}(k)$), però no propi estrictament. El que importa és que entre els nodes de $\mathcal{L}(\alpha)$ es considerin tots els exponents possibles (no hem d'ignorar subvarietats amb exponent menor que la varietat que les conté); en alguna situació, controlarem aquest conjunt d'exponents possibles d'una manera molt senzilla, però no esporgarem les possibles repeticions d'exponents, perquè ens duria a complicar la descripció del poset.

Anàlogament, en la fórmula del Teorema 10.4 podem substituir el poset $\mathcal{L}_{\gamma,G}^{\rm pr}$ per posets $\mathcal{L}$ que satisfan condicions més febles:

Definició 10.7. *Un subposet $\mathcal{L} \subseteq \mathcal{L}_{\gamma,G}$ direm que és semipropi respecte de l'exponent si satisfà:*

(1) $\mathcal{L}_{\gamma,G}^{\rm pr} \subseteq \mathcal{L} \subseteq \mathcal{L}_{\gamma,G}$,

(2) $V \cap \sigma^i(V) = \emptyset,\ \forall\, 0 < i < \deg(V),\ \forall V \in \mathcal{L}$.

En efecte, gràcies a la segona condició continuen sent vàlids els Corol·laris 9.12 i 10.3. Anàlogament al cas anterior, a la secció següent introduirem un concepte de G-subtipus lleugerament diferent i associarem a cada G-subtipus α un poset semipropi $\mathcal{L}_G(\alpha)$, molt proper a $\mathcal{L}^{\mathrm{pr}}_{\gamma,G}$ però no necessàriament igual.

10.2 Descripció dels subtipus i els seus posets associats

Continuem treballant amb un element $\gamma \in \Gamma := \mathrm{PGL}_{N+1}(k)$ fixat, i denotem també per $\gamma \in \mathrm{GL}_{N+1}(k)$ l'elecció d'un representant a GL_{N+1}.

10.2.1 Descripció intrínseca del conjunt $\mathcal{T}$ i els posets $\mathcal{L}(\alpha)$

La descripció del poset $\mathcal{L}^{\mathrm{pr}}_\gamma(k)$ es dedueix de la descripció de $\mathcal{L}^{\mathrm{pr}}_\gamma$ que es fèia al Teorema 9.8. Suposem que el polinomi característic de γ descompon en producte de factors irreductibles:

$$P_\gamma(x) = \prod_{i=1}^{r} h_i(x)^{e_i}, \tag{48}$$

amb els $h_i(x) \in k[x]$ polinomis mònics irreductibles de grau w_i, diferents dos a dos, i denotem per $\lambda_1, \ldots, \lambda_r \in \overline{k}$ una elecció qualsevol d'una arrel de cada polinomi. Aleshores, γ admet una forma normal de Jordan: $\gamma = \mathrm{diag}(\gamma_1, \ldots, \gamma_r)$, amb:

$$\gamma_i = \mathrm{diag}(B_i, \overset{n_1^{(i)}}{\ldots}, B_i, B_i(2), \overset{n_2^{(i)}}{\ldots}, B_i(2), \ldots, B_i(s_i), \overset{n_{s_i}^{(i)}}{\ldots}, B_i(s_i)), \tag{49}$$

on $B_i(s)$ és un bloc de Jordan de mida s associat al polinomi irreductible $h_i(x)$:

$$B_i(s) = \begin{pmatrix} B_i & & & & & \\ J & B_i & & & & \\ & J & B_i & & & \\ & & \ddots & \ddots & & \\ & & & & B_i & \\ & & & & J & B_i \end{pmatrix} \in \mathrm{GL}_{sw_i}(k), \tag{50}$$

on B_i, J són les matrius bàsiques:

$$B_i = \begin{pmatrix} 0 & & & & -a_{w_i} \\ 1 & 0 & & & -a_{w_i-1} \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & -a_2 \\ & & & 1 & -a_1 \end{pmatrix}, \qquad J = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix}, \tag{51}$$

amb $h_i(x) = x^{w_i} + a_1 x^{w_i-1} + \cdots + a_{w_i}$ (cf. (28) i (29) del capítol 3).

Anàlogament a com fèiem a la secció 9, podem considerar morfismes de posets:

$$D\colon \mathbf{B}_r \longrightarrow \mathbf{D}_{\mathbb{N}}, \qquad \delta\colon \mathbf{B}_r \longrightarrow \mathbb{N},$$

definits per, si $\Lambda = \{i_1, \ldots, i_t\}$:

$$D(\Lambda) = \min\{d \in \mathbb{N} \mid \lambda_{i_1}^d = \lambda_{i_2}^d = \cdots = \lambda_{i_t}^d \in k\}, \tag{52}$$

$$\delta(\Lambda) = \min\{\ell \in \mathbb{N} \mid p^\ell \geq s_{i_1}, \ldots, s_{i_t}\}. \tag{53}$$

És clar que el mínim natural d tal que $\lambda_i^d \in k$ no depèn de l'elecció de l'arrel λ_i entre les arrels del polinomi $h_i(x)$; per tant, la definició del morfisme D és independent de l'elecció inicial d'una arrel de cada factor irreductible del polinomi característic. D'altra banda, l'exigència de què $\lambda_{i_1}^d = \lambda_{i_2}^d = \cdots = \lambda_{i_t}^d \in k$ sembla diferent de com definíem D a la secció 9. No és així; com que només ens interessen subvarietats k-definides, quan escollim $\lambda_i \in \Lambda$ és com si obliguem a què Λ contingui també tots els conjugats de λ_i. D'aquesta manera, noteu que el morfisme D ara definit coincideix amb el morfisme D de la secció 9 avaluat en el conjunt format per $\lambda_{i_1}, \lambda_{i_2}, \ldots, \lambda_{i_t}$ i tots els seus conjugats galoisians.

Com a conseqüència immediata del Teorema 9.8 i el Corol·lari 9.9, les subvarietats γ-invariants pròpies i k-definides vénen parametritzades per parells $V(\nu, \Lambda)$, amb $\Lambda \in \mathbf{B}_r$ D-propi, i ν un enter no negatiu, $0 \leq \nu \leq \delta(\Lambda)$. Clarament,

$$V(\nu, \Lambda) \subseteq V(\nu', \Lambda') \iff \nu \leq \nu', \quad \Lambda \subseteq \Lambda',$$

$$\dim(V(\nu, \Lambda)) = -1 + \sum_{i \in \Lambda} \left(n_1^{(i)} + 2n_2^{(i)} + \cdots + (p^\nu - 1)n_{p^\nu - 1}^{(i)} + p^\nu \left(n_{p^\nu}^{(i)} + \cdots + n_{s_i}^{(i)} \right) \right) w_i,$$

$$\exp(V(\nu, \Lambda)) = p^\nu D(\Lambda).$$

Ens agradaria descriure aquest poset, i els pesos de cada vèrtex, exclusivament en termes de dades numèriques independents de γ. A tal fi, estudiem algunes propietats del morfisme D.

Lema 10.8. *Per a qualssevol i, $j \in [r]$ i Λ_1, $\Lambda_2 \subseteq [r]$ tenim:*

1. $D(\{i\}) | \dfrac{q^{w_i} - 1}{q - 1}$, $\quad D(\{i\}) \nmid \dfrac{q^w - 1}{q - 1}$, $\forall w < w_i$.
2. $D(\{i, j\}) = \operatorname{mcm}(D(\{i\}), D(\{j\})) \cdot d$, *per a cert* $d | (q - 1)$.
3. $D(\Lambda_1 \cup \Lambda_2) = \operatorname{mcm}(D(\Lambda_1), D(\Lambda_2))$, *si* $\Lambda_1 \cap \Lambda_2 \neq \emptyset$.

Demostració. La primera afirmació es dedueix de $D(\{i\}) = \mathrm{ord}_{k_w^*/k^*}(\lambda_i)$ i del fet que $h_i(x)$ és irreductible.

Per provar la segona afirmació, posem $\lambda_i^{d_i} = a \in k$, $\lambda_j^{d_j} = b \in k$, amb d_i, d_j mínims amb aquesta propietat. Considerem $e = \mathrm{mcm}(d_i, d_j)$; si $\lambda_i^D = \lambda_j^D \in k$, amb D mínim, necessàriament $D = ed$ per a algun enter d. Ara, $d = \mathrm{ord}_{k^*}((\lambda_i/\lambda_j)^e)$ i per tant, $d|(q-1)$.

Finalment, per provar la tercera afirmació, posem: $D_1 = D(\Lambda_1)$, $D_2 = D(\Lambda_2)$, $e = \mathrm{mcm}(D_1, D_2)$. Si $\ell \in \Lambda_1 \cap \Lambda_2$, tenim:

$$\lambda_\ell^{D_1} = \lambda_i^{D_1} \in k,\ \forall i \in \Lambda_1, \quad \lambda_\ell^{D_2} = \lambda_j^{D_2} \in k,\ \forall j \in \Lambda_2 \implies \lambda_j^e = \lambda_\ell^e = \lambda_i^e,$$

per a tot $i \in \Lambda_1$, $j \in \Lambda_2$. □

Tipus i Subtipus

Definició 10.9. *Una partició de $N+1$ amb pesos $0 < w_1 \leq w_2 \leq \cdots \leq w_r$ ve donada per r famílies*

$$\left((n_1^{(i)}, n_2^{(i)}, \ldots, n_{s_i}^{(i)})\right)_{1 \leq i \leq r}$$

d'enters no negatius, satisfent:

$$\sum_{i=1}^{r} \left(n_1^{(i)} + 2n_2^{(i)} + \cdots + s_i n_{s_i}^{(i)}\right) w_i = N+1.$$

Denotem per $\mathcal{P}_{N+1}$ el conjunt de totes les particions de $N+1$ amb pesos, variant r i els w_i de totes les maneres possibles.

A cada partició d'aquestes li podem associar un morfisme de posets $\delta\colon \mathbf{B}_r \longrightarrow \mathbb{N}$ donat per (53).

Hem vist més amunt que cada $\gamma \in \mathrm{GL}_{N+1}(k)$ té associada una partició d'aquestes, que anomenem el *tipus de* γ. Clarament, el tipus de γ no depèn de la classe de γ a $\mathrm{PGL}_{N+1}(k)$ i podem considerar

$$t\colon \mathrm{PGL}_{N+1}(k) \longrightarrow \mathcal{P}_{N+1}, \qquad \gamma \mapsto t(\gamma),$$

l'aplicació que assigna a cada k-automorfisme de $\mathbb{P}^N$ el seu tipus. Les classes de conjugació de $\mathrm{PGL}_{N+1}(k)$ es corresponen amb famílies $(t; h_1(x), \ldots, h_r(x))$, on $t \in \mathcal{P}_{N+1}$ i els h_i són polinomis mònics irreductibles de grau w_i, diferents dos a dos, classificats per la relació d'equivalència:

$$(h_1(x), \ldots, h_r(x)) \sim (h_1^\lambda(x), \ldots, h_r^\lambda(x)), \quad \forall \lambda \in k^*.$$

Definició 10.10. *Una distribució d'exponents, amb pesos* $0 < w_1 \leq w_2 \leq \cdots \leq w_r$, *és una doble família:*

$$(d_i)_{1\leq i\leq r}\,, \qquad (d_{i,j})_{1\leq i<j\leq r}\,,$$

d'enters positius, satisfent:

1. $d_i | \dfrac{q^{w_i}-1}{q-1}$; $\qquad d_i \nmid \dfrac{q^{w}-1}{q-1}$, $\forall w < w_i$.
2. $d_{i,j} = \mathrm{mcm}(d_i, d_j)\cdot e_{i,j}$, *per a cert* $e_{i,j} | (q-1)$.
3. $\mathrm{mcm}(d_{i,j}, d_{i,k}) = \mathrm{mcm}(d_{i,j}, d_{j,k})$, $\forall i,j,k \in [r]$.

Denotem per $\mathcal{D}$ *el conjunt de totes les distribucions d'exponents amb pesos, variant* r *i els* w_i *de totes les maneres possibles.*

Tota distribució d'exponents $\tau \in \mathcal{D}$ determina de manera evident un morfisme de posets:

$$D_\tau \colon \mathbf{B}_r \longrightarrow \mathbf{D}_{\mathbb{N}}, \qquad \Lambda \mapsto D_\tau(\Lambda),$$

$$D_\tau(\Lambda) := \begin{cases} d_i, & \text{per a } \Lambda = \{i\}, \\ d_{i,j}, & \text{per a } \Lambda = \{i,\, j\}, \\ \mathrm{mcm}(D_\tau(\Lambda_1), D_\tau(\Lambda_2)), & \text{per a } \Lambda = \Lambda_1 \cup \Lambda_2, \text{ amb } \Lambda_1 \cap \Lambda_2 \neq \emptyset. \end{cases}$$

Hem vist més amunt que cada $\gamma \in \mathrm{GL}_{N+1}(k)$ té associada una distribució d'aquestes, que anomenem la *distribució d'exponents de* γ. Un altre cop, la distribució d'exponents és invariant per l'acció de k^* sobre $\mathrm{GL}_{N+1}(k)$ i podem considerar l'aplicació

$$\tau \colon \mathrm{PGL}_{N+1}(k) \longrightarrow \mathcal{D}, \qquad \gamma \mapsto \tau(\gamma),$$

que assigna a cada k-automorfisme de $\mathbb{P}^N$ la distribució d'exponents determinada per la igualtat $D_{\tau(\gamma)} = D$, on D és l'aplicació donada per (52).

Definició 10.11. *Un subtipus és un element del conjunt* $\mathcal{T}$ *format pels parells* (t, τ), *on* t *és una partició de* $N+1$ *amb pesos i* τ *una distribució d'exponents amb els mateixos pesos* $0 < w_1 \leq \cdots \leq w_r$ *que* t.

A cada subtipus $\alpha \in \mathcal{T}$ li podem associar un poset $\mathcal{L}(\alpha)$, amb nodes $V(\nu, \Lambda)$ parametritzats per parells (ν, Λ), amb $\Lambda \in \mathbf{B}_r$ i ν un enter, $0 \leq \nu \leq \delta(\Lambda)$. La relació d'ordre és la natural:

$$V(\nu, \Lambda) \subseteq V(\nu', \Lambda') \iff \nu \leq \nu', \quad \Lambda \subseteq \Lambda'.$$

Podem associar a cada node $V(\nu, \Lambda)$ d'aquest poset pesos *dimensió* i *exponent* donats per:

$$\dim V(\nu,\Lambda) = -1+ \sum_{i\in\Lambda}\left(n_1^{(i)} + 2n_2^{(i)} + \cdots + (p^\nu-1)n_{p^\nu-1}^{(i)} + p^\nu\left(n_{p^\nu}^{(i)} + \cdots + n_{s_i}^{(i)}\right)\right) w_i,$$

$$\exp V(\nu,\Lambda) = p^\nu D_\tau(\Lambda).$$

Cada $\gamma \in \mathrm{PGL}_{N+1}(k)$ té associat un subtipus $\alpha := \mathrm{st}(\gamma) := (t(\gamma),\tau(\gamma))$ i de manera tautològica tenim una inclusió de posets

$$\mathcal{L}_\gamma^{\mathrm{pr}}(k) \subseteq \mathcal{L}(\alpha),$$

que preserva el pes $(\dim, \exp)$ dels nodes. El poset $\mathcal{L}_\gamma^{\mathrm{pr}}(k)$ s'identifica al subposet de $\mathcal{L}(\alpha)$ format pels nodes $V(\nu,\Lambda)$ amb Λ D_τ-propi.

En la implementació pràctica de la fórmula del Teorema 10.2 és més eficient treballar amb aquest poset semipropi $\mathcal{L}(\alpha)$ que fer-ho estrictament amb el poset $\mathcal{L}_\gamma^{\mathrm{pr}}(k)$. D'una banda, ens estalviem la tasca de destriar els $\Lambda \in \mathbf{B}_r$ que són D_τ-propis; de l'altra, la funció de Möbius de $\mathcal{L}(\alpha)$ és molt senzilla; cada parell $V(\nu,\Lambda) \leq V(\nu',\Lambda')$ determina un interval del poset $\mathcal{L}(\alpha)$ isomorf a un producte d'intervals de posets molt simples:

$$[V(\nu,\Lambda), V(\nu',\Lambda')] \simeq [\nu,\nu'] \times [\Lambda,\Lambda'].$$

Per tant, la funció de Möbius val:

$$\mu(V(\nu,\Lambda),V(\nu',\Lambda')) = \mu(\nu,\nu')\mu(\Lambda,\Lambda') = \begin{cases} (-1)^{|\Lambda'|-|\Lambda|}, & \text{si } \nu=\nu', \\ (-1)^{|\Lambda'|-|\Lambda|+1}, & \text{si } \nu=\nu'-1, \\ 0, & \text{en altre cas.} \end{cases}$$

Anàlogament, la funció de Möbius de $\mathcal{L}_\gamma^{\mathrm{pr}}(k)$ s'expressa essencialment com la del poset producte $[\delta]\times\mathbf{B}_r^{\mathrm{pr}}$, però la funció de Möbius del poset $\mathbf{B}_r^{\mathrm{pr}}$ és molt complicada de calcular.

No és cert que per a cada possible subtipus hi hagi elements $\gamma \in \mathrm{PGL}_{N+1}(k)$ que el realitzin. El problema de destriar quins subtipus es realitzen forma part del càlcul de N_α, que pot prendre el valor 0 en alguns casos, com ja hem comprovat al capítol 1 quan hem calculat els valors de N_α quan la dimensió és $N=2$ (vegeu els Corol·laris 2.7 i 2.12).

10.2.2 Descripció intrínseca del conjunt $\mathcal{T}_G$ i els posets $\mathcal{L}_G(\alpha)$

La descripció d'aquest poset és anàloga, amb l'inconvenient de què cal considerar totes les subvarietats γ-invariants $\overline{k}$-definides i pròpies. Aquestes subvarietats han estat descrites a la secció 9, però sense preocupar-nos pel seu grau. Per manipular-les d'una manera més adequada per als nostres propòsits, introduirem una notació especial per identificar-les.

D'entrada, en aquesta secció introduïm una notació especial per a l'acció de Frobenius. Per a qualsevol $\lambda \in \overline{k}$, denotem:

$$\lambda^{(i)} := \sigma^i(\lambda) = \lambda^{q^i}.$$

Per a $i = 1, 2, 3$ també utilitzarem $\lambda' := \lambda^{(1)}$, $\lambda'' := \lambda^{(2)}$, $\lambda''' := \lambda^{(3)}$.

Suposem que la descomposició del polinomi característic de γ en producte de factors irreductibles ve donada per (48) i continuem denotant per $\lambda_1, \ldots, \lambda_r \in \overline{k}$ una elecció qualsevol d'una arrel de cada polinomi $h_i(x)$. Sabem que γ admet una forma normal de Jordan racional: $\gamma = \mathrm{diag}(\gamma_1, \ldots, \gamma_r)$, amb els γ_i donats per (49):

$$\gamma_i = \mathrm{diag}(B_i, \overset{n_1^{(i)}}{\ldots}, B_i, B_i(2), \overset{n_2^{(i)}}{\ldots}, B_i(2), \ldots, B_i(s_i), \overset{n_{s_i}^{(i)}}{\ldots}, B_i(s_i)),$$

on $B_i(s)$, donat per (50), és el bloc de Jordan de mida s associat al polinomi irreductible $h_i(x)$. Treballant a $\overline{k}$, un conjugat de γ tindrà la forma de Jordan canònica:

$$\tilde{\gamma} := \rho\gamma\rho^{-1} = \mathrm{diag}(\tilde{\gamma}_1, \ldots, \tilde{\gamma}_r),$$

$$\tilde{\gamma}_i = \mathrm{diag}(\tilde{B}_i, \overset{n_1^{(i)}}{\ldots}, \tilde{B}_i, \tilde{B}_i(2), \overset{n_2^{(i)}}{\ldots}, \tilde{B}_i(2), \ldots, \tilde{B}_i(s_i), \overset{n_{s_i}^{(i)}}{\ldots}, \tilde{B}_i(s_i)),$$

$$\tilde{B}_i(s) = \begin{pmatrix} \tilde{B}_i & & & & & \\ I & \tilde{B}_i & & & & \\ & I & \tilde{B}_i & & & \\ & & & \ddots & & \\ & & & & \tilde{B}_i & \\ & & & & I & \tilde{B}_i \end{pmatrix} \in \mathrm{GL}_{sw_i}(\overline{k}),$$

on el bloc bàsic racional de Jordan B_i, donat per (51), s'ha convertit en:

$$\tilde{B}_i = \mathrm{diag}(\lambda_i, \lambda_i^{(1)}, \lambda_i^{(2)}, \ldots, \lambda_i^{(w_i-1)}).$$

De fet, aquesta encara no és la forma canònica de Jordan. Reordenant les files de la matriu $\tilde{B}_i(s)$, podem suposar que

$$\tilde{B}_i(s) = \mathrm{diag}(C_i, C_i^{(1)}, C_i^{(2)}, \ldots, C_i^{(w_i-1)}),$$

amb C_i el bloc bàsic de Jordan de mida $s \times s$ sobre un cos algebraicament tancat:

$$C_i = \begin{pmatrix} \lambda_i & 0 & 0 & \cdots & 0 \\ 1 & \lambda_i & 0 & \cdots & 0 \\ 0 & 1 & \lambda_i & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & \lambda_i \end{pmatrix}.$$

A la secció 9 hem descrit les subvarietats invariants pròpies de l'automorfisme lineal $\tilde{\gamma}$. Són les subvarietats $\tilde{V}(\Sigma;\nu)$ associades a qualsevol elecció Σ d'una família D-pròpia d'arrels del polinomi característic (sense tenir en compte cap condició de racionalitat) i ν és un enter $0 \leq \nu \leq \delta(\Sigma)$. Les subvarietats $\tilde{V}(\Sigma;\nu)$ tenen equacions molt senzilles; si $(x_0, x_1, \ldots, x_N)$ denoten les coordenades homogènies de $\mathbb{P}^N$, aquestes subvarietats vénen determinades per:

$$x_{i_1} = \cdots = x_{i_m} = 0,$$

on els subíndexs $i_1, \ldots, i_m$ corresponen a les posicions on a la diagonal de la matriu $\tilde{\gamma}$ no hi figura una de les arrels escollides, o bé hi figura però el vector que té un 1 en aquesta posició i 0 a les altres genera un espai invariant d'exponent dividit per una potència de p superior a ν. Per exemple, si

$$\tilde{\gamma} = \begin{pmatrix} \lambda & 0 & 0 & 0 \\ 1 & \lambda & 0 & 0 \\ 0 & 0 & \lambda' & 0 \\ 0 & 0 & 1 & \lambda' \end{pmatrix}$$

i prescindim del caràcter D-propi en l'elecció d'un conjunt d'arrels, obtenim els següents subespais $\tilde{\gamma}$-invariants:

$$\tilde{V}(\lambda;0) = (0,*,0,0), \quad \tilde{V}(\lambda;1) = (*,*,0,0), \quad \tilde{V}(\lambda';0) = (0,0,0,*),$$

$$\tilde{V}(\lambda';1) = (0,0,*,*), \quad \tilde{V}(\lambda,\lambda';0) = (0,*,0,*), \quad \tilde{V}(\lambda,\lambda';1) = (*,*,*,*).$$

Recordem que a la secció 9 calculàvem $\exp \tilde{V}(\Sigma;\nu) = p^\nu D(\Sigma)$. La dimensió és igualment senzilla d'explicitar:

$$\dim(\tilde{V}(\Sigma;\nu)) = -1 + \\ + \sum_{i=1}^{r} \left(n_1^{(i)} + 2n_2^{(i)} + \cdots + (p^\nu - 1)n_{p^\nu-1}^{(i)} + p^\nu \left(n_{p^\nu}^{(i)} + \cdots + n_{s_i}^{(i)} \right) \right) w_{i,\Sigma},$$

on $w_{i,\Sigma}$ compta quantes arrels del polinomi ireductible $h_i(x)$ hem seleccionat dins del conjunt Σ. Finalment, totes aquestes subvarietats $\tilde{V}(\Sigma;\nu)$ són k-definides i tenen grau 1.

Doncs bé, denotarem per $V(\Sigma;\nu)$ la subvarietat γ-invariant que es correspon amb $\tilde{V}(\Sigma;\nu)$ via l'automorfisme ρ:

$$V(\Sigma;\nu) := \rho^{-1}(\tilde{V}(\Sigma;\nu)).$$

La dimensió i l'exponent de $V(\Sigma;\nu)$ es calculen per les expressions anteriors perquè són respectats per l'automorfisme ρ. Pel que fa al grau, sobre cada bloc bàsic de Jordan l'automorfisme ρ ve representat per una matriu invertible M tal, que:

$$M \begin{pmatrix} 0 & & & & -a_{w_i} \\ 1 & 0 & & & -a_{w_i-1} \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & -a_2 \\ & & & 1 & -a_1 \end{pmatrix} M^{-1} = \operatorname{diag}(\lambda_i,\, \lambda_i^{(1)},\, \lambda_i^{(2)}, \ldots, \lambda_i^{(w_i-1)}).$$

Les columnes de la matriu M són un vector propi de valor propi λ_i i els seus conjugats galoisians. D'altra banda, les equacions lineals que defineixen $V(\Sigma;\nu)$ vénen donades per certes columnes de la matriu ρ, i l'acció de Frobenius sobre aquestes columnes reflecteix fidelment l'acció de Frobenius sobre els λ_i. Per tant, l'acció de Frobenius sobre aquestes varietats es reflecteix fidelment en l'acció de Frobenius sobre el conjunt Σ. Per tant,

$$\sigma(V(\Sigma;\nu)) = V(\sigma(\Sigma);\nu) \implies \deg(V(\Sigma;\nu)) = \deg(\Sigma) := \min\{m \mid \Sigma^{(m)} = \Sigma\}.$$

Per acabar de tenir $\mathcal{L}^{\mathrm{pr}}_{\gamma,G}$ controlat ja només ens falta determinar els subconjunts D-propis del conjunt $\mathrm{VP}(\gamma)$ de tots els valors propis de γ. Aquesta pot ser una tasca molt complexa si la volem acomplir estrictament. En comptes d'això, com hem mencionat al principi de la secció, considerarem només una certa família

$$\mathbf{B}(\mathrm{VP}(\gamma))^{\mathrm{pr}} \subseteq \mathbf{B}(\mathrm{VP}(\gamma))^{\mathrm{spr}} \subseteq \mathbf{B}(\mathrm{VP}(\gamma)),$$

de conjunts *semipropis* Σ, molt més propera a $\mathbf{B}(\mathrm{VP}(\gamma))^{\mathrm{pr}}$ que a $\mathbf{B}(\mathrm{VP}(\gamma))$. La condició (2) de la Definició 10.7 es tradueix simplement en:

$$\Sigma \cap \sigma^i(\Sigma) = \emptyset,\ \forall\, 0 < i < \deg(\Sigma). \tag{54}$$

Per descriure aquesta família $\mathbf{B}(\mathrm{VP}(\gamma))^{\mathrm{spr}}$ anem a pams i tractem primer amb un cert detall els casos en què el polinomi característic de γ té respectivament 1 o 2 factors irreductibles. Recordem que cada node del nostre poset és en realitat una òrbita sencera d'una d'aquestes varietats $V(\Sigma;\nu)$ sota l'acció de Frobenius. A la pràctica, pensarem que cada node és una sola varietat, però escollida d'un sistema de representants sota l'acció de Frobenius sobre totes les varietats invariants; com acabem de veure, això es tradueix en classificar els subconjunts de $\mathrm{VP}(\gamma)$ mòdul l'acció de Frobenius i seleccionar per a cada node només un representant.

Polinomi característic potència d'irreductible

Els valors propis de γ són les arrels d'un polinomi irreductible $h(x)$ de grau w: $\mathrm{VP}(\gamma) = \{\lambda, \lambda^{(1)}, \lambda^{(2)}, \ldots, \lambda^{(w-1)}\}$. Podem fixar un representant de cada òrbita per l'acció de Frobenius considerant només subconjunts $\Sigma \subseteq \mathrm{VP}(\gamma)$ que continguin l'arrel λ. Hi ha 2^{w-1} subconjunts amb aquesta propietat; en canvi, per al nostre poset considerarem només un subconjunt per a cada divisor positiu de w.

Definició 10.12. *Per a cada divisor positiu u de w, definim:*

$$\Sigma(u) := \{\lambda, \lambda^{(u)}, \lambda^{(2u)}, \ldots, \lambda^{(w-u)}\}.$$

Noteu que $\Sigma(w) = \{\lambda\}$ i $\Sigma(1) = \mathrm{VP}(\gamma)$.

Lema 10.13. *La família dels $\Sigma(u)$ és semipròpia.*

Demostració. Es evident que els $\Sigma(u)$ satisfan la condició (54). Només cal comprovar, doncs, que tot subconjunt D-propi de $\mathrm{VP}(\gamma)$ que conté λ coincideix amb un $\Sigma(u)$, per a algun divisor positiu u de w.

Sigui $\Sigma \subseteq \mathrm{VP}(\gamma)$ un subconjunt D-propi que conté λ i sigui $d = \exp(\Sigma)$. Comprovem que $\Sigma = \Sigma(u)$ per a $u := \mathrm{mcd}\{n \mid \lambda^{(n)} \in \Sigma\}$. Evidentment, $\Sigma \subseteq \Sigma(u)$ i només es tracta de provar la inclusió contrària.

Clarament:

$$\lambda^d = (\lambda^{(n)})^d \iff \lambda^d = \sigma^n(\lambda^d) \iff \lambda^d \in k_n. \tag{55}$$

Recordem que k_n és el subcos de grau n sobre k, de l'extensió k_w/k. En particular, si $\lambda^{(n)} \in \Sigma$, tenim:

$$\lambda^d = (\lambda^{(n)})^d = (\lambda^{(2n)})^d = \cdots = (\lambda^{(w-n)})^d,$$

i, pel caràcter propi de Σ, a la força $\Sigma \supseteq \Sigma(n)$. D'altra banda, per a cada parell $\lambda^{(n)}$, $\lambda^{(m)} \in \Sigma$, tenim $\lambda^d \in k_n \cap k_m = k_{\mathrm{mcd}(n,m)}$, de manera que, pel mateix argument, també $\Sigma \supseteq \Sigma(\mathrm{mcd}(n,m))$. Això prova que $\Sigma \supseteq \Sigma(u)$. □

Noteu que els $\Sigma(u)$ formen un poset isomorf a $\mathbf{D}_w$. Podem calcular explícitament el grau i l'exponent de cada $\Sigma(u)$. El càlcul de l'exponent es dedueix immediatament de (55).

Lema 10.14. *Per a qualsevol divisor positiu u de w, tenim:*

$$\deg \Sigma(u) = u, \qquad \exp \Sigma(u) = \mathrm{ord}_{k_w^*/k_u^*}(\lambda) = \min\{d \mid h(x) | x^{d(q^u-1)} - 1\}.$$

En particular, $\exp \Sigma(w) = 1$; efectivament, l'elecció de $\Sigma = \{\lambda\}$ dóna lloc a la varietat $V(\lambda; 0)$ que té grau w i està formada per punts fixos de γ.

Finalment, observem que els exponents dels $\Sigma(u)$ estan tots determinats per l'exponent de $\Sigma(1)$. Com a conseqüència immediata del lema anterior i l'estructura cíclica de k_w^*/k^*, tenim:

Lema 10.15. *Per a qualsevol divisor positiu u de w, denotem:*

$$Q_u := (q^w - 1)/(q^u - 1) = |k_w^*/k_u^*|, \qquad D(u) := \exp \Sigma(u).$$

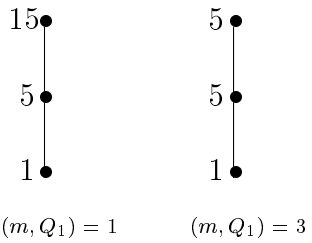
Aleshores, $D(u) = Q_u/\operatorname{mcd}(Q_u, Q_1/D(1))$.

Els $\Sigma(u)$ són tots propis exactament quan els exponents $D(u)$ són tots diferents. És fàcil comprovar que no sempre és el cas. Per exemple, considerem el cas $w = 4$ i fixem un generador $\zeta \in k_4^*$ del grup cíclic k_4^*. L'elecció d'un polinomi irreductible de grau 4 equival a fixar un enter m que no sigui múltiple de Q_2 i considerar $\lambda = \zeta^m$. Tenim:

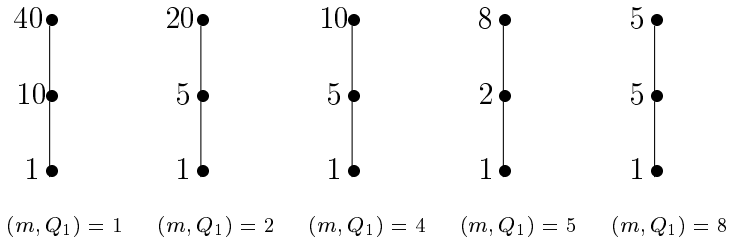
$$D(1) = \frac{Q_1}{\operatorname{mcd}(Q_1, m)}, \qquad D(2) = \frac{Q_2}{\operatorname{mcd}(Q_2, m)}, \qquad D(4) = 1.$$

Com que m no és múltiple de Q_2, tindrem sempre $D(2) > 1$. La majoria de les vegades tindrem també $D(4) > D(2)$, però no sempre. Els diagrames següents il·lustren la situació per a $q = 2, 3$. En cada node del poset indiquem l'exponent.

Per a $q = 2$, tenim $Q_1 = 15$, $Q_2 = 5$ i només dues possibilitats:



Per a $q = 3$, tenim $Q_1 = 40$, $Q_2 = 10$ i cinc possibilitats, només una de les quals conté un node no propi:



En el cas que estem tractant no costaria gaire destriar els nodes propis dels que no ho són. D'altra banda, de cara a la fórmula final recollida en el Teorema 10.5, el poset $\mathcal{L}_G(\alpha)$ ha de ser descrit en els termes més simples possibles. El guany que podria significar eliminar uns pocs nodes es contrarestaria pel fet de què la tria d'aquests nodes també requeriria afegir altres passos a l'algorisme. A més a més, en el cas general la tria dels nodes propis és molt més complicada del que ho és en aquest cas en què hi ha un únic factor irreductible del polinomi característic.

Polinomi característic amb dos factors irreductibles

Suposem que el polinomi característic de γ és producte de potències de dos polinomis irreductibles $h_1(x)$, $h_2(x)$ de graus respectius w_1, w_2 i arrels:

$$\mathrm{VP}(\gamma) = \{\lambda_1,\, \lambda_1^{(1)}, \lambda_1^{(2)}, \ldots, \lambda_1^{(w_1-1)}\} \cup \{\lambda_2,\, \lambda_2^{(1)}, \lambda_2^{(2)}, \ldots, \lambda_2^{(w_2-1)}\}.$$

Denotem $w := \mathrm{mcd}(w_1, w_2)$.

D'entre els subconjunts de $\mathrm{VP}(\gamma)$ que constin només d'arrels d'un dels dos polinomis, n'escollim només els semipropis considerats a la subsecció anterior. Discutim ara com hem d'escollir subconjunts que contenen simultàniament arrels de tots dos polinomis. Com abans, podem fixar un representant de cada òrbita per l'acció de Frobenius considerant només subconjunts $\Sigma \subseteq \mathrm{VP}(\gamma)$ que continguin l'arrel λ_1.

Definició 10.16. *Per a cada divisor positiu u de w i per a cada $j \in \mathbb{Z}_u$, definim:*

$$\Sigma_j(u) := \{\lambda_1,\, \lambda_1^{(u)},\, \lambda_1^{(2u)}, \ldots, \lambda_1^{(w-u)}\} \cup \{\lambda_2^{(j)}, \lambda_2^{(j+u)}, \ldots, \lambda_2^{(j+v-u)}\}.$$

Noteu que, per a $u = 1$, necessàriament $j = 0$ i $\Sigma(1) := \Sigma_0(1) = \mathrm{VP}(\gamma)$.

Aquests $\Sigma_j(u)$ són ara els nostres subconjunts semipropis. El poset que formen aquests subconjunts ordenats per la inclusió queda determinat per:

$$\Sigma_j(u) \subseteq \Sigma_{j'}(u') \iff u' | u, \quad j \equiv j' \pmod{u'}. \tag{56}$$

Lema 10.17. *La família dels $\Sigma_j(u)$ és semipròpia.*

Demostració. És evident que els $\Sigma_j(u)$ satisfan la condició (54). Considerem un subconjunt D-propi $\Sigma \subseteq \mathrm{VP}(\gamma)$, que conté λ_1 i algun $\lambda_2^{(n)}$. Si $d = \exp(\Sigma)$, tenim:

$$\lambda_1^d = (\lambda_2^{(n)})^d \implies \lambda_1^d \in k_{w_1} \cap k_{w_2} = k_w. \tag{57}$$

Sigui u el mínim divisor positiu de w tal que $\lambda_1^d \in k_u$. Com que λ_1^d i $(\lambda_2^{(n)})^d$ són invariants per σ^u, tenim $\Sigma \supseteq \Sigma_j(u)$, amb $j = n + u\mathbb{Z}$. Tenint en compte (56), la minimalitat de u comporta la igualtat entre els dos conjunts. □

Clarament, $\deg \Sigma_j(u) = u$. L'exponent no és tan fàcil de determinar. Posem:

$$D_j(u) := \exp \Sigma_j(u) = \min\{d \mid \lambda_1^d = (\lambda_2^{(j)})^d \in k_u\}.$$

Usualment denotarem $D_0(1)$ simplement per $D(1)$.

Lema 10.18. $\mathrm{mcm}(D_j(u), D_{j'}(u')) = D_j(e) = D_{j'}(e)$, *per a* $e = \mathrm{mcd}(j' - j,\, u,\, u')$.

Demostració. Sigui $d = \mathrm{mcm}(D_j(u), D_{j'}(u'))$ i $u_0 = \mathrm{mcd}(u, u')$. Tenim:

$$(\lambda_2^{(j)})^d = \lambda_1^d = (\lambda_2^{(j')})^d \in k_u \cap k'_u = k_{u_0}.$$

En particular, $\sigma^{j'-j}(\lambda_1^d) = \lambda_1^d$, de manera que, de fet, $\lambda_1^d \in k_e$. D'altra banda, és evident que d és mínim amb aquesta propietat. □

En particular, els $D_j(w)$, per a $0 \leq j < w$, determinen tots els exponents $D_j(u)$. Per exemple, $D(1) = \mathrm{mcm}(D_0(w), D_1(w))$ i, més generalment, $D_j(u) = \mathrm{mcm}(D_j(w), D_{j+u}(w))$.

Lema 10.19. *Per a j fixada, tenim $D_j(u) = \frac{Q_u D_j(w)}{\mathrm{mcd}(Q_u, (Q_1 D_j(w)/D(1))}$.*

Demostració. Sigui $d = D_j(w)$ el mínim enter positiu satisfent $\lambda_1^d = (\lambda_2^{(j)})^d$. Si denotem $a = \lambda_1^d$, tenim $D(1) = d \,\mathrm{ord}_{k_w^*/k^*}(a)$. D'altra banda, $D_j(u) = d \,\mathrm{ord}_{k_w^*/k_u^*}(a)$ i hem vist al Lema 10.15 que $\mathrm{ord}_{k_w^*/k^*}(a)$ determina tots els $\mathrm{ord}_{k_w^*/k_u^*}(a)$:

$$\frac{D_j(u)}{d} = \mathrm{ord}_{k_w^*/k_u^*}(a) = \frac{Q_u}{\mathrm{mcd}(Q_u, (Q_1/\,\mathrm{ord}_{k_w^*/k^*}(a))} = \frac{Q_u}{\mathrm{mcd}(Q_u, (Q_1/(D(1)/d))}.$$

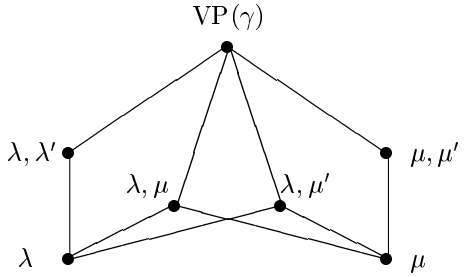
□

No és senzill controlar les repeticions que puguin aparèixer entre aquests valors bàsics $D_j(w)$. Per exemple, considerem el cas $w_1 = w_2 = 2$, prenem $\lambda_1 = \zeta$ un generador del grup cíclic k_2^* i $\lambda_2 = \zeta^m$, amb m no múltiple de $q+1$ i $m \neq 1, q$. Tenim:

$$D_0(2) = \frac{q^2-1}{\mathrm{mcd}(m-1, q^2-1)}, \qquad D_1(2) = \frac{q^2-1}{\mathrm{mcd}(qm-1, q^2-1)},$$

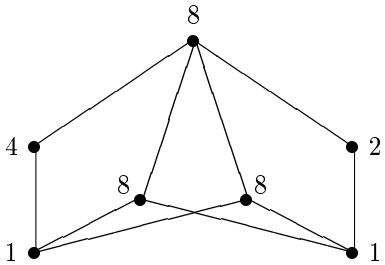
$$D(1) = \frac{q^2-1}{\mathrm{mcd}(m-1, q-1)}.$$

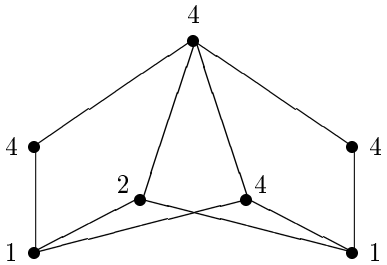
Genèricament hi ha repeticions entre aquests nombres; usualment $D(1)$ coincideix amb algun dels dos nombres "inferiors" i en alguna ocasió coincideixen els tres nombres. També hi ha situacions esporàdiques en què són tots tres diferents. Dibuixem el diagrama de Hasse del poset $\mathbf{B}^{\mathrm{spr}}(\mathrm{VP}(\gamma))$ en alguns casos; canviant la notació λ_1, λ_2 per λ, μ, l'estructura general d'aquest poset és:



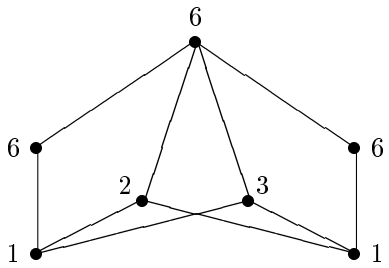
i només indicarem l'exponent de cada node.

Per a $q = 3$, hi ha només dos posets diferents; el primer correspon a $m = 2$ i el segon a $m = 5$:

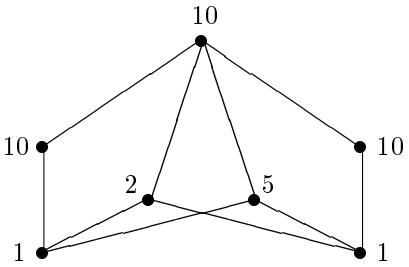




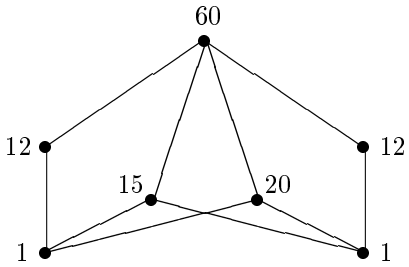
Per a $q = 4$, els nombres $D(1)$, $D_0(2)$, $D_1(2)$ sempre presenten alguna repetició; prenen els valors $(15, 15, 15)$, $(15, 15, 3)$ i $(5, 5, 5)$. En canvi, per a $q = 5$, hi ha un cas en què tots són diferents; poden valer: $(24, 24, 8)$, $(12, 12, 12)$, $(12, 12, 4)$, $(6, 6, 3)$ i $(6, 3, 2)$. El poset en aquest darrer cas (que correspon a $m = 13$) és:



D'altres casos en què els nombres són diferents són:



$q = 9$, $m = 41$



$q = 11$, $m = 17$

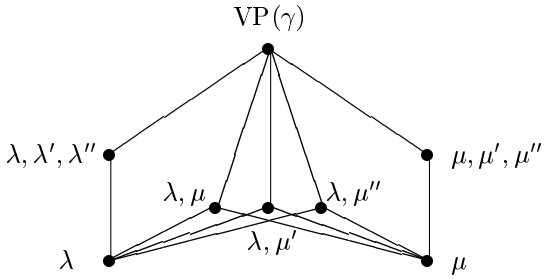
D'entre tots aquests exemples, l'únic en què tots els nodes són propis és el darrer.

En el cas $w_1 = w_2 = 3$, tenim una situació similar. Si prenem $\lambda = \zeta$ un generador del grup cíclic k_3^*, i $\mu = \zeta^m$, amb m no múltiple de q^2+q+1 i $m \neq 1,\ q,\ q^2$. Tenim:

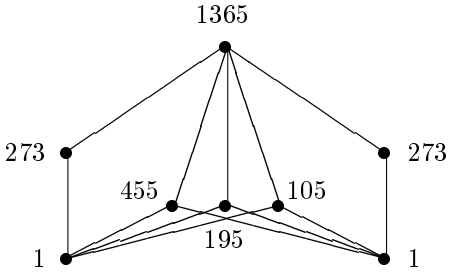
$$D_0(3) = \frac{q^3-1}{(m-1, q^3-1)}, \quad D_1(3) = \frac{q^3-1}{(qm-1, q^3-1)}, \quad D_2(3) = \frac{q^3-1}{(q^2m-1, q^3-1)},$$

$$D(1) = \frac{q^3-1}{(m-1, q-1)}.$$

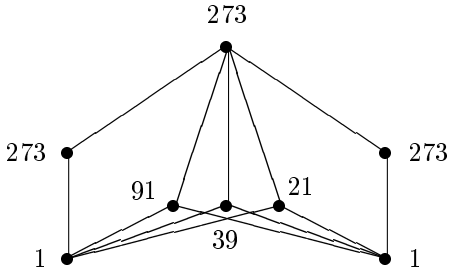
L'estructura general dels posets és:



Una petita exploració amb magma revela que genèricament hi ha repeticions entre els exponents dels quatre nodes "centrals", però torna a haver casos en què tots són diferents; per exemple:



$q = 16,\ m = 100$

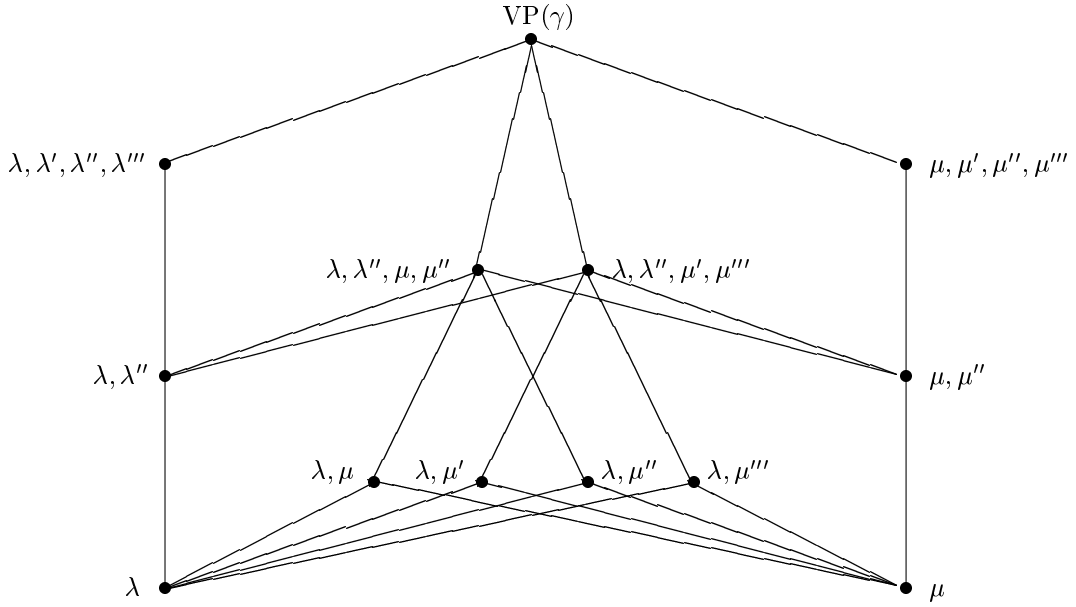


$q = 16,\ m = 211$

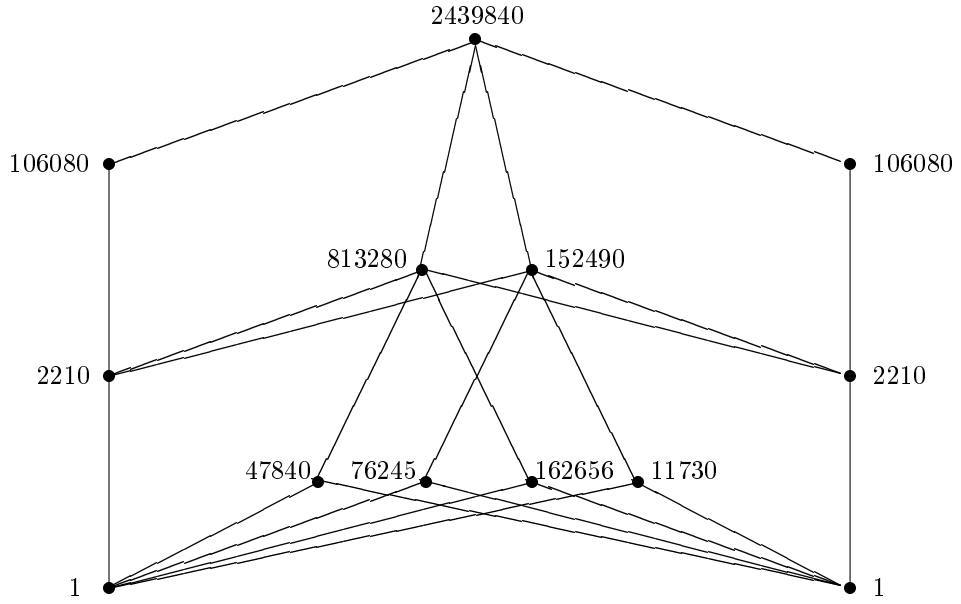
En el cas $w_1 = w_2 = 4$, apareixen tres nivells entre els nodes centrals que corresponen a seleccionar arrels dels dos polinomis irreductibles. Prenem $\lambda = \zeta$ un generador del grup cíclic k_4^*, i $\mu = \zeta^m$, amb m no múltiple de q^2+1 i $m \neq 1,\ q,\ q^2,\ q^3$. Tenim:

$$D_i(e) = \frac{q^4-1}{(q^i m-1, q^e-1)}, \quad 0 \leq i < e, \quad e = 1,\ 2,\ 4.$$

L'estructura general dels posets és:



Doncs bé, ens trobem amb un fenomen similar. No podem eliminar genèricament cap node perquè hi ha casos en què tots són propis; per exemple, per a $q = 47$, $m = 2959$, tenim els següents exponents en cada node:



Polinomi característic amb més de dos factors irreductibles

Suposem que $h_1(x), \ldots, h_r(x)$ són els factors irreductibles del polinomi característic i fem una elecció $\lambda_1, \lambda_2, \cdots, \lambda_r$ d'una arrel de cada polinomi. Per a cada subconjunt d'índexs $\Lambda \in \mathbf{B}_r$, el poset $\mathcal{L}$ ha de contemplar tots els nodes que corresponen als subconjunts de $\mathrm{VP}(\gamma)$ determinats per eleccions d'arrels de tots els polinomis amb subíndex que pertany a Λ. Per exemple, per a $r = 2$, els posets $\mathcal{L}$ que hem descrit al paràgraf anterior contenien els subposets corresponents a $\Lambda = \{1\}$, $\Lambda = \{2\}$, que hem ubicat a les columnes exteriors (esquerra i dreta) i el subposet corresponent a $\Lambda = \{1, 2\}$, representat pels nodes que anomenàvem *centrals*.

Per a cada Λ, considerem:

$$w_\Lambda := \mathrm{mcd}\{\deg(h_i(x)) \mid i \in \Lambda\}.$$

La part del poset $\mathcal{L}$ que correspon a aquest Λ tindrà un "nivell" per a cada divisor positiu u de w_Λ, amb $u^{|\Lambda|-1}$ nodes etiquetats $V_J(u;\Lambda)$, on l'índex J recorre el conjunt:

$$J(u;\Lambda) := \left(\mathbb{Z}_u^{|\Lambda|}\right) / \sim .$$

D'entrada, cada $J = (j_1, \ldots, j_{|\Lambda|}) \in \mathbb{Z}_u^{|\Lambda|}$ correspon a una determinada elecció d'arrels de cada $h_i(x)$, amb $i \in \Lambda$:

$$\bigcup_{i\in\Lambda} \{\lambda_i^{(j_i)}, \lambda_i^{(j_i+u)}, \ldots, \lambda_i^{(j_i+w_i-u)}\},$$

i la relació d'equivalència $\sim$ reflecteix la classificació d'aquests conjunts sota l'acció de Frobenius:

$$(j_1, \ldots, j_{|\Lambda|}) \sim (j'_1, \ldots, j'_{|\Lambda|}) \iff j'_1 - j_1 = j'_2 - j_2 = \cdots = j'_{|\Lambda|} - j_{|\Lambda|}.$$

Les inclusions entre els diferents nodes vénen determinades per:

$$V_J(u;\Lambda) \le V_{J'}(u';\Lambda') \iff \Lambda \subseteq \Lambda', \quad u'|u, \quad \mathrm{pr}(J') = J,$$

on $\mathrm{pr}\colon J(u';\Lambda') \longrightarrow J(u;\Lambda)$ és la projecció natural que consisteix en ignorar les coordenades de $\Lambda' \setminus \Lambda$ i aplicar la projecció canònica $\mathbb{Z}'_u \longrightarrow \mathbb{Z}_u$ a les coordenades de Λ. Sovint abusarem de la notació i escriurem simplement J en comptes de $\mathrm{pr}(J)$.

Per a cada $J \in J(u;\Lambda)$, els exponents $D_J(u;\Lambda)$ del node corresponent han estat determinats als paràgrafs anteriors en els casos $|\Lambda| = 1, 2$, i es dedueixen d'aquests valors per a $|\Lambda| \ge 3$, ja que sempre que $\Lambda = \Lambda_1 \cup \Lambda_2$, amb $\Lambda_1 \cap \Lambda_2 \neq \emptyset$, tenim evidentment:

$$D_J(u;\Lambda) = \mathrm{mcm}(D_J(u;\Lambda_1), D_J(u;\Lambda_2)).$$

Lema 10.20. *La família dels $V_J(u;\Lambda)$ és semipròpia.*

Demostració. És evident que els $V_J(u;\Lambda)$ satisfan la condició (54). Només cal comprovar, doncs, que tot subconjunt D-propi de $\mathrm{VP}(\gamma)$ és equivalent a un $V_J(u;\Lambda)$, per a alguna elecció de Λ, u, J. La comprovació és completament anàloga a la dels casos anteriors. □

Tipus i G-subtipus

De cara a la definició del poset $\mathcal{L}_G(\alpha)$ el concepte de *tipus* és el mateix d'abans; un tipus és un element del conjunt $\mathcal{P}_{N+1}$ de particions de $N+1$ amb pesos. El concepte de *G-subtipus* canvia, adaptant convenientment el concepte de distribució d'exponents a la situació que ara ens ocupa.

Definició 10.21. *Fixem pesos $0 \leq w_1 \leq w_2 \leq \cdots \leq w_r$ i denotem $w_{i,i'} := \mathrm{mcd}(w_i, w_{i'})$. Una G-distribució d'exponents respecte d'aquests pesos, és una col·lecció de famílies d'enters positius*

$$D\{i\},\ 1 \leq i \leq r, \qquad D_j\{i,\, i'\},\ 1 \leq i < i' \leq r,\ 0 \leq j < w_{i,i'},$$

satisfent les següents propietats:

1. $D\{i\} \mid \frac{q^{w_i}-1}{q-1}, \quad D\{i\} \nmid \frac{q^{w}-1}{q-1},\ \forall w < w_i.$
2. $D_j\{i,i'\} \mid \mathrm{mcm}(D\{i\}, D\{i'\})(q-1),\ \forall j,\, i,\, i'.$
3. *Per a cada terna $1 \leq i < i' < i'' \leq r$, si $w := \mathrm{mcd}(w_i, w_{i'}, w_{i''})$, tenim:*

$$\mathrm{mcd}(D_j\{i,\, i'\}, D_k\{i,\, i''\}) = \mathrm{mcd}(D_j\{i,\, i'\}, D_{k-j}\{i',\, i''\}),\ \forall 0 \leq j \leq k < w.$$

4. *Per a cada $1 \leq i \leq r$ i cada divisor positiu u de w_i, definim:*

$$D(u;\{i\}) := \frac{(q^{w_i}-1)/(q^u-1)}{\mathrm{mcd}((q^{w_i}-1)/(q^u-1), (q^{w_i}-1)/(q-1)D\{i\})}.$$

Per a cada parell $1 \leq i < i' \leq r$ d'índexs, cada divisor positiu u de $w_{i,i'}$ i cada $0 \leq j < u$, tenim:

$$D_j(u;\{i,i'\}) := \mathrm{mcm}(D_j\{i,\, i'\}, D_{j+u}\{i,\, i'\}) = \mathrm{mcm}(D_j\{i,\, i'\}, D(u;\{i\}).$$

Establim ara una relació d'equivalència entre G-distribucions d'exponents. Dues G-distribucions d'exponents, $\mathcal{D}$, $\mathcal{D}'$ són considerades equivalents, $\mathcal{D} \sim \mathcal{D}'$, si existeix un nombre natural M tal, que per a tot parell $1 \leq i < i' \leq r$, tenim:

$$D'_j\{i,\, i'\} = D_{j+M}\{i,\, i'\},\ \forall 0 \leq j < w_{i,i'},$$

on el subíndex $j+M$ cal entendre'l mòdul $w_{i,i'}$.

Denotem per $\mathcal{D}_G$ el conjunt quocient del conjunt de totes les G-distribucions d'exponents per aquesta relació d'equivalència.

Cada $\gamma \in \mathrm{GL}_{N+1}(k)$ té associada una G-distribució d'exponents, determinada per una elecció $\lambda_1, \ldots, \lambda_r$ d'una arrel de cadascun dels factors irreductibles del polinomi característic de γ. Podem considerar

$$D\{i\} := \mathrm{ord}_{k^*_{w_i}/k^*}(\lambda_i), \qquad D_j\{i, i'\} := \mathrm{ord}_{\overline{k}^*}(\lambda_i/\sigma^j(\lambda_{i'})).$$

En principi, aquests valors depenen de l'elecció de les arrels, però la classe de la G-distribució respecte de la relació d'equivalència que hem definit, és independent d'aquesta elecció. Igualment, la G-distribució d'exponents és invariant per l'acció de k^* sobre $\mathrm{GL}_{N+1}(k)$ i podem considerar l'aplicació

$$\tau_G \colon \mathrm{PGL}_{N+1}(k) \longrightarrow \mathcal{D}_G, \qquad \gamma \mapsto \tau_G(\gamma),$$

que assigna a cada k-automorfisme de $\mathbb{P}^N$ la seva G-distribució d'exponents.

Definició 10.22. *Un G-subtipus és un element del conjunt $\mathcal{T}_G$ format pels parells (t, τ), on t és una partició de $N+1$ amb pesos, i $\tau \in \mathcal{D}_G$ una classe d'equivalència de G-distribucions d'exponents amb els mateixos pesos que t.*

A cada G-subtipus $\alpha \in \mathcal{T}_G$ li associem un poset $\mathcal{L}_G(\alpha)$ amb nodes $V(J, u, \nu, \Lambda)$ parametritzats per:

- $\Lambda \in \mathbf{B}_r$ arbitrari.
- $0 \leq \nu \leq \delta(\Lambda)$.
- u divisor positiu de $w_\Lambda := \mathrm{mcd}\{w_i \mid i \in \Lambda\}$.
- $J \in (\prod_{i\in\Lambda} \mathbb{Z}_u)/\sim$ classe de multiíndexs, $J = (j_i)_{i\in\Lambda} \in \prod_{i\in\Lambda} \mathbb{Z}_u$, respecte de la relació d'equivalència

$$(j_i)_{i\in\Lambda} \sim (j_i + M)_{i\in\Lambda}, \ \forall M \in \mathbb{Z}.$$

La relació d'ordre entre aquests elements ve donada per:

$$V(J, u, \nu, \Lambda) \leq V(J', u', \nu', \Lambda') \iff \Lambda \subseteq \Lambda', \quad , \nu \leq \nu', \quad u'|u, \quad (j_i)_{i\in\Lambda} \sim (j'_i)_{i\in\Lambda}.$$

Cada node de $\mathcal{L}_G(\alpha)$ té un pes $(\dim, \exp, \deg)$ donat per:

$$\deg(V(J, u, \nu, \Lambda)) = u, \qquad \exp(V(J, u, \nu, \Lambda)) = p^\nu D_J(u; \Lambda),$$

$$\dim(V(J, u, \nu, \Lambda)) = -1 + \\ + \sum_{i\in\Lambda} \left(n_1^{(i)} + 2n_2^{(i)} + \cdots + (p^\nu - 1)n_{p^\nu-1}^{(i)} + p^\nu \left(n_{p^\nu}^{(i)} + \cdots + n_{s_i}^{(i)} \right) \right) w_{u,\Lambda},$$

on

$$w_{u,\Lambda} = \left| \bigcup_{i\in\Lambda} \{\lambda_i^{(j_i)},\ \lambda_i^{(j_i+u)}, \ldots, \lambda_i^{(j_i+w_i-u)}\} \right| = \frac{1}{u}\sum_{i\in\Lambda} w_i,$$

i la part $D_J(u;\Lambda)$ coprimera amb p de l'exponent està determinada per:

$$D_J(u;\Lambda) := \frac{(q^{w_i}-1)/(q^u-1)}{\mathrm{mcd}((q^{w_i}-1)/(q^u-1),(q^{w_i}-1)/(q-1)D\{i\})}, \quad \text{per a } \Lambda=\{i\},$$

$$D_J(u;\Lambda) := \mathrm{mcm}\left(D_j\{i,\ i'\}, D_{j+u}\{i,\ i'\}\right), \quad \text{per a } \Lambda=\{i,\ i'\},\ j=j_{i'}-j_i,$$

$$D_J(u;\Lambda) := \mathrm{mcm}\left(D_{J_1}(u;\Lambda_1), D_{J_2}(u;\Lambda_2)\right), \text{ per a } \Lambda=\Lambda_1\cup\Lambda_2, \text{ amb } \Lambda_1\cap\Lambda_2\neq\emptyset,$$

on J_1, J_2 són les projeccions naturals de J obtingudes respectivament ignorant les coordenades indexades per elements que no pertanyen a Λ_1, Λ_2.

Referències

[BFKWZ98] A. Betten, H. Fripertinger, A. Kerber, A. Wassermann, K.-H. Zimmermann, *Codierungstheorie*, Springer-Verlag, Berlin-Heidelberg (1998).

[BG01] B.W. Brock, A. Granville, *More points than expected on curves over finite field extensions*, Finite Fields and Their Applications, Vol. 7 (2001), pp. 70-91.

[DO88] I. Dolgachev, D. Ortland, *Point sets in projective spaces and theta functions*, Astérisque, Vol. 188, Soc. Math. de France, Paris, 1988.

[Fri97] H. Fripertinger, *Cycle Indices of Linear, Affine i Projective Groups*, Linear Algebra i its Applications, Vol. 263 (1997), pp. 133-156.

[Fri98] H. Fripertinger, *Enumeration, construction and random generation of block codes*, Designs, Codes and Cryptography, Vol. 14 (1998), pp. 213-219.

[Har92] J. Harris, *Algebraic Geometry*, GTM Vol. 133, Springer-Verlag 1992.

[Hir79] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, Clarendon Press, Oxford, 1979.

[LMNX02] A. López, D. Maisner, E. Nart, X. Xarles, *Orbits of galois invariant n-sets of $\mathbb{P}^1$ under the action of* PGL_2, Finite Fields and Their Applications, Vol. 8 (2002), pp. 193-206.

[LN99] A. López, E. Nart, *Classification of Goppa codes of genus zero*, Journal für die reine und angewandte Mathematik, Vol. 517 (1999), pp. 131-144.

[MN04] R. Martí, E. Nart, *Isometry classes of codes arising from sets of points in the projective plane*, European Journal of Combinatorics, Vol. 25 (2004), pp. 1003-1023.

[Sil86] J.H. Silverman, *The Arithmetic of Elliptic curves*, GTM Vol. 106, Springer-Verlag 1986.

[Sta99] R.P. Stanley, *Enumerative Combinatorics*, Cambridge Studies in Advanced Mathematics 62, Vol. I, Cambridge University Press 1999.

[TV91] M.A. Tsfasman- S.G. Vlădut, *Algebraic-Geometric Codes*, Kluwer Ac. Publishers, Dordrecht 1991.